JILPT REPORT

No. 14
2014

Protection of Employees' Personal Information and Privacy

– 2014 JILPT Comparative Labor Law Seminar –

The Japan Institute for Labour Policy and Training

Protection of Employees' Personal Information and Privacy

— 2014 JILPT Comparative Labor Law Seminar—

JILPT REPORT No. 14
2014

The Japan Institute for Labour Policy and Training

Published by the Japan Institute for Labour Policy and Training 2014
8-23, Kamishakujii 4-chome, Nerima-ku, Tokyo, 177-8502 Japan
Telephone: 81-3-5903-6111 Facsimile: 81-3-3594-1113
Printed in Japan

Foreword

The Japan Institute for Labour Policy and Training (JILPT) held the twelfth Comparative Labor Law Seminar on March 3rd and 4th, 2014 in Tokyo. This Comparative Labor Law Seminar has been held biannually for the purpose of providing researchers in this area with the opportunity to discuss and learn across borders. In the seminar, we engaged in cross-national discussion and analyses on the theme of "Protection of Employees' Personal Information and Privacy". We invited ten scholars from Australia, China, France, Germany, Korea, Spain, Taiwan, the UK, the US and Japan to present their national papers on the theme.

Protection of employees' personal information and privacy has become a keen legal issue among developed countries in recent years. Rapid developments in information technologies and the spread of their use in the society are giving rise to many new issues in the workplace, such as electronic monitoring, search of work computer drives and email, and leakage of personal data to outsiders. There should be effective legal rules to protect employees from improper collection and / or use of their personal information while still paying due consideration to employers' valid business necessities.

This Report is a compilation of papers presented to the seminar. We very much hope that this report will provide useful and up-to-date information and also benefit those who are interested in comparative study of the issue.

We would like to express our sincere gratitude to the guests who submitted excellent national papers and also to Prof. Hiroya Nakakubo and Prof. Takashi Araki for the effort to coordinate the seminar.

September 2014

Kazuo Sugeno
President
The Japan Institute for Labour Policy and Training

Table of Contents

Introduction

Hiroya Nakakubo
Hitotsubashi University

Takashi Araki
University of Tokyo

The Theme and Its Background

The Japan Institute for Labor Policy and Training (JILPT) hosted its 12th Comparative Labor Law Seminar, or the "Tokyo Seminar," on March 3rd and 4th, 2014. As the organizers of the seminar, we chose the theme of "Protection of Employees' Personal Information and Privacy" and invited distinguished scholars from Australia, China, France, Germany, Japan, Korea (ROK), Spain, Taiwan, the U.K. and the U.S. The following memo was sent to these participants to explain the theme.

Protection of employees' personal information and privacy has become a keen legal issue among developed countries in recent years. Rapid developments in information technologies and the spread of their use in the society are giving rise to many new issues in the workplace, such as electronic monitoring, searches of work computer drives and email, and leakage of personal data to outsiders. There should be effective legal rules to protect employees from improper collection and/or use of their personal information while still paying due consideration to employers' valid business necessities.

In European countries, the EU Directive on the protection of personal data (95/46/EC) was adopted in 1995, and the EU member states have developed legislation and held ongoing discussions on personal data protection at workplaces in accordance with the Directive. A new proposal was made by the European Commission in 2012 to replace the existing framework of data protection legislation, which further stimulated discussion on the subject.

In the United States, where there is no comprehensive legislation on this matter, problems regarding employees' personal information and privacy are being addressed by a variety of statutes and tort theories. Such statutes include the Genetic Information Notification Act of 2008 (GINA), which specifically bans acquisition of, and discrimination because of, employees' genetic information. In addition, most states have laws concerning data security and notification, and this growing body of law is becoming increasingly important to employers.

Asian countries are also facing similar new legal issues related to employees' personal information. In Japan, damages have been awarded under tort in cases of improper blood testing of an employee without his consent. And the Act on the Protection of Personal Information, enacted in 2005, mandates many employers to take appropriate measures concerning employees' personal information.

It is true that this is a relatively new area to many labor and employment law scholars. Legal tools are still developing as new problems emerge in real workplaces. Some issues are regulated by specific legislation to protect employees' data or personal information. Others may be regulated by legislation on employment discrimination. Even where no relevant legislation exists, employer actions can be challenged under the traditional framework of tort liability, such as illegal infringement of privacy.

We anticipate that it will be exciting and rewarding to tackle this vibrant subject. We encourage you to take this opportunity to share the experiences and insights among various countries, in the hope that we will find better policy directions for the future.

Suggested Discussion Points

Together with the explanation of the theme, we provided the following discussion points to the participants as a general guideline for their country papers. It was noted at the outset that we were planning to focus on employment relations in the private sector, though it would be all right to mention the matters in the public sector that are especially relevant from a comparative viewpoint.

1. Introduction

- *General overview of the current situation concerning employees' personal information and privacy protection in your country: Are there many lawsuits? New legislation? Potential legal disputes covered by media? How are they related to developments of new information technologies such as e-mail, internet, global positioning systems, etc.?*

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

- *Does your country have a constitution, international instruments, or national legislation which provide legal basis to protect employees' personal information and privacy? Do these regulatory tools specifically address employees? Or do they provide a general framework applicable to both employment and non-employment relationships?*
- *What are the remedies against the violation of these regulations?*

3. Employer's legitimate business purposes?

- *Employers seek to obtain employers' personal information for a variety of purposes. These purposes may include matters of recruitment, disciplinary actions, effective human resource management such as job allocation, transfer of employees, health and safety compliance, work-related injuries and their compensation disputes, preventing the leakage of trade secrets etc. When should these purposes be regarded as proper and reasonable?*
- *If the purpose is regarded as proper and reasonable, how does your country's legal system strike a balance between business necessity and employees' privacy protection?*

4. Personal information and privacy protection in the hiring process

- *Is there any personal information (address, telephone, e-mail address, password of social networking, marital status, family structure, pregnancy, health and medical condition, sexual orientation, religion, political affiliation or activities, union membership, credit information, criminal convictions, litigation history, etc.) that an employer is prohibited from requesting or obtaining? Do those prohibitions stem*

from regulations on discrimination? Or from those on personal information protection?

- *Is there any personal information that an employer is entitled to obtain regarding its employees?*

5. Personal information and privacy protection during the employment relations

- *Under what conditions (if at all) is an employer entitled to obtain the personal information of its employees? Is there any difference between on-duty conduct and off-duty conduct?*
- *How about monitoring employee conduct by video surveillance, or electronic monitoring such as inspection of web-browsing, e-mail, social networking, etc. Is there any difference between on-duty conduct and off-duty conduct?*
- *Is there any discussion on the disclosure of a disciplined employee's name or other work-related information within the firm or outside the firm?*
- *Does an employee have a right to access and confirm his/her personal information retained by the employer and to request correction if it is inaccurate?*

6. Personal information and privacy protection after the employment relations

- *Are there any legal issues for a prior employer to provide information concerning the former employee at the request of a prospective employer?*

7. Evaluation and future directions

- *How do you evaluate the regulations protecting personal information and privacy in the labor and employment law in your country?*
- *Does the current regulatory scheme in your country provide effective regulations and remedies? Are there any side effects caused by the protective regulations such as hindering or distorting labor market function?*
- *Any idea about future policy directions?*

Some Observations

At the seminar the participants made presentations based on their papers and lively discussions followed. The papers are contained in the following chapters, with some revisions to reflect those discussions. They are simply too rich in substance to be summarized here, but we would like to make several points in the hope that readers will have some kind of analytical guidance when going through this volume.

First of all, it was agreed at the seminar that the issue of employees' personal information and privacy has become extremely important. It is essential to keep in mind that in terms of information technology we are living in a totally different society from, say, 30 years ago. It is very easy today--and it will be much more so in the future--to acquire, store, and transfer personal information through electronic devices, and this inevitably affects the scope and the nature of legal problems. There are some classic issues of privacy in the workplace that have been discussed for quite a while, but others are novel and may well require new regulatory frameworks.

Secondly, there is a trend toward protection of personal information by special legislation. Most notable in this regard is the EU Directive on the protection of personal data (95/46/EC) of 1995, which prompted Germany and France to revise their preexisting statutes and Spain and the U.K. to adopt new laws. Meanwhile, it seems that Korea, Taiwan, Japan, and Australia are headed in the same direction, legislating their own version

of data protection. These statutes are comprehensive and not specifically targeted at employment relations, but they are in fact an important element of today's employment law.

Thirdly, as the initial stage of employment, the hiring process requires special attention. Certain types of information are usually classified as "sensitive" and given more protection at the time of recruitment and hiring under the personal information legislation. In addition, the law of employment discrimination is becoming increasingly relevant, in effect deterring potential employers from asking about those traits of the applicant. Some countries have specific regulation regarding the applicant's health conditions, criminal record, or even social media passwords. However, employers also have legitimate interests in obtaining information about the applicants, and there are different ways of striking a balance among the counties.

Fourthly, at the later stages of employment, we are all facing a variety of legal issues such as video monitoring in the workplace, interception of e-mails, drug and alcohol testing, and surveillance of employees' off-duty conducts. Efforts are being made in each country to protect the realm of privacy, and in so doing some countries rely on special statutes regulating electric devices or telecommunication.

Fifthly, in order to understand the significance of statutory regulation, it would be beneficial to identify the default rules of the country regarding employees' personal information and privacy. Even prior to a specific statute, some countries were providing a considerable degree of protection through the constitution and/or civil laws including torts, while other countries had less aggressive default rules. Of course legislation should be valuable in the former countries, too, because it can clarify, expand, or streamline the rules with necessary adjustments.

Sixthly, the employee's consent plays a critical role in many aspects of personal information and privacy, and it would be essential for us to look into this notion more deeply. For instance, the protection of personal information or privacy might be deemed waived by the employee's consent. However, employees are often compelled to give consent to the employer due to the nature of employment relationship, and there should be safeguards to secure "consent" in the true sense. Perhaps it will help to have a labor union or employees' representative get involved. However, personal information and privacy are peculiarly personal by nature. Thus the role of employee representatives would be not to replace individual's consent by their collective agreement with the employer but to provide procedural regulations for securing individual's bona fide consent.

Finally, after studying the various measures taken in respective countries from a comparative viewpoint, it would be necessary to ponder exactly what they are designed to protect. It seems that the realm of private life is more clearly demarcated and detached from the workplace in Western countries. On the other hand, Japan and other Asian countries may be allowing employers to obtain and utilize employees' personal information more widely to accommodate their needs in various aspects of the employment relationship. In these countries, the purpose for obtaining employees' personal information is not only to control and discipline employees, but also to implement measures for their employees' benefit such as to care for employees' health and safety and to consider family situations in ordering transfers. This will lead us to review the employment system of each country before identifying the common and essential standards of protection regarding employees' personal information and privacy.

Data Protection in the Employment Relationship
- The German View -

Gregor Thüsing*
University of Bonn

I. Introduction

In a nutshell, data protection law is the legal response to the various threats posed to privacy[1] – no matter whether they originate from the state or an individual.

It has a comparatively long history in Germany: It first received public attention in connection with profiling done to combat the "Rote Armee Fraktion (RAF)" left wing terrorists. This led to the adoption of the first law worldwide on data protection in the state of Hessen in 1970.[2] The first federal act on the protection of personal data, the Bundesdatenschutzgesetz (BDSG = Federal Data Protection Act), dates back to 1977. Another step forward was the Volkszählungsurteil (Census case) of the Bundesverfassungsgericht (Federal Constitutional Court)[3] in 1983 which created the constitutional mandate for the protection of personal data. In this decision, the Constitutional Court held that the Grundgesetz (Basic Law, i.e. the German Consitution) does not only protect privacy as such but that the respect of a person's private life also encompasses the protection of personal data.[4] Thus the constitution mandates some degree of legal protection for personal data.

Whereas data protection at first was mainly focused on protection from privacy infringing state actions, the need for an effective protection of personal data was highlighted in recent years by several scandals involving processing by private companies. Among the best-known was widespread screening of employees by the Deutsche Bahn AG (the state-run rail company) in 2009 and 2010 and the Deutsche Telekom AG (the former state telecommunications carrier) in 2010. Retail chain Lidl was heavily criticized for employee surveillance in the same timeframe. These incidents have scandalized the populace and have seriously jeopardized the reputation of the companies involved and made data protection an everyday topic even before the NSA scandal.

Due to those scandals as well as a general awareness of threats to privacy as a consequence of new technologies, the social-political debate deals much more with this field of law nowadays. As regards the employment relationship, the European Commission

---

* With collaboration of Dr. Gerrit Forst, Dr. Stephan Pötters and Dr. Johannes Traut.

[1] Cf. Nick Platten, Background to and History of the Directive, in: David Bainbridge, EC Data Protection Directive (1996), ch. 2.

[2] Alexander Genz, Datenschutz in Europa und den USA (2004), p. 9; see alsohttp://www.iuscomp.org/gla/statutes/BDSG.htm (as at April 14th, 2014).

[3] Bundesverfassungsgericht (Constitutional Cour, BVerfG), 15 December 1983, cases 1 BvR 209/83 et alia.

[4] This important case is summarized below (chapter IX) .

pointed out that 'the emergence of a knowledge based economy with technological progress and the growing role attributed to human capital have intensified the collection of workers' personal data in an employment context. These developments give rise to a number of concerns and risks and brought the issue of effective protection of employees' personal data into focus.[5]

Since 1995 with the adoption of the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) data protection law is harmonized by European law, its reform is no longer a purely national but rather primarily a European topic. Therefore, the focus discussion is currently on the reforms proposed by the European Commission in 2012.[6]

But in spite of all new technical threats, scandals and recent developments – the fundamental conflict in the employment relationship as regards the field of data protection remains the same: How to strike a balance between the employee's understandable desire for privacy on the one hand and the employer's vital interests on the other, such as preventing crimes or any other violation of rules set out for his firm by means of surveillance etc.?[7] This conflict of interests is at the heart of each problem that is going to be discussed in this paper. Ensuring proportionality between these contrary principles is therefore of paramount importance for the interpretation of data protection provisions in an employment law context, no matter whether they are European or national rules.

II. At a glance: General principles governing German and European data protection law

1. Justifying the processing of personal data (Section 4 BDSG)

The structure of data protection law is simple and strict: All processing of personal data has to be justified. As far as the national data protection law is concerned, this principle is enshrined in Section 4 (1) of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG). According to this provision, "the collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent." The same principle applies to the law of the European Union (cf. Article 7 of the Data Protection Directive 95/46/EC).

This principle does not only apply to public bodies such as the police, but also restricts the use of personal data by private individuals like an employer. Hence, every employer has to justify all collection, processing and use of the employees' personal data. According to Section 4 (1) BDSG, there are three permissible grounds for justification:

- the processing is allowed under the BDSG,
- the processing is allowed under another law addressing data protection issues, or

[5] See First Report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final.

[6] In particular the "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", COM(2012) 11 final, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (as at April 14th, 2014).

[7] Cf. Gregor Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), para. 2.

- the data subject (i.e. the employee) has given his or her consent.

2. Fundamental principles governing the processing of the employee's personal data by the employer

Data protection law is governed by several other general requirements that have to be met when processing personal data in the employment relationship. Those principles are laid out in a 2001 opinion of the **Article 29 Working Party** on the processing of personal data in the employment context:[8]

- ✓ FINALITY: Data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes.
- ✓ TRANSPARENCY: As a very minimum, workers need to know which data is the employer collecting about them (directly or from other sources), which are the purposes of processing operations envisaged or carried out with these data presently or in the future. Transparency is also assured by granting the data subject the right to access to his/her personal data and with the data controllers' obligation of notifying supervisory authorities as provided in national law.
- ✓ LEGITIMACY: The processing of workers' personal data must be legitimate. Article 7 of the Directive lists the criteria making the processing legitimate.
- ✓ PROPORTIONALITY: The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Assuming that workers have been informed about the processing operation and assuming that such processing activity is legitimate and proportionate, such a processing still needs to be fair with the worker.
- ✓ ACCURACY AND RETENTION OF THE DATA: Employment records must be accurate and, where necessary, kept up to date. The employer must take every reasonable step to ensure that data inaccurate or incomplete, having regard to the purposes for which they were collected or further processed, are erased or rectified.
- ✓ SECURITY: The employer must implement appropriate technical and organizational measures at the workplace to guarantee that the personal data of his workers is kept secured. Particular protection should be granted as regards unauthorised disclosure or access.
- ✓ AWARENESS OF THE STAFF: Staff in charge or with responsibilities in the processing of personal data of other workers need to know about data protection and receive proper training. Without an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace.

[8] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014).

III. National data protection law within the European regulatory framework: It's all about proportionality

Data protection law applicable in Germany can be derived from two sources: the law of the European Union and national German law. In case of a conflict between the different provisions, the law of the Union reigns supreme: National law that is in breach of European primary law – that is the law of the treaties – may not be applied nationally. All national legislation has to be applied and interpreted by the courts as far as possible in conformity with the law of the Union, regardless whether it is primary or secondary law.

It is therefore worthwhile to first look at the law of the Union in order to grasp the system of data protection law as it is in Germany: Data Protection law and the protection of privacy are deeply rooted in European law. Even the primary law of the European Union places great emphasis on the protection of citizens' privacy and personal data and mandates protection of personal data as can be gleaned from the Charter of Fundamental Rights. According to Art. 6 para. 1 of the Treaty of the European Union the Charter of Fundamental Rights is part of the primary law of the Union. Art. 8 of the EU Charter of Fundamental Rights contains an explicit guarantee of the protection of personal data. It reads as follows:

> **Article 8 Protection of personal data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

On the level of the secondary law the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (**Data Protection Directive**) is the central instrument regulating the processing of personal data. This directive was developed and has to be interpreted according to the law of the European treaties, in particular Art. 8 of the EU Charter of Fundamental Rights.

The Data Protection Directive applies to all automated processing of personal data with the exception of the fields which fall outside the scope of the law of the European Union – such as national security or defence – and processing by a natural person in the course of a purely personal or household activity. Thus the Directive regulates not only data processing by private citizens – in particular data processing in a commercial setting – but also data processing by state agents, for instance in the field of law enforcement or social security. Since the Data Protection Directive has no specific rules for the processing of employee data by the employer, the general rules apply for processing in an employment relationship.

The legal form "Directive" is a legislative act of the European Union which requires member states to achieve a particular result without dictating the means of achieving the result (Art. 288 Sec. 3 TFEU). This contrasts with the self-executing regulation which is directly applicable in all Member States (Art. 288 para. 2 TFEU).

Thus the Directive necessarily requires a national implementing act, which is then directly applicable in that member state. The Data Protection Directive has the peculiarity to be implemented not by one but by several German implementing Acts on both federal

and state level, which individually only cover part of the Directive's scope. Data Processing by private citizens as well as data processing by federal agencies is covered by the Bundesdatenschutzgesetz (Federal Data Protection Act – BDSG). Data processing by agencies of the federal states – for instance by law enforcement purposes – is regulated by the respective state Data Protection laws. In practice the BDSG is by far the most important implementing act, as it covers data processing by private citizens.

Despite length and multitude of these implementing acts, the member states actually have very limited leeway in determining the legality of processing: The Directive does not merely establish a basic standard but aims to reconcile – as can be gleaned from its name – the protection of personal data with the free flow of data within the common market. In order to set uniform rules for the common market, the data protection directive 95/46/EC sets a European uniform standard from which member states may not derogate – neither in the direction of stricter rules nor by relaxing them.[9] The substantial law standards are – at least as long as the directive is properly implemented into national law – the same in all member states.

Article 6 and 7 of the Directive contain the most important provisions in regard to the substantial standard of law. Article 6 establishes the principles relating to data quality:

> **Article 6**
>
> 1. Member States shall provide that personal data must be:
> (a) processed fairly and lawfully;
> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
>
> 2. It shall be for the controller to ensure that paragraph 1 is complied with.

Most important of these principles is the principle enshrined in lit. b and c which may be summarily called the principle of purpose limitation. Data may only be processed for specified purposes and only insofar as it is necessary to fulfill that purpose. This obliges the person controlling the data processing (**controller,** Art. 2 lit. d of the Data Protection Directive) to reflect his processing activities and define the purposes clearly.

Art. 6 lit. a of the Directive also requires that processing must occur lawfully. Meant by this is that any processing needs an explicit legal basis – this is echoed by Section 4 of the BDSG (see above). The legal grounds for processing are enumerated in Art. 7 of the Data Protection Directive:

[9] Court of Justice of the European Union (CJEU), 6 November 2003, case C-101/01, paras. 96 f. (Lindqvist).

Article 7

Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

These alternatives are non-exclusive. Most important in the context of private processing is certainly lit. f), the balance of interest. All other variants enumerated in Art. 7 are no more than descriptions of particular cases in which the balance of interest may tip in favour of the controller. Since this balance of interest can only be assessed on a case by case basis, implementing acts which ban certain kinds of processing altogether are quite problematic at least in the private sector. It is unlikely that one can assume that the balance of interest will always tip in favour of the person whose data is being processed (**data subject**).

Therefore in many cases implementing acts have to be interpreted quite broadly in order to meet the standard of the Directive. The Directive does not only require the member states to adopt implementing acts in accordance with the Directive, but also requires their interpretation in accordance with the Directive.

Nevertheless, within its scope the influence of the Directive is very far-reaching and even derogates the national Constitution: Even though personal data may also be protected by the member states constitution – as is the case in Germany with Art. 2 in conjunction with Art. 1 of the Grundgesetz ("Basic Law", ie the Constitution of Germany; GG) – these provisions also have to be interpreted in accordance with the EU Charter of Fundamental Rights and the Directive. Bearing in mind that the Directive itself strikes the balance between the protection of personal data and in particular commercial interests, this balance has to be transferred to the national Constitutions. It is currently unclear if and to what extent the member states have leeway in determining the balance.

However, it is safe to say, that the Court of Justice of the European Union (CJEU) and its interpretation of the Directive does not leave a large margin for manoeuvre for the Member States. In its leading case *Lindqvist* the Court held that the harmonisation of the national laws is "not limited to minimal harmonisation but amounts to harmonisation which is generally complete. […] It is true that Directive 95/46 allows the Member States a margin for manoeuvre in certain areas and authorises them to maintain or introduce particular rules for specific situations as a large number of its provisions demonstrate. However, such possibilities must be made use of in the manner provided for by Directive 95/46 and in accordance with its objective of maintaining a balance between the free

movement of personal data and the protection of private life."[10]

IV. Processing of personal data under Section 32 BDSG

As pointed out above, all processing of personal data has to be justified by the responsible controller. This is expressed by Section 4 (1) BDSG: "The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent."

In the employment context, the most important provision that serves as a basis for the justification of the processing of personal data is Section 32 BDSG. Section 32 BDSG – in the government provided, but unofficial English translation[11] – reads:

> **Section 32: Data collection, processing and use for employment-related purposes**
>
> (1) Personal data of an employee may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees' personal data may be collected, processed or used to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in excluding the collection, processing or use, and in particular the type and extent are not disproportionate to the reason.
> (2) Sub-Section 1 shall also be applied when personal data are collected, processed or used without being processed by automatic procedures nor processed, used in or from a non-automated filing system, nor collected in such a filing system for the purpose of processing or use.
> (3) The rights of participation of staff councils shall remain unaffected."

Para. 1 allows data processing only insofar as it is "necessary" for hiring decisions or carrying out or terminating the employment contract. This wording led several commentators to interpret the provision very narrowly and for instance exclude employee screenings without concrete grounds for suspicion.[12] This approach, however, is treacherous and often not in line with the Directive. The latter applies, as everywhere else, the interest of balance test which does not limit processing to cases where this is strictly speaking necessary. One example is the aforementioned employee screening: Processing only slightly interfering with employees privacy – for instance automatically checking that payments made by the company to contractors are not paid to the same bank account as an employee's salary – can be justified by the employers overwhelming interest to combat fraud in his company.

Moreover, Section 32 (3) BDSG extends the scope of the protection beyond the scope of the Data Protection Directive as it implements and includes also non-automated.

---

[10] CJEU, 6 November 2003, case C-101/01, paras. 96 f. (Lindqvist).; This approach was reaffirmed very distinctly in CJEU, 16 December 2008, case C-524/06, paras. 51 f. (Huber v Germany), and lately in CJEU, 24 November 2011, case C‑468/10 (ASNEF).

[11] See http://www.gesetze-im-internet.de/englisch_bdsg/index.html (as at April 14th, 2014).

[12] See Achim Seifert in: Spiros Simitis (ed.), Bundesdatenschutzgesetz (7th ed. 2011), § 32 paras. 103, 108; Martin Kock and Julia Francke in: Neue Zeitschrift für Arbeitsrecht (NZA) 2009, p. 646, 648; unclear Michael Kort in: Der Betrieb (DB) 2011, p. 651, 653.

This, of course, is very far reaching as even an employer looking at his employee could be interpreted as processing personal data, e.g. his skin colour. This is, however, not per se prohibited as the Directive explicitly does only apply for automated processing and processing involving a file (Art. 3 para. 1 of the Directive 95/46/EC). Therefore member states are free to regulate non-automated processing.

V. The data subject's consent (Section 4a BDSG)

Apart from Section 32 BDSG, another important option to justify the processing of personal data in the employment context is the employee's consent. As laid down in Sections 4 and 4a BDSG, consent is one of the grounds on which personal data may be processed legitimately.

But what exactly is "consent"? Pursuant to Article 2(h) of the Directive 95/46/EC 'the data subject's consent shall mean "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." In general, the data subject's consent has to be given "unambiguously", see Article 7(a) of the Directive 95/46/EC.

From these provisions we can derive four requirements that have to be met: Consent must be

- freely given,
- specific,
- and informed.
- It may consist of any indication of the data subject's wishes by which he/she signifies his/her agreement to personal data relating to him being processed.

1. Freely given

The first condition can be considered as the most contentious notion in relation to employment law. Economic pressure may amount to duress so as to vitiate consent.[13] It is even arguable that in the context of employment consent is basically never given entirely freely. Although this might be going too far,[14] special attention has to be paid to whether the worker has a genuine free choice. If this is the case, there is no reason why the employee's consent should not, according to current EU law, legitimize the processing. This interpretation is also in conformity with the Union's primary law, especially the subject's fundamental rights. The European Court of Human Rights (ECHR) has held that individuals are capable of consenting to waive fundamental rights under the EU Charter of Human Rights (EChHR).[15] Article 8(2) of the EU Charter of Fundamental Rights also explicitly mentions consent as a possible justification.

It also has to be pointed out that the employee's consent does not constitute a blank cheque for the employer. The processing still has to comply with the other data protection principles, in particular the principle of proportionality. In short, it may be difficult but not impossible to show that the employee's consent has been given freely.

[13] Cf. UK Privy Council, 6 April 1979, case *Pau On v Lau Yiu Long*.
[14] Cf. Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.
[15] ECHR, 9 April 1997, case 29107/95, (Stedman v UK); cf. Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.

2. Specific

The second requirement to be examined is the term specific. This notion is rather vague. *Jay* holds that consent clauses may still be broad as long as they are clear about all relevant matters.[16] This interpretation is too generous. The German wording of the Directive ("für den konkreten Fall" = "in a concrete case") suggests a narrower approach limiting the legitimising effect of the employee's consent to a specific processing of specific personal data. Hence the requirement of specificity rules out all vague and generalised forms of consent that would legitimise any data processing in relation to an employment relationship.

3. Informed

Thirdly, the consent must also be informed. The data subject must be aware of the nature of the processing and any important features which might affect him or her.[17] This also implies that the data subject must be able to assess the consequences of his or her consent with regard to his fundamental rights. Otherwise the consent would not be in conformity with the primary law. It is of particular importance that the subject knows which personal data will be processed and for what purpose.[18] As to the degree of knowledge necessary to make consent valid it might be useful to draw parallels to the doctrine of informed consent that has been developed for negligence cases in relation to medical treatment;[19] these parallels may be particularly instructive in regard to the processing of sensitive data.

4. Indication of the data subject's wishes

Fourthly, the consent has to consist of an indication of the data subject's wishes. Therefore, silence or mere passive acquiescence is not sufficient.[20] On the other hand, consent can be inferred from conduct[21] as long as it does not have to be "explicit" as it is the case in relation to sensitive data. According to recital (17) of the Directive 2002/58/EC "consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website." The national German law seems to be even stricter – but this is misleading as it has to be interpreted in conformity with the EU law. According to Section 4a BDSG, the data subject's consent has to be in *written* form. This is not necessary in order to be in conformity with the Directive and therefore shouldn't be interpreted too literally, but it clearly shows that the subject's consent must be founded on a clear indication of the agreement to a particular processing.

---

[16] Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.
[17] Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 152.
[18] Cf. Peter Gola and Rudolf Schomerus, Bundesdatenschutzgesetz (10th ed. 2010), section 4a paras. 10 ff.
[19] For comprehensive information about the doctrine of informed consent see Alasdair Maclean, The doctrine of informed consent: does it exist and has it crossed the Atlantic?', Legal Studies (LS), Vol. 24 (2004), pp. 386ff. and Josephine Shaw, 'Informed consent: a German lesson', International and Comparative Law Quarterly (ICLQ), Vol. 35 (1986), pp. 864ff., who demonstrates that this doctrine is well developed in civil law countries like France, Switzerland and Germany.
[20] Cf. Rosemary Jay, Data Protection – Law and Practice (3rd ed., 2007), p. 153.
[21] Cf. CJEU, 21 November 2001, case C-414/99 (Zino Davidoff SA v A&G Imports Ltd).

5. Consent in the employment context

The underlying rationale of the provisions regarding consent is a very old doctrine that applies to various areas of law: *volenti non fit iniuria*. Nevertheless, the legitimacy of this universal idea has been questioned in relation to data protection in the employment relationship. As has already been mentioned (see above II.2.), in 2001 the Article 29 Working Party issued an opinion on the processing of personal data in the employment context.[22] The Working Party held that consent "should only be a fall-back position if no other Art. 7 criteria or Art. 8 exception is applicable." Reliance on consent should only be confined to situations where the employee has a genuine free choice and is subsequently able to withdraw the consent without detriment.[23] It is indeed arguable whether the employee's consent could still be freely given in situations where none of the other criteria of Article 7 or Article 8 of the Directive is satisfied. For example, if the giving of consent is a condition of employment, it is very likely that the employee will accept the relevant clause in order to not lose the job opportunity.[24] To sum it up, the inequality of bargaining power which is inherent in the employment relationship[25] may force the employee to consent to a certain processing of data.

For this reason, the German government is discussing a reform of the national data protection law that would (in principle) lead to an abolition of consent in the employer employee relationship.[26] In Finland, the Act on Protection of Privacy in Working Life prescribes that the employer is entitled to process personal data only in cases where this is necessary for the observation of the rights and obligations of the parties to the employment relationship; there can be no exemption from this necessity requirement, even with the consent of the employee.[27] In Belgium, the employee's consent alone may not legitimise the processing of sensitive data.[28]

This issue was further discussed on a European level. The social partners were consulted by the Commission and research studies were undertaken.[29] The Commission

[22] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014).

[23] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014), p. 23.

[24] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf (as at April 14th, 2014), p. 23.

[25] See Otto Kahn-Freund, Labour and the Law (1972), p. 7; the inequality of bargaining power as an "axiom" of labour law is not uncontested today, cf. Abbo Junker, Individualwille, Kollektivgewalt und Staatsintervention im Arbeitsrecht, in: NZA 1997, p. 1305; Lord Wedderburn, Labour law 2008: 40 years on, in: International Law Journal (ILJ), Vol. 36 (2007), pp. 39.

[26] See Section 32l of the bill proposal (24.08.2010). The bill is available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.pdf?__blob=publicationFile (as at April 14th, 2014).

[27] See http://www.eurofound.europa.eu/eiro/2001/06/feature/fi0106191f.htm (as at April 14th, 2014).

[28] See the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, p. 11.

[29] The different communications and studies are available at http://ec.europa.eu/social/main.jsp?catId=708&langId=en (as at April 14th, 2014).

also took the view that the role consent can play in an employment relationship is limited, due to the dependant and subordinate situation of the worker.[30] But later on, after the social partners had failed to conclude a European agreement on the protection of personal data in the employment context, the Commission held that the Directive 95/46/EC should not be amended.[31]

So, in the end: just much ado about nothing? Not quite. In summary, it can be said that the employee's consent still serves as ground for justification in EU and national data protection law. But, as the discussions have shown, the relevant provisions have to be applied restrictively and attention has to be paid whether the subordinate structure of the employment relationship does not exclude the possibility of freely given consent.

VI. Risk-based approach: Different categories of personal data and different purposes for processing them

As pointed out above, data protection in the employment context is primarily about ensuring a proportionate balance between the employer's and the employee's fundamental rights and interests. The central question is: How to strike a balance between the employee's understandable desire for privacy on the one hand and the employer's vital interests on the other?[32]

The employer's interests can be very diverse. As long as his or her objective is legitimate, it can theoretically justify all processing of personal data, as long as the employer respects the principle of proportionality. The employer may, for example, process data in order to prevent crimes or any other violation of rules set out for his firm by means of surveillance, he may process data for matters of recruitment, effective human resource management such as job allocation, transfer of employees, health and safety compliance, work-related injuries and their compensation disputes, for preventing the leakage of trade secrets, etc. This leads us to the conclusion that there are few *per se* illegitimate purposes. Criminal activities of the employer would be one, but most seriously considered purposes can possibly justify data processing.

But not all goals the employer pursues have the same validity. Some objectives are more important than others and those differences are mirrored in the structure of the different provisions of data protection law. For example, there is a special provision dedicated to the processing of personal data to investigate crimes (Section 32(1), second sentence BDSG).

Another important distinction made by the BDSG (and the Data Protection Directive 95/46/EC) relates to certain types of personal data. For example, the provisions on certain data, which are categorized as being particularly sensitive, are much stricter. Section 3(9) BDSG defines sensitive data as all information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life (cf. also Article 8 of the Data Protection Directive). The processing of those sensitive data has to

[30] Communication from the Commission, Second stage consultation of social partners on the protection of workers' personal data, p. 10 f., available at http://ec.europa.eu/social/main.jsp?catId=708&langId=en (as at April 14th, 2014).
[31] Communication from the commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, p. 5, 10.
[32] Cf. Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), para. 2.

fulfil stricter legal requirements than the processing of other data. Section 28, for instance, regulates the processing of personal data for commercial purposes. Under Section 28(1) no. 2 BDSG, personal data may be processed, "as far as necessary to safeguard legitimate interests of the controller" and if "there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use." However, this very broad clause does not apply to sensitive data. Under Section 28(6) BDSG, the collection, processing and use of sensitive personal data shall only be lawful if

> "1. necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent,
> 2. data are involved which the data subject has manifestly made public,
> 3. necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of collection, processing or use, or
> 4. necessary for the purposes of scientific research, where the scientific interest in carrying out the research project significantly outweighs the data subject's interest in ruling out the possibility of collection, processing and use and the purpose of the research cannot be achieved in any other way or would require a disproportionate effort."

Another example for the distinction between sensitive and other data are the provisions on the data subject's consent: In general, the consent has to be given 'unambiguously', see Article 7(a) and Article 26(1)(a) of the Data Protection Directive. In relation to sensitive data, the provisions of the Data Protection Directive are stricter, as the data subject has to give his 'explicit' consent, see Article 8(a) of the Data Protection Directive.

Whereas the law is stricter whenever sensitive information is concerned, the processing of "generally accessible data" is much easier to justify, cf. Section 28(1) no. 3 BDSG or Section 29(1) no.2 BDSG.

These examples demonstrate that the legislator has pre-balanced the balancing of interests that has to be done in every individual case (proportionality test).

VII. Central issues of data protection law in the employment relationship

1. Personal information in the hiring process / job interviews

Job seekers around the world need to be prepared to answer a range of questions before being employed. However, the German courts have limited the right of the prospective employer to ask questions for decades.[33] According to jurisprudence, in a job interview the prospective employer may only ask questions when he has a legitimate interest to know the answer. If the prospective employer asks a question he may not ask, the applicant is allowed to lie without having to be afraid to be dismissed for the lie later on.[34]

Since 2009, the „legitimate interest" test has a statutory basis in Section 32 Federal Data Protection Act. According to this rule, the prospective employer may process data only if the processing of this data is „necessary", meaning proportionate (see above under

[33] Seminal Bundesarbeitsgericht (Federal Labour Court, BAG), 5 December 1957, case 1 AZR 594/56.
[34] See e.g. BAG, 6 September 2012, case 2 AZR 270/11.

VI.). Moreover, Sections 19 pp. Genetic Diagnosis Act (Gendiagnostikgesetz) render it illegal to process the data of applicants and employees (very limited exceptions apply for health security reasons). Finally, the General Antidiscrimination Act (Allgemeines Gleichbehandlungsgesetz) prohibits to discriminate against applicants on the ground of race or ethnic origin, sex, religion or philosophical belief, disability, age or sexual orientation. If the prospective employer processes data on any of these subjects, this may indicate a discrimination of the applicant. The prospective employer will then have to prove that in fact, he did not discriminate against the job seeker.

On this background, the prospective employer is allowed to ask an applicant for contact details such as his name, address, phone number, driver's licence etc., as long as the processing of this data is necessary.

On the other hand, the employer is usually not allowed to inquire into the ethnic origin or race of an applicant, a trade union membership (exceptions may apply for trade unions as employers and/or employers' unions), disability, sickness or disease (as long as it does not pose a threat to others and does not limit the ability of the applicant to work), religion or philosophical belief (exceptions may apply for religious groups as employers), sexual orientation, pregnancy (as it indicates a discrimination on the basis of sex)[35] or membership in a political party (exceptions may apply for political parties as employers).

Also, the employer is not allowed to inquire into data that does not relate to the prospective employment relationship in any way. Usually this covers data such as family structure, marital status, credit information, litigation history, club membership and so on. In some countries, prospective employers seem to ask applicants for their social networking passwords. In Germany, a question like that is virtually unthinkable and would probably trigger a public outcry as well as administrative action in the form of fines, or worse.

Finally, the employer may be allowed to ask for criminal convictions or pending investigations.[36] However, he is limited to processing data that might affect the applicant to pick up the prospective work and/or to do it properly. Therefore it may be legal for a logistics company to ask a prospective lorry driver whether he has ever been convicted for traffic related crimes, but they would not be allowed to ask him for, e.g., a conviction for insulting people. A financial institution may ask an applicant for criminal convictions related to business (fraud, money laundering etc.), but not whether he has been convicted for, e.g., drunk driving. Pending investigations may be inquired into if they might limit the ability of an applicant to pick up work or might otherwise affect the employment relationship. However, the presumption of innocence needs to be respected, so that jurisprudence is rather restrictive with respect to pending investigations.[37]

2. Video surveillance / CCTV in the workplace

Nowadays, video surveillance of publicly accessible areas or also of private company premises is widely used.

a) Applicable provisions of the Federal Data Protection Act (BDSG)

The use of CCTV / video surveillance is mainly governed by three provisions of the

[35] BAG, 6 February 2003, case 2 AZR 621/01.
[36] See e.g. BAG, 6 September 2012, case 2 AZR 270/11 and BAG, 15 November 2012, case 6 AZR 339/11.
[37] See BAG, 15 November 2012, case 6 AZR 339/11.

Federal Data Protection Act (BDSG) that can be relied on by the employer in order to justify the processing of the personal data of the people monitored by the cameras:

- Section 6b BDSG: This provision governs the use of CCTV technologies in publicly accessible areas, e.g. supermarkets, train stations, shops, etc.
- Section 32 BDSG: This provisions is applicable for the surveillance of employees in any other situation, i.e. non-publicly accessible areas of the workplace
- Section 28 BDSG: This provision is applicable if the video surveillance is used for purposes not related to the employment relationship, e.g. when customers or other third parties are being monitored

All of those provisions require a legitimate interest or purpose for the video surveillance and a proportionality test.

b) Legitimate purposes

The purposes have to be stipulated in a concrete way before the installation of the surveillance system, meaning they have to be documented and made available by means of an index of procedures to any interested person, see Section 4g (2) BDSG.

The main reason why employers install CCTV technologies is probably to protect the company against vandalism, theft or other property crimes or to protect persons (employees, clients etc.) from criminal activities. So in general, the main purpose of video surveillance is not the monitoring and control of employees. However, both are often congruent. Thus, at banks or in parking garages, in the area of cash desks of department stores or museums – virtually casually –employees are also being monitored. Be it casually or intentionally, video surveillance of employees is only admissible within strict limits.

c) Proportionality test

Irrespective of which particular provision of the BDSG is applicable (whether Section 6b BDSG governing the use of video surveillance in publicly accessible areas or Section 28 BDSG or Section 32 BDSG) – when it comes to the assessment of the permissibility of video surveillance, the central yardstick of evaluation is always a proportionality test. It has to be evident that surveillance is “necessary”, i.e. there must not be any other effective alternative to video surveillance. In addition, the relation of means and purpose has to be proportionate. It is not allowed to use video surveillance in connection with minor offences, e.g., in order to control an existing ban on smoking.

If video surveillance of publicly accessible areas complies with Section 6b BDSG and those publicly accessible areas also happen to be workplaces – e.g., the video surveillance in a bank or a supermarket – the employees will have to accept video surveillance as immanent in their workplace. However, in cases where the employees are not the real object of observation, any evaluation of the results of monitoring for the purpose of a control of productivity or behaviour-related information is inadmissible. Therefore, the evaluation of video surveillance of a bank used for the purpose of protection against robbery would be justified, but not for the purpose of controlling the employees’ behaviour. However, in a department store, video surveillance might perhaps be legitimately used for the purpose of protection against theft by the employees.

But in general, work is usually not performed in publicly accessible areas. In that case, it is only allowed to use video surveillance in compliance with Section 28 or 32 BDSG. In this context, the principle of proportionality has to be observed strictly. The

Federal Labour Court held that even the mere possibility of surveillance at any time puts considerable pressure on the employee which is incompatible with his right to the respect of his personal rights.[38] The Federal Labour Court draws the conclusion that video surveillance in the workplace is only justified in exceptional cases where the employer has vital interests. In general, it has to be assumed that the following principles are established case law:

- Before starting video surveillance, there have to be sufficient grounds for suspicion (for example in case of theft, etc.), which justify an intrusion into the data subject's personal rights. Any vague assumption or a general suspicion of all employees is not sufficient.
- In principle, video surveillance is generally only permissible if carried out openly rather than secretly, by means of visible equipment and only after the staff has been provided with sufficient information.
- As an "ultimo ratio", last ditch measure, surveillance by hidden cameras is permissible if it is the only possibility to protect the employer's legitimate interest.
- Video surveillance is subject to co-decision by the works council or by the staff council.
- Findings obtained by illegal monitoring are subject to a ban on any further use. They also cannot be used as evidence in a dismissal lawsuit.

3. Surveillance of internet and e-mail at the workplace

The use of the internet at work generates vast amounts of data. From a technological point of view, employers may use this data to survey the behaviour of their employees. From a legal perspective, monitoring the use of the internet and applications like e-mail by employees raises a range of questions: A crucial point is whether such surveillance is covered by the *Telekommunikationsgesetz* (Telecommunications Act, TKG) or not.

If the TKG is applicable, an employer is allowed to survey the use of the internet and applications like e-mail only for technical purposes (such as virus scanning) and to calculate fees (if the employee has to pay for private usage). The TKG does not allow an employer to monitor data for, e.g., reasons of corporate compliance. For employers it is seminal to note that a violation of the TKG is likely to constitute a crime under Section 206 *Strafgesetzbuch* (Criminal Code, StGB). In practice, it is therefore strongly recommended to act as if the TKG is applicable, even if it should not be from a theoretical perspective.

If the TKG is not applicable, surveillance of internet and e-mail usage by employees is covered by the BDSG. As seen above, Section 32 BDSG allows a processing of data if it is "necessary", meaning proportionate.

Although it is therefore of utmost importance for employers to know whether the TKG applies, this is arguable and quite uncertain. The decisive question is whether the employer is a *Diensteanbieter* (provider of services) in the meaning of the TKG or not. If he is a provider of services, he is subject to most of the rules of the TKG. The crucial rule here is Section 3 No. 6 TKG. According to this provision, a provider of services is a person that provides telecommunication services professionally or that helps to provide such services.

[38] Cf. in particular BAG, 21 June 2012, case 2 AZR 153/11.

In the past, the prevailing opinion in Germany held that an employer was a provider of services if he allowed his employees to use his telecommunication facilities for private purposes (e.g. calling home or using private webmail services), even if they were allowed to do so to a limited extend or in brakes only. The employer was not considered to be a provider of services if he prohibited the private use of such facilities. This differentiation is still quite common. This means in effect that internet and e-mail surveillance is not possible (other than for technical or billing reasons) if the employer allows his employees to use telecommunications facilities for private purposes.

During the last couple of years however, several Landesarbeitsgerichte (Higher Labour Courts, LAG) argued that the employer is not a provider of services even if he allows his employees to use telecommunications facilities privately.[39] The main argument for this opinion is that the TKG governs the competition on the market for telecommunication services. But an employer does not compete with telecommunications companies if he allows his employees to use the telecommunications facilities for private purposes. He does not act for profit. An employer simply wants to create some amenities for his employees and wishes to facilitate their work-/life-balance. Therefore, he should not be covered by the TKG.

As the second opinion is quickly gaining ground, it is likely that it will become predominant in the near future. The effect is that internet and e-mail surveillance will have to be proportionate under Section 32 BDSG. Although the legal situation is uncertain and every processing will have to be assessed in the light of the individual case, one can identify certain principles: Data that is obviously private (e.g. invitation for a dinner) may not be processed. Log files containing technological data only (e.g. time when an e-mail was sent, amount of data transferred) can be processed more easily than files with "real" content (e.g. text or pictures). The amount of data processed needs to be reduced as much as possible. Transparent processing is the rule, secret processing the absolute exception. Secret processing may take place to prove criminal behaviour, but even then it has to be considered carefully and can be a last resort only.

4. Transfer of data in international corporate groups

Corporate groups regularly need to transfer personal data of employees between group members: Employee data often is processed by the head of the group, at least for certain purposes (e.g. pension schemes). Also, certain group-wide services may be pooled in one of the group members (e.g. IT services). Under these circumstances, data often needs to be transferred from group member A to group member B. This transfer is a processing of data that needs to be justified. A justification of the transfer of data within Germany is subject to the same rules as any other processing of data. However, things get more complicated if group member A and group member B are not located within the same country.

As long as group member A and group member B are both located within the European Union, a transfer of personal data is to be treated like a transfer of data within Germany. However, under the Directive 95/46/EC, special rules apply if group member A

[39] Higher Labor Court (Landesarbeitsgericht, LAG) of Berlin and Brandenburg, 16 February 2011, case 4 Sa 2132/10; LAG Hamm, 10 July 2012, case 14 Sa 1711/10, cf. also Higher Administrative Court of Hessen (Verwaltungsgerichtshof, VGH), 19 May 2009, case 6 A 2672/08.Z.

is located in an EU country and group member B in a non-EU-country ("third country"). Germany implemented these rules in ss. 4b, 4c BDSG.

According to Article 25 Directive 95/46/EC, the Member States shall provide that the transfer of personal data to a third country may happen only if the third country in question ensures an adequate level of protection. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances of a data transfer. The European Commission may find that a third country ensures an adequate level of protection. A decision of the European Commission on this subject is binding for the Member States.

Third countries featuring an adequate level of protection from the point of view of the European Commission currently are Andorra, Argentina, Australia, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand and the Eastern Republic of Uruguay.[40]

Article 26 Directive 95/46/EC allows for derogations from the principle set out in Art. 25 Directive 95/46/EC. Derogations may apply if

- the data subject has given his consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

However, the applicability of these derogations needs to be assessed in the light of each individual case. Therefore, they do not form a reliable basis for a data transfer in an international group of companies.

If the third country does not feature an adequate level of protection and none of the derogations set out above applies, group member A may nevertheless transfer the data to group member B located in a third country, provided that group member A adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.

There are various ways to adduce such adequate safeguards:

- *Standard contractual clauses:* The European Commission has published three

[40] A list of countries is available at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-1 (as at April 14th, 2014).

sets of model contracts governing the transfer of data between parties located in a Member State and a third country.[41] These standard contractual clauses need to be agreed by the parties without amendments to create adequate safeguards in the meaning of Art. 26 Directive 95/46/EC. Standard contractual clauses are preferable if no more than two (or very few) members of a group need to transfer data between each other. However, they are no longer manageable if data transfer is to take place between various group members, as this would require a complex network of contracts. In such a situation, binding corporate rules are preferable (see below).

- *Individual contractual clauses:* In theory, it is possible for the parties to agree upon individual contractual clauses adjusted to the needs of the parties. However, these clauses would have to be accepted by the data protection authorities. Even if these are willing to give their consent, bureaucratic burdens render individual contractual clauses a highly impractical instrument.
- *Binding corporate rules:* Binding corporate rules are an alternative to standard contractual clauses in cases where more than two (or very few) group members need to transfer data to each other.[42] As to the arrangement of such corporate rules it is crucial that they are drafted in a legally binding way, equally mandatory for all companies of the group, and that this arrangement is implemented within the respective company in form of instructions by the respective employer vis-à-vis all employees.

Special rules apply with respect to the United States of America:[43] The USA are considered to be one of the states *without* an adequate level of data protection by the EU. However, in 2000, the EU entered an agreement with the USA on a so-called "safe harbour" (Safe Harbor Agreement). According to the agreement, an adequate level of data protection is assumed in companies which avow that they respect the principles stipulated in the agreement and which have their practises examined accordingly. In theory, the implementation of these obligations is controlled by independent audit firms, and the Federal Trade Commission of the US Department of Commerce is entitled to punish violations by imposing considerable fines. Recent studies however revealed that the safe harbor principles are widely disregarded in practice.[44]

[41] For details, see http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm (as at April 14th, 2014).

[42] For details, see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm (as at April 14th, 2014).

[43] For details, see Commission Decision 520/2000/EC and at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm sub USA (as at April 14th, 2014).

[44] For details on the transfer of data in international corporate groups see Gerrit Forst, Verarbeitung personenbezogener Daten in der internationalen Unternehmensgruppe, in: Der Konzern 2012, p. 170 – 185.

VIII. Some remarks on the proposed reform of the European legal framework

While there is much debate on how specific questions should be solved by German legislation, the more important developments are currently happening on the European level, in particular the reform of the data protection legislation.

In 2012, the European Commission proposed a major reform of the EU legal framework on the protection of personal data. The cornerstone of the reforms initiated by the Commission is the **proposal** for a "**General Data Protection Regulation**".[45]

This proposal explicitly addresses data processing in the employment context for the first time on the European level. However, it is rather a non-regulation as Article 82 of the proposed Regulation establishes a so-called opening clause for the Member States. Section 1 of this Article reads as follows:

> "Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment."

What is really meant by this clause, remains unclear: Can the Member States substantially derogate from the regulation's standard? The wording of Article 82 ("within the limits of this regulation") suggests otherwise. But if this is true, what is Article 82 good for? Does it merely express a request?

Moreover, the utility of an opening clause can be justly questioned. One of the major shortcomings of the current framework is less the substantive law – the balance of interest allows adequate and above all flexible solutions – but rather its disparate implementation and application throughout the Union.

In particular the administrative practices of the national supervisory authorities competent for the application are so far not effectively harmonized. This is a serious flaw: As the field data protection is particularly dependent upon efficient enforcement by state agencies,[46] the administrative practice significantly determines the practical application of the substantive data protection rules. The existence of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data.[47] The current consultation process within the framework of the Article 29 working Party (WP), while producing helpful input and guidelines, cannot set mandatory standards and enforce them. It is even less capable to overrule individual decisions by national supervisory authorities. The general lack of cohesion is aggravated by structural weaknesses of some supervisory authorities which lack financial and personnel resources

---

[45] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (as at April 14th, 2014).

[46] Cf. BVerfG, 15th December 1983, case 1 BvR 209/83 et. alia.

[47] CJEU, 16th October 2012, Case C-614/10, para 37 (Commission ./. Austria).

to properly discharge their mission.

The Commission now tries to tackle that problem by strengthening the supervisory authorities and ensuring harmonization of their practice:

- The proposed regulation's provisions on structure, duties and competences of supervisory authorities are far more detailed than currently (cf. Articles 46-54 of the proposed Regulation).
- The supervisory authorities are given broad powers to levy fines against offenders (Article 79) and powers of investigation (Article 53).
- A new and potentially very powerful consistency mechanism is introduced to ensure the uniform application of the regulation.[48]

These measures combined have the potential to achieve a unification of the administrative practices. Therefore the call for more harmonization is rightly one of the Commission's major selling points for the proposed Data protection regulation.[49] The hope of a truly harmonized data protection framework has in particular led business, on the whole, to speak out in favor of the reform.

Certainly the benefits of a better harmonization would be enormous. However, it would be a heavy blow indeed if the harmonization would not extend to the field of employee data processing. The latter is one of the more burdensome hurdles to working in several member states.

Article 82 could therefore call the entire reform package into question. This may be an exaggeration as most likely its impact is very limited as any legislations would have to be "within the limits of the regulation". In any case, its exact meaning should be clarified at least.

Another questionable novelty is the approach the regulation takes towards the employee's consent as a possible justification for a processing operation. Under the regulatory framework as proposed by the Commission, the employee's consent may be too restricted to be of any practical use.

IX. List of important cases

1. The mother of all data protection cases: The Census verdict of the Federal Constitutional Court[50]

What is the case about?

In 1982, the German federal parliament (Bundestag) passed an Act on a population census to be conducted in the following year. This brought on a huge societal debate about the data protection risks and the usefulness of the population census. Most of the arguments of the opponents focused on data protection problems. There were fears that the

[48] For more detail see Gregor Thüsing and Johannes Traut, The Reform of European Data Protection Law: Harmonisation at Last?, in:, Intereconomics, Vol. 48, No. 5, September/October 2013, p. 271.

[49] European Commission, "How will the EU data protection reform strengthen the internal market", available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf and "Why do we need an EU data protection reform?", available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (as at April 14th, 2014).

50 BVerfG, 15 December 1983, case 1 BvR 209/83 et al.

data could be linked back to the individuals, as there were more than 160 questions to be answered in the questionnaire. In addition, the forms contained code numbers and were to be kept for a considerable length of time. The data was to be collected, under the supervision of local authorities, by 600.000 collectors. The data was not only to be used for statistical purposes, but also for comparison with and correction of resident registers.

The Court held:

In this decision, the court developed the legal meaning of the citizens' fundamental right of informational self-determination as a part of the general right of personality as laid down in Article 2 and Article 1 of the Grundgesetz (Basic Law, i.e. the German Constitution). The general aim of the population census was upheld, but the judges demanded further procedural safeguards to protect this right. Additionally, the data transfer to the local authorities was considered to be unconstitutional as it blurred the boundaries between data collection for anonymous statistical purposes and the processing of personal data by those authorities. In developing the fundamental right of informational self-determination the court laid the foundations of both constitutional and sub-constitutional German data protection law.

2. Telephone surveillance I (Federal Constitutional Court)[51]

What is the case about?

The constitutional complaint concerned the authority of the Bundesnachrichtendienst (Federal Intelligence Service) to monitor, record and evaluate telecommunications traffic and to transfer the obtained data to other public agencies. Under the challenged legal provisions, monitoring was permissible in two forms: "Monitoring of Individuals" (Section 2 of the so-called G 10 Act) and "Strategic Surveillance" (Section 3 of the G 10 Act). The complainants questioned whether these regulations were compatible with Article 10 of the Basic Law that guarantees the "Privacy of correspondence, posts and telecommunications" as a fundamental right.

The Court held:

Article 10 of the Basic Law not only provides protection from the state taking note of telecommunications contacts. Its protection also extends to the procedures by which information and data are processed following permissible acts of taking note of telecommunications contacts, and it extends to the use that is made of the obtained knowledge. Furthermore, Article 10 of the Basic Law obliges the Federal Intelligence Service to take precautionary measures against the dangers which result from the collection and utilisation of personal data. These precautionary measures include, in particular, that the use of obtained knowledge be bound to the objective that justified the collection of the data in the first place. The court also decided that the competence of the Federal Intelligence Service under Section 1 and Section 3 of the G 10 Act to monitor, record and evaluate the telecommunications traffic for the timely recognition of specified serious threats to the Federal Republic of Germany from abroad and for the information of the Federal government is, in principle, consistent with Article 10 of the Basic Law. The transfer of personal data that the Federal Intelligence Service has obtained from

[51] BVerfG, 14 July 1999, case 1 BvR 2226/94 et al.

telecommunications monitoring for its own objectives to other government authorities is consistent with Article 10 of the Basic Law; it must, however, comply with the following prerequisites: (1) the data is necessary for the receiving agency's objectives; (2) specific requirements placed on changes of objective are met; and (3) the statutory thresholds for transfer comply with the principle of proportionality.

3. Online searches and reconnaissance of the Internet (Federal Constitutional Court)[52]

What is the case about?

This case dealt with the "North-Rhine Westphalia Constitution Protection Act". As a reaction to international terrorism and organized crime, this Act enabled the police and other public authorities to use software for secret access to information technology systems ("online searches" through so-called Trojan horse software and other forms of spyware) and reconnaissance of the internet.

The Court held:

The Constitutional Court held that the provision on "online searches" violated the general right of personality (Article 2 and Article 1 of the Grundgesetz) in its particular manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems, and that the Act was null and void. The provision in particular does not meet the requirements of the principle of proportionality. In view of the gravity of the encroachment, the secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read is constitutionally only permissible if factual indications exist of a concrete danger to a predominantly important legal interest. What is more, the encroachment is in principle to be placed under the reservation of a judicial order.

The Court also held that also the empowerment to secret reconnaissance of the Internet violates the constitution. The secret reconnaissance of the Internet encroaches on the secrecy of telecommunication (Article 10 of the Basic Law) if the authority monitors secured communication contents by using access keys which it collected without the authorisation or against the will of those involved in the communications. Such a grievous encroachment on fundamental rights is, in principle at least, also conditional on the provision of a qualified substantive encroachment threshold. This was not the case in the relevant provision of the challenged Act. The provision permitted intelligence service measures to a considerable degree in the run-up to concrete endangerment without regard to the grievousness of the potential violation of legal interests, and even towards third parties. What is more, the provision did not contain any precautions to protect the core area of private life.

If, by contrast, the state obtains knowledge of communication contents which are publicly accessible on the Internet, or if it participates in publicly accessible communication processes, in principle it does not encroach on fundamental rights.

[52] BVerfG, 27 February 2008, cases 1 BvR 370/07 and 1 BvR 595/07.

4. Search of the employee's locker (Federal Labour Court)[53]

What is the case about?

The employer was running a wholesale market. The plaintiff was one of his employees. The employer suspected the employee of stealing lingerie from the market. Without the employee's permission, the employer secretly opened a locker that was used by the employee for storing personal items, and found ladies underwear in the locker.

The Court held:

Opening and searching the locker was illegal under Section 32 BDSG. The purpose (fighting theft) was legitimate, but the secret opening of the locker violated the principle of proportionality as it was not necessary in order to pursue this legitimate aim. It would have been sufficient if the employer had opened the locker after informing and in presence of the employee. The BAG also held that the information obtained from this illegal search could not be used as evidence in a subsequent dismissal protection case.

5. The video surveillance / CCTV cases of the Federal Labour Court

What are the cases about?

There are many data protection cases on video surveillance. Even before the relevant provisions of the BDSG entered into force (Section 32 BDSG was added to the BDSG in 2009), the BAG had already established the major principles of the law.[54] The legislator merely codified this case law. Many of the cases dealt with CCTV installations in supermarkets[55] or similar shops.[56]

The Court held:

Substantiating the proportionality test in all individual cases, the BAG held that before installing CCTV devices, there have to be sufficient reasons for suspicion (for example an unsolved theft), which justify the surveillance. Some vague assumption or a general suspicion with respect to all employees is not sufficient. In principle, video surveillance has to be carried out openly rather than secretly. Secret surveillance is only acceptable as an *ultima ratio*, in order to protect the employer from grave violations of his interests (e.g. theft or other criminal activities). If these conditions are met, information gathered by means of secret surveillance techniques can be admissible in dismissal protection cases. In this context, Section 6b (2) BDSG, that prescribes the use of warning signs, has to be interpreted as a procedural provision that does not hinder the use of such information in lawsuits.

[53] BAG, 20 June 2013, case 2 AZR 546/12.
[54] The leading case is BAG, 27 March 2003, case 2 AZR 51/02.
[55] BAG, 21 June 2012, case 2 AZR 153/11.
[56] A recent case was about video surveillance in a liquor/beverages store: BAG, 21 November 2013, case 2 AZR 797/11; cf. also BAG, 27 March 2003, case 2 AZR 51/02.

6. Data processing on the basis of an employer/works council agreement (Federal Labour Court)

What is the case about?

According to Section 77 *Betriebsverfassungsgesetz* (Works Councils Act, BetrVG), the employer and the works council – a shop level representative body elected by the employees – may enter a *Betriebsvereinbarung* (works agreement) that is, in principle, binding for the employer and for all the employees of the respective enterprise. These works agreement are an "other legal provision" in the meaning of Section 4 (1) BDSG and they may therefore justify the processing of data (see above).

In a 1986 case,[57] the BAG had to decide whether the parties to a works agreement were allowed to agree upon terms and conditions of the processing of data that were disadvantageous to the employees in comparison to the rules of the BDSG.

In this case, a works agreement regulated the use of telephones of the employer for private purposes by the employees. The employees were allowed to use the telephones for private purposes, but they had to pay for it. The agreement entitled the employer to process the telephone numbers dialled as well as the time and the length of the connections, so that he was able to calculate the fees owed by the employees and to combat fraud.

The works council later argued – for reasons that are of no importance here – that the agreement was illegal as it *firstly* violated fundamental rights of the employees and as it *secondly* contradicted the rules of the BDSG.

The Court held:

The BAG rejected the first argument. Considering the second argument, it held that the potential content of a works agreement was not limited by the BDSG. If the agreement was an "other legal provision" in the meaning of Section 4 (1) BDSG, it was – according to the judges – not limited to substantiating the rules of that act. Instead, the parties were free to agree upon terms and conditions for the processing of data that were disadvantageous to the employees compared to the rules of the BDSG. Limitations to the freedom of the parties to agree upon such terms and conditions were to be derived from the constitution and sub-constitutional mandatory law (not including the BDSG) only. Although the court upheld this position in a 1995 decision, it is highly contested in the contemporary debate.[58] However, in 2013, the BAG upheld the earlier decision again and repeatedly stressed that a works agreement was an "other legal provision" in the meaning of Section 4 (1) BDSG and to be valid, it had to be proportionate to be compatible with fundamental rights only.[59]

[57] BAG, 27 May 1986, case 1 ABR 48/84; upheld by BAG, 30 August 1995, case 1 ABR 4/95.
[58] For details, see Gregor Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), paras. 99 – 116.
[59] BAG, 9 July 2013, case 1 ABR 2/13 (A).

X. Enforcing data protection law: Important supervision and advisory bodies

1. The Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI)

The BfDI's key task is to control other public authorities, see Section 24 BDSG. The public authorities may also seek the BfDI's advice in data protection matters, see Section 26(3) BDSG. The BfDI also supervises and controls the execution of the Law on Prerequisites and Procedures for Security Clearance Checks Undertaken by the Federal Government (Security Clearance Check Act, Sicherheitsüberprüfungsgesetz, SÜG). This law governs the prerequisites and the procedures for carrying out a security check on a person who is to be assigned to a security-sensitive type of employment (e.g., the Secret Service).

The BfDI does not enforce the rules on data protection vis-à-vis private companies, because this is done by local enforcement authorities of the different German States (the Länder).

The BfDI represents Germany within the Article 29 Working Party.

2. The Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI)

The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and seeks out appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry. Even in technically secure information and telecommunications systems, risks and damage can still occur as a result of inadequate administration or improper use. To minimise or avoid these risks, the BSI's services are intended for a variety of target groups: it advises manufacturers, distributors and users of information technology. It also analyses development and trends in information technology.

The BSI also warns the public if it is aware of internet-related criminal activities that could affect larger groups of consumers. For example, the BSI provides help to victims of identity theft and identity fraud.

3. The Data Protection Working Party established by Article 29 of the EC-Data Protection Directive

The Working Party is a key player in European Data Protection Law. In addition to advising the European Commission, one essential task of the Working Party is to advance harmonisation of data protection within the European Union. As a general rule, the group meets five times per year for two-day sessions in Brussels, and subgroups support its work. Until the end of 2005, it has adopted more than 100 opinions. In the past years, subgroups were actively dealing with subjects like Internet, passenger data and binding corporate rules.

4. The European Data Protection Supervisor (EDPS)

The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by supervising and monitoring the EU administration's processing of personal data, advising on policies and legislation that affect privacy, and cooperating with similar authorities to ensure consistent data protection. The supervision of other EU bodies takes various forms. The bulk of it is based on notifications of processing operations presenting specific risks. These need to be prior checked by the EDPS. Based on the facts submitted to him, the EDPS will examine the processing of personal data in relation to the Data Protection Regulation (Regulation (EC) No 45/2001). In most cases, this exercise leads to a set of recommendations that the institution or body need to implement so as to ensure compliance with data protection rules.

Protection of Employee's Personal Information and Privacy in France

Benjamin Dabosville
Université de Strasbourg

Introduction

Protection of employees' personal information and privacy is one of the central issues of employment relationships in the twenty-first century. Since several decades, technologies have given the employer the opportunity to make more enquiries about the workers' personal life and to record many data. On the other hand, protecting individual liberties from management authority has been a greater concern since the 1980s. This dilemma to manage the employer's and employee's interests is altogether enhanced by the difficulty in drawing the boundaries between "personal" and "professional" life. It is now common that an employee uses his house as workplace or asks his colleagues as "friend" on Facebook.

French law has been paying attention to this topic for a long time. The framework of the legislation results from two important Acts voted on January 6, 1978 and on December 31, 1992. Since then, the law has been adapted to the evolution of technology and management by the interpretation of an independent authority, the "*Commission Nationale de l'Informatique et des Libertés" (CNIL)*, and by the case law of both the "*Cour de cassation*" and the "*Conseil d'Etat*", which are the highest civil and administrative courts. The protection has also been reinforced due to the impact of the European Union, especially the directive 95/46 of October 24, 1995.

Nevertheless, having regards to the paramount importance to this theme, the consideration on employee's personal information and privacy protection seems to be insufficient in France, especially by comparison with Germany and other Europeans countries. Of course some scandals, such as Ikea's illegal spying[1], have drawn the attention of the press. Newspapers and TV shows also provide explanations about the appropriate way to use professional e-mail addresses or personal Facebook's profiles. Meanwhile, there are no substantial discussions in the global media or in the academic literature about a better way to protect legally the individuals against the danger of new information technologies. The government seems to focus on the applications developed by Google, Facebook or Apple concerning consumers' personal data. Moreover, French employees and trade unions seem to be more preoccupied by the social dimension of the employment relationship and the reform of labor market than by the protection of worker's information and privacy. So far, no government bill and no trade-union's proposal have been planned on the topic of employee's information and privacy.

Despite this lack of controversies, the examination of the French law highlights many

[1] *Le Monde*, July 27, 2013.

interesting issues of this topic. First, the analysis of the regulatory schemes shows the existence of a dual protection system that may be substantially changed in the coming years (I). Secondly, it seems that various methods are used to strike a balance between the interests of the employer and the interests of the employees (II). Lastly, the provisions regarding the employment relationship point out several difficulties, related to the role of the duty of transparency, the implementation of the proportionality principle and the gradation of the protection of employees personal information and privacy (III).

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

The primary basis for the protection of the employees' personal information and privacy is not the French constitution, but international treaties (A).

Concerning the detailed arrangements for this protection, it should be noted that, even if national legislation and case-law originally played a major role, the impact of European rules has been steadily increasing (B).

A. Primary basis of the protection

The French constitution does not mention anything important about the employees' personal information and privacy, neither about the right of privacy nor about the protection of personal's data information. This lack has been filled by the constitutional judge, the "*Conseil constitutionnel*", that recognized the right of privacy in 1996[2] and started to develop the protection of personal information in 2004[3]. In recent years, the opportunity to change the Constitution in order to explicitly guarantee the right of privacy and the protection of personal data has been discussed. However, the Committee on the Preamble of the Constitution considered in 2008 that this modification should not be a priority[4]. The guarantees arising from the case-law of the constitutional court and from the international instruments are considered as sufficient.

Indeed, several international instruments protect privacy and personal information. The most important are those elaborated within the context of the Council of Europe and within the context of the European Union[5].

In the Council of Europe, mention must be made of article 8 of the European Convention on Human Rights, which protects the right of privacy. Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data dated January 28, 1981 should not be forgotten as well. Not only because this text played a major role over the last century in the elaboration of the guidelines of the personal information protection, but also because many states are now member of this Convention. All the Member States of the European Union and the European Union itself have signed the Convention. Countries like Ukraine, Russia or even Uruguay have also signed the Convention recently[6].

---

[2] Conseil Constitutionnel, July 23, 1999, decision n°1999-416. The Right of privacy is provided for in Article 9 of the "*Code civil*" (Civil Code) since 1970 (Act n° 70-643 of July 17, 1970).

[3] Conseil Constitutionnel, July 29, 2004, decision n°2004-499.

[4] *Rapport Veil sur le préambule de la Constitution*, La documentation française, 2008.

[5] Article 12 of the Universal Declaration of Human Rights of December 10, 1948 and Article 17.1 of the International Covenant on Civil and Political Rights of November 16, 1966 should be mentioned too.

[6] Adhesion of Morocco is in progress.

The EU also has a great influence on this topic. The directives about non-discrimination and equal treatment[7] of course have some impact on this theme, protecting some characteristic of the individuals, like age, gender, sexuality preference. Nevertheless, the most important instrument is no doubt the directive 95/46/CE of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[8]. Protection of privacy and personal information has also been later reinforced by the Charter of Fundamental Rights of the European Union signed in 2000. Article 7 of this text states that "everyone has the right to respect for his or her private and family life, home and communications" while Article 8 §1 provides that "everyone has the right to the protection of personal data concerning him or her".

B. Protection rules

Regarding the rules governing the protection of employee's personal information and privacy, two periods may be distinguished. From 1978 to 1992 was the time for legislative action. Two important Acts have been adopted, one in 1978, the other one in 1992. Since 1992, major change came rather from the action of the EU, meanwhile national judges and administrative authorities adapted the legal provisions to the problems caused by new technologies or new management's methods.

The French law is now characterized by a dual system (1) that has already been modified by the European legislation and that could be changed by the proposal from the European Commission in progress (2).

1) A dual system

Two mechanisms have been set up by legislation in order to protect the employee's personal information and privacy.

The Act n°78-17 of January 6, 1978 on "Information Technology, Data files and civil Liberties"[9] had the ambition to solve most of the problems resulting from the use of computer. A wide debate and intensive work of a commission took place before the vote in Parliament[10]. Although this piece of legislation is considered as one of the most symbolic Acts of the French legislation, it may be noted that it is mainly a defensive law, which primary aimed at preventing the emergence of a Big Brother State. Neither the more frequent use of new information technology in the labor relationships nor the development of the "information society", in which individuals use Internet to collect and send information, had been imagined and anticipated. Nevertheless, Directive 95/46/CE of October 24, 1995 led to modifications to this Act by providing a more suitable legal framework to these societal developments. In addition, it seems that, even if this Act has been elaborated to be used in the public sector, its provisions are pretty adapted to the private sector and the employment relationship.

The Act n°92-1446 of December 31, 1992 had a different ambition. Only five articles

[7] Especially the Council Directive 2000/78/EC of November 27, 2000 establishing a general framework for equal treatment in employment and occupation.

[8] Directive 95/46 and Convention 108 have the same guidelines.

[9] "*Loi du 6 janvier 1978 relative à informatique, aux fichiers et aux libertés*". The current and full version of this Act can be consulted by connecting to www.cnil.fr. Quotes in this contribution are from the unofficial translation provided by the *CNIL*.

[10] *Rapport de la Commission informatique et liberté*, dir. B. TRICOT and P. CATALA, La documentation française,1975.

of this patchwork piece of legislation deals with employee's rights and liberties[11]. Meanwhile, these articles had a major purpose. Their enactment has been preceded by an important work of a Commission[12] that aims to protect employees' privacy and personal information from employer's power[13]. Those 5 articles have been codified in the "*Code du travail*" (Labor Code) and, symbolically, they were placed among the firsts in the new Code voted in 2008.

Act n°78-17 of January 6, 1978 and Act n°92-1446 of December 31, 1992 have different scopes. The first Act applies when anyone processes personal information, be it the employer or anybody else[14]. The second Act applies when an action of the employer creates a danger for the employee's rights and liberties. In addition, even though both Acts deal with the protection of the employees' personal information and privacy, they each develop different protection mechanisms. We should therefore examine the Information Technology, Data files and civil Liberties Act (i) and the special provisions of the Labor Code separately (ii).

i) Protection by the Information Technology, Data files and civil Liberties Act

When the employer uses a technology in order to collect or save personal information, he must comply with several conditions, enumerated in the 1978 Act[15], and he must also perform some formalities, like notifying the processing of personal data to an independent administrative authority or obtaining its agreement[16]. If these requirements are infringed, criminal penalties are provided for[17]. In practice, these sanctions are rarely applied[18]. The most useful remedies are the order to comply with the provisions of the Act and the prohibition to use the data illegally collected as evidence in a disciplinary action or

[11] Articles 25 to 29. Other articles of this law deals with various subjects about the employment relationship.

[12] *Les libertés publiques et l'emploi, rapport pour le ministre du Travail, de l'Emploi et de la Formation professionnelle*, dir. G. LYON-CAEN, La documentation française, 1992.

[13] The Commission's researches were inspired by Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981 and by Act n°78-17 of January 6, 1978 on Information technology, Data files and civil liberties.

[14] Article 2 of the Act states that it shall apply to any processing of personal data. Processing of personal data "means any operation or set of operations in relation to such data, whatever the mechanism used, especially the obtaining, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion or destruction".

[15] Article 6 states that "Processing may be performed only on personal data that meet the following conditions : 1° the data shall be obtained and processed fairly and lawfully; 2° the data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes (…); 3° they shall be adequate, relevant and not excessive in relation to the purposes for which they are obtained and their further processing; 4° they shall be accurate, complete and, where necessary, kept up-to-date (…) 5° they shall be stored in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed". Article 7 provides that "Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: 1° compliance with any legal obligation to which the data controller is subject; 2° the protection of the data subject's life; 3° the performance of a public service mission entrusted to the data controller or the data recipient; 4° the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract; 5° the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject".

[16] About these formalities, see Articles 22 to 31 of the 1978 Act.

[17] Article 50 of the 1978 Act, which refers to Articles 226-16 and seq. of the "*Code pénal*" (Criminal Code).

[18] C. BLOUD-REY, "Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles?", *Recueil Dalloz* 2013, pp. 2795-2801, pt. 20.

a lawsuit.

The French data protection authority, called the *CNIL,* which is an independent administrative authority, plays a major role in the enforcement of the Act. The *CNIL* has two missions[19]. Its members and officers control if the "data controller", namely the employer who processes of personal data, complies with the law. Therefore, a worker who faces difficulties about his personal data may submit his case to the *CNIL*. Nevertheless, the action of the *CNIL* is not significant on this point. The *CNIL* has got only limited prerogatives: in case of minor violation, the commission may send formal notifications and impose financial sanctions, but in case of major violation, it falls under the jurisdiction of the public prosecutor and the criminal courts[20]. Moreover, the *CNIL* doesn't have sufficient resources. In 2012, the commission was composed by 171 members who had to deal with more than 6000 complaints. As a small organization, the *CNIL* cannot face all the problems generated by the enforcement of the 1978 Act. Above all, the *CNIL* doesn't consider the repression of prohibited behavior as its major mission. Therefore, the most appreciable impacts of *CNIL*'s activity might be actually linked to his second mission, that is the advice given to the companies, the employees and the citizens. With its "Deliberations"[21], the *CNIL* contributes to regulate the use of new technologies. Even if these "Deliberations" are not compulsory, this "soft law" has a substantial influence on the legal practices, especially because members of the *CNIL* may give an opinion right away without having to wait for litigation. In a word, the *CNIL* is nowadays more an organization that elaborates a doctrine on the topic of personal information and privacy protection that an authority that controls the behavior of the employer.

Within the firm, the action of the *CNIL* is relayed by the personal data protection officer, called the "*Correspondant Informatique et Liberté*" (*CIL*). That is worth noticing that the 1978 Act does not give a significant role to the traditional checks and balances: trade unions and elected staff representatives are ignored. This choice to create a new institution within the firm can be questioned[22]. The *CIL* has to control the employer's behavior[23] but in order to accomplish this task, he needs to display many qualities: computer skills, good knowledge of the law and of the firm's organization as well as a patent independence from his head-manager. This collection of qualities is hard to find. In addition, the legislative has not provided the *CIL* with a status similar to the status of employee representative bodies. The *CIL* is most of the time an employee of the firm and is not granted legal protection against the employer. In practice, the *CIL* is able to propagate the doctrine of the *CNIL* rather than control the action of the employer. Consequently, compliance of the practice with the Information technology, data files and civil liberties Act can't be guaranteed.

ii) Protection by the Labor Code

The protection created by the 1992 Act is only relevant when workers' liberties are in danger. For instance, the rules apply when an employer plans to introduce a close circuit

[19] Article 11 of the 1978 Act.

[20] It shall be note that this situation is evolving since a few years: the *CNIL*'s sanctioning power is constantly reinforced.

[21] A "deliberation" is an interpretation of the law and a recommendation about its implementation.

[22] R. De QUENAUDON, « La cote mal taillée du salarié correspondant à la protection des données à caractère personnel », *Revue droit du travail* 2006, p. 32.

[23] Article 24 of the 1978 Act.

television (CCTV) in the firm[24] or when an employer takes an individual decision based on the employee's privacy.

In this situation, the employer must demonstrate that the interference with employee's rights and liberties is justified by a legitimate aim and is proportionate to that aim[25]. In many cases, he must also comply with a disclosure duty[26].

The most important civil remedies are the nullity of the employer's decision, the award of damage and the impossibility for the employer to use information illegally collected as evidence. Criminal penalties may also be imposed to the employer[27], but these sanctions are in practice rarely adopted.

The enforcement means of the Act n°92-1446 of December 31, 1992 are more traditional than those of the Act n°78-17 of January 6, 1978. If the Act is infringed, the workers could refer to the civil judge - in case of an individual decision or if an employee has suffered from a personal damage - or to the administrative judge - in case of a decision concerning all the employees -. On the top of the judicial system, the rulings of the two highest civil and administrative courts, the *Cour de cassation* and the *Conseil d'Etat*, contribute to define the meaning of this legislation regarding the development of new technologies or the use of new management methods.

Within the firm's premises, a representative elected by other employees, called the "*Délégué du personnel*" (DP), plays the most important role[28]. The *DP* is not able to veto the employer's decision. However, he could question the employer about his aim and methods. If the *DP* is not convinced by the employer's arguments, he can refer to a judge by a summary procedure[29].

Voting the Act n°78-17 of January 6, 1978 and the Act n°92-1446 of December 31, 1992, the French legislative has created a dual protection system. The criteria developed for the application of the two acts are quite different. That's why, in many cases, the two texts shall be applied together. In such situations, both the *CNIL* and the judge have to ensure that the employer's action complies with the provisions of the law.

This dual organization may change if the proposal of the European Commission to modernize the directive 95/46 is adopted.

2) A "Europeanized" protection

The impact of the European instruments on the legal protection of employee's personal information and privacy has been increasing for many years. The incidence of the European Convention on Human Rights and of the Convention 108 is rather indirect. Those texts are often mentioned by the judges, the *CNIL* and the legal literature to justify their reasoning and solutions. The impact of the directive 95/46/EC of October 24, 1995 is easier to find out. This Directive has been implemented in France in 2004 in the Information Technology, Data Files and Civil Liberties Act[30]. By this implementation, the

[24] In this case, the 1978 Act also applies.
[25] Article L. 1121-1 Labor Code.
[26] Article L. 1222-4 Labor Code provides that « employee's personal information must not be collected by a device that has not been previously brought to his attention ».
[27] Article 226-1 to 226-7 Criminal Code. Theses sanctions apply if the employer has illegally collect or use personal information about the employee.
[28] The "*comite d'entreprise*", a group of representative elected by the workers shall also be consulted in many cases.
[29] Article 29 of the 1992 Act, now codified in article L. 2313-2 Labor Code.
[30] The modifications have been introduced by the Act n°2004-801 of August 6, 2004 relative to the

repressive powers of the *CNIL* have been reinforced and the *CIL* has been created. The Information Technology, Data Files and Civil Liberties Act has to be interpreted according to the directive now.

New changes may be done in the coming years due to European instruments. Modernization of the Convention 108 is in progress since 2010 and modernization of the directive 95/46 since 2012[31].

The combination of these two projects will be interesting to follow. On the one hand, many countries are affected by the Convention 108. Therefore, a modernization of this Convention may have a larger impact. On other hand, the rules created by the directive 95/46 are more efficient, because the implementation of its provisions is made under the control of the Commission and the European Court of Justice. It may also be easier to have cooperation between the supervisory authorities within the EU.

Having regards to the French system, the proposal of the Commission seems to modify the missions of the supervisory authorities, which would have in the future more powers in the repression of law infringements. Such evolution would impose a significant change in the organization and the action of the *CNIL*. Until now, the *CNIL* has always preferred handling pedagogically than punishing breaches of law[32].

II. The balances of interests

Various methods are used to strike a balance between the interests of the employer and those of the employees. If, like in other countries, the proportionality principle plays a seminal role, other approaches are sometimes developed. Once explained the balance achieved when the employer seeks to obtain employee's personal information (A), the solution adopted when the employer wants to make a decision related to the personal life of the employee will be set out (B).

A. The collect of the employees' personal information

When the employer seeks to collect personal information, the guiding principle of the French law is quite simple: the action of the employer must have a legitimate aim and the interference with employee's liberty must be proportionate to this purpose.

Article L. 1121-1 of the Labor Code provides that "no one may restrict personal rights nor individual or collective liberties if this restriction is not *justified* by the nature of the work to be performed and *proportionate* to the aim pursued" and article L. 1222-2, al 2 of the Labor Code states that the information requested from an employee "must have a *direct* and *necessary* link with the evaluation of his professional skills". In addition, Article 6 of the Information Technology, Data Files and Civil Liberties Act provides that the personal data "shall be obtained for specified, explicit and *legitimate* purposes…" and "shall be adequate, *relevant and not excessive* in relation to the purposes for which they are obtained and their further processing…". Even if the texts are drafted in different ways, they have a common thread: the decision of the employer shall be legitimate and

protection of individuals with regard to the processing of personal data and modifying Act n°78-17 of January 6, 1978.

[31] On this theme, see N. MARTIAL-BRAZ, J. ROCHFELD, E. GATTONE, "Quel avenir pour la protection des données à caractère personnel en Europe ? », *Recueil Dalloz* 2014, pp. 2788-2794 ; C. BLOUD-REY, "Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ?", *Recueil Dalloz* 2014, pp. 2795-2801.

[32] C. BLOUD-REY, pt. 12.

proportionate[33].

The legitimacy of the purposes is usually not difficult to prove. The employer can easily demonstrate that his action may protect the firm against thefts or may improve the company's performance[34]. The key concept in order to strike a balance between the interests is therefore the proportionality principle. The proportionality of the interference with employee's liberty is assessed on a case by case basis. This approach gives a central role to the case law. That's why we could regret that there are only a few judgments on this topic.

B. Decision related to the personal life of the employee

When the employer seeks to make a decision related to the personal life of the employee, the French legislation tries to strike a balance by defining a principle and some exceptions[35]. The proportionality test is less important here.

The principle is that the employer has to do "as if" he ignores everything about the worker's "personal life"[36]. This guideline is reinforced by the rules regarding the prohibition of discrimination. The law establishes a list of themes that must not be taken in consideration by the employer[37]. These criteria are, on one hand, the state of the person (health, color, sexual preference etc…) and, on the other hand, his/her activities (politics, trade-union or religious preferences). It shall be noted that, even if those rules are made in order to protect the employees' personal life, there is no contradiction with the protection of the firm' interests: such criteria are not involved in profit maximization.

Nevertheless, two exceptions may be invoked by the employer. The first is linked with the proportionality principle, but not the second.

The first exception is related to the employee's task within the firm. The employer is entitled to consider some aspects of the identity or personal life of the employee when

[33] This common thread is due to the impact of European instrument. Article 5 Convention 108 stated that "Personal data undergoing automatic processing shall be (…) b) stored for *specified and legitimate purposes* and not used in a way incompatible with those purposes; c) *adequate, relevant and not excessive* in relation to the purposes for which they are stored…". Article 6 § 1 Directive 95/46/EC of October 24, 1995 provided that "Member States shall provide that personal data must be (…) (b) collected for *specified, explicit and legitimate purposes* and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards ; (c) *adequate, relevant and not excessive* in relation to the purposes for which they are collected and/or further processed…".

[34] Advice of the *CNIL* may help employers and employees to know if an aim is legitimate or not. For example, Article 2 Deliberation 2006-067 of March 16, 2006 enumerates purposes relevant to monitor employees with GPS.

[35] See M. DESPAX, « La vie extraprofessionnelle du salarié et son incidence sur le contrat de travail », *JCP* 1963, I, 1776 ; P. ADAM, « Sur la vie personnelle : cinquante ans après Despax », *Revue de droit du travail* 2012, pp 100-104.

[36] The highest civil Court distinguishes the "protection of privacy", which is a civil law concept, and the "protection of the personal life", which is a labor law concept. By using the term "personal", the judges refer to everything that is not "professional". Thus, an employer is not allowed to take any disciplinary measure against the worker based on the worker's behavior outside the firm, even if many people have observed the worker. This behavior might not belong to the "privacy" in the strict sense of the civil law but remains "personal" – and not "professional" – in the sense of the labor law. (On this distinction between « privacy » and « personal life », see Ph. WAQUET, "La vie personnelle du salarié", *Droit social* 2004, pp. 23-30 ; A. LEPAGE, « La vie privée du salarié, une notion civiliste en droit du travail », *Droit social* 2006, pp. 364-377).

[37] Article L. 1132-1 Labor Code.

there is a close link between the employee's work and these elements. This exception has a broad scope, but is expressed differently in the law depending if the decision of the employer is favorable or unfavorable to the employee.

For new job opportunity (as recruitment or promotion), the employer can consider the employee's features if they constitute "a genuine and determining occupational requirement, provided that the objective is legitimate and the requirement is proportionate"[38].

For a disciplinary action against a worker, the employer shall demonstrate that the behavior of the employee is "an infringement of an obligation related to his mission in the firm"[39]. Only very few situations satisfy this criteria. The most frequent case where an employer seeks to blame an employee because of the violation of a professional obligation is the revocation of his driving license while the worker needs this license to accomplish his job. Meanwhile, both the *Cour de cassation* and the *Conseil d'Etat* decide that the dismissal of an employee because of the revocation of his driving license does not have to be disciplinary[40].

The second and most important exception is linked to the global functioning of the company. When an important disorder within the firm results from the behavior of an employee - situation called in the case law as an "objective and characterized disorder" - the employer is allowed to take a non-disciplinary decision against the worker[41]. A decision of the *Cour de cassation* of May 18, 2007 illustrates this situation. In this case, an employee received a newspaper of a swinger's community at his professional postal address[42]. The employer wanted to sanction the employee, but the judges estimated that he could take only a decision based on the "disorder" created within the firm[43].

The balance between the interests of the employer and the interests of the employee is here found in the exceptional nature of this second exception. The personal life of an employee rarely causes significant damage to the company.

Finally, it should be noted that the employee's consent has not been important until now in the French law. This role may increase in the future, despite its questionable value, because of the subordination of the employee to the employer. If such evolution is adopted in French labor law, it will be necessary to clarify the relationship between the request of the employee's consent and the control of the legitimacy and proportionality of the employer's decision: are they alternative requirements or additional conditions? The last solution seems to be the most appropriate. Personal information and privacy are not only protected in the interest of the individuals. This protection also ensures that the rule of law and principles such as freedom of opinion and expression are respected. Therefore, the

[38] Article 4 of the Council Directive 2000/78/EC of November 27, 2000 establishing a general framework for equal treatment in employment and occupation.

[39] Cour de cassation, May 3, 2011, case n° 09-67464 ; Conseil d'Etat, December 15, 2010, n°316856.

[40] Cour de cassation, May 3, 2011, n°09-67464. In this case, in accordance with the second exception, the employer is only entitled to take a decision based on the disorder created by the employee's behavior within the firm.

[41] Cour de cassation, January 22, 1992, case n°90-42517 ; Cour de cassation, March 9, 2011, case n°09-42150.

[42] Cour de cassation, May 18, 2007, case n°05-40803.

[43] In another decision of March 9, 2011, the court reaffirmed the principle that only a dysfunction within the firm could justify the employer's decision (Cour de cassation, March 9, 2011, case n°09-42150). It shall be noted that in such cases, the employer never tries to collect information or to be informed about the worker's life.

consent of the individual should remain insufficient to justify the employer's action. The control by a judge of the legitimacy and proportionality of the employer's decision also seems to be required.

III. Personal information and privacy protection in the employment relationship

Employee's personal information and privacy is protected in the hiring process (A), during the employment relation (B) and after the termination of the employment contract (C).

A. Personal information protection in the hiring process

About the hiring process, the first point that must be paid attention to is the prohibition of employer's decisions based on non-professional criteria (1). Then, a gradation in the protection of the employee's personal information and privacy is brought into focus (2).

1) Control of the employer's decision

The legislative aims at avoiding employer's decisions based on non-professional criteria. Many provisions are inspired by this purpose.

Article L. 1221-6 of the Labor Code, created by 1992 Act, provides that "information requested (…) to the job applicants could not have any other aim than assessing their ability to hold the job offered or their occupational functioning. The information must have a direct and necessary link with the job offered". Article L. 1132-1 of the Labor Code also prohibits any decision excluding applicants based on a list of characteristics, like their origin, sex, morality, sexual orientation, age, marital status or pregnancy, genetic characteristics, political opinions, etc… However, this article is not applicable when the employer could demonstrate that this feature constitutes "a genuine and determining occupational requirement" for the job[44]. Article 8 of the Information Technology, Data Files and Civil Liberties Act should also be taken into consideration. This article prohibits processing of sensitive categories of data, as racial origins and political opinions. Lastly, article R. 4624-11 of the Labor Code provides that the medical fitness to do the proposed job must be examined only by an occupational health doctor.

2) Gradation of the protection

In accordance with the provisions stated above, it seems that three categories of personal information could be identified. They do not show just one but different levels of protection.

For a first group of information, prohibition of collecting inquiries about the workers is not absolute. The employer is allowed to collect information if he could demonstrate that it is proper and reasonable to consider this to choose the best applicant. For the employer and the employees, the core question is to assess whether the information is relevant or irrelevant for a job in accordance with article L. 1221-6 of the Labor Code. The advice of the *CNIL* may help the actors but not solve all the problems[45]. Will an applicant looking for

[44] Article 4 Directive 2000/78/EC of November 27, 2000.

[45] In his "Guide pour les employeurs et les salariés" (Guide for employers and employees), that can be found on the internet address of the *CNIL* (www.cnil.fr), a list of prohibited questions is drawn up (page 9 of the

a job since months or years refuse to answer a question if the employer thinks that the question is relevant to appreciate his professional skills? Article L. 1132-1 of the Labor Code, and Article 8 of the Information Technology, Data Files and Civil Liberties Act avoid this ambiguity for some aspects of the life and identity of the employee. These provisions enumerate characteristics that must not be taken in consideration by the employer, except for some specific organizations. For instance, a question about the religion of the employee is only relevant in religious organization. A question about the political opinions is only relevant when the applicant seeks to obtain a job in a political party. This clarification reinforces the position of the employee.

Beside this category of information, we find situations where data are relevant for the job although employer's knowledge of this information must be avoided. This dilemma explains the specific mechanism regarding applicant's health. Even when it is necessary to appreciate if an individual is medically fit for a job, an employer is not entitled to ask a candidate about his health. The mission is the hands of a third party, the occupational health doctor.

In the third and last category, prohibition of processing personal information is absolute because in all cases, no link can be found between the job and the candidate's characteristics. For instance, the employer is never allowed to reject a candidate because of his skin colour[46], nor allowed asking anyone for his password of social networking.

This gradation in the protection of employees' personal information and privacy has two explanations. First, it seems that the link between some information and the individual is sometimes so close that some special protection is required. In other words, such information doesn't just belong to the "privacy" of the individual, but also to his "intimacy", which is the core of privacy. For example, the link between the individual and his body is so particular and so strong that it requires a specific protection. Second, global issues justify more intensive attention from the legislative power too. For example, collecting political opinions or trade-union activities is mentioned by article L. 1132-1 of the Labor Code and by Article 8 of the Information Technology, Data Files and Civil Liberties Act because such information doesn't only deal with the privacy of the employees. Freedom of opinion and freedom of association may also be at stake.

In conclusion, it may be added that both applicants and elected staff representatives have to be informed by the employer about the technologies or methods he will used to appreciate the professional skills of the candidate[47]. With this transparency's duty, the legislative hopes that a control of the hiring process will be made within the firm. Unfortunately, despite these provisions, the application of the rules is not fully satisfying. Recruitment is considered basically as a choice of a personality and employers often take into account criteria prohibited by the law. Nevertheless, this legislation seems to preserve the candidate's dignity by avoiding major abuses during the hiring process.

B. Personal information and privacy protection during the employment relations

In order to give an exhaustive panorama of the rules regarding the employment

Guide). We doubt that most employers do comply with this list. Do the employers agree with the opinion of the *CNIL* that the "association's activity" of the applicant is not relevant to appreciate his professional skills?

[46] The principle confirmed by the labour law in 2012 (article L. 1221-7 Labor Code), is to preserve as long as possible the candidate's anonymity in the hiring process.

[47] Article L. 1211-8 Labor Code and article L. 2323-32 Labor Code.

relationships, two kinds of actions could be distinguished: those that aim at or result in collecting personal information about the worker (1) and those concerning an employer using his knowledge about the personal life of the employee (2).

1) The collect of personal information

There are different ways for an employer to collect information about a worker. The simplest is to ask directly the employee. The provisions are here the same than the ones that apply during the hiring process. Pursuant to the Labor Code, "information requested to an employee (…) must not have any other aim than assessing his professional skills"[48].

The other actions have not been specified by the legislative. Following the distinctions used in criminal law[49], it seems relevant to separate to types of actions: the inspection of premises or objects within the firm (1) and the surveillance of worker's activity (2).

i) Inspection

By using the term "inspection", we refer to the action where an employer searches to identify the content of an object or the content of a closed place: for instance, the inspection of the desk of an employee, the inspection of his computer or the inspection of his e-mails.

Historically, the first decision of the highest civil court about inspection was the decision "*Nikon*" in 2001[50]. The right of privacy was mentioned in this ruling but the judges acknowledged that they were not sure about the opportunity of their solution. In 2005, the court adopted another position with the decision "*Klajers*". This new solution is less protective towards the employees' interests[51]. Nowadays it is necessary to identify the realm to which the objects or premises inspected belong in order to determine the rules that the employer must comply with. Three realms may be distinguished.

Some elements seem to be strongly protected. For the search of the personal bag of the employee, the employer shall of course demonstrate that the interference with employee's privacy has a legitimate aim and is proportionate to that aim but, except in case of emergency, he must also prove that the worker consented to this search[52]. The reason for this specific legal regime remains unclear: is this element stronger protected because it belongs to the employee's "intimacy" realm or because it's the employee's legal property? The legislation and the case-law did not rule on this point, probably because this kind of claim is uncommon.

On the opposite, the protection of an object that belongs to the "professional" realm[53] is very weak. Indeed, the employer can conduct the inspection of the object without complying with substantive or procedural rules.

---

[48] Article L. 1222-2 Labor Code.

[49] In the Criminal procedure law, one must distinguish, on one hand, operations of "*perquisition*" and "*fouille*" (article 94 and seq. of the "*Code de procédure pénale*" – Code of Criminal Procedure) and, on other hand, operations of "*interceptions de communication*" and "*captation d'images et de paroles*" (Article 100 and seq. Code of Criminal Procedure ; Article 706-96 and seq. Code of Criminal Procedure). "*Perquisition*" means search of an enclosure place and "*fouille*" means body search or search of an object. "*Interpection*" and "*captation*" refer to the operation where sounds or images are recorded.

[50] Cour de cassation, October 2, 2001, case n°99-42942.

[51] Cour de cassation, May 17, 2005, case n°03-40017.

[52] Conseil d'Etat, July 11, 1990, case n°86022. Cour de cassation, February 11, 2009, case n°07-42068. The judges watch carefully the consent of the employee. The employer must inform the employee about his right to refuse the inspection and about his right to require the attendance of a witness.

[53] Or the "not personal" realm as stated by the Cour de cassation.

Finally, about things falling under the employee's "personal" realm, the judges, inspired by criminal law, have decided that the employer has to warn the employee about his inspection[54]. Although the employee's agreement is not required, the worker has the possibility of discussing with the employer the opportunity of this inspection. This rule has one exception: in case of emergency[55], the employer is entitled to search for anything that belongs to the personal realm of the employee without telling him. For instance, this exception applies when the detection of a computer virus that could make important damage to the firm's intranet requires searching into the personal files of an employee immediately. It should be also noted that it remains undecided if the action of the employer must or not have a legitimate aim and be proportionate to that aim. According to article L. 1121-1 of the Labor Code, the employer should demonstrate that his action complies with these two requirements. Nevertheless, there is no decision of the *Cour de cassation* about this.

This outline of the rules regarding inspection pointed out that the legal characterization is decisive: opening a file on the professional employee's computer or reading a mail received by the employee at his professional address requires the employer to determine whether the box, file and mail belong to the "professional" or to the "personal" realm. The judge uses of a formal criterion: only if the employee has characterized the box, files or mail as "personal" are these elements related to the personal realm[56]. By comparison, neither the file called "my documents"[57], nor the file identified by the employee's initials[58] belong to the personal realm. A USB stick connected to the professional computer of the employee also belong to the professional realm[59]. In these cases, the employer is therefore allowed to conduct a thorough search without having to warn the employee.

Rulings concerning inspection are open to criticism. The criterion used by the *Cour de cassation* in order to distinguish « professional » and « personal » realms is controversial. Moreover, the fact that an employer may inspect personal objects or premises without the consent of the employee or without having to demonstrate that this inspection is justified by a legitimate aim and is proportionate to that aim is questionable. The employer should not have more leeway to collect personal information about the employees than the police do[60]. At least, comparison between labor law and criminal law suggest a proposal: privacy of the citizen against police's inquiries is protected by distinguishing in some situations preventive and repressive action[61]. Why not applying such criterion in the employment context[62]?

---

[54] Cour de cassation, May 17, 2005, case n°03-40017.

[55] "Particular risk or event" according the case law (Cour de cassation, May 17, 2005, case n°03-40017).

[56] In this situation, the employer can contest this personal use of professional instruments. If the use is abusive, the employer is entitled to punish the employee. Nevertheless, he is not entitled to disqualify the element from the "personal" to the "professional" realm.

[57] Cour de cassation, May 10, 2012, case n°11-13884.

[58] Cour de cassation, October 21, 2009, case n°07-43877.

[59] Cour de cassation, February 12, 2013, case n°11-28649.

[60] According to article 76 Code of Criminal Procedure, the consent of the concerned citizen in required for a police inspection, except if this inspection is done under the authorization and control of the judge or in the special case of "*enquête de flagrance*" (article 53 and seq. Code of Criminal Procedure).

[61] Conseil d'Etat, May 11, 1951, *Dame Baud*, *Recueil du Conseil d'Etat,* p. 265 and *Tribunal des conflits*, June 7, 1951, *Époux Noualek*, *Recueil du Conseil d'Etat* p. 636. This distinction is, for instance, used about body

ii) Surveillance

By using the term "surveillance", we refer to the action where an employer seeks to know employee's activity at a certain point of time or in a certain location. For instance, the employer surveys his employees by using a CCTV device or a global positioning system[63].

Historically, the first important rules about surveillance came from case law. Cases of employees who had been subject to disciplinary actions have been brought to the judges. These employees denied the lawfulness of the evidence adduced by the employer, claiming that the monitoring system was unfair. With the emblematic decision "*Neocel*" dated November 20, 1991[64], the *Cour de cassation* forced the employer to comply with a disclosure duty when using a surveillance device. A year later, by the 1992 Act, the legislative expanded on this ruling and established the conditions under which the employer may control the employees. In addition, *CNIL*'s deliberations often give instructions about the use of such devices. Most of the time, *CIL*, members of Trade Unions and staff representatives who have a doubt about the lawfulness of a surveillance system refer their case to the *CNIL* and not to the judge.

The current rules are the following: as for the inspection, three kinds of situations should be distinguished.

First of all, the employer is never entitled to monitor employees outside working hours and outside the working place. An employer spying on his employees at home will be guilty of a violation of privacy and will be punished in accordance with the criminal law[65] and civil law[66].

The situation is different when the employer monitors his employee in order to control the quality of work.

In such a case, he has to demonstrate that this monitoring complies with the substantive rules from article L. 1121-1 of the Labor Code. According to this text, the use of a technological system to control the employees' activity must have a legitimate aim and be proportionate to that aim. Although there is no problem with this first requirement[67], compliance with the second condition is harder. For instance, using GPS in order to monitor employee's activity is disproportionate if the employment contract recognizes to the employee a large autonomy in his work's accomplishment[68]. Unfortunately, there are so far few decisions regarding this condition.

In addition to these substantive rules, the employer has to comply with procedural guarantees. Using a surveillance system is only permitted after having informed the staff representative[69] and the employees[70]. One can expect that an employee who knows he is monitored will act in a way that protects his privacy. By the way, the scope of this

search. In case of preventive action, the policemen are only entitled to palpate the body of the individuals, but are not allowed to conduct an authentic body-search.

[62] Such a distinction was used in an administrative text, the Circulaire DRT n° 5-83 of March 15, 1983. Nevertheless, the judges didn't refer to this distinction in labor law.

[63] We exclude here the direct surveillance, without the help of technologies.

[64] Cour de cassation, November 20, 1991, case n°88-43120.

[65] Article 226-1 and seq. Criminal Code.

[66] Article 9 Civil Code.

[67] It is of course legitimate to control the quality of work.

[68] Cour de cassation, November 3, 2011, case n°10-18036.

[69] Article L. 2323-32 Labor Code.

[70] Cour de cassation, November 20, 1991, *Neocel*, case n°88-43120 and Cour de cassation, May 22, 1995, case n°93-44078. Article L. 1222-4 Labor Code.

obligation to inform is stronger that in other European countries: the employer is never entitled to use hidden cameras. By comparison with the criminal law, such a rule seems to be justified. A judicial authorization is required to entitle the police to use a hidden data-collecting technique[71]. It is appropriate that the employer doesn't have more prerogatives than the police: his mission is not to conduct criminal investigation within the firm.

The third and last situation concerns the employer using a surveillance system for other purposes than controlling employee's work.

In this case, the monitoring system has to pursue a legitimate aim and must be proportionate to that aim. According to the *CNIL*, if an employer uses CCTV in order to prevent thefts caused by the customers inside the firm, he cannot use this monitoring system on the floors where the customers are not allowed to go. If he does, the employer's behavior is considered as disproportionate[72].

The scope and incidence of the disclosure obligation are open to debate. First of all, the *Cour de cassation* denies the employer the right to use a monitoring system in order to control the activity of the employee when it was initially dedicated to another aim[73]. On the other hand, the employer does not have to comply with a disclosure duty if he uses a CCTV in premises where the employees are not allowed to go[74].

2) The use of personal information

For the employer, his knowledge about employee's personal life may have an incidence on three categories of actions.

First, the employer could have the intent to make a management decision such as dismissal, disciplinary sanction or promotion, based on the personal life of the employee. In this case, as explained above, the principle is that the employer is not entitled to do so. By exception, the behavior of the employee could be taken in consideration only if it has caused an "objective and characterized disorder" within the firm or if it is "an infringement of an obligation related to his mission in the firm" [75].

Secondly, the employer may wish to reveal information regarding the personal life of an employee to other workers or outside the firm. Such a revelation is prohibited for it breaks the protection of privacy according to article 9 Civil Code.

Lastly, the employer may want to record personal information about his employees in a file. In this case, information is transformed into "data" and the information technology, data files and civil liberties Act applies. Therefore, the processing of personal data is entitled only if the employer has a legitimate aim and if the storage is proportionate to that aim. In addition, the employee is allowed to access to his personal data and, if these data

[71] Articles 706-96 et seq Code of Criminal Procedure.
[72] CNIL, April 16, 2009, Deliberation n°2009-201.
[73] Cour de cassation, November 3, 2011, case n°10-18036 (a GPS system may not be used by the employer for other purposes than those declared to the CNIL and brought to the attention of the employees"). We should nevertheless note that in a previous decision, less important, the solution was quite different. In this decision, dated February 2, 2011 (case n°10-14263), a CCTV system had been implemented in a casino for the safety of people and property. A barman was dismissed, because of major faults committed on his job : video shows that he didn't collect revenue for many drinks. He contested the right for the employer to adduce the video record as evidence. The Cour de cassation rejected his demand, meanwhile the employer didn't demonstrate that he had informed the employees that he will use CCTV in order to control their activity.
[74] Cour de cassation, January 31, 2001, case n°98-44290.
[75] On this point, see "II. The balance of interests".

are inaccurate, a correction has to be done. The *CNIL* sometimes reminds these rights in the scope of the employment relationship[76].

C. Personal information and privacy protection after the employment relations

After the dismissal of the contract, the employee has to face two sorts of problems regarding his personal information and privacy.

The transfer of data between the former and the prospective employer is one of these problems. On this topic, the French Labor Code states that "information about a person applying for a job cannot be collected by a device that has not been brought to his attention"[77]. Therefore, the application of this rule is tricky. The breach of the law is hard to prove. In addition, a candidate has few incentives to sue the employer when he has been illegally excluded from the hiring process. Even if the irregularity of the process is recognized, the judges will not force the employer to recruit the candidate.

The course of the "individual file" of the employee proceeded by the former employer is another problem. In many firms, information about the employee's career (*curriculum vitae*, mutations, promotions, disciplinary sanctions etc…) is gathered in a file. This information is used by the employer during the employment relationship[78]. After the dismissal of the contract, the employer often keeps some documents in order to prove his assertions in case of judicial action initiated by the employee. The rules relating to these files are still fuzzy[79], especially about the duration of the storage. A clarification of the legal regime of this file would be convenient.

IV. Conclusion

As a conclusion, three points should be brought into focus about the protection of employee's personal information and privacy in France.

The framework of this protection, especially about the rules governing the action of the employer, seems to be quite sufficient. Basis assertions, as the prohibition of decisions based on employee's personal life or the double test of and proportionality required when an employer seeks to collect personal information, attract a broad consensus. The remaining problems are due to the vagueness of the law or result of the hardness to find the appropriate yardstick. For instance, there is no discussion about the opportunity to distinguish "professional" life and "personal life", but the choice of the pertinent criterion remains contested.

---

[76] For instance, the deliberation n°02-001 dated January 8, 2002 about « Automated processing of personal information concerning implementation in the workplace for the management of access to premises, schedules and catering » states the right for the employee to access to his personal data saved in this file.

[77] Article L. 1222-4 Labor Code.

[78] The employer doesn't use this information only for his own interest, but needs it sometimes to comply with the law. For instance, the employer has to know the employee's address to send him his pay slip. When an additional health insurance or complementary welfare and pension scheme exist in the firm, its management also requires information about the employee, like his marital status, the number of dependent children, the beneficiaries of the funds.

[79] By comparison, the rules in the public sector have been specified by the law. The article 18 of the Act n°83-6354 of July 13, 1983 about the rights and obligations of the employees in the public sector claims that all administrations have to possess an individual file for each employee. The contents of this file and its use are determined by the law. On this theme, see also Article 26 of the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union.

On the law enforcement topic, discussions are more intense.

Within the firm, the role and the status of the *CIL* should be reviewed. We doubt that the *CIL* is actually able to control employer's activity. Therefore, the articulation with traditional check and balances system within the firm should be reexamined, in the direction of a closer link with the staff representative. At least, some better legal protection of the *CIL* remains indispensable.

The role of both the *CNIL* and the judge should also be clarified. According to the last European Commission proposal, the role of the *CNIL* may evolve and be more repressive. Such evolution will make a major change in the organization of the *CNIL* necessary and question the allocation of competences between the *CNIL* and the judge.

In addition, one can suspect that the articulation between a protection by the individual and protection by a third party will be disputed in the coming years. That points out the role of the consent of the employee and its consequences. We reject the idea that the individual is the only one concerned by the protection of personal information and privacy. This question is again of paramount importance for freedom of opinion and expression of the individuals[80]. That's why the employer should in every case act for a legitimate aim and in a proportionate way. Only an independent authority should estimate if the employer complies with these requirements.

Finally, it seems that the French law will have an important choice to make in the next few years between a "passive" and an "active" protection of the personal information and privacy.

By "passive protection", we refer to a system under which the decisions taken by the employer cannot be linked with the personal life of employees. For instance, an employer should not transfer an employee because of his sexual orientation.

By "active protection", we refer to a legal system under which the employer has to consider the personal imperatives of the employees, for instance childcare issues, when taking a decision, as a transfer[81].

It raises a tricky dilemma. Of course one can state, as the French legislation does, that the employer has to take into consideration the personal characteristics of the employees only in some cases. However, once personal information falls into the employer's knowledge, it is difficult to prevent the employer from a later use of this information.

The trade-off between passive or active protection is therefore determining, since it has a decisive impact on the elaboration of the law about the gathering of personal information.

[80] On this point, see the utmost decision "Voklzählungsurteil" of the German Constitutional Court dated December 15, 1983.

[81] On this point, it should be noted that Act n°2013-504 of June 14, 2013 provides that, in case of concluding a specific collective bargaining, called "accord de mobilité interne", the employer shall comply with a preliminary dialogue phase. In this phase, the employee may bring to the attention of the employer their personal and familial duties and the employer shall take in consideration these duties (Article L. 2242-23 Labor Code).

Protection of Employees' Privacy and Personal Information in Spain: General Patterns and Case Law Trends

Diego Álvarez Alonso[*]
University of Oviedo

1. Protection of employees' privacy and personal information in the Spanish system: general framework overview

The protection of employees' privacy and personal data is nowadays an issue of raising concern, in particular in regard to the impact of the rapid development of information and communication technologies, multimedia tools and increasingly sophisticated audio-visual devices. Obviously, the growing influence of these technical instruments in the workplace context has significantly intensified the chances and possibilities for monitoring of employees. On the other hand, it involves a tendency to fainting borders between personal and professional realm. As a result, workers are more easily exposed not only to a deeper scrutiny by the employer, but also to innovative risks of intrusion in their private sphere and of personal data leakage[1]. The already existing

[*] The author acknowledges with gratitude the collaboration of Professor Joaquín García Murcia (University Complutense of Madrid), who provided especial contribution to the first section and useful comments and suggestions for the whole paper. On the other hand, this presentation has been prepared in the framework of national I+D research project DER 2010-21428 ('El ideal social del Tribunal Constitucional español a partir de su jurisprudencia laboral y de seguridad social').

[1] GAETA, L., 'La dignidad del trabajador y las 'perturbaciones' de la innovación', in APARICIO TOVAR, J./ BAYLOS GRAU, A. (Eds.), *Autoridad y democracia en la empresa*, Trotta, 1992, p. 68 et seq.; MERCADER UGUINA, J. R., 'Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?', *Relaciones Laborales,* num. 10, 2001, p. 11 et seq.; BIAGI, M./ TREU, T., 'Lavoro e *Information Technology*: rifflessioni sul caso italiano', *Diritto delle Relazioni Industriali,* num. 1, 2002, p. 5 et seq.; SEMPERE NAVARRO, A. V./ SAN MARTÍN MAZZUCCONI, C., *Nuevas tecnologías y Relaciones Laborales*, Aranzadi, 2002, p. 32 et seq.; MARTÍNEZ LÓPEZ, F. J./ LUNA HUERTAS, P./ INFANTE MORO, A./ MARTÍNEZ LÓPEZ, L., 'Los sistemas de control de la actividad laboral mediante las nuevas tecnologías de la información y las comunicaciones', *Relaciones Laborales,* num. 12, 2003, p. 95 et seq.; RAMOS LUJÁN, H. V., 'La intimidad de los trabajadores y las nuevas tecnologías', *Relaciones Laborales*, num. 17, 2003, p. 41 et seq.; ALARCÓN CARACUEL, M. R., 'La informatización y las nuevas formas de trabajo', in ALARCÓN CARACUEL, M.R/ ESTEBAN LEGARRETA, R. (Eds.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo,* Bomarzo, 2004, p. 11 et seq.; CAMAS RODA, F. 'La intimidad y la vida privada del trabajador ante las nuevas modalidades de control y vigilancia de la actividad laboral', in ALARCÓN CARACUEL, M.R/ ESTEBAN LEGARRETA, R. (Eds.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo,* Bomarzo, 2004, p. 161 et seq.; GONZÁLEZ ORTEGA, S., 'La informática en el seno de la empresa. Poderes del empresario y condiciones de trabajo', in ALARCÓN CARACUEL, M.R/ ESTEBAN LEGARRETA, R. (Eds.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo,* Bomarzo, 2004, p. 19 et seq.; GOÑI SEIN, J. L., 'Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos', in ALARCÓN CARACUEL, M.R/ ESTEBAN LEGARRETA, R. (Eds.),

awareness on this matter has been ultimately boosted by some latest judgements of the Spanish higher courts, which have been moderately covered by mass media and highly discussed in academic comments recently published[2].

However, in despite of this quite widespread consciousness on the new challenging threats for employees' privacy and personal data protection, Spanish Labour Law does not offer a complete and detailed statutory regulation on this subject. Nevertheless, it contains at least some general provisions of great importance in this field. First of all, it expressly recognises workers' right to safeguard of their privacy and dignity, including protection against harassment, especially in the cases of discriminatory, gender-related or sexual grounds. This is established as a basic right of the employee in the main legal piece of Spanish Labour Law, the Statute of Workers [SW for short, Royal Legislative Decree 1/1994, 24th March, art. 4.2.e)], in connection to the fundamental right to privacy established in the Spanish Constitution (art. 18)[3]. On the other hand, a similar right is also recognised to public employees of the civil service in their specific legislation [Act 7/2007, 12th April, Basic Statute of the Public Employee, art. 14.h)].

The Statute of Workers itself provides some further guidelines for protection of this basic right to privacy previously proclaimed. According to article 20 SW, the employer shall respect employees' dignity and privacy when using his managerial powers, and in

Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo, Bomarzo, 2004, p. 49 et seq.; GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 12 et seq.; CALVO GALLEGO, J. 'TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales', *Aranzadi Social,* num. 9, 2012, p. 125 et seq.

[2] Constitutional Court Judgements 241/2012, 29/2013 and 170/2013; Supreme Court Judgement 26th September 2007. Some of these decisions have been mentioned in general or financial newspapers (*El País*, 9-10-2013, http://sociedad.elpais.com/sociedad/2013/10/09/actualidad/1381308839_163115.html; *Cinco días,* 9-10-2013, http://cincodias.com/cincodias/2013/10/09/economia/1381313335_489651.html?rel=rosEP; *Expansión,* 24-10-2007, http://www.expansion.com/2007/10/24/juridico/1049656.html).

For academic comments about those judgements, CARDONA RUBERT, M. B., 'Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás', *Revista de Derecho Social,* num. 60, 2012, p. 169 et seq.; MARÍN ALONSO, I., 'La mensajería electrónica en la empresa: un paso atrás en la protección constitucional del derecho al secreto de las comunicaciones', *Relaciones Laborales,* num. 3, 2013, p. 89 et seq.; MUÑOZ RUIZ, A. B., 'Social Networking: New Challenges in the Modern Workplace', *Spanish Labour Law and Employment Relations Journal*, V. 2, 2013, p. 32 et seq.; SEPÚLVEDA GÓMEZ, M., 'Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites', *Temas Laborales,* num. 122, 2013, p. 197 et seq.; CARRASCO DURÁN, M., 'El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa', *Revista Aranzadi Doctrinal*, num. 9, 2014, p. 53 et seq.; MARTÍN VALVERDE, A., 'Uso extralaboral del correo electrónico empleando medios informáticos de la empresa. Control empresarial: requisitos', *Actualidad Laboral*, num. 2, 2014, p. 184 et seq.; MONEREO PÉREZ, J. L./ DEL MAR LÓPEZ INSÚA, B., 'El control empresarial del correo electrónico tras la STC 170/2013', *Aranzadi Social,* num. 11, 2014, p. 225 et seq.

[3] About employee's right to privacy in general, GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador*, Civitas, 1988, p. 21 et seq.; DE VICENTE PACHÉS, F., *El Derecho del Trabajador al respeto de su intimidad*, CES 1998, p. 81 et seq.; RODRÍGUEZ- PIÑERO Y BRAVO- FERRER, M., 'Intimidad del trabajador y contrato de trabajo', *Relaciones Laborales,* num. 8, 2004, p. 1 et seq.; ARIAS DOMÍNGUEZ, A./ RUBIO SÁNCHEZ, F., *El derecho de los trabajadores a la intimidad,* Thomson- Aranzadi, 2006, p. 19 et seq.; FERNÁNDEZ LÓPEZ, M. F., 'La intimidad del trabajador y su tutela en el contrato de trabajo', in CASAS BAAMONDE, M. E./DURÁN LÓPEZ, F./CRUZ VILLALÓN, J., (Eds.), *Las transformaciones del Derecho del Trabajo en el marco de la Constitución Española*, La Ley, 2006, p. 615 et seq.

particular in regard to the adoption of surveillance and control measures for monitoring workers' performance[4]. Article 50 SW allows the employee to claim paid termination of the employment contract when that right has been violated. On the other hand, the employer is entitled by several legal provisions to use disciplinary faculties in order to penalise employees for harming another worker's dignity and private sphere, for example in the case of harassment (namely, art. 54 SW). Finally, some rules stand for protection of employees' privacy and personal data concerning documents transmitted to the workers' representatives for purposes related to information and consultation collective rights (art. 64 and 65 SW).

Moreover, some other legal pieces within Labour Law set up additional provisions on protection of privacy. In the first place, legislation on health and safety at work establishes several cautions concerning monitoring over employees' physical conditions and medical examinations, as it will be explained below. In the second place, regulations on infringements and penalties to be applied by the Labour Inspectorate (Royal Legislative Decree 5/2000, 5th August) explicitly foresee penalties for employers regarding harassment against the employee or violation of his right to privacy. On the other hand, the statutory act on Labour Law litigation (Act 36/2011, 10th October) enables preferential and brief procedures –and some especial facilities and guarantees too- for actions aiming at protecting the constitutional fundamental rights of the worker, including privacy among all others. As a result of this kind of trials, the final judgement can compel to remove any effect of behaviours declared against the worker's constitutional rights, and tort damages can also be awarded. In addition, this procedural law also adopts some caution rules in order ensure respect to privacy within the process itself.

Anyway, Spanish Labour Law offers only general clauses and quite isolated rules in the field of the protection of employees' privacy and personal information, thus requiring integration with support on other provisions. Above all, attention must be paid to the constitutional framework, considering in particular four fundamental rights proclaimed in the Constitution of 1978 with the highest statutory rank and the maximum level of protection: the right to privacy (art. 18.1), the right on self- image (art. 18.1), the right to confidentiality of communications (art. 18.3) and the right to data protection (art. 18.4). As established by the Constitution itself (art. 10), the reference to some of these rights must be additionally interpreted according to applicable supranational texts, namely the regulation of similar rights in the European Convention on Human Rights (art. 8, respect for private and family life) and the EU Charter of Fundamental Rights (art. 7, respect for private and family life; art. 8, data protection).

The recognition of these fundamental rights in the Constitution and in the supranational texts does not specifically address employees in the context of the employment relationship. However, they are applicable in this ground as a result of the aforementioned statutory provisions that proclaim the worker's right to respect for his privacy and dignity [art. 4.2.e) and 20 SW] and, above all, of case law interpretation. In this sense, the Spanish Constitutional Court has repeatedly affirmed the directly binding effects of fundamental rights also within the workplace, considering that 'the conclusion of an employment contract does not imply deprivation of the citizen's rights for […] the worker', and stating that salaried working for an employer shall not involve 'temporary

[4] RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., 'Intimidad del trabajador y contrato de trabajo', *Relaciones Laborales*, num. 8, 2004, p. 8 et seq.

dispossession or unjustified limitations in regard to Fundamental Rights and Freedoms' of the employees[5]. This includes, among others, the rights to privacy, the right on self-image and the right to data protection[6]. Nonetheless, this case law also remarks that the effects of fundamental rights can be subject to some 'modulations' in the framework of the employment contract in order to safeguard the fulfillment of contractual obligations and the adequate performance of professional tasks[7]. But, at the same time, the Court outlines that these adjustments are acceptable only to the strictly necessary extent required on the basis of legitimate business needs[8].

Below the constitutional level, further development on constitutional fundamental rights to privacy, self-image and data protection is provided by some statutory provisions that shall be taken into account in regard to the protection of employees' personal and private sphere, although they are general acts outside the boundaries of Labour Law. The first one to mention is Organic Act 1/1982, 5th May, on civil protection of the rights to honour, privacy and self-image, which defines these rights and the basic rules fore their exercise, describing also different types of behaviours to be considered as unlawful intrusions against them. Besides, especial attention must be paid to Organic Act 15/1999, 13th December, on Personal Data Protection (LOPD for short), which was adopted as national transposition of Directive 95/46/EC, the EU common legal framework on data protection. This legal piece provides regulations of a general character, but nonetheless

[5] Constitutional Court Judgement 88/1985. In the same sense, Constitutional Court Judgements 6/1988, 6/1995, 4/1996, 90/1997, 57/1999, 98/2000, 186/2000, 20/2002 and 49/2003. MOLINA NAVARRETE, C., 'Bases jurídicas y presupuestos políticos para la eficacia social inmediata de los derechos fundamentales (El paradigma de la 'Drittwirkung' laboral a propósito de la reciente jurisprudencia constitucional)', *Revista de Trabajo y Seguridad Social*, num. 3, 1991, p. 63 et seq.; PEDRAJAS MORENO, A. *Despido y derechos fundamentales,* Trotta, 1992, p. 25 et seq.; DEL REY GUANTER, S., 'Derechos fundamentales de la persona y contrato de trabajo: notas para una teoría general', *Relaciones Laborales*, num. 3, 1995, p. 15 et seq.; BILBAO UBILLOS, J. M., *La eficacia de los derechos fundamentales frente a particulares*, BOE/ Centro de Estudios Políticos y Constitucionales, 1997, p. 233 et seq.; ORTIZ LALLANA, C., 'Derechos fundamentales y relación laboral', *Revista del Ministerio de Trabajo y Asuntos Sociales*, num. 13, 1998, p. 17 et seq.; NARANJO DE LA CRUZ, R., *Los límites de los derechos fundamentales en las relaciones entre particulares*, BOE/ Centro de Estudios Políticos y Constitucionales, 2000, p. 206 et seq.; RIVERO LAMAS, J., 'Derechos fundamentales y contrato de trabajo: eficacia horizontal y control constitucional', in MONTOYA MELGAR, A. (Eds.), *El trabajo y la Constitución. Estudios en homenaje al Profesor Alonso Olea*, Ministerio de Trabajo y Asuntos Sociales, 2003, p. 491 et seq.

[6] Referring explicitly to the rights to privacy and to confidentiality of communications, Constitutional Court Judgements 98/2000, 186/2000, 241/2012 and 170/2013; in regard to the right on self-image, Constitutional Court Judgement 99/1994; concerning the right to data protection, Constitutional Court Judgements 11/1998, 202/1999, 153/2004 and 29/2013.

[7] Among others, Constitutional Court Judgements 120/1983, 6/1988, 126/1990, 4/1996 and 20/2002. MARTÍN VALVERDE, A., 'Contrato de Trabajo y derechos fundamentales', *Revista de Derecho Social,* num. 6, 1999, p. 14; RODRÍGUEZ- PIÑERO Y BRAVO- FERRER, M., 'La integración de los derechos fundamentales en el contrato de trabajo', in SEMPERE NAVARRO, A. V./ MARTÍN JIMÉNEZ, R. (Eds.), *El modelo social en la Constitución Española de 1978,* Ministerio de Trabajo y Asuntos Sociales, 2003, p. 214 et seq.; GARCÍA MURCIA, J., 'Los derechos de la persona en el ámbito del trabajo asalariado', in GARCÍA MURCIA, J. (Ed.), *Derechos del trabajador y libertad de empresa. 20 casos de jurisprudencia constitucional,* Thomson- Aranzadi, 2013, p. 35 et seq.

[8] Among others, Constitutional Court Judgements 99/1994, 1/1998 and 186/1996.

applicable in the scope of the employment relationship too, where they can play in fact a relevant role, as seen in sections below[9].

Collective bargaining agreements could also establish regulations on the protection of employees' privacy and limits to the employer's managerial powers and surveillance faculties, of course within respect to statutory provisions. According to case law, they could play a relevant role by previously determining the terms and circumstances in which monitoring of work shall be implemented. This could be useful to clarify what actions and spaces would be under observation for legitimate business reasons, therefore excluding any expectation of confidentiality, and which others could conversely be preserved as areas suitable for personal or private behaviour. For instance, collective agreements can detail conditions for the employees' use of communication and information technologies at the workplace, consequently enabling some sort of control by the employer, in the sense pointed by an important judgement that will be commented below. This type of practice is increasing rapidly, but it is not really widespread in Spanish collective bargaining nowadays[10]. On the other hand, the exact extent to which the collective regulation of these issues shall be admitted and the value that should be given to such collectively agreed rules are still a matter of debate, as it will be seen afterwards.

Anyhow, in the absence of an exhaustive statutory regulation, the frequent conflicts between employer's business aims and the employees' rights to privacy and data protection (art. 18 Constitution) are often solved on the basis of balancing by judges and courts. In fact, specifically in regard to emerging challenges related to the impact of new technologies in the employment relationship context, it has been said that the regulation framework currently available in Spain is basically made of case law patterns[11]. Accordingly, especial attention must be paid to the relevant guidelines delineated by some leading cases of the Supreme Court of Justice and even of the Constitutional Court, which have already dealt with several disputes about the employer's control over employees and its limits arising from due respect to the workers' constitutional rights, referring in particular to the deployment of audio-visual surveillance devices and to monitoring on the use of computers and electronic communications in the workplace. At the international level, the European Court of Human Rights has also drawn up remarkable standards in this field, declaring the applicability of the rights to privacy and confidentiality of communications established by the European Convention on Human Rights (art. 8) within the framework of the employment relationship, and interpreting their extent in this context by means of very important criteria followed later by the Spanish courts.

[9] About the impact of Organic Law 15/1999 on Data Protection in the framework of the employment relationship, MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, CES, 2002, p. 201 et seq.; FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral,* Thomson-Aranzadi, 2003, p. 117 et seq.; DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, 2012, p. 79 et seq.

[10] For an exhaustive analysis of the regulations on this matter contained in collective bargaining agreements, SAN MARTÍN MAZZUCONI, C./ SEMPERE NAVARRO, A. V. (Eds.), *Derechos fundamentales inespecíficos y negociación colectiva,* Aranzadi, 2011, p. 138 et seq.

[11] CALVO GALLEGO, J. 'TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales', *Aranzadi Social,* num. 9, 2012, p. 128.

2. Personal data management in the employment relationship and in the hiring process

Spanish Labour Law does not regulate explicitly the employer's management of workers' personal data during the execution of the contract or in the hiring process. It provides only the already mentioned general clauses and a single reference to excluding the employees' private information from the documents passed on to workers' representatives for information and consultation aims (art. 64 SW). Although general legislation aiming at preserving personal information is applicable in many different contexts, and the employment relationship is not an exception. Organic Act 15/1999 on Data Protection and its complementary regulations are applicable to collection, registration, management and transmission of the employees' personal information by the employer, particularly –although not exclusively- in the case of 'especially protected data' as health condition and clinical facts, trade union or political membership, ideological preferences, religious belief, etc.

Therefore, dealing with personal data in the workplace must be in accordance to both general principles and security rules contained in these legal provisions, which have been interpreted and clarified by the Constitutional Court in its Judgement 292/2000: appropriateness of data handling according to legitimate aims, prohibition of deviated use and proportionality (as set in art. 4 LOPD); prerequisite of previous information and consent by the concerned person, except for data to be considered as strictly necessary for concluding or maintaining the employment contract (as regulated in arts. 5, 6 and 7 LOPD); confidentiality and other guarantees over collecting and keeping of personal information (arts. 10 to 12 and 25 to 32 LOPD), including duties of notification and registration before the Data Protection Agency, the specific public body created for monitoring and ensuring compliance with Data Protection legislation; finally, personal rights legally recognized to rejection, access, correction and cancellation in regard to personal data registration. Additionally, this legislation involves important consequences concerning some kind of measures for monitoring of work, namely the use of video cameras, but this will be explained later.

According to this framework, the employer can access the employees' personal data only on the grounds of pertinent and lawful business reasons and avoiding disproportionate excess in regard to those deemed objectives. The employee must be precisely informed in advance of the aims and extent of data collection, registration and handling. The employer's management of the collected data is limited by these terms of the previous information provided, so the employee's personal facts cannot be used for different purposes or as a basis for broader consequences. Express consent of the worker is needed except in the case of information that is strictly necessary for concluding or maintaining the employment contract (art. 6.2 LOPD). Concerning the 'especially protected data' mentioned above (ideology, trade union membership, health, religion, etc.), the employee's consent shall be not only explicit but also written (art. 7 LOPD). Last but not least, the creation of personal data files and passing on of this kind of information must be notified by the employer to the Data Protection Agency, in the detailed terms established by law (arts. 25 to 34 LOPD).

Especial mention must be made to the information on trade union membership. The employer's awareness of employee's association to a union is quite usual and sometimes even necessary in regard to specific aims legally foreseen and supported (i.e., application

of special guarantees for dismissal of trade union members or discount of trade union contributions from salaries). Nevertheless, this does not imply loss of the protected status of this information, which must be treated accordingly to its consideration as 'specially protected data' in Organic Act 15/1999, in the terms aforementioned. This also means that the employers can only use their knowledge of trade union affiliation of the workers for the concrete objectives that justified the communication of that circumstance. In this sense, a large series of rulings of the Constitutional Court leaded by Judgement 11/1998 declares unlawful the use of affiliation files created in regard to collection of associates' contributions for the deviated purpose of practising discounts due to strike on the earnings of those employees who were affiliated to the promoter union. On the other hand, the faculty of keeping trade union membership undisclosed is additionally protected by the right to reject revealing ideological or religious belief (art. 16.2 Constitution), as it is highlighted in Judgements 292/1993 and 145/1999 of the Constitutional Court [12]. According to these decisions, the workers and their representatives can refuse to communicate this information to the employers, even when this type of requests are authorised by Law or collective agreements in order to check the representativeness of each trade union at the company level, on the grounds of legitimate aims such as assigning collective rights proportionally. In this sort of situations, the Constitutional Court calls for the application of alternative procedures allowing the preservation of the identity of the affiliates unrevealed, in harmony with the orientations on the matter given by the ILO Freedom of Association Committee[13].

Referring in particular to the hiring process, any tests or enquiries applied must respect constitutional fundamental rights –among others, the rights to privacy, to data protection and the right to refuse revealing ideological or religious belief- and shall also be in line with the application of the commented prescriptions of the legal framework basically contained in Organic Act 15/1999, fulfilling the requirements of pertinence, proportionality, previous information and consent of the interested person. This means that information requests on, for example, affective relations, sexual orientation, ideological preferences or religious belief are in general forbidden, as they are in opposition to legislation on data protection, to good faith principle and, in some cases, to non-discrimination provisions too[14]. The employer's scrutiny on these non-professional fields can therefore be rejected by job applicants, who can refuse to answer questions, elude them

[12] GARCÍA MURCIA, J., 'Implantación sindical y acreditación del número de afiliados: entre los derechos fundamentales y el sentido común' (Sentencia 145/1999, de 22 de julio), in ALONSO OLEA, M./ MONTOYA MELGAR, A. (Eds.), *Jurisprudencia Constitucional sobre Trabajo y Seguridad Social*, V. XVII, Civitas, 2000, p. 204 et seq.; MONTOYA MELGAR, A., 'Poder del empresario, libertad sindical y libertad ideológica en la comprobación de los presupuestos para la designación de delegado de Sección Sindical' (Sentencia 292/1993, de 18 de octubre), in ALONSO OLEA, M./ MONTOYA MELGAR, A. (Eds.), *Jurisprudencia Constitucional sobre Trabajo y Seguridad Social*, V. XI, Civitas, 1994, p. 712 et seq.

[13] ILO Freedom of Association Committee, 336 Report, case num. 2153, par. 166; 302 Report, case num. 2132, par. 661; 327 Report, case num. 2132, par 661.

[14] DE VICENTE PACHÉS, F., *El Derecho del Trabajador al respeto de su intimidad,* CES, 1998, p. 81 et seq.; RODRÍGUEZ- PIÑERO Y BRAVO- FERRER, M., 'Intimidad del trabajador y contrato de trabajo', Relaciones Laborales, num. 8, 2004, p. 4 et seq.; FERNÁNDEZ LÓPEZ, M. F., 'La intimidad del trabajador y su tutela en el contrato de trabajo', in CASAS BAAMONDE, M. E./ DURÁN LÓPEZ, F./ CRUZ VILLALÓN, J. (Eds.), *Las transformaciones del Derecho del Trabajo en el marco de la Constitución Española*, La Ley, 2006, p. 664 et seq.

or even lie, as it would be justified in order to preserve his private life without suffering any harmful consequences in the field of employment[15].

3. Audio-visual surveillance in the workplace

The use of audio-visual surveillance devices in the workplace can be justified on the basis of different purposes such as general business or trade security, monitoring of work performance by the employees or compliance with health and safety requirements. And, at least in regard to closed- circuit TV, this is a quite widespread practice in Spain[16]. Even though some limits are to be applied, as the deployment of these tools involves a high potential risk for workers' fundamental rights, namely the right to privacy, the right on self-image and the right to personal data protection (art. 18 Constitution)[17]. However, Spanish Labour Law does not establish an explicit and detailed statutory regulation specifically referred to audio-visual technologies. As said before, it only provides some general clauses on the safeguard of dignity and privacy as a basic right of the employee [art. 4.2.e) SW], and as a limit to the employer's managerial powers (art. 20 SW).

Nevertheless, there are some general statutory provisions outside the borders of Labour Law, which are also relevant regarding audio-visual surveillance in the workplace. The first legal piece to mention is Organic Act 1/1982 on protection of the rights to honour, privacy and self-image. This act considers that placement of audio, video and optical devices or any other technical instruments for recording or reproducing peoples' private life is an illicit intrusion against the protected rights (art. 7.1 and 2). In addition, it also prohibits the use of photographs, video or any other procedure for capturing, reproducing or publishing the personal image of an individual at any place or moment of his life, private or not (art. 7.5). Nevertheless, these actions can be legitimated both on the basis of

[15] In this sense, it is discussed whether there is a 'right to lie'. Although this might be quite excessive, most academics agree nonetheless that not saying the truth is at least a lawful behaviour when it is the only way for the job applicant to safeguard his personal and private sphere before inappropriate and unlawful enquiries in the hiring process. GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador*, Civitas, 1988, p. 63; DE VICENTE PACHÉS, F., *El Derecho del Trabajador al respeto de su intimidad*, CES, 1998, p. 96; RODRÍGUEZ CARDO, I. A., *Poder de dirección empresarial y esfera personal del trabajador*, Consejo Económico y Social del Principado de Asturias, 2009, p. 151.

[16] GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 42.

[17] About audio-visual surveillance, DE VICENTE PACHÉS, F., *El Derecho del Trabajador al respeto de su intimidad*, CES, 1998, p. 323 et seq.; LÓPEZ PARADA, R., 'Análisis jurisprudencial acerca de la instalación por el empresario de sistemas de videovigilancia en el lugar de trabajo', *Información Laboral (Jurisprudencia)*, V. 3, 1999, p. 5043 et seq.; MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, CES, 2002, p. 67 et seq.; FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral,* Thomson- Aranzadi, 2003, p. 71 et seq.; FERNÁNDEZ LÓPEZ, M. F., 'La intimidad del trabajador y su tutela en el contrato de trabajo', in CASAS BAAMONDE, M. E./ DURÁN LÓPEZ, F./ CRUZ VILLALÓN, J. (Eds.), *Las transformaciones del Derecho del Trabajo en el marco de la Constitución Española*, La Ley, 2006, p. 631 et seq.; DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., 'El control de la prestación del trabajador a través de las nuevas tecnologías: un estudio sobre la videovigilancia en la doctrina judicial', *Justicia Laboral,* num. 44, 2010, p. 14 et seq.; ÁLVAREZ ALONSO, D., 'Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: Sentencia TC 98/2000, de 10 de abril', in GARCÍA MURCIA, J. (Ed.), *Derechos del trabajador y libertad de empresa. 20 casos de jurisprudencia constitucional,* Thomson- Aranzadi, 2013, p. 338 et seq.

express consent by the concerned person or in the case of an explicit legal entitlement (art. 2).

In this sense, Act 23/1992 on Private Security (art. 5) allows the installation of video cameras or closed-circuit TV in business places for ensuring security of goods and persons, provided that these devices are fitted and maintained –under certain conditions- by a security firm with previous authorization of the Home Affairs Ministry, not by companies or employers themselves. Besides, Labour Law enables the employer to adopt any surveillance measures he deems in order to verify compliance of working duties and obligations by the employee, albeit it imposes paying due consideration to 'human dignity' (art. 20.3 SW). These provisions have been seen as enough legal entitlement for audio-visual monitoring of the workplace, even without the previous consent of workers[18]. But they circumscribe the allowance of those surveillance instruments to the mentioned legitimate aims of business security and supervision of working duties compliance, in the strict terms described, thus being unlawful their use in other contexts or for different purposes to those specifically authorised. This means, for instance, that it is banned to focus on some areas of the workplace not directly related to work performance such as bathrooms, locker rooms and rest zones, as case law has emphasised[19]. And, as a general rule, it should also be considered forbidden for the employer to apply audio-visual control over the employees' personal life outside the workplace, except in case of a strong professional reason making it strictly necessary[20].

Moreover, the mention of art. 20.3 SW to the worker's dignity as a limit to the employer's surveillance powers calls for additional consideration of general law on the protection of fundamental rights and, further ahead, for striking a balance between business necessity and the respect to constitutional rights of the employee which might be involved[21]. In the first place, as audio and video are useful means for registration or transmission of personal information concerning identified or identifiable individuals, the use of audio-visual surveillance may affect the right to data protection (art. 18.4 Constitution) and it is to be submitted to the general provisions on the matter, contained in Organic Act 15/1999 on Personal Data Protection and its complementary regulations. This has been underlined by the Data Protection Agency (AEPD, regulated in the mentioned

[18] GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador*, Civitas, 1988, p. 141.

[19] Constitutional Court Judgement 98/2000. Referring to a significant amount of judgements of the labour courts in this sense, DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, 2012, p. 31 et seq. See also MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, CES, 2002, p. 105 et seq.

[20] However, the labour courts have sometimes admitted audio-visual surveillance of employees outside the workplace too generously. For instance, some judgements accept the use of photographs and video recordings obtained by private investigators in public places as valid proof in order to adopt disciplinary decisions against employees for simulating a state of illness. In this sense, Galicia Higher Court Judgement 27th November 2004 and I. Balears Higher Court Judgement 17th October 2008. GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 51.

[21] MERCADER UGUINA, J. R., 'Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?', *Relaciones Laborales,* num. 10, 2001, p. 15 et seq.; FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral,* Thomson- Aranzadi, 2003, p. 83 et seq.

act) regarding in particular the use of video cameras, closed- circuit TV systems, webcams or similar technologies[22].

According to this legal framework, these practices shall meet the following requisites[23]: the control will be limited to legitimate purposes recognised by law, as said above; monitoring must be circumscribed to what is strictly necessary for business reasons, avoiding intrusion in private behaviours or conversations; the concerned people must be previously informed by means of posters, hand-outs, personalized information and communication to the workers' representatives, in terms legally detailed[24]; registered images must be cancelled within 30 days (they can be preserved longer only in case of recording an infraction or breach of occupational duties) and third-party access to them is forbidden except in the case of certain legally based grounds; security rules and personal rights to rejection, access, modification and cancellation of personal data registration shall be guaranteed; last but not least, the proportionality principle will be strictly abided[25].

The essential role of the proportionality principle has also been highlighted by case law of the Constitutional Court on monitoring of work by audio-visual means, which has established key guidelines to deal with these issues in the absence of fully detailed statutory regulations. The Constitutional Court has declared that the employer's use of these technical surveillance instruments may be lawful, although it must be made compatible with the obliged respect to the fundamental constitutional rights of the worker, in particular the right to privacy (art. 18.1 Constitution), which can be submitted to modulations in the professional context, but only to the strictly necessary extent on the ground of justified reasons. These considerations lead to a balance between the employee's constitutional rights and the employer's needs, for which the main guidelines are given in leading cases 98/2000 and 186/2000 of the Constitutional Court, where the proportionality principle arises as the main tool[26].

Judgement 98/2000 refers to the installation of hearing devices for monitoring some areas of a casino (i.e. roulette table), a new surveillance method added to the previously installed closed-circuit TV with the declared aim of enhancing business and clients security. This measure was claimed against by the employees, who considered it as an infringement of the right to privacy, as the Constitutional Court finally did too. The reasoning of this decision states that it had not been proven that audio capturing and recording was absolutely necessary for ensuring security in the game room, sufficiently safeguarded by the already existing closed circuit TV system. On the other hand, this very

[22] Royal Decree 1720/2007, 21st December, art. 5.1; AEPD Instruction 1/2006. GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 43 et seq.

[23] GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 45 et seq.

[24] AEPD Instruction 1/2006, art. 3.

[25] AEPD Instruction 1/2006, art. 4.

[26] DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., 'El control de la prestación del trabajador a través de las nuevas tecnologías: un estudio sobre la videovigilancia en la doctrina judicial', *Justicia Laboral,* num. 44, 2010, p. 16 et seq.; ÁLVAREZ ALONSO, D., 'Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: Sentencia TC 98/2000, de 10 de abril', in GARCÍA MURCIA, J. (Ed.), *Derechos del trabajador y libertad de empresa. 20 casos de jurisprudencia constitucional,* Thomson- Aranzadi, 2013, p. 338 et seq.

narrow contribution to improving security in the casino was in contrast with the excessive intrusion on privacy caused by the continuous and indiscriminate hearing of all conversations of workers and clients, including those of private nature. The conclusion is that the use of hearing devices was to be considered disproportionate and consequently a violation of the right to privacy[27]. Since then, labour courts tend to consider audio surveillance of work as unlawful except in very few cases in which it can be justified in the light of the proportionality principle (i.e. recording commercial telephone calls for security reasons in the telemarketing sector, as it will be seen later)[28].

Not much later, Judgement 186/2000 of the Constitutional Court deals with the use of a hidden video camera for discovering who among the employees of a supermarket was to be held responsible for repeatedly stealing money from the cash register, in order to subsequently dismiss them on disciplinary grounds. The court makes a balance between the worker's right to privacy and business legitimate needs, applying even more explicitly the proportionality principle as a three-step test on the requirements that any audio-visual surveillance measure adopted by the employer must fulfil to be considered lawful: 1) it shall be useful and adequate in regard to legitimate business aims (adequateness test); 2) it shall be strictly necessary, in the sense that those legitimate aims would not be successfully achieved with less aggressive methods (necessity test); finally, 3) it shall be a balanced measure, avoiding the excessive sacrifice of the worker's rights on behalf of minor business interests (strict sense proportionality test)[29].

This scheme is applied by Judgement 186/2000 to the particular circumstances of the case, emphasizing as relevant facts that the video camera was installed only after the appearance of consistent suspicions on stealing, just for the brief period of time needed for the subsequent investigation and exclusively focusing on a very limited area, not recording anything else than the cash register and the workers' hands. These appreciations lead to declare the employer's behaviour lawful, even the furtive nature of watching by means of a hidden camera. This sort of surveillance was considered adequate, necessary and proportionate in the concrete situation examined, as far as a visible device would surely fail in the attempt to get evidence of the previously suspected infringement and to find out who was the guilty employee. Anyhow, following these criteria, later decisions of the labour courts judge monitoring of the workplace by video capturing or recording in regard to the proportionality principle, thus requiring sufficient justification on unfailing business grounds, declaring it unlawfully disproportionate if the observed areas or the number of

[27] DEL REY GUANTER, S., 'Los límites del control por el empresario en el centro de trabajo mediante mecanismos auditivos (Comentario a la STC 98/2000, de 10 de abril)', in ALONSO OLEA, M./ MONTOYA MELGAR, A. (Eds.), *Jurisprudencia Constitucional sobre Trabajo y Seguridad Social*, V. XVIII, Civitas, 2000, p. 192 et seq.

[28] DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, 2012, p. 28 et seq.

[29] ESCRIBANO GUTIÉRREZ, J., 'El derecho a la intimidad del trabajador. A propósito de la STC 186/2000, de 10 de julio', *Relaciones Laborales*, num. 1, 2001, p. 85 et seq.; MONTOYA MELGAR, A., 'Control del trabajador desleal y alcance del derecho de este a la intimidad (Comentario a la STC 186/2000, de 10 de julio)', in ALONSO OLEA, M./ MONTOYA MELGAR, A. (Eds.), *Jurisprudencia Constitucional sobre Trabajo y Seguridad Social*, V. XVIII, Civitas, 2000, p. 315 et seq.

cameras are excessive and rejecting surreptitious surveillance with hidden devices, except in the case of previous suspicions on a breach of workers' duties[30].

More recently, Judgement 29/2013 of the Constitutional Court refers again to the use of video cameras at the workplace, this time in the light of the right to data protection (art. 18.4 Constitution), and assessing in particular the prerequisite of previous information to the observed people, as laid down in Organic Act 15/1999 and its complementary regulations. The facts refer to an employee of the University of Seville who was disciplinary banned for continuous breaches of his working time schedule, using as evidence the recording of his frequent late incoming to the office by the video cameras for controlling access to the buildings. The reasoning of this decision states that the utilization of cameras for monitoring of work requires giving in advance explicit, precise and clear information to the employees about the extent of image capturing and its use for supervision on working duties compliance, except in the case of an explicit legal exemption to this general obligation. In the case, the Court (as the AEPD) considers that these conditions were not properly accomplished, because, although the implementation of video cameras met the terms of law and was correctly adverted by posters in regard to building security aims, there was however no earlier information concerning their deviated use for the different purpose of controlling workers. The judgement concludes therefore declaring the existence of a violation of the fundamental right to data protection, clearly outlining the unlawful character of surreptitious video surveillance not previously announced, to some extent in contradiction with the preceding Judgement 186/2000.

This latest decision could be quite controversial. In fact, a dissenting opinion signed by Judge Andrés Ollero Tassara emphasizes the mentioned discordance in regard to Judgement 186/2000 and criticizes the absence of an adequate balancing between the protection of the worker's rights and legitimate business needs according to the proportionality principle, suggesting that this could have led to a different solution. It also remarks that the reasoning of Judgement 29/2013 ignores some relevant facts of the case that, from this other point of view, should have been considered more carefully: on the one hand, that governmental authorizations given to the University of Seville for the use of video recording files included one explicitly referred to 'monitoring access of persons belonging to University's community'; on the other hand, that the areas under video surveillance were public places and that the presence of cameras was clearly adverted by informative posters which were noticeable for anyone[31].

Anyhow, the new case law guidelines provided by Judgement 29/2013 could be of great importance. First of all, this decision underlines the relevance of giving precise information in advance as a general prerequisite for the use of cameras or CCTV for the monitoring of workers, therefore questioning undisclosed video observation in a more strict way that it had been already done before. This statement should lead to the revision of the former criteria adopted by several labour courts, which used to accept the utilisation of hidden devices in too broad terms, on the basis of mere suspicions of a breach of

[30] DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, 2012, p. 25 et seq.; ÁLVAREZ ALONSO, D., 'Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: Sentencia TC 98/2000, de 10 de abril', in GARCÍA MURCIA, J. (Ed.), *Derechos del trabajador y libertad de empresa. 20 casos de jurisprudencia constitucional,* Thomson- Aranzadi, 2013, p. 361 et seq.

[31] Sharing that criticism, RODRÍGUEZ COPÉ, M. L., 'Facultades de control empresarial y circuito cerrado de televisión', *Temas Laborales,* num. 121, 2013, p. 199 et seq.

working obligations and regardless of the seriousness of those infringements[32]. But, furthermore, this innovative doctrine of the Constitutional Court also reinforces the conditions and limits applicable to the deployment of these video surveillance instruments with the aim of controlling employees, even when it is done in open access areas and by means of perfectly visible equipments, without an unrevealed or furtive nature. This points again to the reconsideration of the traditional orientations followed by some earlier judgements, which quite often tended to validate video surveillance over workers without previous explicit announcement when it was done in public places open to observation by anyone[33].

4. Control over employee's communications (I): general rules and traditional tools

Communication instruments available in the workplace, as telephones or postal service facilities among the most traditional, are to be seen above all as tools of the employer's property that are meant to be used by employees primarily for business aims. Given the fact that they are supposed to be applied mainly for commercial and professional tasks and they entail costs and risks of improper utilization, it is reasonable to admit the employer's legitimate interest in establishing some controls. Nevertheless, as long as those resources easily offer possibilities for a double professional and personal use, which is often culturally assumed and tolerated in our societies, monitoring must surely be submitted to some cautions, in order to safeguard the workers' private sphere and to avoid the employers' abuse. Although there are not explicit and detailed statutory provisions on the matter in Spanish Labour Law, some already mentioned general clauses [art. 4.2.e) and 20.3 SW] validate this type of controls, but abiding respect to the employee's dignity and right to privacy (art. 18.1 Constitution). In addition, attention must be paid to another fundamental right particularly relevant in this specific field: the right to confidentiality of communications (art. 18.3 Constitution)[34].

This framework shall be applied taking into consideration important case law on the matter drawn up by the European Court of Human Rights. The leading Judgement of 25th June 1997 (Halford vs. UK) refers to a female police officer, whose office telephones were submitted to interception by higher rank officers for the purpose of obtaining information to use against her in discrimination proceedings she had initiated before. The Court declares that this was a violation of the European Convention on Human Rights, stating important criteria that can be summarized as follows: calls made from or to businesses may also be covered by the right to private life and the guarantees against interception of communications established in art. 8 of the Convention, which is violated when the employer intercepts them surreptitiously and without any previous warning, acting thus

[32] GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 48.

[33] Referring to several decisions of labour courts in this sense, DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, 2012, p. 35 et seq. See also, FERNÁNDEZ VILLAZÓN, L., 'Tiempos de labor y otros tiempos retribuidos: los controles y sus límites', in ARGÜELLES BLANCO, A. R./ ROMERO BURILLO, A. M. (Eds.), *Régimen jurídico y gestión racional del tiempo en la empresa,* Aranzadi, 2013, p. 160 et seq.

[34] Particularly in regard to telephone calls and postal service communications, FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral,* Thomson- Aranzadi, 2003, p. 92 et seq.

against a 'reasonable expectation of confidentiality' held by the employee on the basis of preceding authorization or simply tolerance of private use of office telephones.

These guidelines have been followed by Spanish Labour Courts, assuming in particular the standard of the 'reasonable expectation of confidentiality'. Nonetheless, they allow phone tapping or even recording of calls in the workplace when some requirements are fulfilled, in order to preserve the workers' right to privacy. In this sense, the leading case is surely a Judgement of 5th December 2003 of the Supreme Court, which validates control over communications between clients and employees in the telemarketing sector, as long as applied to telephones provided expressly and exclusively for professional use, with previous explicit warning and information to workers on the monitoring system, and just to the extent strictly needed for legitimate business aims, according to the proportionality principle[35].

To conclude this summary of relevant case law, one should also mention Judgement 114/1984 of the Constitutional Court, which clarifies the correct interpretation of the specific right to confidentiality of communications (art. 18.3 Constitution) in the case of a telephone call between a worker and one of his bosses, recorded by the last and subsequently used as evidence for disciplinary dismissal. The Court outlines that this right protects freedom and confidentiality of correspondence and telephonic communications in the sense of forbidding third- party interception of the message and intrusive external access to its content –regardless of being of private character or not- or to other data as the interlocutors' identity. However, it does not prevent the recording of or storing the conversation by one of its internal partners, although further transmission to other people might be against the right to privacy (art. 18.1 Constitution) when the information is in fact of private nature. On this basis, the judged capturing of the telephone call, which was not of private substance, was considered not contrary to the fundamental right alleged by the employee.

5. Control over employee's communications (II): e-mail and other Internet messaging software

Obviously, new technologies have hugely increased facilities and the variety of tools available for communication in the workplace context and also the possibilities for their monitoring, hence deepening the problem of harmonizing the employer's legitimate interest in supervision and, on the other hand, the safeguard of the employee's privacy and dignity against abusive intrusions. The already common use of instruments as e-mail or Internet messaging software (i.e. MSN Messenger, Whatsapp, Line, Trillian…) and widespread social networking (among others, on Facebook, Twitter, Google+ or LinkedIn), often with an unclear mix of personal and professional purposes or private and public contents, involves innovative potential risks and challenges for Law in different fields, including the one of the employment contract.

[35] DESDENTADO BONETE, A./MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, 2012, p. 28 et seq.; ÁLVAREZ ALONSO, D., 'Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: Sentencia TC 98/2000, de 10 de abril', in GARCÍA MURCIA, J. (Ed.), *Derechos del trabajador y libertad de empresa. 20 casos de jurisprudencia constitucional,* Thomson- Aranzadi, 2013, p. 362.

However, legislation goes clearly behind reality in this ground and, not surprisingly, Labour Law does not offer explicit statutory regulations on the matter[36]. Therefore, the rapidly growing amount of conflicts arising is being dealt with by means of *ad hoc* solutions of the courts in the light of the constitutional rights to privacy (art. 18.1 Constitution) and confidentiality of communications (art. 18.3 Constitution), frequently using the method of balancing and the proportionality principle and applying analogically some previous case law guidelines originally drawn up in regard to more traditional instruments as video cameras and telephones, as it has been explained in the sections above. Although the resulting judicial answers to these issues are not sufficiently unified and consolidated, some leading cases within case law of the higher courts can at least be summarized here[37].

Judgement 3rd April 2007 (Copland vs. UK) of the European Court of Human Rights declares the violation of the right to privacy and confidentiality of communications (art. 8 of European Convention on Human Rights) in the case of a female worker of a Higher Education College whose telephone calls, e-mails and Internet navigation were widely spied by her supervisor, adducing as justifiable aim the investigation of a possible abuse in personal use of College's facilities. The Court recognizes that monitoring of the employee's use of telephones, e-mail and Internet in the workplace may be allowed to the employer on the ground of legitimate purposes foreseen by law and under certain conditions. But these practices are rejected when they are applied, as in the judged case, in the lack of a consistent legal entitlement and in a surreptitious way, without previously informing the employee and outside the boundaries of a clear and published general policy on control measures and privacy. The absence of these earlier warnings would create a 'reasonable expectation on privacy' for workers, a context of confidence for private behaviours and communications that are to be protected against unforeseen and unapproved intrusions, in the sense already outlined by the aforementioned Judgement of 25th June 1997 (Halford vs. UK).

Among case law of the Constitutional Court, the first decision to mention is Judgement 241/2012, about two employees who were disciplinary banned for offensive comments on other workers, clients and supervisors made in conversations through an Internet instant messaging programme (Trillian) that they had installed in a computer at the workplace. Another worker discovered by chance those conversations and informed the supervisors, who decided to fully read the whole content of the dialogues by means of checking the folders and temporary files of the computer in which they were automatically recorded. The involved employees claimed that this behaviour was a violation of their rights to privacy (art. 18.1 Constitution) and to confidentiality of communications (art. 18.3 Constitution). However, the Court refused this allegation relying in two relevant facts:

[36] In the absence of a more precise statutory regulation on employer's monitoring of employees' electronic communications, some scholars have drawn up different proposals of guidelines to follow. FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral,* Thomson-Aranzadi, 2003, p. 123 et seq.; GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 32 et seq.; COLÀS NEILA, E., *Derechos fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia,* Bomarzo, 2012, p. 145 et seq.

[37] For a more exhaustive analysis of the guidelines outlined by the labour courts in regard to the employer's control on the employees' use of e-mail, MARÍN ALONSO, I., *El poder de control empresarial sobre el uso del correo electrónico de empresa,* Tirant lo Blanch, 2005, p. 126 et seq.

1) the computer was for common use of different workers, and anyone had full access to it even without a password; 2) there were explicit and previous instructions given by the employer forbidding installation of software without authorization in the office computers and preventing their use for non-professional purposes.

Taking into account those particular circumstances, the judgement declares that there was not a 'reasonable expectation of confidentiality' in the sense of the above explained European case law, denying the existence of violation of the right to privacy as the workers themselves were who decided to carelessly make those comments in a context in which confidentiality was not likely. And, in regard to the right on confidentiality of communications, the Court outlines that it refers exclusively to closed transmission channels, therefore not being applicable to those which are open to foreseeable third-party access, as was considered in this case[38]. Nevertheless, the solution given in this judgement is quite controversial, and it has been emphatically criticised in a dissenting opinion signed by two of the members of the Court (Fernando Valdés Dal-Ré and Adela Asua Batarrita). In their opposite view, the open access of office computers and previously established general prohibition of installing software in those equipments are not enough basis to enable any kind of employer's monitoring over Internet messaging between employees. These judges highlight that supervisors could have adopted disciplinary measures as soon as they had noticed unauthorized use of the computers, with no need of reading the private content of the messages among the workers. But they preferred to wait and –for more than two months- furtively spy employees' communications by exhaustively searching temporary files and fully reading the conversations, behaviour that should have been considered as absolutely unlawful. On the other hand, the disagreement also refers not only to the concrete decision adopted in this case, but also to the idea underlying its reasoning in the sense that the employer seems to be entirely free for unilaterally establishing prohibitions and conditions in regard to the use of information and communication technologies in the workplace.

More recently, Judgement 170/2013 of the Constitutional Court refers to an employee of a chemical company who was disciplinary dismissed for passing on industrial information to another company, unfaithfulness that was evidenced by checking some e-mails sent from his business account. Conversely to the allegations of the worker, the Court declares that those checks did not violate the right to privacy (art. 18.1 Constitution), nor the right to confidentiality of communications. The decision deems that in the circumstances of the case there was no 'reasonable expectation of confidentiality' to be protected, given that disciplinary regulations in the collective bargaining agreement applicable explicitly banned non-professional use of business e-mail account, implicitly pointing to the employer's monitoring on those tools as foreseeable, and leading consequently to decline its consideration as a surreptitious intrusion on the private sphere or as an unlawful interception over closed-channel communications. On the other hand, the control is considered not disproportionate as it was adopted regarding a previously suspected infringement of occupational duties and just to the necessary extent, referring to just a few mails of strictly professional –not private- content.

This last decision can be subject to some discussion too. In particular, it is doubtful to what extent the disciplinary regulations contained in collective bargaining agreements in

[38] MUÑOZ RUIZ, A. B., 'Social Networking: New Challenges in the Modern Workplace', *Spanish Labour Law and Employment Relations Journal*, V. 2, 2013, p. 34.

regard to electronic communications can be deemed as sufficient previous warning to workers in order to make all 'expectations of confidentiality' decline, consequently enabling any kind of interception of e-mails or Internet messaging by the employer[39]. In this sense, the aforementioned case law of the European Court of Human Rights requires information in advance to the concerned people about what is going to be submitted to supervision, specifying clear and precise indications on the concrete methods and instruments of control which are going to be applied[40]. These strict requirements do not seem to be adequately accomplished by the sole regulation of prohibitions and disciplinary consequences related to improper use of information technologies in sector collective agreements. In a more correct understanding of the guidelines given by the European Court, expectations of confidentiality could only be fully excluded on the basis of a much more explicit and detailed announcement of surveillance measures and privacy policy at the company level[41].

In conclusion, although the general patterns outlined by these latest judgements of the Constitutional Court are surely correct, they are probably not enough to solve all kinds of conflicts concerning monitoring of electronic communications in the workplace, and they also are arguable in some aspects. In fact, they have raised up an intense debate among scholars, many of whom regard Judgements 241/2012 and 170/2013 as 'a step backwards' in the protection of employees' privacy and personal sphere at the workplace[42], whilst some others consider them equilibrate decisions[43]. Hence, further clarifying on those particular issues pointed out and, in broader terms, on possibilities and limits of employer's control over e-mails and other Internet messaging tools is surely needed. New interesting contributions by scholars and forthcoming judgements are surely to be expected.

6. Further control on computers and Internet browsing

Leaving apart the specific issue of the interception of e-mails and other electronic communications, employers can be interested in monitoring the use of computers in the

[39] SEPÚLVEDA GÓMEZ, M., 'Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites', *Temas Laborales,* num. 122, 2013, p. 209 et seq.; MONEREO PÉREZ, J. L./ DEL MAR LÓPEZ INSÚA, B., 'El control empresarial del correo electrónico tras la STC 170/2013', *Aranzadi Social,* num. 11, 2014, p. 225 et seq.

[40] European Court of Human Rights Judgements of 25th June 1997 (Halford vs. UK) and 3rd April 2007 (Copland vs. UK).

[41] CARRASCO DURÁN, M., 'El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa', *Revista Aranzadi Doctrinal*, num. 9, 2014, p. 53 et seq.

[42] CARDONA RUBERT, M. B., 'Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás', *Revista de Derecho Social,* num. 60, 2012, p. 169 et seq.; MARÍN ALONSO, I., 'La mensajería electrónica en la empresa: un paso atrás en la protección constitucional del derecho al secreto de las comunicaciones', *Relaciones Laborales,* num. 3, 2013, p. 89 et seq.; MONEREO PÉREZ, J. L./ DEL MAR LÓPEZ INSÚA, B., 'El control empresarial del correo electrónico tras la STC 170/2013', *Aranzadi Social,* num. 11, 2014, p. 216 et seq.; SANTIAGO REDONDO, K. M., 'Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE', *Relaciones Laborales,* num. 1, 2014, p. 119 et seq.

[43] In regard to Judgement 170/2013, MARTÍN VALVERDE, A., 'Uso extralaboral del correo electrónico empleando medios informáticos de la empresa. Control empresarial: requisitos', *Actualidad Laboral*, num. 2, 2014, p. 184 et seq.

workplace in a broader sense. In particular, they might be concerned by the proper use of Internet browsing for several reasons: ensuring that employees do not waste their working time in non-professional activities as, for example, reading newspapers, watching YouTube videos or social networking[44]; preventing potential risks for the equipment as cookies, viruses and spy software upcoming from navigation on unsecure websites; last but not least, preventing the use of professional computers as an instrument for unlawful behaviours or even criminal offences as, for instance, sharing illicit pornography. There are not explicit statutory rules in regard to this matter, but case law of the Supreme Court has already dealt with some conflicts related to the employer's supervision of internet browsing by the employees, mainly through checking of temporary files stored in computers, as they are like the track left behind of the visited websites.

In a case solved by a Judgement of 26th September 2007 of the Supreme Court, the repair of a virus infection in an employee's computer allowed to discover (by checking temporary files) that the source of contamination was Internet navigation on unsecure sites of pornographic content, and this lead subsequently to the dismissal of that worker. Reasoning on the involved rights and interests, the Court declares that, on the one hand, the employer is entitled to monitor computers of his own property; but, on the other hand, that should be done respecting the workers' right to privacy, which extends its protection to private information deduced from internet temporary files. Looking for a balanced solution, the judgement follows the above explained guidelines of the European Court of Human Rights in Judgements Halford and Copland, therefore considering that employer's controls on Internet browsing are lawful when they are predictable according to previous warnings or company level regulations, but they are on the contrary a violation of the worker's fundamental rights when practised without earlier information and therefore against a 'reasonable expectation of privacy', as it had happened in the judged case.

The Supreme Court gives a very similar answer in a more recent Judgement of 8th March 2011, this time in regard to the dismissal of a worker after a technical audit of informational systems in the company, which revealed that he had been spending a huge part of his working time browsing on Internet contents as videos and other multimedia entertainment resources, commercial advertisements and piracy software websites. As in the aforementioned case, the Court relies on earlier case law on 'reasonable expectations of confidentiality', therefore concluding that this sort of monitoring is to be considered as a violation of the right to privacy when unexpectedly applied in the lack of a previous warning or regulation on the matter.

Finally, in a later Judgement of 6th October 2007, the Supreme Court deals with the disciplinary dismissal of an employee who, ignoring the explicit instructions and prohibitions set by the employer, repeatedly used the Internet during working time and from her office computer for personal aims such as selling used goods, visiting travel agency websites and managing a small business of her own. All this was evidenced by means of installing spy software that enabled to furtively capture and to reproduce afterwards all the screens successively shown in the computer. In this case, the Court denies the existence of a violation of the right to privacy, considering that no 'reasonable expectation of confidentiality' could be alleged, given the fact that there was a previous

[44] Referring in particular to social networks, CALVO GALLEGO, J. 'TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales', *Aranzadi Social,* n. 9, 2012, p. 146 et seq.; MUÑOZ RUIZ, A. B., 'Social Networking: New Challenges in the Modern Workplace', *Spanish Labour Law and Employment Relations Journal*, Vol. 2, 2013, p. 32 et seq.

explicit instruction -lawfully adopted by the employer- in the sense of absolutely prohibiting any non-professional use of telephones, computers, Internet and any other tools provided by the company.

However, a dissenting opinion to this judgement signed by five judges considers that the existence of an absolute prohibition of using computers for personal aims is not sufficient by itself for making expectations of confidentiality decline, thus legitimating any kind of monitoring by the employer. According to this opposite view, the employer should additionally have informed on the type and extent of the exact control measures to be applied. The conclusion in regard to the circumstances of the case is that a violation of the right to privacy should have been declared, as there was no previous warning on the use of such a specific surveillance mean as spy software, by the way seen as a particularly invasive method.

In conclusion, the doctrine on 'reasonable expectations of confidentiality' has become an important milestone in the field of monitoring on computers and Internet browsing at the workplace, according to European and national relevant case law. This scheme tends to give great importance to the previous publishing of the employer's 'privacy and control' policy on the matter or even to the adoption of preceding company level regulations and prohibitions in regard to the use of new technologies by the employees, as these instruments seem to be entitled to respectively delimitate in advance which areas are to be considered within the confidential sphere and which others are exposed to legitimate supervision. Nevertheless, some aspects of these reasoning patterns could be still unclear or even controversial. Firstly, it is doubtful to what extent the employers can absolutely ban employees' personal use of new technologies through that kind of rulings. Some authors reasonably argue that the employer should not be considered entirely free to unilaterally forbid any sort of non professional utilisation of those tools, demanding at least an analysis of proportionality according to legitimate business needs and supporting that a minimum space for autonomous behaviour is needed to preserve employee's dignity[45]. Secondly, it is also questionable if the sole existence of those prohibitions is sufficient basis for making all expectations of confidentiality vanish. In fact, to some extent in contradiction with the last ruling of the Supreme Court mentioned, a closer look at the criteria outlined by the European Court of Human Rights leads to affirm that a simple interdiction of a broad and general character is not enough to exclude any kind of privacy expectations, which can only be effectively weakened by much more explicit and precise warnings on the control measures deployed. Finally, this matter should also be regarded in the light of other different criteria that seem to be currently underrated by some courts, namely the rules and principles arising from legislation on data protection (Organic Act 15/1999), that are surely applicable to processing of personal information by means of information technologies, especially when using such invasive tools as 'spy software'[46].

[45] CALVO GALLEGO, J. 'TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales', *Aranzadi Social,* n. 9, 2012, p. 131 and 140; FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral,* Thomson- Aranzadi, 2003, p. 111 et seq.

[46] In this sense, FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral,* Thomson- Aranzadi, 2003, p. 113 et seq.; GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num.

7. Medical examinations and health data

Medical examinations on employees at the request of the employer are explicitly legitimated in Spanish legislation in regard to justifiable aims mainly related to health and safety at work. Nevertheless, they often involve invasive practices and allow to obtain sensitive personal data, so they must be submitted to some cautions. In this sense, Act 31/1995 on Prevention of Hazards at Work (art. 22) establishes the following rules and principles: the monitoring on workers' health must be performed within respect to the worker's privacy and dignity; the check-ups require previous consent of the employee, with the exception of explicit legal entitlement in regard to specific hazards or when strictly necessary either for the evaluation of the impact of working conditions on health or to prevent danger to the worker himself or to others[47]; the proportionality principle shall be abided, so medical examinations must be in correspondence with the risks to prevent and the less invasive as possible; finally, the results of health analyses must be treated confidentially and cannot be used for discriminating or harming the employee. Besides, information on an individual's physical condition is to be regarded under the framework of Organic Act 15/1999 on Personal Data Protection, therefore being also applicable not only its regulations on confidentiality of health data, but also all other guarantees foreseen in this legal piece.

There is also some important case law in regard to medical examinations. First of all, Judgement 196/2004 of the Constitutional Court declares the existence of a violation of the right to privacy in the case of an employee dismissed due to the results of a check-up, which revealed consumption of 'cannabis'[48]. The Court emphasises that the right to privacy involves several different conditions and limits to these examinations over workers, some of them explicitly endorsed by statutory law, and some others stated in this case law decision. In the first place, they must be voluntarily accepted, except in the case of a specific legal entitlement for establishing their obligatory character in regard to individual or collective rights and interests of other people or strict necessity. In the second place, valid consent to medical inspection requires earlier information on the aims and the extent of the checks to be made. Finally, the data obtained must be treated confidentially and cannot be used for different purposes to those mentioned in the information previously provided, unless the interested person gives express authorisation[49]. According to these requirements, the absence of 'informed consent' and the deviated use of the analysis results determined the unfairness of the dismissal in the concrete case judged.

39, 2009, p. 30 et seq.; THIBAULT ARANDA, J., 'La vigilancia del uso de internet en la empresa y la protección de datos personales', *Relaciones Laborales,* num. 5-6, p. 67 et seq.

[47] About these medical examinations of compulsory character, DE VICENTE PACHÉS, F., *El Derecho del Trabajador al respeto de su intimidad*, CES, 1998, p. 279 et seq.; MARTÍNEZ FONS, D., *La vigilancia de la salud de los trabajadores en la Ley de Prevención de riesgos laborales,* Tirant lo Blanch, 2002, p. 35 et seq.

[48] RUIZ CASTILLO, M. M., 'Derecho a la intimidad y controles de salud en la persona del trabajador: sentencia TC 196/2004, de 15 de noviembre', in GARCÍA MURCIA, J. (Ed.), *Derechos del trabajador y libertad de empresa. 20 casos de jurisprudencia constitucional,* Thomson- Aranzadi, 2013, p. 35 et seq.

[49] DE VICENTE PACHÉS, F., *El Derecho del Trabajador al respeto de su intimidad*, CES, 1998, p. 272 et seq.; MARTÍNEZ FONS, D., *La vigilancia de la salud de los trabajadores en la Ley de Prevención de riesgos laborales,* Tirant lo Blanch, 2002, p. 29 et seq.; FERNÁNDEZ LÓPEZ, M. F., 'La intimidad del trabajador y su tutela en el contrato de trabajo', in CASAS BAAMONDE, M. E./DURÁN LÓPEZ, F./CRUZ VILLALÓN, J. (Eds.), *Las transformaciones del Derecho del Trabajo en el marco de la Constitución Española*, La Ley, 2006, p. 658 et seq.

Moreover, Judgements 202/1999 and 153/2004 of the Constitutional Court refer to the protection of facts and figures related to health as personal and reserved information, covered by the protection of constitutional fundamental rights. Both cases deal with the employer's attempt to keep a file for registering and controlling employees' absences to work because of illness. The Court recognises that fighting against absenteeism at work is a legitimate aim. Nevertheless, these two judgements disclaim the described practice, which is to be considered as a violation of the rights to privacy (art. 18.1 Constitution) and to data protection (art. 18.4 Constitution)[50]. On the other hand, except in the case of some explicit legal entitlements, storing information on employee's medical circumstances without their consent (or against their will) is clearly in direct contradiction to statutory provisions contained in Organic Act 15/1999 on Personal Data Protection (art. 7).

8. Conclusions

Spanish Labour Law does not provide a fully detailed statutory regulation framework on the protection of employees' privacy and personal information. In the absence of sufficiently explicit and complete legal rules, judgements of the higher courts have accomplished a key role in this matter, delineating useful patterns in regard to disputes between the employer's legitimate interest in monitoring of work or using personal information and, on the opposite side, the need to safeguard the employees' rights. In general, this case law response by means of instruments like the proportionality principle or the standard referred to 'reasonable expectations of confidentiality' has allowed suitable solutions for conflicts arising from the use of new technologies.

In fact, this approach has shown enough adaptability and flexibility to adequately deal with new problems not sufficiently foreseen within written legislation. However, it is doubtful whether *ad hoc* balancing by judges -even through the proportionality principle and the criteria based on confidentiality expectations- is the most appropriate method to face every kind of challenges that the rapid innovation of information and communication tools entails in relation to conflicts amongst business interests and the protection of workers' privacy. As seen above, these case law solutions are quite often controversial and sometimes not completely unified, therefore leaving in the air some feeling of uncertainty[51]. In particular, as it has been already remarked, some of the commented latest judgements about interception of electronic communications by the employer have risen up an intense debate between dissenting opinions among judges and scholars, what undoubtedly points to the convenience of a more explicit statutory regulation.

Consequently, further completion of the existing legal regulation would surely be desirable, for instance, by providing some basic statutory rules on the employees' use of computers and the Internet at the workplace and on the extent and limits of the employer's control over it. Besides, it would be also recommendable to establish more explicit provisions on how legislation on data protection should be applied in the scope of the employment relationship. In this sense, the current revision process regarding the European Union common framework on the matter contained in Directive 95/46/EC could be a good

[50] RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., 'Intimidad del trabajador y contrato de trabajo', *Relaciones Laborales*, num. 8, 2004, p. 7.

[51] GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 18.

chance for more specifically and clearly addressing the application of these rulings in the workplace. Finally, regardless of that supplementary development, it seems opportune to remind that the rules and principles contained in Organic Act 15/1999 on Data Protection are already binding in that context, and cannot therefore be 'forgotten' or replaced by judges' own valuations when solving disputes through balancing between the employer's needs and the employee's rights, as it may have occurred sometimes[52].

[52] Pointing in a similar direction, GOÑI SEIN, J. L, 'Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos', *Justicia Laboral,* num. 39, 2009, p. 15 et seq.

Protection of Employees' Personal Information and Privacy in English Law

Gillian Morris
University College London

1. Introduction

1.1 The protection of employees' personal information and privacy has become an important area of debate in the light of technological developments which allow much greater scope for employers to monitor the activities of their workers both in and outside work. The problem is exacerbated by the blurring of the work/home divide as new technology permits workers to perform many roles away from the traditional workplace. One particular area of controversy in Britain has been the practice of employers examining the social media profiles of job applicants in order to vet them for inappropriate language or behaviour, sometimes demanding passwords or to be a social media 'friend' in order to access these profiles.[1] Until fairly recently many people seemed unaware of the potential implications for employment of their social media profiles[2] although the press publicity this has received may change behaviour. However the high profile lawsuits have focussed on the rather different issue of those who have disparaged their employers or their colleagues on-line, or revealed work-related misconduct such as feigning illness, and have been disciplined as a consequence.

1.2 The relative absence of litigation relating to the protection of employees' personal information may be due in part to the complexity and weakness of the law. As this paper shows, English law in this area is fragmented and offers inadequate protection in the employment sphere in many important respects

1.3 The paper begins by outlining the regulatory framework for the protection of employees' personal information and privacy. It then examines the purposes for which obtaining employees' personal information and monitoring their activities may be seen as appropriate and reasonable and how English law strikes a balance between business necessity and employees' privacy protection. There follows an analysis of the specific protections which apply during the hiring process; employment relationship; and following termination of that relationship. The concluding section evaluates the effectiveness of the current regulatory provisions and makes some proposals for reform.

[1] The term 'Britain' refers to England, Wales and Scotland. As Scottish law differs in some material respects from the law of England and Wales this paper deals specifically with 'English' law.
[2] A. Broughton, T. Higgins, B. Hicks and A. Cox *Workplaces and Social Networking: The Implications for Employment Relations*, Acas, 2010: p 22.

2. The Regulatory Framework

2.1 There is no single, comprehensive piece of legislation in England which regulates the protection of employee's personal information and privacy; rather the relevant law is derived from several different sources, some specific to the employment context, some of wider application. These sources are as follows:

(a) Human rights treaties and legislation
(b) Data protection legislation
(c) Legislation on the interception of communications
(d) Legislation on access to medical reports
(e) Legislation on information about criminal offences
(f) Equality legislation
(g) The common law.

This section provides a brief outline of the scope of protection afforded by each of these sources, together with the mechanisms of enforcement and remedies. Greater detail about the application of these provisions to particular stages of the employment relationship is given later in the paper. There are two recurring issues which it is appropriate to highlight at the outset, however. The first is the relevance of an individual's 'consent' in relation to the collection of personal information by employers under many of these provisions. The extent to which individuals are adequately protected in the event that they refuse consent or challenge whether the employer has the right to specified information is discussed in the concluding section of the paper. The second issue is that of the remedies available to the individual where the law is breached, which are not well-suited to the employment context.

Human rights treaties and legislation

2.2 The UK is a signatory to the *European Convention on Human Rights* ('ECHR') , Article 8 of which provides that:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. [3]

2.3 The European Court of Human Rights ('ECtHR') has made clear that 'private life' is not confined to the 'inner circle' in which individuals live but that it must 'comprise to a certain degree the right to establish and develop relationships with other human beings', a notion which extends to activities of a professional and business nature given that it is 'in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world'.[4] It is also clear that personal communications to and from business premises, including telephone calls, e-mails and information derived from monitoring internet usage, fall

[3] See also the Charter of Fundamental Rights of the European Union (2010), articles 7 (respect for private and family life) and 8 (protection of personal data).
[4] *Niemietz* v *Germany* judgment of 16 December 1992, (1993) 16 EHRR 97, para 29.

within Article 8.[5] One important question is the extent to which the scope of the right to respect for private life can be shaped by the employment contract; there is some support in the cases for the view that a worker's expectation of privacy may be removed by agreement between the parties, or possibly even by a warning on the part of the employer, so allowing the employer unilaterally to define the 'private' zone.[6] However in other cases (outside the employment field) the court has emphasised that 'a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor'.[7] A more transparent approach than permitting the scope of the right to respect for private life to be limited by contract or a warning, and one consistent with its status as a fundamental right, is to require any interference to be justified under Article 8(2).[8] It is also possible that some more extreme forms of interference with a worker's private life, such as surveillance of staff toilets, could be regarded as 'degrading treatment', contrary to Article 3 of the ECHR, which cannot be justified in any circumstances.

2.4 If the ECtHR finds that a right protected by the ECHR has been violated and the internal law of the respondent state allows only partial reparation to be made the Court may award 'just satisfaction' to the injured party which may include awards for both pecuniary and non-pecuniary loss, such as the stress and anxiety caused by the interference with the right.[9] The Court has held that the State's obligations under Article 8 are not confined to abstention from interference but 'may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves.' [10]

2.5 The *Human Rights Act* ('HRA') 1998 gives 'further effect' in the UK to rights and freedoms guaranteed under the ECHR. Article 8 has an impact on English law in three major ways:

(a) The HRA requires all legislation (whenever passed) to be 'read and given effect in a way which is compatible' with 'the Convention rights' '[s]o far as it is possible to do so'.[11] Article 8 may, therefore, influence the interpretion given to the legislation discussed below.[12] If primary legislation cannot be read compatibly with a Convention right (or, in the case of subordinate legislation which is incompatible, the primary legislation prevents removal of the incompatibility) a court may make a 'declaration of incompatibility'.[13] This

[5] *Copland* v *UK* judgment of 3 April 2007, (2007) EHRR 37, para 41.
[6] *Halford* v *UK* judgment of 25 June 1997, (1997) 24 EHRR 523, para 45; *Copland* v *UK*, above, para 42.
[7] *PG and JH* v *UK* judgment of 25 September 2001, (2001) ECHR 550.
[8] See generally G.S. Morris 'Fundamental Rights: Exclusion by Agreement?' 30 *Industrial Law Journal* 49. For a recent review of ECHR case law see Frank Hendrickx and Aline van Bever 'Article 8 ECHR: Judicial Patterns of Employment Privacy Protection' in *The European Convention on Human Rights and the Employment Relation* ed F Dorssemont, K Lörcher and I Schömann, 2013.
[9] See *Copland* v *UK*, above, note 5, for an example of an award for non-pecuniary damage in the employment context.
[10] *X and Y* v *The Netherlands* judgment of 26 March 1985, (1985) ECHR 4. See *Köpke* v *Germany* judgment of 5 October 2010, [2010] ECHR 1725 on the State's positive obligation relating to video surveillance of workers.
[11] HRA 1998, s 3.
[12] For a recent example of Article 8 arguments being used to influence the interpretation of the Data Protection Act 1998 see *Vidal-Hall and others* v *Google Inc* [2014] EWHC 13 (QB), [83]-[103].
[13] HRA 1998, s 4. For limits to the capacity to read legislation compatibly with Convention rights see *Ghaiden* v *Godin-Mendoza* [2004] UKHL 30.

does not affect the continuing validity of the offending legislation but a special 'fast-track' procedure may be used to amend it.[14]
(b) The Act makes it unlawful for a 'public authority' (including a court or tribunal) to act in a way which is incompatible with a Convention right unless, as a result of the provisions of primary legislation, it could not have acted differently. 'Victims' of such acts may bring proceedings against a public authority, or rely upon Convention rights in any other proceedings. Thus, workers employed by 'public authorities' who allege that their employer has violated their rights under Article 8 may bring proceedings directly against them; if it upholds the claim the court may grant such remedy within its powers as it considers 'just and appropriate', taking into account, if it decides to award damages, the principles applied by the ECtHR.[15]
(c) The application to courts of the duty not to act unlawfully in (b) above has been interpreted to mean that Convention rights should be taken into account in common law proceedings, regardless of the legal identity of the claimant or defendant. Article 8 has been highly instrumental in recent cases relating to breach of confidence to provide a remedy for unauthorised disclosure of private information and although there is as yet no tort of breach of privacy *per se* there is some judicial support for a tort of misuse of private information.[16] The requirement for courts and tribunals not to act incompatibly with Convention rights may also be material in interpreting the contract of employment. There is a strong argument that employees should not be required to obey instructions which breach their Article 8 rights and that conduct by an employer that breached those rights would breach the implied contractual duty of trust and confidence.[17]

Data protection legislation

2.6 The *Data Protection Act* ('DPA') 1998 was enacted to implement EC Directive 95/46 on personal data. All those who determine the purposes for, and manner in, which 'personal data' is to be 'processed' ('data controllers') have obligations under the DPA; the Act therefore is capable of covering, but is not confined to, employers. The term 'data' does not include all the information which employers may obtain about their workers, however. It covers information which is 'being processed by means of equipment operating automatically in response to instructions given for that purpose', is recorded with the intention of being processed by such means; or 'is recorded as part of a relevant filing system or with the intention that it should form part of' such a system'. A 'relevant filing system' means 'any set of information relating to individuals' to the extent that 'the set is structured … in such a way that specific information relating to a particular individual is readily accessible'.[18] The English courts have held that manual records are covered only if they are of 'sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system', requiring a filing system so referenced or indexed that it

[14] HRA 1998, s 10.
[15] As above, ss 6-8. There is voluminous case law and academic literature on the meaning of 'public authority'. As this is of little relevance to the subject-matter of this paper it is not explored further here.
[16] See *Campbell* v *MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457; *OBG Ltd* v *Allen and Douglas v Hello!* [2008] 1 AC 1 and other cases cited in *Vidal-Hall,* above, note 11. For a sceptical view of the impact of the HRA 1998 on the common law in general see Jane Wright, 'A Damp Squib? The Impact of Section 6 HRA on the Common Law: Horizontal Effect and Beyond' [2014] *Public Law* 289.
[17] See S. Deakin and G.S. Morris, *Labour Law* 6th edn, 2012, paras 4.105-4.107 for this duty.
[18] Data Protection Act 1998, s 1. Information forming part of an 'accessible record' as defined by s 68 is also covered, as is recorded information held by a public authority.

enables the data controller's employee 'to identify at the outset of his search with reasonable certainty and speed the file or files in which the specific data relating to the person requesting the information is located … without having to make a manual search of them'.[19] This approach focusses, therefore, on the method of recording information and the ease with which it can be found rather than its sensitivity or importance to the individual worker and constitutes a major gap in data protection.[20] 'Personal data' means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession, or likely to come into the possession, of the data controller; also included is any expression of opinion about, and any indication of the intentions of any person in respect of, the individual.[21] The 'processing' of data is widely defined to cover 'obtaining, recording or holding the information or data or carrying out any operation or set of operations' on it; this specifically includes retrieving, consulting, using, erasing or destroying data.[22]

2.7 'Data controllers' must comply with eight 'data protection principles' in respect of personal data.[23] Those of greatest relevance to protection of personal information in the employment context are as follows:

(a) The duty to process data 'fairly and lawfully' (the 'first principle'). This duty requires the data subject to consent to the processing or one of a number of other conditions, discussed in paragraph 3.2 below, to be met. An additional condition (including 'explicit consent')[24] must be met in the case of 'sensitive personal data', defined as information as to the racial or ethnic origin of the data subject; his or her political opinions, religious beliefs or other beliefs of a similar nature; whether he or she is a member of a trade union; his or her physical or mental health or condition or sexual life; or the commission or alleged commission of a criminal offence or any proceedings for any such offence, the disposal of such proceedings or the sentence of the court.[25] The employer must ensure so far as practicable that the data subject is provided with, or has readily available to him or her, specified information, including the purposes for which the data are intended to be processed and any further information which is necessary in the circumstances to enable processing to be fair.[26]

(b) Personal data must be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes (the 'second principle').

(c) Personal data must be adequate, relevant and not excessive in relation to the purposes for which they are processed (the 'third principle').

---

[19] *Durant* v *Financial Services Authority* [2004] FSR 28, Auld LJ at [48]. The 'property rights' of data controllers, who were allowed only a limited time to respond to requests for information and entitled only to a limited fee (see para 5.11 below), weighed heavily with the Court of Appeal.

[20] The Information Commissioner (see para 2.8 below) considers that the system 'must amount to more than a bundle of documents about each worker filed in date order' and that a personnel file with nothing to guide a searcher to where specific information such as the worker's leave entitlement can be found is unlikely to be covered by the DPA 1998: *Employment Practices Data Protection Code* (2005).

[21] DPA 1998, s 1.

[22] As above.

[23] DPA 1998, s 4; Scheds 1-3.

[24] See para 7.2 below for discussion of 'consent' and 'explicit consent'.

[25] DPA 1998, s 2.

[26] DPA 1998, Sched 1, Part II.

(d) Personal data must be accurate and, where necessary, kept up to date (the 'fourth principle').
(d) Personal data processed for any purposes must not be kept for longer than is necessary for those purposes (the 'fifth principle').
(e) Personal data must be processed in accordance with the rights of data subjects under the Act (the 'sixth principle'), such as the rights to be supplied with information on request or to require, in specified conditions, that the employer should cease processing the data (see paragraph 5.11 below).

2.8 The DPA 1998 provides for the appointment of an 'Information Commissioner' who performs various duties under the Act, including publishing codes of practice.[27] Published codes include an Employment Practices Data Protection Code (the 'EPDPC') which makes recommendations on recruitment, employment records, monitoring at work, and information relating to workers' health. These codes are not legally binding but are likely to be cited by the Commissioner in connection with any enforcement action taken by him.

2.9 The Information Commissioner is obliged to make an assessment as to whether it is likely that processing is being carried out in accordance with the DPA 1998 at the request of the person directly affected or another person acting on his or her behalf.[28] The Commissioner can also make a range of orders to enforce the Act.[29] The main ones potentially relevant to employment are information notices;[30] enforcement notices;[31] and monetary penalty notices (up to a maximum of £500,000).[32] In addition the DPA creates a number of specific criminal offences, including failing to register as a data controller with the Information Commissioner and breaching the 'enforced subject access' prohibition described in paragraph 4.2 below. Finally, an individual who suffers damage by reason of any contravention of the DPA 1998 is entitled to compensation for that damage, although the data controller can defend the action by proving that he or she had taken all reasonable care to comply with the requirement.[33] It is unclear whether 'damage' is limited to pecuniary loss[34] or whether it extends to non-pecuniary loss such as stress and anxiety; there are persuasive arguments that it should so extend.[35] In practice enforcement notices are relatively rare, although they were issued in 2009 to some companies in the

[27] As above, s 51.
[28] As above, s 42.
[29] See generally Rosemary Jay, *Data Protection Law and Practice*, 4th edn, 2012, chapter 20.
[30] A notice to provide the Commissioner's Office with specified information within a specified period to determine whether the data protection principles are being followed: DPA 1998, s 43.
[31] A notice requiring the data controller to take specified steps such as destroying data or refraining from processing specified data , which may be served if the Information Commissioner is satisfied that a data controller has contravened any of the data protection principles: DPA 1998, s 40.
[32] These may be issued if there has been a 'serious' contravention of any of the data protection principles of a kind likely to cause substantial damage or substantial distress and either the data controller knew or ought to have known that there was a risk of a contravention of this nature which it failed to take reasonable steps to prevent or the contravention was deliberate: DPA 1998, s 55A. There is a right of appeal against the decision to issue an information, enforcement or monetary penalty notice.
[33] DPA 1998, s 13.
[34] *Johnson* v *MDU* [2007] EWCA Civ 262, (2007) 96 BMLR 99.
[35] *Murray* v *Express Nwespapers Ltd* [2008] EWCA Civ 446, [2009] Ch 481, [63]; see also *Vidal-Hall and others* v *Google Inc*, above, note 12, at [83]-[103] which refers to the Reasoned Opinion to the UK issued by the European Commission which requested the UK to apply the right to compensation for 'moral damage' when personal information is used inappropriately (press release 24 June 2010) .

construction industry which had purchased information on workers whose trade union activity and other details appeared on a 'blacklist' of workers compiled by an organisation called the 'Consulting Association'.[36] Litigation is currently being pursued by their union on behalf of individuals known to have been affected by this 'blacklisting', which includes a claim for damages under the DPA 1998. I have been unable to find any other reported cases of individuals suing for damages under the Act in the employment context.

Legislation on the interception of communications

2.10 The *Regulation of Investigatory Powers Act* ('RIPA) 2000 regulates the interception of communications and was designed to implement the EC Telecommunications Data Protection Directive.[37] The Directive (now succeeded by the Privacy and Electronic Communications Directive[38]) requires the confidentiality of electronic communications to be respected but allows for certain derogations, of which interceptions for business purposes is one. Like the DPA, RIPA covers employers but also applies beyond the employment context.

2.11 RIPA permits the sender or recipient of a communication on a private telecommunications network to seek an injunction against, or damages for any loss incurred from, an employer who intercepted a communication to or from its own system if the interception was without 'lawful authority'.[39] RIPA specifies a range of circumstances where 'lawful authority' is deemed to exist. Those most relevant to employment are set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,[40] which allow interception of communications on the system used for the purposes of a business by, or on behalf of, the person carrying on the business where specified conditions are met. These Regulations are discussed in greater detail in paragraph 5.4 below.

Access to medical reports

2.12 The *Access to Medical Reports Act* ('AMRA') 1988 gives individuals a right of access to reports on their health (physical or mental) by a medical practitioner responsible for their clinical care which are to be supplied for employment or insurance purposes.[41] Individuals are entitled to see a report before it is supplied and to request amendments to any part which they consider incorrect or misleading. The medical practitioner may refuse to make the amendments but must, if the individual so requests, attach a statement of the individual's views to the report.[42] An employer or prospective employer who proposes to apply for a report must notify the worker in advance of this and must inform him or her of

[36] See K Ewing, *Ruined Lives: Blacklisting in the UK Construction Industry*, Institute of Employment Rights, 2009. In 2010 legislation was introduced specifically prohibiting blacklisting: see Deakin and Morris, above, note 17, paras 8.27-8.32.
[37] EC Directive 97/66 EC.
[38] Directive 2002/58/EC.
[39] RIPA 2000, s. 1(3). 'Private telecommunications system' and 'interception' are defined in s. 2.
[40] SI 2000 No 2699.
[41] AMRA 1988, s 1, 2. Note that the restriction to a practitioner 'responsible for their clinical care' may exclude the employer's occupational health doctor: see further para 4.4 below.
[42] As above, ss 4,5. There are certain exemptions to the right of access, including where the practitioner considers that disclosure would be likely to cause serious harm to the physical or mental health of the individual or others or would indicate the intentions of the practitioner in respect of the individual: s 7. The report cannot then be supplied to the employer unless the individual explicitly consents to this.

the right to withhold consent; of the rights relating to access to the report and its amendment; and of the right, once given access, to withhold consent to the report being supplied.[43] Individuals who consider that their rights under the Act have been, or are likely to be, breached can apply to the courts which can order compliance with the Act.[44] Rights under AMRA need to be considered in the context of other restrictions on medical reports discussed in paragraphs 4.3 and 4.4 below.

Information about criminal offences

2.13 The Rehabilitation of Offenders Act ('ROA') 1974 provides that after periods ranging between two and 11 years, depending on the sentence, criminal convictions become 'spent', although prison sentences exceeding 48 months are excluded.[45] ROA applies in the employment context although it also applies more widely. For the purposes of employment, an individual is entitled to conceal a 'spent' conviction in answer to a question from a prospective employer and 'the person questioned shall not be subjected to any liability or otherwise prejudiced in law by reason of any failure to acknowledge or disclose a spent conviction or any circumstances ancillary to a spent conviction'.[46] In this context, therefore, an individual may give false information without this giving rise to the normal legal consequences of misrepresentation. There are numerous exemptions to the right to conceal a 'spent' conviction in relation to posts in the criminal justice system and other areas of public employment, the professions, and other occupations involving trust and confidence such as those in the medical and financial service sectors.[47]

Equality legislation

2.14 The Equality Act ('EqA) 2010 makes it unlawful to discriminate against an individual because of a 'protected characteristic' in the area of employment[48] and in several other fields, including the provision of goods and services. The protected characteristics are age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; and sexual orientation.[49] Although (pre-employment health inquiries apart)[50] it is not unlawful under EqA to obtain information relating to protected characteristics it is unlawful to use such information to discriminate against individuals and a number of these characteristics[51] constitute 'sensitive personal data' under the DPA 1998. Individual equality rights in the employment field are enforced by complaining to an employment tribunal which may award a declaration of rights; financial compensation to put the claimant in the position he or she would have been in had the discrimination not occurred, including injury to feelings; and a

[43] As above, s 4.
[44] As above, s 3.
[45] ROA 1974, s 5.
[46] ROA 1974 ,s 4(2)(b).
[47] Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, SI 1975/1023.
[48] The legislation covers persons employed under a contract of employment, apprenticeship or a contract 'personally to do work': EqA 2010, s 83(2).
[49] EqA 2010, s 4.
[50] See para 4.3 below.
[51] The racial or ethnic origin of the data subject; religious beliefs or other beliefs of a similar nature; and his or her physical or mental health or condition or sexual life.

recommendation that the respondent takes steps to obviate or reduce the adverse effect of the matter to which the proceedings relate on the complainant or any other person.[52]

Common law

2.15 Misuse of employees' personal information may give rise to actions for breach of confidence; or (possibly) the tort of misuse of private information (see paragraph 2.5 above).[53] Recent proceedings of this kind have focussed on alleged intrusions into the private lives of 'celebrities' by the media rather than by employers and although in theory workers could seek an injunction or damages from the courts, in practice the expense of doing this, and complexity of the law, makes this an unlikely option. Where there is a subsisting employment relationship a failure to protect an employee's personal information would almost certainly breach the contract of employment, and it is strongly arguable that any conduct by an employer that breached the employee's rights under Article 8 of the ECHR would breach the implied contractual duty of trust and confidence.[54]

3. Obtaining Information and Monitoring Employees: Legitimate Purposes

3.1 With a few exceptions (such as tax and social security law) English law does not identify the particular purposes for which it is proper and reasonable for employers to obtain employees' personal information. Rather determining what is proper and reasonable is decided by applying general criteria to particular situations. This section starts by outlining those general criteria and then gives some examples of how they may apply in given situations. It should be noted that, with specific exceptions, the law does not directly prohibit employers *seeking* to obtain information to which they may not be entitled, a considerable gap in protection.

3.2 All the English legislation directly regulating the provision of employees' personal information and monitoring of employees envisages circumstances where an employer's legitimate business interests may allow information to be obtained even if the employee does not consent to this. Under the DPA 1998 the tests of whether personal data is processed 'fairly and lawfully' include the processing being 'necessary' for one of the following:

(1) the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract;

(2) compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract; and

(3) 'the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.'[55]

[52] EqA 2010, s. 124.

[53] See *Campbell* v *MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457; *OBG Ltd* v *Allen and Douglas v Hello!* [2008] 1 AC 1 and other cases cited in *Vidal-Hall,* above, note 12.

[54] This would entitle the employee to claim damages and, probably, to terminate the contract without notice.For discussion of this complex area see Deakin and Morris, above, note 17, chapter 5.

[55] DPA 1998, Sched 1, para 1; Sched 2.

The first two of these tests are very specific. An example of (1) would be obtaining a worker's bank account details for payment purposes; an example of (2) obtaining the worker's tax and social security references so that appropriate statutory deductions from pay could be made. The third is much more open-ended and, according to the UK Supreme Court (UKSC) in *South Lanarkshire Council* v *The Scottish Information Commissioner*, requires three questions to be addressed:

> (a) is the employer pursuing a legitimate interest or interests?
> (b) is the processing involved necessary for the purposes of those interests?
> (c) is the processing unwarranted in this case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject?[56]

In the case of 'sensitive personal data' one of a number of additional tests must also be satisfied. Other than 'explicit consent' those most likely to apply in the context of employment are that:

> (1) the processing 'is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment' and
> (2) the information 'has been made public as a result of steps deliberately taken by the data subject'.

A further test allows monitoring of information relating to racial or ethnic origin in order to promote equality of opportunity.[57]

3.3 In *South Lanarkshire Council* the UKSC held, following the decision of the European Court of Justice in *Rechnungshof* v Ö*sterreighischer Rundfunk* (the *Austrian Radio* case),[58] that if data processing involves an interference with the data subject's right to respect for private life under Article 8(1) of the ECHR then, to be lawful under the DPA 1998, Article 8(2) must be satisfied. Article 8(2) requires the restriction to be 'in accordance with the law'; to pursue a legitimate aim; and to be 'necessary in a democratic society'. 'In accordance with the law' requires the restriction not only to have a basis in domestic law but also to be adequately accessible and formulated with sufficient precision to enable the individual to regulate his conduct and to be able to foresee, to a degree that is reasonable in the circumstances, the consequences which a given course of action may entail'.[59] In the employment context these criteria suggest that any restrictions on private life should be clearly specified in writing and that this document should be made available to all those to whom the restrictions apply. 'Legitimate aims' under Article 8 include 'protection of the rights and freedoms of others'; protection of the employer's property interests against theft[60] and the safety of fellow workers and passengers[61] have been regarded by the ECtHR as legitimate aims. For an interference with the right to be 'necessary in a democratic society' there must be a 'pressing social need' for it; the interference must be 'proportionate to the legitimate aim pursued' and the reasons for it must be 'relevant and sufficient'.[62]

---

[56] *South Lanarkshire Council* v *The Scottish Information Commissioner* [2013] UKSC 55; [2013] IRLR 899, Lady Hale at [18].
[57] DPA 1998, Sched 1, para 1; Sched 3.
[58] Case 465/00, C-138/01, C-139/01 [2003] ECR 1-4989.
[59] *Sunday Times* v *UK* judgment of 26 April 1979, (1979-80) 2 EHRR 245, para 49.
[60] *Köpke* v *Germany* decision of 5 October 2010, [2010] ECHR 1725.
[61] *Madsen* v *Denmark*, App 58341/00, 7 November 2002.
[62] *Handyside* v *UK* judgment of 12 December 1976, (1979-80) 1 EHRR 737, paras 48-50.

3.4 It is possible that data processing may not involve an interference with an individual's private life. This may be on the basis that the individual has already placed the information in the public domain (it is hard to see that obtaining information from an individual's open-access web-site would intrude on privacy, for example),[63] or if the court adopts the view that the employer has shaped the scope of 'private life' by contract or a warning (see paragraph 2.3 above). Even then, however, the UK courts have emphasised that the requirement in the DPA 1998 for the processing of any personal data (consent aside) to be 'necessary' for a specified purpose means that it must serve a 'pressing social need' and be 'both proportionate as to means and fairly balanced as to ends'.[64]

3.5 Beyond these general principles there is very little 'hard law' as to the purposes for which employers may properly and reasonably obtain information and how these purposes are to be balanced with employees' privacy protection. The Information Commissioner's Employment Practices Data Protection Code ('EPDPC'), referred to in paragraph 2.8 above, considers in detail how employers should decide what information they need at particular stages of the employment relationship and emphasises that they should always ask themselves why they require it and whether they are asking for more information than they really need . However, whilst it provides very useful guidance, this Code has no legal status. The paragraphs that follow are, therefore, based on the application of the general principles outlined in paragraphs 3.2 - 3.4 above, with examples taken from the EPDPC, and the 'Supplementary Guidance' ('SG') to it, where appropriate .

3.6 Looking first at recruitment, this will necessarily involve an employer collecting a basic level of information about all applicants, such as their contact details, qualifications and previous experience. It is hard to see how this could prejudice applicants' legitimate interests. However the collection of more detailed information, such as identity checks, may be appropriate only in relation to short-listed candidates and more intrusive forms of pre-employment vetting appropriate (if at all) only in relation to a candidate it is intended, subject to satisfactory vetting, to appoint. Specific restrictions on personal information in the hiring process are dealt with in section 4 below.

3.7 Once employment starts, employers will need to keep records of employees' attendance/absence from work in order to calculate pay and allowances. However the EPDPC/SG recommends that, work-related injuries aside,[65] employers should either avoid keeping records of employees' specific illnesses or injuries, which constitute 'sensitive personal data', or, if such records are needed to monitor the ability of an individual to work or to detect hazards at work, should at least segregate them from absence data. Keeping records for disciplinary purposes is also legitimate and indeed, employers are advised to keep such records[66] although disciplinary procedures should specify whether a disciplinary sanction, such as a warning, that has expired should be removed from the record. Where an undertaking is being transferred there is now a statutory obligation on the transferor to supply 'employee liability information' to the transferee which identifies the employees to

[63] See also DPA 1998, Sched 3, para 5.

[64] *Corporate Officer of the House of Commons* v *Information Commissioner* [2008] EWHC 1084, [1009] 3 All ER 403, cited with approval in *South Lanarkshire Council* v *The Scottish Information Commissioner*, above, note 56, at [19]; see also [27].

[65] Employers are advised to maintain an 'accident book' as part of their health and safety policy and there is a statutory duty to report some injuries and diseases: see Reporting of Injuries, Diseases and Dangerous Occurances Regulations 2013 SI 2013 No 1471.

[66] See Acas Code of Practice *Disciplinary and Grievance Procedures* (2009), foreward; *Acas Guide: Discipline and Grievances at Work* (2009).

be transferred and includes specified information about them including their age and any disciplinary procedure against them.[67] This is exempt from the non-disclosure provisions of the DPA 1998[68] but other obligations relating to personal data will need to be observed.

3.8 It is generally recognised that employers have a legitimate interest in monitoring their employees' performance at work, including the output and quality of their work and whether they are following safe working practices. However the method by which this is done should be proportionate and not unnecessarily intrusive. The EPDPC suggests that employers should conduct an 'impact assessment' which involves looking at the purposes behind monitoring and the benefits it is likely to deliver; identifying any likely adverse impact; considering the alternatives to monitoring; and then judging whether monitoring is justified. The EPDPC emphasises the importance of ensuring that workers are aware that monitoring is taking place and why, unless exceptional circumstances justify covert surveillance (see paragraph 5.9 below). The protection of the employer's trade secrets and other property interests would be a proper reason for monitoring but probably only on a targeted basis following specific intelligence that such property is at risk from a particular worker or group of workers. Specific issues relating to video surveillance and the monitoring of electronic communications are dealt with in paragraphs 5.3-5.7 below.

4. Personal Information Protection in the Hiring Process

4.1 Job applicants are particularly badly protected in English law. The only areas where employers are specifically restricted in asking for information relate to health and criminal records and even then the restrictions are fairly narrow.

Criminal proceedings

4.2 Under the *Rehabilitation of Offenders Act* ('ROA') 1974, described in para 2.13 above, (excepted employments apart) an individual is entitled to conceal a 'spent' conviction without being subject to any liability for non-disclosure.[69] The ROA itself does not make it unlawful for the employer to *seek* to obtain this information but obtaining it could breach the principle in the DPA 1998 that data should be processed 'fairly and lawfully' and support a claim for damages if the applicant was denied a job as a result.[70] Moreover, it is a criminal offence under the DPA for an employer "in connection with" the recruitment of a person as an employee, or their continued employment, to require that person (or a third party) to supply the employer with specified information obtained under the right of access to data described in paragraph 5.11 below.[71] The information covered by this ban on enforced subject access relates, broadly speaking, to criminal records and

[67] Transfer of Undertakings (Protection of Employment) Regulations 2006, SI 2006 No 246, reg 11, as amended. Where due diligence exercises outside these provisions are being undertaken, or information is sought beyond the scope of TUPE reg 11, the Information Commissioner recommends that wherever possible information about workers should be anonymised.
[68] DPA 1998, s 35.
[69] ROA 1974, s 4(2)(b).
[70] DPA 1998, s 13.
[71] DPA 1998, s 56. See Jay, above, note 29, chapter 27 for discussion of this provision, which was introduced to prevent what the then Data Protection Registrar saw as a growing practice of individuals being required by employers to use their right of access to obtain a copy of their criminal record from the police. The EPDPC goes beyond the Act in stating that applicants should not be forced to use their subject access rights to obtain *any* records from another organisation (para 1.3.1).

national insurance records which can reveal if time has been spent in custody or gaps in employment (although at the time of writing only part of this provision has been brought into force).[72] Of more general current relevance, the commission or alleged commission of a criminal offence or any proceedings for any offence committed by an individual; the disposal of such proceedings; or the sentence of the court constitute 'sensitive personal data' under the DPA; these matters are therefore subject to the tighter controls relating to the processing of such data set out in paragraph 3.2 above. The EPDPC states that employers should seek information about an applicant's criminal convictions only to the extent that this has a direct bearing on his or her suitability for the job in question.

Health and medical information:

4.3 The *Equality Act* ('EqA') 2010 makes it unlawful for a person (A) to 'whom an application for work is made' to 'ask about the health of the applicant (B)' either 'before offering the work to B' or, where A is not in a position to offer the work, 'before including B in a pool of applicants from whom A intends (when in a position to do so) to select a person to whom to offer work'.[73] Whether or not a person has a disability is an aspect of that person's health,[74] and the provision is designed to ensure that disabled applicants are assessed objectively for their ability to do the job in question.[75] However the protection it offers is qualified. First, the fact that an employer has asked an applicant about his or her health does not give the applicant an automatic right of action, although if the applicant takes a case to an employment tribunal and contends that the employer's conduct in reliance on information given in response to such a question amounts to direct discrimination the employer will then bear the burden of proving that it did not discriminate.[76] Second, there are a number of situations in which employers can continue to make pre-employment health checks under EqA 2010. These include where the purpose of the question is to establish whether B 'will be able to comply with a requirement to undergo an assessment' or in establishing whether A will need to make reasonable adjustments in connection with such a requirement; in establishing whether 'B will be able to carry out a function that is intrinsic to the work concerned' once reasonable adjustments have been made; and in monitoring diversity in the range of persons applying to A for work.[77]

4.4 A person's 'physical or mental health or condition' constitutes 'sensitive personal data' under the DPA 1998 so the employer would need to satisfy the tests discussed in paragraph 3.2 above to obtain such information. The inclusion of 'condition' as well as health seems wide enough to include pregnancy; whether biometric data, particularly genetic data, is covered is unclear.[78] The *Access to Medical Reports Act* ('AMRA') 1988, outlined in paragraph 2.12 above, will also need to be complied with if the employer seeks

[72] The provision relating to those barred from working with children and vulnerable adults is now governed by a specific regime (see para 4.7 below). As Jay explains, the aim is that, where appropriate, employers have legitimate access to information under a regulated channel.
[73] EqA 2010, s 60(1).
[74] Above, s 60(13).
[75] Equality and Human Rights Commission, *Code of Practice on Employment* (2011), para 10.27.
[76] Above, s 60(3)-(5). The prohibition on asking questions can be enforced directly by the Equality and Human Rights Commission: s 60(2), 120(8).
[77] Above, s 60(6),(7).
[78] The draft EU General Data Protection Regulation, art 9, specifically refers to 'genetic data': COM (2012) 11 final.

a medical report at the hiring stage, although as it is limited to reports provided by a medical practitioner 'who is or has been responsible for the … [applicant's] … clinical care' it would probably not apply to a report by the employer's occupational health service with which the applicant had no prior relationship. A weakness of both the DPA and AMRA is that there is no protection against discrimination in either Act for an applicant on the ground that they have refused to comply with an employer's request for a report or other data.

Information on other matters

4.5 English law does not specifically prevent an employer *requesting* information about matters beyond those discussed above, although the DPA 1998 applies to *obtaining* and otherwise processing personal data or 'sensitive personal data'. In particular there are no restrictions like those in ROA 1974 relating to a candidate's civil litigation history, including employment litigation, although it may be a breach of the Equality Act 2010 not to hire someone because they have previously brought proceedings under that Act.[79] Civil litigation history (unlike criminal proceedings) does not constitute 'sensitive personal data' for the purposes of the DPA 1998. Employers can obtain an individual's 'public credit record' which includes electoral roll information (including address), insolvency records, county court judgments and any notices of correction. They have no right of access to an individual's credit history beyond this, such as their payment record, but if an employer insisted on a candidate providing such information and the candidate refused there seems nothing to prevent the employer declining to recruit the individual for that reason.

4.6 The fact that an employer sought information about matters that constitute 'protected characteristics' under EqA 2010 (see para 2.14 above) could be used in evidence in a claim of direct discrimination if the employer decided subsequently not to employ the individual, although in practice comparatively few discrimination cases have been brought in connection with recruitment, which raise particular problems of proof.[80] (It would be easier to show discrimination if the employer sought particular information from some applicants and not others, for example selectively asking about religious beliefs on the basis of applicants' race or colour.) Employers who access applicants' social media profiles are likely to learn about many of their characteristics, such as their age, marital status, sexual orientation, and ethnicity. However mounting a successful discrimination claim on the basis of this evidence alone would be extremely difficult. It is unlawful to deny an individual employment on the basis of their union (or non-union) membership (including membership of a specific union).[81] Again inquiring about an applicant's union membership status could constitute evidence of discrimination.[82] Specific measures to prohibit the compilation of 'blacklists' of union members and activitists to which employers can subscribe have recently been introduced following exposure of the

[79] EqA 2010 s 27 states that a person A victimises another person B if A subjects B to a detriment because B does a protected act (or A believes that B has done or may do a protected act), which includes bringing proceedings under EqA 2010 or doing any other thing in connection with it and s 39 makes it unlawful to victimise a person by, among other things, not offering them employment. The point has not been tested in the courts.

[80] Broughton *et al*, above, note 2, p 10.

[81] See generally Deakin and Morris, above note 17, paras 8.21-8.37 for detailed discussion of this area.

[82] This also constitutes 'sensitive personal data' under the DPA 1998, s.2.

widespread use of such blacklists in the construction industry.[83] Although 'religion or belief' are 'protected characteristics' under EqA 2010 there is no express protection at the hiring stage against discrimination on the basis of political views.[84] The English courts have held that political opinions which are capable of amounting to a 'philosophical belief' fall within the term 'belief' but not membership of a political party *per se*.[85] An individual's 'political opinions' are 'sensitive personal data' under the DPA 1998.

4.7 English law does not in general specify in positive terms the information that an employer is entitled to obtain regarding its employees, although all employers are required to check that workers have the legal right to work in the UK which involves scrutiny of official documentation such as passports or residence or work permits.[86] However there are particular provisions which govern particular occupations: candidates for appointment as police officers, for example, can be required to undertake tests for substance misuse.[87] A government 'Disclosure and Barring Service' is designed to prevent people from being recruited to work with vulnerable groups by processing requests for criminal record checks and placing people on children's and adults' 'barred lists' which employers must check before recruiting staff.

5. Personal Information and Privacy Protection during the Employment Relationship

5.1 The general principles which govern the purposes for which employers are entitled to obtain employees' personal information have been outlined in section 3 above. In addition, once the employment relationship has started the contractual terms that govern it may be significant in demonstrating the worker's 'consent' or 'explicit consent' to the employer obtaining and holding information.[88] The only direct restriction on contract terms in this area[89] is contained in the DPA 1998 which makes void any contractual requirement that an individual should use their right of subject access to supply a 'health record', defined as any record consisting of 'information relating to the physical or mental health or condition of an individual" made "by or on behalf of a health professional in connection with the care of that individual".[90] This definition is wide enough to cover a record compiled by a previous employer's occupational health adviser as well as by the worker's own physician.

[83] Employment Relations Act 1999 (Blacklists) Regulations 2010, SI 2010/493. See para 2.9 above and Deakin and Morris, above, note 17, paras 8.27-8.32.
[84] In 2013 the UK Government removed the requirement of a qualifying period of employment to bring an unfair dismissal claim where the dismissal relates to the employee's 'political opinions or affiliation' (Employment Rights Act 1996, s 108, as amended) in response to the ECtHR decision in *Redfearn* v *UK* judgment of 6 November 2012, (2012) ECHR 1878 that there was a breach of Article 11 of the ECHR because the applicant had been dismissed because of his membership of the British National Party with no right for the justification for this to be considered by a court or tribunal.
[85] *Grainger* v *Nicolson* [2010] IRLR 4, EAT; *Baggs* v *Fudge* ET/1400114/05.
[86] See generally Home Office, *Full guide on preventing illegal working in the UK for employers*, 2013.
[87] The Police Regulations 2003, SI 2003/527.
[88] See further paras 2.3 above and 7.2 below.
[89] See also para 2.5 for the effect of Article 8 of the ECHR under the HRA 1998 on interpretation of the contract.
[90] DPA 1998, ss 57, 68. Employment legislation generally provides that an agreement by an individual to waive protective rights is void: see, for example, Employment Rights Act 1996, s. 203(1).

5.2 Where the employee has not 'consented' to the provision of personal information the principles that will govern whether the employer is entitled to obtain personal information will be those set out in paragraphs 3.2 - 3.4 above. Some examples of the types of information that employers would seem entitled to obtain was given in paragraphs 3.6-3.8. The application of the general principles suggests that employers should not collect information about workers' off-duty conduct unless it has clear implications for their ability to do their job or poses a real risk to the employer (for example in areas of financial services information about a worker's gambling habit may justify investigation). Other examples would be to ascertain whether the worker is working elsewhere, which may have implications for statutory working time limits or the protection of trade secrets. Moreover, the ECtHR has held that the fact that drug or alcohol testing at the commencement of a shift may reveal information about a worker's off-duty conduct will not, of itself, make collecting that information unlawful if it is otherwise justified for safety reasons.[91]

5.3 Video surveillance is a particularly intrusive form of monitoring. There are no legal provisions in English law relating to video surveillance of workers beyond those applicable to monitoring in general. However the Information Commissioner has issued a (non binding) Code on closed-circuit television ('CCTV') which considers that continuous monitoring should be used only in very exceptional circumstances, such as where hazardous substances are used and failure to follow procedures would pose a serious risk to life, and workers should be told it is being deployed. The Code considers that CCTV may also be justified in an area of its premises that a employer considers particularly vulnerable to theft, such as a store room, but not in areas such as toilets or private offices. Where CCTV is being used to prevent and detect crime by customers, such as in shops, it should not be used to monitor the workforce for non-criminal matters such as performance or compliance with company procedures.[92]

5.4 Monitoring of workers' electronic communications, like other forms of monitoring, is subject to the DPA 1998. Where monitoring involves the interception of a communication between a sender and recipient, such as a telephone call or e-mail, the interception will need to be lawful under RIPA 2000, outlined in paragraphs 2.10 and 2.11 above. [93] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations ('LBPR') 2000 made under RIPA allow interceptions to monitor or keep a record of electronic communications relevant to the employer's business for a range of purposes including ascertaining compliance with regulatory or self-regulatory practices or procedures; investigating or detecting unauthorised use of telecommunications systems; and monitoring communications to see if they are of a business nature (the 'routine access' exception). The employer must make 'all reasonable efforts' to inform every person who may use the system that communications may be intercepted but need not obtain their consent.[94] There is no restriction on what employers

[91] *Madsen* v *Denmark* above, note 61.
[92] Information Commissioner, *CCTV Code of Practice*, 2008, App 3.
[93] 'Interception' occurs when, in the course of its transmission, the contents of a communication are made available to someone other than the sender or intended recipient. In *R v Coulson* [2013] EWCA Crim 1026 the Court of Appeal held that 'the course of transmission' may continue even though the message has already been received and read by the intended recipient.
[94] See generally reg 3. Interception is lawful under RIPA 2000 where both the sender and recipient consent to the interception but obtaining the consent of external third parties is likely to be difficult. The need to inform under LPBR could also be difficult where the communication is initiated by an external third party.

may designate as 'unauthorised' use nor does LBPR require them to demonstrate that they have any grounds to suspect unauthorised use prior to instigating interception or that interception is a proportionate response to any problem.

5.5 Concern was expressed that interceptions authorised under LBPR for business purposes could also mean that workers' personal telephone calls and e-mails could be intercepted, which would breach the right to respect for private life unless justified under Article 8(2) of the ECHR.[95] On one view it can be argued that if employers have a clear policy that forbids the use of its communications systems for private purposes, which is enforced in practice to avoid any expectation of privacy, workers take the risk that any personal communications sent or received are at risk of interception under the 'unauthorised use' or 'routine access' provisions.[96] Although at one time such a policy may have been seen as unreasonably restrictive the widespread ownership of mobile and smart phones could be seen as lessening this objection as workers can continue to receive communications when at work. However there is still the risk that workers will receive communications from external parties of a personal nature or communications from those within the organisation such as the occupational health department or a trade union. The Information Commissioner suggests a range of steps that employers can take to reduce the risk of intercepting such communications, such as setting up a system that avoids messages from particular individuals or sections of the organisation being subject to monitoring.[97]

5.6 The fact that data has been obtained lawfully under LBPR does not mean that its processing is lawful under the DPA; processing will need to comply with criteria which, as discussed in paragraphs 3.2-3.4 above, scrutinise much more closely the need for monitoring and whether it is proportionate. In relation to other aspects of internet use, such as web-browsing and use of social media, employers are also recommended to have clear policies on what is acceptable and how these policies will be enforced; in this area the Advisory, Conciliation and Arbitration Service ('Acas') recommends having equivalent standards of behaviour for the 'on-line' and 'off-line' worlds. Acas also recommends developing these policies in consultation with the workforce, an approach which may assist an employer in defending its policies against challenge. The Information Commissioner suggests that, if private internet access is allowed, it could be separated from business access by having a different log-on for private use and then limiting the collection of information on private use to the length and time of the session.[98]

5.7 The distinction between on and off-duty conduct may be particularly difficult to draw in the 'on-line' world where workers may move rapidly between the personal and business realms. Moreover, off-duty activities in the on-line world may affect the workplace. Acas recommends employers' bullying and harassment policies should cover cyber-bullying of other workers regardless of when and where it occurs and that employers should monitor social networking sites if employees report breaches of the policy.

Telephone calls can be preceded by a pre-recorded messages; for e-mails this can be done only after the first communication but the employer who does this would probably be seen as having made 'reasonable efforts'.

[95] *Copland* v *UK* above note 5.

[96] The requirement that interception be 'effected solely for the purpose of monitoring or … keeping a record of communications relevant to the … business' probably means that even unauthorised personal e-mails cannot be the *target*, as opposed to the by-product, of monitoring but the matter is not free from doubt. Monitoring to detect leakage of trade secrets would seem to be lawful.

[97] *EPDPC Supplementary Guidance*, para 3.2.7.

[98] Above.

5.8 Technology enabling workers to work away from the workplace may mean that employers fund workers' electronic equipment, such as a mobile phone or landline, which is used for both personal and business use. The EPDPC emphasises the need for employers to make workers aware of the information they receive as a result of these arrangements (itemised bills, for example) and states that they should not make use of information about private calls 'unless they reveal activity which no employer could reasonably be expected to ignore' such as criminal activity, gross misconduct or practices that jeopardise the safety of others. It takes the same approach to the monitoring of vehicle use by devices which can record or transmit information such as the location, distance travelled, and the individual worker's driving habits. Here the EPDPC suggests the installation of a 'privacy button' or similar arrangement to enable the monitoring to be disabled when the vehicle is being used for private purposes.

5.9 In general, workers should always be informed of surveillance or monitoring. However there are circumstances where 'covert' monitoring or surveillance will be regarded as legitimate.[99] The EPDPC stresses that it should be used only in exceptional circumstances such as where there are grounds for suspecting criminal activity or equivalent malpractice and notifying individuals about the monitoring would prejudice its prevention or detection. However, in assessing whether an employee's dismissal was fair on the basis of evidence obtained through covert monitoring the courts have taken a less restrictive approach than this Code suggests. In a 2004 decision the Employment Appeal Tribunal (EAT) considered that where the employer suspected that the employee, who worked in a water treatment plant and lived nearby, was falsifying time sheets, covert surveillance of his house served a legitimate aim (the protection of company assets); was not disproportionate in the circumstances; and did not breach Article 8 of the ECHR.[100] In a more recent decision the EAT held that covert surveillance showing the claimant at a sports centre during the time when he should have been at work (following initial sightings by a co-employee) either did not constitute an 'interference' with his right to respect for private life, as the claimant was in a 'public place' or, if it did, the employer was pursuing the legitimate aim of protecting its contractual rights.[101] The Employment Tribunal (the first instance decision-maker) in this case had found the employer's decision unfair because the employer had not followed the EPDPC and, indeed, seemed to be ignorant of it. The EAT did not see why 'ignorance of a code which the employer was not bound in law to have regard to in any event would render an investigation into the wrongdoing of the claimant unreasonable when it would otherwise have been reasonable'.[102] This is an example of the lack of integration of English data protection and employment law to which I return in the concluding section of this paper.

5.10 The disclosure of a disciplined employee's name or other work-related information within or outside the employer's organisation has not been a general issue of discussion from a privacy perspective.[103] The advice of Acas is that disciplinary records

[99] See *Kopke* v *Germany*, above, note 60, where the employee's complaint that covert video surveillance by the employer infringed Article 8 of the ECHR was dismissed.
[100] *McGowan* v *Scottish Water* [2005] IRLR 167. The court did not clearly separate the issues arising under Article 8(1) and 8(2).
[101] *City and County of Swansea* v *Gayle* [2013] IRLR 768.
[102] Above at [29].
[103] EqA 2010, s 77 introduced a new provision making unenforceable a contractual term which seeks to prevent a person obtaining disclosure from a colleague about that colleague's pay but that is in the specific context of finding out whether there is unlawful discrimination.

should be kept confidential, and disclosing them without the employee's consent would be a breach of the DPA 1998, assuming that the records constituted 'data' within the meaning of the Act (see paragraph 2.6 above). Disclosure would also be likely to constitute a breach of the implied duty of trust and confidence owed to the employee.[104] However there may be circumstances where disclosure could be seen as justified. In *Rechnungshof* v Ö*sterreighischer Rundfunk*[105] the ECJ stated that disclosing data about the pay of those working for certain public bodies had the legitimate aim of the economic well-being of the country (exerting pressure on those bodies to keep salaries within reasonable limits) and was 'necessary in a democratic society' to achieve that aim. The British Home Secretary has recently announced the intention of compiling a national register of dismissed police officers with the aim of preventing them from being recruited by other local police forces.[106]

5.11 Workers' rights of access to personal information held by their employer is governed by the general principles regulating all 'subject access' contained in the DPA 1998. On receipt of a request in writing and a maximum £10 fee employers must supply workers with the information, including information as to its source, within 40 days of the request. The information must be communicated to the worker 'in an intelligible form' with an explanation of any non-intelligible terms (codes, for example).[107] In addition, where an employer processes the worker's personal data by automatic means to evaluate matters such as work performance, conduct and reliability, and that processing is likely to constitute the sole basis for any decision significantly affecting him or her, the worker is entitled to be informed of the logic of that decision-taking.[108] An individual may give written notice to the employer to cease processing any personal data on the ground that the processing is causing or is likely to cause substantial and unwarranted damage or distress to him or her, or another, which may be enforced by court order but there are certain exceptions to this right, including the worker having consented to the processing and the processing being necessary to the performance of the worker's contract or compliance with an employer's legal obligation.[109] An employer may be ordered by a court to correct, erase or destroy inaccurate personal data;[110] in practice, it is to be hoped that this could be done in the employment context by agreement between the parties. It is strongly arguable that failure by an employer to correct inaccurate data would constitute a breach of the implied contractual term of trust and confidence.[111]

6. Personal Information and Privacy Protection after the Employment Relation Ends

6.1 The general legal principles concerning personal information and privacy protection continue to apply once the employment relationship ends. In accordance with

[104] See generally Deakin and Morris *Labour Law*, above, note 17, paras 4.105-4.107.
[105] Above, note 58.
[106] Speech by the Home Secretary on police integrity, 12 February 2013.
[107] DPA 1998, ss7, 8. There are certain exceptions to the right of access: see s. 37; Sched 7. There are specific provisions relating to access to information which identifies third parties, including identifying them as a source: s7(4)-(6); see further para 6.2 below.
[108] DPA 1998, s 7(1)(d). See s 12 for rights in relation to automated decision-taking.
[109] Above, s 10.
[110] Above, s 14.
[111] See note 104 above.

the data protection principles in the DPA 1998 former employers should not keep personal data about individuals for longer than necessary.

6.2 A prospective employer will commonly wish to obtain a reference from an applicant's former or current employer and applicants will generally be asked to consent to the disclosure of their personal information for that purpose. References given by the 'data controller' in confidence for the purposes of the employment or prospective employment of the data subject are exempt from the right of subject access described in paragraph 5.11 above.[112] However an individual may be able to obtain a copy of the reference if this is part of the personal data held by the new employer as the exception for references applies only to references 'given by' the data controller. In the case of a information (including a reference) which identifies a specific individual as the source, either the source must consent to the disclosure or it must be 'reasonable in all the circumstances to comply with the request' for disclosure; factors relevant here include any steps taken by the employer to seek consent and whether the source has expressly refused consent.[113] The Information Commissioner considers that references should be released unless the referee provides a 'compelling reason' why they should be edited or not released[114] and it is not uncommon for those seeking references to warn the referee in advance that their reference may be disclosed to its subject.

7. Conclusion

7.1 This paper has sought to explain the broad principles that govern the protection of employees' personal information and privacy in English law. Much of the legislation is technically very complex and its fragmented nature adds to its obscurity. The Code and Supplementary Guidance relating to employment issued by the Information Commissioner is helpful but it has no legal status and cannot, therefore, be relied upon as authoritative (and, indeed, one court has said that it should be completely disregarded: see paragraph 5.9 above). There is now a strong argument for the rights of workers and prospective workers in this area to be the subject of specific legislation which takes full account of, and is integrated into, employment law.[115]

7.2 Important substantive weaknesses in the current law which need correcting include the following:

(a) Ambiguity as to what constitutes 'consent', which is often key to assessing whether employers have lawfully obtained and retained employees' personal data. Under Directive 95/46/EC 'consent' means 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed' and Member States must provide that data may be processed only if the data subject has 'unambiguously' given consent.[116] The DPA 1998 does not define 'consent' and the European Commission has found that Member States have interpreted 'consent' differently, ranging from a general requirement of written consent to the acceptance of

[112] DPA 1998, s 37; Sched 7, para 1.
[113] Above, s 7(4)-(6).
[114] *EPDPC Supplementary Guidance*.
[115] For the argument for greater integration at international level see Hendrickx and Van Bever, above, note 7. The ILO Code of Practice on Protection of Personal Data, 1997, offers a good starting-point for considering what such legislation should contain.
[116] Arts 2(h), 7(a).

implicit consent.[117] For 'sensitive personal data' the Directive and the DPA require 'explicit' consent'.[118] This suggests that something additional to what is required for 'bare' consent is needed but it is not clear what this might be.

(b) The absence of protection against discrimination for those who do not 'consent'.[119] At present an individual who refuses to provide personal information, or who challenges the employer's right to seek it and is subsequently prejudiced in employment on that ground, has no statutory protection, nor do individuals who enforce their statutory rights under the DPA 1998 or AMRA 1988.[120] If in employment, it may be possible to argue that an employer's demand for information that breached an employee's rights under Article 8 would breach the implied term of trust and confidence enabling the employee to claim that he or she had been constructively dismissed. However to pursue such a claim in the employment tribunal requires a minimum period of employment (one or two years, depending on when the employment started).[121] The protection for job applicants is even more limited and in today's employment market it is an insufficient response to say that they can always choose to work elsewhere.

(c) There is no general prohibition on an employer *seeking* information which exceeds permitted purposes nor a general protection, like that in ROA 1974, for giving inaccurate or evasive answers if such information is sought (see paragraph 2.13 above).

(d) The remedies for workers are inadequate. The right to damages under the DPA 1998 requires an individual to show that they have suffered 'damage' *by reason of* the employer having contravened the Act, which may not be easy.[122] Those who wish to object to privacy invasions in advance have no right of action and the Information Commissioner's enforcement remedies have not, to date, been widely used. Remedies as well as substantive rights which are specific to employment law are needed.

(e) Workers should have a right to access without charge and to amend (or attach comments to) the personal information which their employers hold regardless of whether that information constitutes 'data' as defined in the DPA 1998 (see paragraph 2.6 above). The general principles governing personal information and privacy should also apply irrespective of the form in which information is collected and stored.

At present there is no indication that the British Government intends to change the law in this area beyond the discussions that are taking place at EU level about changes to wider data protection law.

[117] Commission Communication COM (2010) 609 final of 4 November 2010, para 2.1.5.

[118] Directive 95/46/EC, art 8(2)(a); DPA 1998, s 4(3); Sched 3, para 1.

[119] Cf the conclusions of the Article 29 Data Protection Working Party that consent is not valid if there is a 'real or potential relevant prejudice that arises from not consenting': Opinion 15/2011 on the definition of consent, p 13. The draft General Data Protection Regulation COM (2012) 11 final art 7(4) provides that consent should not provide a legal basis for data processing where there is a 'significant imbalance' between the position of the data subject and the controller.

[120] Cf the protection against victimisation for bringing proceedings or alleging contravention of the Equality Act 2010: EqA 2010, s. 27.

[121] Employment Rights Act 1996, s 108(1), as amended. Where the employee's period of continuous employment began before 6 April 2012 the period is one year.

[122] The Information Commissioner gives as an example a former worker losing a new job offer owing to a reference from the ex-employer which is based on inaccurate data.

Privacy as Sphere Autonomy

Benjamin I. Sachs[*]
Harvard Law School

I. Introduction

In United States employment law, employee "privacy" encompasses two seemingly distinct ideas:[1] first, an employee's right to be unwitnessed by or undisclosed to her employer, and, second, an employee's right to personal autonomy – or, better, sovereignty – over certain life decisions.[2] In many important respects, these two forms of privacy are quite different from one another.[3] But this paper will argue that, within the realm of U.S. employment law, the right to be unwitnessed and undisclosed and the right to personal sovereignty are united conceptually by a commitment to what the paper will call "sphere autonomy."[4] In brief, sphere autonomy suggests that an employer's authority both to know about her employees and to control what her employees do is derived from the employment relationship, and, as a result, that authority should be deployed *only* within the sphere of employment. When an employer attempts to use her authority beyond the confines of the employment relationship – by inquiring into an employee's private life or attempting to control that private life – we have a violation of the principle of sphere autonomy and thus an impermissible exercise of employer authority. Employee privacy rights in U.S. employment law can thus usefully be understood as an attempt to police sphere boundaries and ensure sphere autonomy.

The paper will proceed as follows. Part II will identify several areas of U.S. employment law that display a commitment to employee privacy as a right to be unwittnessed and undisclosed vis-à-vis the employer, what the paper will call privacy as confidentiality. Part III will then identify a few areas of U.S. employment law that manifest commitment to employee privacy as a right to personal sovereignty: the employee's right to control certain aspects of her life unimpeded by the demands of employer and firm, what

[*] Professor of Law, Harvard Law School. The author thanks Carly Rush for superb research assistance.

[1] *See generally* Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 Chi-Kent L. Rev. 221 (1996).

[2] *Cf.* Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?*, 58 Notre Dame L. Rev. 445 (1983). Feinberg usefully speaks of "autonomy as sovereignty" and I will follow him here in part to distinguish "personal sovereignty" from the "sphere autonomy" that will be my focus. *See infra*. He also describes another version of privacy as "the right to to be unintruded upon, unwitnessed, and undisclosed in one's solitude." Id. at 486.

[3] *Compare* Elizabeth L. Beardsley, *Privacy: Autonomy and Selective Disclosure*, NOMOS XIII: PRIVACY 56 (1971) *with* Hyman Gross, *Privacy and Autonomy*, NOMOS XIII: PRIVACY 169 (1971), *cited in Feinberg*, *supra* n.X at 446 n.2.

[4] *See generally* Michael Walzer, Spheres of Justice: A Defense of Pluralism and Equality 26 (1983); see also Linda Bosniak, *Membership, Equality, and the Difference that Alienage Makes*, 69 N.Y.U. L. Rev. 1047, 1081 (1994) (discussing the role that "sphere autonomy" plays in Walzer's theory of justice).

the paper will call, following Joel Feinberg, privacy as personal sovereignty.[5] Then, Part IV will review Michael Walzer's argument that power derived in one sphere of social life ought only be deployed within the sphere where it was obtained and not exported from one sphere to another. Part V will show how both aspects of privacy in U.S. employment law can be understood as manifesting a commitment to sphere autonomy. The paper concludes in Part VI.

Two important caveats before beginning. First, the intent of the discussion here is *not* to capture the predominant or majority view among U.S. jurisdictions on the law of employee privacy.[6] Instead, the paper aims only to show that, within U.S. employment law, there exist strands of doctrine motivated by two seemingly distinct types of privacy and that these strands can helpfully be understood as unified by a commitment to sphere autonomy.

Second, to understand employee privacy rights as a commitment to sphere autonomy is not to answer the important, and vexing, question of how we ought to delineate the relevant spheres. Where, for example, does the "employment sphere" – as the paper will call it – end and other spheres of social life begin? To take an example that will recur in the paper: when an employer attempts to control an employee's romantic partnerships, the employee might understand that as interference in a sphere of the employee's life quite distinct from the employment relationship. But the employer, for her part, might view the partnership as a problem for the firm and thus very much a matter within the employment sphere.[7]

Delineating sphere boundaries is, however, beyond the scope of what this paper hopes to do. The point of this paper is to argue, more simply, that these two seemingly distinct strands of employee privacy rights both make sense as expressions of a commitment to sphere autonomy. The precise boundaries of the employment sphere – and the other spheres of social life that employees inhabit – remain undefined in the cases and statutes that protect employee privacy. What is apparent in these legal regimes, however, is a commitment to the principle that there are distinct spheres, and that an employer's authority ought to be cabined to the employment sphere where it was derived.

II. Privacy as Confidentiality

The first, and in some senses most intuitive type of employee privacy that U.S. employment law protects is the employee's right to keep certain things *private* – or confidential – from her employer.[8] The range of cases and statutes that protect this type of privacy is broad,[9] and this Part will discuss only a few.

Perhaps the classic example of privacy as a right to confidentiality comes in cases involving an employer's physical search of an employee's body. *Bodewig v. K-Mart,*

[5] *See* Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?*, 58 Notre Dame L. Rev. 445 (1983).

[6] Indeed, at times the paper will invoke cases that have remained relative outliers within employment law doctrine.

[7] For a helpful discussion of these points, *see* Stephen D. Sugarman, *"Lifestyle" Discrimination in Employment*, 24 Berkeley J. Empt & Lab. L. 377, 384-95 (2003).

[8] Feinberg calls this type of privacy the "familiar pre-technical sense" of privacy and that seems accurate. *Feinberg*, *supra* n.X at 486.

[9] *See*, e.g., *Finkin*, supra n.X at 225-35; *see also* MATTHEW W. FINKIN, PRIVACY IN EMPLOYMNET LAW (2003).

Inc.,[10] for example, involved a check-out clerk at a Kmart in Oregon. A disgruntled customer named Golden alleged that she left $20 in Bodewig's check-out line, and that Bodewig stole the money. When Bodewig, the customer, and the store manager were unable to find the customer's $20, the store manager told Bodewig to go with a supervisor – and the disgruntled customer – to the women's bathroom "for the purpose of disrobing in order to prove to Golden that [Bodewig] did not have the money."
In the bathroom, Bodewig took off all her clothes except her underwear while the customer and the supervisor watched. In the court's words, "[w]hen plaintiff asked Golden if she needed to take off more, Golden replied that it was not necessary because she could see through plaintiff's underwear anyway."

Bodewig quit the next day and sued the employer for outrageous conduct. The Oregon court held that there was sufficient evidence in the record for the case to go to a jury. As the court put it, a jury could find that the K-Mart manager, "put [Bodewig] through the degrading and humiliating experience of submitting to a strip search in order to satisfy the customer . . . [and] that the manager's conduct exceeded the bounds of social toleration and was in reckless disregard of its predictable effects on plaintiff." Thus, *Bodewig* grants legal protection for an employee's right to be unwitnessed and undisclosed.

Similar examples exist in the context of employer searches, not of an employee's body, but of an employee's personal effects. In *K-Mart Corp. Store No. 741 v. Trotti*,[11] for example, K-Mart provided employees with a locker to store their personal items during work hours. Trotti, an employee of K-Mart, placed her purse in her locker when she arrived at work, and locked the locker. But when Trotti returned to her locker during an afternoon break, she found the lock hanging open and the "personal items in her purse in considerable disorder." A store manager ultimately testifies that he had searched the lockers that afternoon because K-Mart's security guards had a suspicion that some employee – not Trotti – had stolen a watch.

Trotti sued K-Mart for invasion of privacy and the Texas court of appeals again held that there was sufficient evidence in the record upon which a jury could find for the plaintiff-employee. As the Texas court wrote, the employer "disregarded [Trotti's] demonstration of her expectation of privacy, operand and searched the locker, and probably opened and searched her purse as well. . . . It is sufficient that an employee in this situation, by having placed a lock on the locker at the employee's own expense and with the [employer's] consent, has demonstrated a legitimate expectation to a right of privacy in both the locker itself and those personal effects within it."[12]

If searches of the *Bodewig* and *Trotti* variety are classic iterations of privacy as confidentiality, two more contemporary versions of this type of employee privacy right can be found in statutory law governing an employee's genetic makeup and an employee's social networking activities. These statutory regimes respond, in different ways, to technological developments that – without new privacy protections – would expose a great deal of personal information to employer view.

[10] 635 P.2d 657 (Ct. App. Or. 1981).
[11] 677 S.W.2d 632 (Ct. App. Tex. 1984).
[12] Again, with respect to both strip searches of the type at issue in *Bodewig* and personal-effects searches of the type at issue in *Trotti*, judicial treatment is far from uniform and many employee claims are rejected by courts. *See*, e.g., *Finkin*, *supra* n. X at 225. The point here is simply that, given adequate facts, this is a type of privacy right that is recognized by U.S. employment law.

In 2008, the United States Congress passed the Genetic Information Non-Disclosure Act (GINA).[13] Title II of GINA prohibits employers from accessing information about an employee's genetic make-up. Thus, the law makes it an unlawful employment practice for an employer to "request, require, or purchase genetic information with respect to an employee or a family member of the employee."[14]
That is, under GINA, employees in the United States have a federal statutory right to keep their genetic information confidential from their employers. The law, moreover, forbids employers not only from accessing employees' genetic information but also from making employment decisions based on such information. Thus, the law makes it an unlawful employment practice for an employer:

> (1) to fail or refuse to hire, or to discharge, any employee, or otherwise to discriminate against any employee with respect to the compensation, terms, conditions, or privileges of employment of the employee, because of genetic information with respect to the employee; or
> (2) to limit, segregate, or classify the employees of the employer in any way that would deprive or tend to deprive any employee of employment opportunities or otherwise adversely affect the status of the employee as an employee, because of genetic information with respect to the employee.[15]

As in many areas of U.S. employment law, moreover, the federal statute leaves room for state and local interventions as well. GINA therefore sets a national floor for employee privacy protection, but it allows state laws to do even more to protect the confidentiality of employee genetic information. In fact, by the time of GINA's enactment, more than thirty states had laws prohibiting genetic discrimination in employment.[16]

While GINA and its state-law analogues protect the confidentiality of employee genetic information, a second set of state laws safeguard employees' online – or "social media" – information from employer access. At least twelve states now prohibit employers – to some extent and in some range of circumstances – from requiring employees, or applicants for employment, to provide employers with access to the employees' social media networks. California's law, enacted in 2012, is illustrative.[17]

---

[13] Genetic Information Nondiscrimination Act of 2008, P.L. 110-233, tit. II (codified at 42 U.S.C. 2000ff-1).
[14] *Id.*
[15] *Id.*
[16] *See* Louise Slaughter, *Genetic Information Non-Discrimination Act*, 50 HARV. J. LEG. 41, 47 (2013), *citing* Susannah Baruch & Kathy Hudson, *Civilian and Military Genetics: Nondiscrimination Policy in a Post-GINA World*, 83 AM. J. HUMAN GENETICS 435, 437 (2008).
[17] 2012 Cal. Legis. Serv. Ch. 619 (West). In addition to California, eleven other states have statutes regulating social networking privacy in the workplace. *See* Ark. Code Ann. §11-2-124 (West 2013) (employers may not request employees' social media passwords); Colo. Rev. Stat. Ann. § 8-2-127 (West 2013) (employers may not cause employees to disclose means of accessing personal electronic or social networking accounts); 820 Ill. Comp. Stat. 55/10 (2014) (employers may not request access to employees' social networking profiles); Md. Code Ann., Lab. & Empl. § 3-712 (West 2013) (prohibits employers from requesting access to employees' personal accounts through an electronic communications device); Mich. Comp. Laws Ann. § 37.271 – 37.278 (West 2012) (forbids employers from accessing or taking adverse employment action against an employee because of observing the employee's personal internet account); 2013 Nev. Legis. Serv. 548 (West) (employers may not cause employees to provide access to social media accounts); 2013 N.J. Sess. Law Serv. Ch. 155 (West) (employers may not request access to a personal account through an electronic communications device); N.M. Stat. Ann. § 50-4-34 (West 2013) (forbids employers from asking for access to a prospective employee's account or profile on a social networking site); 2013 Or. Legis. Serv. 204 (2013) (employers may not request that employees provide access to personal

According to the legislature's official analysis of the bill, the law was enacted based, *inter alia*, on the legislature's conclusion that allowing employers access to employees' social media accounts would result in an unacceptable intrusion, by employer, into employee's private lives. Thus, the California statute begins by defining "social media" very broadly and as extending to an "electronic service or account, or electronic content, including but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations."[18] The statute then goes on to prohibit employers from requiring or requesting that an employee, or applicant for employment:

> (1) disclose a username or password for the purpose of accessing personal social media; (2) access personal social media in the presence of the employer; (3) divulge any personal social media."[19]

It is important to note the *type* of confidentiality that social media laws like California's protect. That is, when an employee posts information on a social media network, the employee clearly intends to disclose that information to some set of other people – quite often, that set can be very large depending on the number of other users who have access to the employees' page. What laws like California's ensure, therefore, is a *selective confidentiality* that applies *only* to employers. As the official Analysis of the California bill stated:

> According to proponents, in this age of electronic correspondence and social media, more and more of a person's personal life is online. However, they argue, when it comes to an employer – employee relationship, it has never been an acceptable request for an employer to ask to see personal correspondence or personal photos of current or prospective employees. They argue that just because these items are now appearing and being stored online does not make it any more germane to determining an employee or prospective employee's work ethic than it was in the past. Proponents further argue that asking for access to a worker's social media account is a major intrusion into a person's personal life by an employer.[20]

Thus, under these state statutes, employees can disseminate personal information broadly while at the same time maintaining protection against their employers having access to that information. An employee's life can remain private – that is, confidential – vis-à-vis the employer while being public vis-à-vis others to whom the employee wishes to disclose.

Finally, although not yet law in the United States, a newly proposed Senate bill merits mention. In December of 2013, Senator Elizabeth Warren of Massachusetts

---

social media accounts, compel employees to add them to contact lists, ask employees to access social media accounts in their presence, etc); Utah Code Ann. §34-48 (West 2013) (employers may not request information related to personal internet accounts); 2013 Wash. Legis. Serv. Ch. 330 (West) (forbids employers from coercing an employee to reveal login information for a social networking account, add an employer to a list of contacts, access the account in the employer's presence, etc); *See also* S.007, 2013 Sess., at 1-2 (Vt. 2013) (creating a Social Networking Privacy Study Committee to issue recommendations for proposed legislation by January, 2014).

[18] Cal. AB 1822 (2012).

[19] *Id.*

[20] Cal. Sen. Rules Com., Off. of Sen. Floor Analyses, 3d reading analysis of Sen. Bill. No 1844 (2011-2012 Reg. Sess.)

introduced a bill titled the Equal Employment for All Act that would make it illegal for employers to require current or prospective employees to disclose their credit histories.[21] More particularly, §2(b)(1) of the bill would make it illegal for an employer to "request a consumer credit report, require or cause consumers to provide them a consumer credit report, or use the information contained in credit reports for employment purposes or adverse action."[22] There are similar laws already in place in ten states that also prohibit employers from requiring disclosure of credit history. Thus, as GINA enables employees to keep their genetic information confidential from employers and the social media laws allow employees to shield their internet activity from employers, Warren's bill would similarly protect the privacy – as confidentiality – of employee financial information.

III. Privacy as Personal Sovereignty

As such, the first sense of privacy protected by U.S. employment law is privacy as confidentiality: a range of protections exist under which employees have legal rights to keep certain things confidential from their employers. But employment law in the United States also protects a second, and quite distinct, form of employee privacy. This second form of privacy, sometimes called "autonomy,"[23] protects employees' ability to make decisions over important matters in their lives without employer interference. Because of the helpful analogy to political sovereignty, Joel Feinberg suggests that the interests ensured by "privacy" of this sort are better described as "personal sovereignty" rather than "autonomy."[24] I will borrow Feinberg's term here, in part because the right to "govern oneself" seems apt in the employment privacy context, and in part to avoid confusing personal autonomy from the kind of sphere autonomy I will describe below. But, whatever term we use, the important point is that U.S employment law's privacy protections go well beyond confidentiality and extend to ensuring employees some freedom to exercise control over a set of important life decisions.

Again, there are classic forms of this type of privacy protection and then some more modern iterations. One of the classic forms involves an employee's right to select for him or herself the romantic and marital partners s/he desires and a concomitant prohibition on employer interference with these choices. For example, in *Rulon-Miller v. International Business Machine Corp.*,[25] an employee, Rulon-Miller, was fired because she was dating a former IBM employee, Matt Blum, who had left IBM and joined a competitor firm.[26] Rulon-Miller sued, bringing claims of both wrongful discharge and intentional infliction of emotional distress. The jury found for Rulon-Miller on both claims, and the court of appeals upheld the verdict. The court's decision was predicated, at least in part, on the existence of an internal employer memo that provided employees this kind of privacy as sovereignty right. The "Watson Memo" as it was called stated:

> The line that separates an individual's on-the-job business life from his other life as a private citizen is at times well-defined and at other times indistinct. But the line does exist, and you and I, as managers in IBM, must

[21] *See* Equal Employment for All Act of 2013, S. 1837, 113th Cong. (2013).
[22] *Id.*
[23] *See*, e.g., *Finkin*, *supra* n.X at 235.
[24] *Feiberg*, *supra* n. X at 446-57.
[25] 208 Cal. Rptr. 524 (Ct. App. 1984).
[26] *See* 208 Cal. Rptr. 524 (Ct. App. 1984).

> be able to recognize that line. . . . When on-the-job performance is acceptable, I can think of few situations in which outside activities could result in disciplinary action or dismissal. . . . IBM's first basic belief is respect for the individual, and the essence of this belief is a strict regard for his right to personal privacy.

Based in part on the Watson memo, and in part on California's duty of fair dealing, the court of appeals held that the jury was entitled to find that Rulon-Miller's discharge was wrongful. The court, moreover, held that the discharge constituted an intentional infliction of emotional distress. That tort requires a finding that the discharge was extreme, outrageous, or atrocious. The court thought that this discharge fit the bill. Why? The court lists several factors as necessary to its conclusion, but among them was the fact that the IBM manager who fired Rulon-Miller deprived her of the *choice* between pursuing her romantic relationship and keeping her job. It was, *inter alia,* the manager's statement to Rulon-Miller that he was "making the decision for [her]" that the court found sufficiently extreme to justify the jury verdict.

Here again, it is important to notice the kind of "privacy" interest at stake in *Rulon-Miller* and to notice the privacy interest that is not at stake. Rulon-Miller did not desire to keep her relationship with Blum confidential from her employer. Indeed, the court repeatedly makes it clear that the relationship was *public* throughout IBM. Thus, for example, the court tells us: "[t]hat they were dating was widely known within the organization." Thus Rulon-Miller has no claim to privacy as confidentiality. Instead, her claim to privacy is a claim to personal sovereignty: a right to decide about intimate personal matters, like romantic relationship, free of interference by the employer. In *Rulon-Miller,* the court enforces exactly this type of privacy as sovereignty.

A related example of this type of employee privacy concerns not romantic relationships but political beliefs and political action. In *Novosel v. Nationwide Insurance Co.*,[27] employees were instructed to engage in political canvassing and signature gathering in support of a piece of legislation that the employer wanted enacted: the "No-Fault-Reform Act." Novosel, an employee of Nationwide, objected to the Act and refused to participate in the political activity that the employer directed. As a result, Novosel was fired. He sued on a tort theory of wrongful discharge and the U.S. Court of Appeals held for Novosel finding that a jury could find his termination to constitute wrongful discharge in violation of public policy. The basis for this tort, the court tells us, is the same type of privacy concern implicated in *Rulon-Miller*. The court quotes from an earlier decision on the subject:

> It may be granted that there are areas of an employee's life in which his employer has no legitimate interest. An intrusion into one of these areas by virtue of the employer's power of discharge might plausibly give rise to a cause of action, particularly where some recognized facet of public policy is threatened.

What is the public policy threatened by Novosel's discharge? Into what area of the employee's life has the employer unjustifiably intruded? The court tells us that the public policy at stake here is the "employee's freedom of political expression." Thus, "an

[27] 721 F.2d 894 (3d Cir. 1983).

important public policy is . . . implicated wherever the power to hire and fire is utilized to dictate the terms of employee political activities."

Again, notice the kind of privacy at issue here. There is no claim to confidentiality; no claim that Novosel should be able to keep his political views secret from his employer. Novosel made his political views quite plain to the employer. Instead, the claim is that political belief and expression – like romantic relationship – is a domain of an employee's life over which the employee ought to have sovereignty. In other words, whether Novosel lobbied for the No-Fault Reform Act should be Novosel's decision, not the employer's.[28]

If *Rulon-Miller* and *Novosel* capture older iterations of privacy as sovereignty in U.S. employment law, more modern instances of this form of privacy can be found in so-called "lifestyle discrimination" statutes. In the United States today, twenty-nine states and the District of Columbia have some form of a lifestyle discrimination statute.[29] Generally,

[28] Both *Rulon-Miller* and *Novosel* are important cases in the U.S. employment law cannon and both are featured in prominent textbook treatments of employee privacy. For example, *Novosel* and *Rulon-Miller* both appear in "Part III (Employee Privacy)" of Steven L. Willborn, et al., Employment Law Cases and Materials, Fifth Edition (2012). But neither *Rulon-Miller* nor *Novosel* expresses the majority rule in the U.S. law of employee privacy, and there are many cases that reach contrary holdings with respect to both romantic relationships and rights of political expression. *See*, e.g., *Finkin*, *supra* n.X at 237-38 ("fraternization" and "association"); *Brunner v. Al Attar*, 786 S.W.2d 784 (Texas 1990)(political expression). Thus, for example, Matthew Finkin concludes that although "California's commitment to privacy has arguably been extended to limit employer prohibitions on sexual relationships with employees of competitors," in "most jurisdictions employers are free to restrict employees in their off-duty sexual behavior." *Finkin*, supra n.X at 237. The point here, again, is not to establish the majority view but only to identify a strand of privacy protection in U.S. employment law in which privacy is best understood as personal sovereignty.

[29] Cal. Lab. Code. §95 (West 2000) (employers may not discriminate against employees because of conduct that is lawful and occurs during nonworking hours); Colo. Rev. Stat. Ann. § 24-34-402.5 (West 2007) (employers may not require employees to refrain from lawful activities during nonworking hours unless the restriction is a bone fide occupational requirement or is necessary to avoid a conflict of interest); Con. Gen. Stat. Ann. §31-40s (West 2003) (employers may not require employees to refrain from smoking or using tobacco products unless the employer's primary purpose is discourage use of tobacco products); D.C. Code § 7-1703.03 (1993) (employers may not discriminate against employee or applicants based on their use of tobacco products); 820 Ill. Comp. Stat. 55/5 (1992) (employers may not discriminate against employees or applicants based on use of lawful products during nonworking hours); Ind. Code Ann. § 22-5-4-1 (West 1991) (an employer may not discriminate against an employee or prospective employee based on use of tobacco products); Ky. Rev. Stat. Ann. § 344.040 (West 2010) (it is unlawful for an employer to discriminate against an individual for smoking or not smoking); La. Rev. Stat. Ann. § 23:966 (1991) (prohibits an employer from discriminating against a person because they are a smoker or nonsmoker); Me. Rev. Stat. tit. 26, § 597 (1991) (employers may not require employees or prospective employees to refrain from using tobacco products outside the course of employment); Minn. Stat. Ann. § 181.938 (West 1992) (employers may not refuse to hire, discharge, or discipline an individual because that person uses lawful consumable products during non working hours, unless the action relates to a bona fide occupational requirement or is necessary to avoid a conflict of interest); Miss. Code. Ann. § 71-7-33 (West 1994) (employers may not require employees or applicants to refrain from using tobacco products during nonworking hours); Mo. Ann. Stat. § 290.145 (West 1992) (employers may not discriminate against an individual because of their use of lawful alcohol and tobacco products during nonworking hours, unless the use interferes with the duties and performance of the employee, coworkers or the employer's business); Mont. Code Ann. § 39-2-313 (1993) (with specific exemptions, an employer may not discriminate against an individual because of the use of a lawful product during nonworking hours); Nev. Rev. Stat. Ann. § 613.333 (West 1991) (an employer cannot discriminate against an employee or applicant because of the lawful use of a product during nonworking hours, unless it affects the employee's ability to do the job or the safety of other employees); N.H. Rev. Stat. Ann. § 275:37-a (1992) (no employer shall require an employee or applicant to abstain from using tobacco products outside the course of employment); N.J. Stat. Ann. § 34:6B-1 (West 1991) (an employer may not discriminate against an individual because of use of tobacco products unless the employer has a rational basis

these statutes protect employees' ability to consume "lawful products" or engage in "lawful conduct" when they are not at work. That is, the statutes make it illegal for an employer to take employment actions based on an employees' lawful off-duty behavior. Many of these statutes – the majority, in fact – apply only to off-duty smoking and alcohol consumption. They accordingly reflect the considerable political influence of the tobacco and alcohol lobbies on American policymaking. But these statutes, and particularly the four broadest, also work to protect employees' privacy interest in personal sovereignty. As Stephen Sugarman puts it, the lifestyle discrimination statutes address the question of "how much should employers be able to intrude into the privacy of workers' off-work, lifestyle choices."[30]

One of the broadest of these statutes is Colorado's, enacted in 1995. The law prohibits employers from requiring employees to refrain from *any lawful activity* during off-work hours and thus protects against employer retaliation "any lawful activity off the premises of the employer during nonworking hours."[31] As one academic account of the statute has concluded, although the case law is still sparse, it may "offer protection based on sexual orientation, employee dating, political or social affiliation, smoking, dangerous sports, and sexual propriety."[32] California's lifestyle statute similarly dictates that

---

for doing so reasonably related to employment); N.M. Stat. Ann. § 50-11-3 (West 1991) (it is unlawful for an employer to discriminate against an employee or applicant because that person is a smoker or nonsmoker unless there is a conflict of interest or a bona fide occupational requirement); N.Y. Lab. Law § 201-d (McKinney 1992) (employers may not discriminate against individuals because of their political activities, legal use of consumable products, legal recreational activities, or membership in a union); N.C. Gen. Stat. Ann. § 95-28.2 (West 1991) (it is unlawful for an employer to discriminate against an employee because of lawful use of products during nonworking hours unless it affects job performance or the safety of other employees); N.D. Cent. Code Ann. § 14-02.4-01 (1993) (employers may not discriminate against individuals because of participation in lawful activity during nonworking hours which is not in conflict with essential business-related interests); Okla. Stat. Ann. tit. 40, § 500 (West 1991) (employers may not discriminate against employees because of their use or nonuse of tobacco products); Or. Rev. Stat. Ann. § 659A.315 (West 2005) (employers may not require employees or prospective employees to refrain from using tobacco during nonworking hours, unless there is a bona fide occupational requirement); R.I. Gen. Laws Ann. § 23-20.10-14 (West 2004) (employers may not discriminate against employees who use tobacco products unless the employer is a nonprofit organization which has as a primary purpose discouraging the use of tobacco products); S.C. Code Ann. § 41-1-85 (1990) (employers may not tae personnel actions based on the use of tobacco outside the workplace); S.D. Codified Laws § 60-4-11 (1991) (employers may not fire employees for their use of tobacco products during nonworking hours unless a restriction relates to a bona fide occupational requirement or is necessary to avoid a conflict of interest); Tenn. Code Ann. § 50-1-304 (West 1990) (no employee may be fired solely for using agricultural products not regulated by the alcoholic beverage commission that is not proscribed by law); Va. Code Ann. § 2.2-2902 (2001) (no Commonwealth employee or applicant for employment is shall be required to use or abstain from using tobacco products); W. Va. Code Ann. § 21-3-19 (West 1992) (employers may not discriminate against individuals because of their use or non-use of tobacco unless the employer is a nonprofit with the primary purpose of discouraging use of tobacco products); Wis. Stat. Ann. § 111.31 (West 2010) (employers may not discriminate against individuals because of their use or nonuse of lawful products during nonworking hours); Wyo. Stat. Ann. § 27-9-105 (West) (it is unlawful for employers to discriminate because of use of tobacco products unless there is a bona fide occupational qualification).

[30] Stephen D. Sugarman, *"Lifestyle" Discrimination in Employment*, 24 Berkeley J. Empt & Lab. L. 377, 379 (2003).

[31] *See* Colo. Rev. Stat. Ann. §24-34-402.5 (West)(1990).

[32] Jean M. Roche, *Why Can't We be Friends?: Why California Needs a Lifestyle Discrimination Statute to Protect Employees From Employment Actions Based on their Off-Duty Behavior*, 7 HASTINGS BUS. L. J.187, 200 (2011), *quoting* Jessica Jackson, *Colorado's Lifestyle Discrimination Statute: A Vast and Muddled Expansion of Traditional Employment Law*, 67 U. COLO. L. REV. 143 n.5 (1996).

employers may not discriminate because of employees' lawful conduct that occurs during non-working time and off the employer's premises,[33] while New York's law prohibits employer discrimination based on political activities and "recreational activities."[34]

These statutes are fairly new and the precise scope of their protections has not yet been fully determined. But it is clear that they intend to protect against employer interference some fairly broad of employee decisions regarding off-work behavior. Whether it is simply the decision to smoke or drink alcohol, or more broadly the decisions about which "lawful activities" to engage in, lifestyle statutes protect a form of employee privacy best understood as personal sovereignty.

IV. Privacy as Sphere Autonomy

On some accounts, confidentiality and personal sovereignty are distinct concepts and ought not be classified as two subtypes of any single principle. On these accounts, "confidentiality" is one thing and "personal sovereignty" is another, and "privacy" is simply a confounding add-on. For example, in his article *Privacy and Autonomy*, Louis Henken argues that using the term "privacy" to encompass autonomy interests is "misleading, if not mistaken."[35] Ken Gormley writes that "privacy consists of four or five different species of legal rights which are quite distinct from each other and thus incapable of a single definition,"[36] while William Prosser argued that the law of privacy encompasses protection against several distinct harms "which are tied together by the common name, but otherwise have nothing in common."[37]

But, within the bounds of U.S. employment law, privacy as confidentiality and privacy as personal sovereignty share a conceptual core. That core is the idea of sphere separation or sphere autonomy.

The importance of sphere autonomy finds clearest articulation in the work of Michael Walzer. Walzer argues that society is comprised of distinct spheres. For example, the market is one sphere, politics is another, and kinship and family is a third.[38] Most important for our purposes, Walzer does not understand a just society as requiring as requiring an equal distribution of goods within any particular sphere. He calls this conception of justice "simple equality" and he rejects it as both implausible and inconsistent with the distributive logic of many social spheres: a market economy, for instance, depends on some measure of economic concentration to enable investment, while government requires some concentration of political power to enable representation. Thus, for Walzer, concentration of goods – including power – within spheres is often consistent with the distributive criteria of that sphere: "within the distributive frame of the market, concentrated economic power is not necessarily unjust; nor is concentrated political power considered inappropriate in the political arena."[39]

---

[33] Cal. Lab. Code § 96 (West) (2005).
[34] N.Y. Lab. Law § 201-d (McKinney) (1992).
[35] Louis Henkin, *Privacy as Autonomy*, 74 Colum. L. Rev. 1410,1410 (1974).
[36] Ken Gormley, *One Hundred Years of Privacy*, 1992 Wis. L. Rev. 1335, 1339, *quoted in* Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087, 1089 n.8 (2002).
[37] William L Prosser, *Privacy [A Legal Analysis]*, *in* Philosophical Dimensions of Privacy 104, 107 (Ferdinand David Shoeman, ed., 1984), *quoted in Solove*, *supra* n.X at 1089 n.8.
[38] *Walzer*, *supra* n.X at 235.
[39] Linda Bosniak, The Citizen and the Alien: Dilemmas of Contemporary Membership 44 (2006), *citing Walzer*, *supra* n.X.

While a just society, for Walzer, does not require simple equality – it does not require the equal distribution of goods and power *within* any particular sphere – it does require what he calls "complex equality." And the key to complex equality is that the goods or power derived in one sphere must be deployed within the sphere where they were obtained and not exported or "converted" from one sphere to another.[40] Thus, for Walzer, justice requires sphere *autonomy*. When sphere autonomy breaks down – when power derived in one sphere is deployed in another sphere – we have what Walzer calls dominance, or tyranny.

Quoting Pascal, Walzer writes that "[t]he nature of tyranny is to desire power . . . outside its own sphere."[41] And, in Walzer's own words, allowing sphere convergence – allowing the power derived in one sphere to be exercised in another – is tantamount to *injustice*:

> To convert one good into another, when there is no intrinsic connection between the two, is to invade the sphere where another company of men and women properly rules. Monopoly is not inappropriate within the spheres. There is nothing wrong, for example, with the grip that persuasive and helpful men and women (politicians) establish on political power. But the use of political power to gain access to other goods is a tyrannical use. [42]

One the other hand, if sphere autonomy can be ensured – if we can ensure that the power and resources derived in one sphere are exercised only within that sphere – we can ensure complex equality:

> In formal terms, complex equality means that no citizen's standing in one sphere or with regard to one social good can be undercut by his standing in some other sphere, with regard to some other good. Thus, citizen X may be chosen over citizen Y for political office, and then the two of them will be unequal in the sphere of politics. But they will not be unequal generally so long as X's office gives him no advantages over Y in any other sphere – superior medical care, access to better schools for his children, entrepreneurial opportunities, and so on.[43]

---

[40] *Walzer*, *supra* n.X at 19.

[41] *Id.* at 18.

[42] *Id.* at 19.

[43] *Id.* Although Walzer did not himself consider the question of employee privacy, he makes a particular observation that is relevant to our analysis of employee privacy rights. In his discussion of the market sphere, Walzer worries about the threat that wealth and what he calls "powerful entrepreneurs" pose to the "integrity of other distributive spheres." One of his concerns relates specifically to the ability of employers to exert power over employees outside the employment relationship. Thus, Walzer argues:

> It would be a mistake to imagine . . . that money has political effects only when it 'talks' to candidates and officials, only when it is discreetly displayed or openly flaunted in the corridors of power. It also has political effects closer to home, in the market itself and in its firms and enterprises. . . . Even within the adversary relation of owners and workers, with unions and grievance procedures in place, owners may still exercise an illegitimate kind of power. They make all sorts of decisions that severely constrain and shape the lives of their employees . . . . Beyond a certain scale, the means of production are not properly called commodities . . . . for they generate a kind of power that lifts them out of the economic sphere.

Id. at 121-22.

Employment law's two conceptions of privacy are united by such a commitment to sphere autonomy. Both understandings of privacy reflect the view that social life consists of multiple spheres: one of these spheres is defined by the employment relationship, while beyond the boundaries of the employment relationship lie other spheres of social life that individuals populate as parents, spouses, patients, political activists, consumers, and so on. Within the employment sphere – where individuals stand in the relation of employer and employee – employers have substantial discretion to control employee behavior and to access information about employees' characteristics, qualifications, and performance. But an employer's exercise of control over employee behavior and an employer's access to employee information are legitimate *only* within the sphere of the employment relationship, from which the employer's power derives. *Outside* the employment sphere, an employer's attempt to control employee behavior or access employee information is illegitimate.

Employment law polices the boundaries between spheres with privacy rights. Privacy as confidentiality cabins employer authority, with respect to employee information, to the employment sphere. Privacy as sovereignty cabins employer authority, with respect to employee conduct, to the employment sphere. Taken together then, both types of employee privacy rights can be understood as an attempt to ensure that the spheres of social life remain autonomous and that the employer's authority is not exported beyond the bounds of the sphere of employment.

V. Sphere Autonomy and U.S. Employment Law

A commitment to the principle of sphere autonomy explains both U.S. employment law's protection of privacy-as-sovereignty and privacy-as-confidentiality. Starting with sovereignty, the sphere autonomy commitment is clearly at work in *Rulon-Miller*. Again, in that case, the employer attempted to intervene in Rulon-Miller's kinship choices – her decisions about her romantic relationships. The employer's action is problematic, because it amounts to a violation of sphere autonomy: the employer's power, derived in the employment sphere is legitimately deployed in that sphere; but when, as in the *Rulon-Miller* case, the employer's power extends into the sphere of "kinship and love," it becomes illegitimate. Indeed, Walzer argues that the boundaries of the kinship-and-love sphere are "highly vulnerable" and that they "often have to be defended . . . against . . . tyrannical intrusion."[44] Walzer, in fact, contends that "[t]he deepest understanding of tyranny probably lies here: it is the dominance of power over kinship."[45]

So too with *Novosel*. There, the employer attempts to control Novosel's political activities. In Walzer's framework, the employer is using its economic power to exert control over the employee's activities in the sphere of politics, and is thus engaging in a conversion of economic into political power. The employer's actions thus constitute a form of dominance, or tyranny, because they violate sphere autonomy. Indeed, the *Novosel* court grounded its holding in this very principle. Again, from the court's opinion: "there are areas of an employee's life in which his employer has no legitimate interest. An intrusion into one of these areas by virtue of the employer's power of discharge might plausibly give rise to a cause of action."

[44] *Id*. at 227.
[45] *Id*.

And the lifestyle discrimination statutes discussed above are easily understood through the frame of sphere autonomy. Those statutes enact the idea that an employee's off-duty, off-premises life takes place in social domains distinct from the employment sphere. When the employee acts legally in these social domains, these statutes dictate that the employer must not interfere with the employee's lifestyle choices. Again, such interference would be problematic because it would amount to the conversion of an employer's power, derived through the employment relationship, into distinct social spheres.

Just as the privacy-as-sovereignty protections are cognizable as applications of the sphere autonomy principle, so are privacy-as-confidentiality protections. *Bodewig*, for example, can be understood as a case involving the employer's intrusion into the most private of all spheres, the sphere of the body.[46] The strip search in that case is impermissible because it amounts to the employer's use of its economic power in a sphere where such economic power ought not have sway. GINA, too, makes sense on the same grounds. Genetic information *is* the body; it is a way of describing the most intimate details of an employee's body. As such, the information that GINA covers resides within the sphere of the body and outside the sphere of employment where an employer's power to know is legitimate. *Trotti* makes sense on similar grounds. Although the search there is not of the Trotti's body, it is of her personal effects. Such personal property can surely be understood as within a domain – or sphere – distinct from the one in which employers legitimately govern.

Both the social media laws and Senator Warren's bill on credit histories, discussed above, also make clear sense as protections for sphere autonomy. As we've seen, the social media laws enact state legislatures' commitment to the idea that if an employer accesses an employee's social media accounts, the employer is intruding into the employee's private life. Which particular non-employment sphere such employer action violates depends on the nature of the information contained in the social media account: perhaps it is "kinship and love"; perhaps it is political. But what matters is that the employer's action is illegitimate because it is an exercise of power "outside its sphere."[47] The same is true of Warren's credit history bill: the employer ought not have access to information about an employee's financial standing and credit rating because to allow such access is to allow the employer's power to extend beyond the appropriate boundaries of the employment sphere.

VI. Conclusion

There are two primary forms of employee privacy protection in U.S. employment law: privacy as confidentiality, and privacy as personal sovereignty. At first blush, these different conceptions of privacy appear quite distinct: one concerns information and the right to keep such information undisclosed; the other, a right to act in accordance with personal preferences free of employer interference.

But both conceptions of privacy are united by a commitment to sphere autonomy. Sphere autonomy dictates that an employer may legitimately use its authority, derived through the employment relationship, in the employment sphere. Within that sphere, the

[46] *Cf. Feinberg, supra* n.X at 452 (noting that, in the most basic sense, "the personal domain is . . . defined by its spatial dimension").
[47] *Walzer*, *supra* n.X at 18.

employer has broad discretion to tell employees what work to do, how to do it, and when it must be done. Within the employment sphere, the employer also has a right to know what work employees have done, how well they have done it, and what they have failed to do. But when the employer takes the authority it derives within the employment sphere and exercises that authority outside the employment sphere – either by attempting to control employee behavior in other spheres or by trying to access information about employee's life in other spheres – then the exercise of employer power violates the principle of sphere autonomy. Both forms of employee privacy protections can be understood as attempts to prevent violations of this principle.

The Personal Information and Privacy Protection of Employees in China

Kungang Li*
Anhui University

I. Introduction

In the past 30 years, China has experienced great unexpected changes in economy, politics, society, as well as in legislations. The rapid economic development under the background of globalization has transformed China from a mainly agricultural economy to an industrialized economy in a relatively short time. According to the study, China has entered into the middle period of industrialization.[1] In this process, the population in the city grew from 19% in 1980 to 51% in 2011 of the whole population, which is a huge figure especially considering the growth of the population. It has never happened in Chinese history, even in the world history that some many people have moved to live in the city in such a short period. Such a big change has made the situations that the culture of the city is a mixture of rural and urban cultures. For example some migrant workers still keep the habit of greeting each other with "Where are you going?" as farmers do, which sounds like inquiring the privacy of others.

While it is true that people's consciousness of privacy in the cities is actually growing, it is very far from that of the industrialized countries. Investigations show that the general Chinese public is still not very sensitive about their personal information and privacy protection, which maybe relates to the social background of China. A research conducted by "Research of Development of Rights of Citizen" showed that in answering the question that "do you think that it will influence you much if others make public of your personal information which you do not want the public to know?" Only 10.1% answered that it would substantially influence their lives; 35.4% answered that there would be some influence; 24% answered that there would not be much influence; 12.5% answered that there would be no influence; the rest said that they were not clear whether there would be any influence. This shows that the public need time to get to understand the importance of privacy right.[2]

The social background of China undoubtedly has greatly influenced the legislation and enforcement of law. In labor law, the protection of personal information and privacy of employees is so neglected that there are no specific regulations regarding to it. Chinese labor laws currently focus more on material benefits of the employee; while not much attention is paid to the protection of personal information and privacy, which is closely

---

* Professor of Law, Law School, Anhui University, China.

[1] Fang Cai (Chiefly Editor), *30 Years of Economic Transformation of China*, Social Sciences Academic Press (China), first ed., 2009.

[2] Zhong Shen & Wenjie Xu, *On the Right of Privacy —— Also on Personality Right,* Shanghai People's Press, July, 2010, p. 263.

related to personal dignity of workers.[3] The protection of personal information and privacy of employees mainly depends on the regulations in constitution, civil laws, criminal laws and other laws relating to it. In practice, there are lots of infringements on the rights of personal information and privacy of employees, which have been largely reported by newspapers, TV news broadcastings, radios, internet news, and other mass media.

From the reports, it could be concluded that infringements on personal information and privacy of employees are very serious in labor fields. In most circumstances the collection and application of personal information are closely connected with the economic interests of employers. In the workplaces, electronic surveillance is widely used because of its convenience and easy availability, which makes it a very easy job for employers to keep an eye on employees. Of course, employers have legal reasons to get the job applicants' personal information with the purpose of hiring the right employees and to watch over the workplaces so as to ensure that they are well organized, efficient and safe etc. However, speaking from the side of employees, they need to protect their personal information to prevent them from being abused and also they need to have their own privacy in the workplaces.

This essay will first introduce the regulations and laws concerning personal information and privacy protection in China. Second, the essay will discuss the problems in three different periods, the period of recruitment, the period of employment and the period of post-employment. The essay will also introduce and discuss some typical cases so as to demonstrate the current situations and find out that the existing problems. At last the essay will summarize the problems and look to the future of the protection of personal information and privacies in China.

In writing this paper, the author faces the following difficulties: (1) there is no basic systematic statistics on this topic so as to help give us an exact evaluation of the current situation in China; (2) there is no access to the relevant cases heard by courts in China because they are not disclosed on the internet and open to public because of the concerning of privacy; (3) this topic has not been very much researched by the academics, therefore only limited research papers have been published about the protection of personal information and privacy of employees. Other discussions are all about the civil law protection of personal information and privacy of citizens. Nevertheless, the author would try his best to piece out the information from internet, newspaper and other resources and answer the questions raised by the topic.

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

Personal information refers to the identifiable symbolic systems which are related to individuals and which can reflect the individual's characteristics, including a person's personal identity, work, family, property, health, and etc.[4] Privacy refers to personal private secrets that are not related to public interests, which include personal information, personal activities and personal space.[5] In China, there are laws and regulations concerning the protection of personal information and privacy, which are contained in

[3] Feng Pan, *On the Protection of the Right of Privacy of Employees: An Analytical Frame,* Hebei Law Review, July, 2008.
[4] Liming Wang, *On the Statue of Right of Personal Information in Personality Right*, Journal of Suzhou University, No. 6, 2012.
[5] Lixin Yang, *On Several Problems Relating Right of Privacy and Its Protection*, People's Procuratorial, No. 1, 2000.

constitution, civil laws, criminal laws and other regulations. The relevant regulations are introduced as follows.

A. Constitution

In the *Constitution of China*, there are no direct regulations concerning the protection of personal information and privacy of employees. However, Chinese Constitution protects the personality rights of citizens, in which the right of personal information and privacy of citizens are included.

Generally, there are three articles that are relating to the protection of personal information and privacy of employees. Article 37 *Constitution of China* provides that unlawful search of the person of citizens is prohibited, and article 38 provides that the personal dignity of citizens is inviolable, and that insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited. Article 40 provides that the freedom and privacy of communication are protected by constitution.

Thus, in accordance with the regulations, the personal information and privacy are protected by *Constitution of China.* However, in practice, in China the constitutional regulations have never been applied to protect the rights of citizens. Some scholars comment that the constitutional rules are like tigers without teeth, which only have some symbolic meanings. It is the application of constitutional rules that make it function.[6] No application means that the constitutional rules have no practical use. Therefore, in China the personal information and privacy of employees are only protected by Constitution in theory, but not in practice.

B. Civil law legislations

In current China, the protection of personal information and privacy of employees mainly depend on the civil law regulations. In the early civil law legislations, *General Principles of the Civil Law of China* enforced from 1987*,* there are no direct protections for personal information and privacy. However, there are protections for the reputation and personality of citizens[7], from which it could be inferred that personal information and privacy were protected by Chinese civil laws. An employee could get protection from civil law legislations if personal information and privacy are infringed, resulting in the damages in reputation and personality.

In 1988 Supreme Court of China issued *Interpretations concerning Enforcement of General Principles of the Civil Law of China* on January 26, article 140 of which provides that anyone who in written or verbal form publicizes the privacy of others, or concoctive fact to openly demonize others personality, or insult, libel to damage the reputation of others, shall be regarded as the behavior of the citizens' reputation, where serious results occur. That was the first direct protection on the right of privacy in China.

In 1993, Supreme Court of China issued *Some Answers to the Questions concerning Trials of Cases of Infringements of the right of Reputation*, in which the answer to question 7 that "How to identify the liability of infringement of right of reputation?" explains the identification shall base on three elements: the infringing facts, violations of law and results. In accordance with the regulations, anyone who insults or libel others in written or

[6] Yuerong Yao, *The Protection of Personal Information in the Field of Constitution*, Law Press China, first ed. 2012, p. 306.

[7] Article 101 of *General Principles of the Civil Law of China* in 1982 provides that citizens and legal persons shall enjoy the right of reputation and the personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited.

verbal forms shall be liable for the infringements to the reputation of others. Anyone who publicizes the privacy of others without their consent, resulting in the damage of reputation of others, shall be liable for the infringement.

In 2001, it was firstly provided that spiritual damages could be claimed for the damages in case that the right of privacy and other personality rights are infringed. Article 1 of *Some Interpretation concerning the Spiritual Damages for Civil Torts* issued by Supreme Court of China on Feb. 26, 2001 stipulates that the victim is entitled to bring a lawsuit in court to claim for spiritual damages in case that his/her rights of privacy and other personality rights are infringed by others in violation of public interest and social public morals. People's court shall accept the case.

The recent new principal civil legislation, *Tort Liability Law of China in 2009*, also provides protections for the rights of personal information and privacy, article 2 of which provides that the privacy of citizens is protected. Besides the protection of constitutional law and civil laws, other laws also mention the protection of the rights of personal information and privacy. Article 39 of *Women's Rights Protection Law* stipulates that reputation and personal dignity of women are protected. Article 21 of *Provisions on HIV/AIDS Monitoring and Management 1987* stipulates that the names and addresses of patients of HIV/AIDS shall not be open to public.

C. Labor law

In Chinese labor and employment laws, there are no specific regulations regarding to the protection of personal information and privacy of employees. However, in *Labor Contract Law of China* enforced from 2008, there is a general limitation on the collection of personal information of job applicants. Article 8 of *Labor Contract Law of China* stipulates that "The Employer has the right to learn from the Employee some basic information which directly relates to the employment contract, and the Employee shall truthfully provide the same."

Obviously, this article admits that an employer has some justifications to get to know employees' personal information, even some private information if it is related to work, but it does not establish any concrete rules to protect the privacy right of an employee. Therefore, an employer may abuse the right in practice, which may result in the infringements of an employee's privacy rights.[8]

In practice, Article 8 functions well to limit the collection of personal information and infringement of privacy of employees. For example, in applying for the position of human resources manager, Ms. Li was asked to fill out a form to give the required information. In the column of marriage status, she put unmarried because of afraid of being discriminated as a married woman. Later, she got the position. However, several months later, the employer got to know that Ms. Li was married, and then fired her for lying about the marriage status. Ms. Li brought a lawsuit against the employer for illegal dismissal. The trial court held that as a job applicant Ms. Li did provide false information to the company. However, considering marriage status was not relevant to the position, the court held that the employer constituted illegal dismissal in firing Ms. Li and the employer shall pay compensation.[9] According to *Labor Contract Law of China*, the compensation she could get is one month wage according to her average monthly wages.

[8] Feng Pan, *On the Protection of the Right of Privacy of Employees: An Analytical Frame*, Hebei Law Review, July, 2008.

[9] Chonggao Hu, *Something Women in the Work Needs to Know,* http://court.gmw.cn/public/detail.php?id=2089&k_title=&k_content=&k_author=&keyword=职场半边天。

Also, there are some other regulations that are related to personal information collection and protection. Article 33 of *Prevention and Treatment Law of Occupational Diseases of China* provides that employers shall set up occupational health records for employees and keep them safe. Employees are entitled to have copies of the occupational health files when leaving the employers, which shall be provided by the employers free of charge. But that rule is only applied to some specific employees, those who work under environments which have some healthy dangers.

D. International conventions

China has acceded to *Universal Declaration of Human Rights* and *International Covenant on Civil and Political Rights* and *Universal Declaration of Human Rights,* which both provide protections for personal information and Privacy. Article 12 of *Universal Declaration of Human Rights* and Article 17 of *International Covenant on Civil and Political Rights*, in which China participated on Oct. 10, 1998, stipulates that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The above international conventions are legal resources in China, and the contents of the regulations are very similar with the domestic laws in China. However, what is more important in practice is the liability of the infringer and the mechanism of claiming for damages when the personal information and privacy are infringed, which would depend on domestic laws to resolve. Chinese legislation has a lot to be improved in these two aspects.

E. Criminal laws

As for criminal punishments, there are no criminal punishments for infringements of personal information and privacy of employees.[10] However, there are several criminal law regulations relating to the protection of personal information and privacy. According to Criminal Law of China, the searching of human body and private property shall only be conducted by policemen and any illegal search shall be punished as a crime[11]. Illegal wiretapping and illegal photographing and illegal interference with the communication shall be punished as crimes[12]. An employer shall be criminally punished where he/she violates these criminal laws.

F. Remedies and punishments

In accordance with the civil legislations, any person who suffers from infringements of personal information and privacy is entitled to bring cases in court and claims for compensation, and has the right to demand that the infringement be stopped, his reputation be rehabilitated, the ill effects be eliminated and an apology be made; he may also demand compensation for losses.[13]

According to the interpretations, the infringement on the privacy can be categorized as reputation damages. In *Replies to the Questions Relating the Trial of Right of Reputation Cases in 1993* by the People's Supreme Court of China, it is explained that any person who

[10] Lizhi Wang, *Criminal Law Protection for the Right of Privacy*, Procuratorial Press China, first ed. 2009, p. 309.
[11] Article 245 of *Criminal Law of People's Republic of China*.
[12] Article 284 of *Criminal Law of People's Republic of China*.
[13] Article 120 of *General Principles of Civil Law of China.*

publicizes the documents concerning the privacies of others, or propagates other's privacy in oral or written forms, infringing other's reputation, shall be deemed as reputation infringement[14].

The victim is also entitled to damages for spiritual distress. *Interpretations on Some Civil Tort Liability Problems concerning Spiritual Distress Compensation* by the People's Supreme Court of China in 2001 stipulates that any person who infringes on the privacy or other personality interests in violation of public interests and social morality, the victim of the infringement is entitled to bring the case in a people's court and claim for compensation for spiritual distress, and the people's court shall accept it according to law.[15]

The remedy procedure is different for employees and non-employees. When the rights of personal information and privacy are infringed in the process of application for jobs, the applicants shall sue in accordance with civil procedure and pay court fees as required for there are no labor relations between applicants and defendants. After the formation of labor relations, applicants could claim for damages in arbitration tribunals, which are swift and free of charge.[16]

Generally, crimes concerning personal information and privacy are misdemeanors. Article 245 of *Criminal Law of People's Republic of China* provides that a person who unlawfully subjects another person to a bodily research shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention. Article 284 provides that any person who illegally uses apparatus for special purpose of wiretapping or photographing secretly shall be sentenced to a fixed-term imprisonment of not more than two years or be subject to detention or control. Article 246 provides that a person who insults in public another person by violence or any other means or fabricates facts to slander another person shall be sentenced to fixed-term imprisonment of not more than three years, criminal detention, public surveillance or deprivation of political rights if a serious result is caused. In practice, criminal punishments are barely applied for the infringements of personal information and privacy of workers.

III. The protection of personal information and privacy in the hiring process

In the application for the job, applicants need to give their information required by employers. Although article 8 of *Labor Contract Law of China* stipulates that an employer is only allowed to collect information relating to the employment, it is not enough to stop employers from abusing their favorable positions in the labor markets in the collection of the personal information of job applicants. Job applicants who are in great need of the work opportunities are especially in the vulnerable situation, which makes it quite easy for employers to obtain any information they need. In practice, an employer could infringe the rights of the workers in the following phases:

A. Job advertisement and interview process

The recruitment for public servants and employees of non-profitable organizations, like public schools, public universities and hospitals, are mainly conducted through several

[14] Article 7 of *Replies to the Questions Relating the Trial of Right of Reputation Cases in 1993* by the People's Supreme Court of China.
[15] Article 1 of *Interpretations on Some Civil Tort Liability Problems concerning Spiritual Distress Compensation* by the People's Supreme Court of China.
[16] Article 2 & 52 of *Labor Dispute Mediation and Arbitration Law of China.*

strict procedures: examinations, interviews, and medical checks. Problems exist in terms of personal information and privacy protection, but they are not as serious as the situation in the commercial working units, because the social security systems for public servants and employees of public organizations are different. For this reason, the situations in the commercial employer units will be primarily introduced and discussed here.

Basically, a company employer recruits employees in two ways. The first way is to put advertisements in labor markets or local news papers, in which the detailed requirements for the position are listed. Those who are qualified will contact the employer and the employer can select from applicants and arrange interviews. Then the employer will pick from those who are qualified to do the medical check. Based on the result of medical check and other information, the employer makes the final decision on who will be hired. At present, employers enjoy such a great freedom that it seems that the employers could ask for any information without worrying about being sued. Usually, we can see that from the job advertisements, there are usually strict requirements of the job applicants' detailed information, such as age, gender, nationality, education, former working experience, hometown, marriage status, family back ground etc. The advertisements which specify detailed requirements for the job applicants are very common.

The second way to recruit employees is to make a simple description of the job and requirements, and then let applicants to fill out the application form to provide detailed information employers need. This way is seemingly impartial and justified, but in fact it collects more information from more people compared with the first method. Because the labor law regulation about collect information limited to "information directly relating to the employment" is not very clear, the employers usually do not worry about the limits in information collection. Often applicants are required to provide information, such as birth date, gender, nationality, ID number, marital status, family background, education, working experience, expected wages, etc., as detailed as possible. Applicants are required to promise that the information provided is true and to sign them. The favorable aspect of the second way is that it avoids the risk of being sued for discrimination and also the information from applicants can be used for future recruitment. In the more developed area, the second way is common while in the less developed area the first way is common.

After the information is collected, employers will decide how many applicants will be interviewed. There are no requirements in law that employers shall provide travelling fees for the interviewees in China, therefore, the employer can interview as many as they like to without worrying about the costs. There are lots of reports that in the process of job interview, some interviewers even ask questions concerning the privacy of applicants. For example, an investigation finds out that the inquiry into the privacy becomes common in the job interview. For example, this dialogue happened in an interview. An interviewer suddenly asked "Do you have a boyfriend?" Faced with such a question the interviewee answered "Yes." "Is he here in Guangzhou or in another city?" The question continued. The interviewee honestly answered "he is preparing for going abroad to continue his research work." "Will you go with him to a foreign country in the future?" "I have not seriously considered this question." "Does this mean that you two would break up in the future?" "……".[17]

According to the internet reports, there are some unusual extreme cases. For example, an interviewer may ask a female applicants questions like "What would you answer if a client of yours asked for sexual benefits?", "What would you do if your boss sexually harassed you?". An investigation found out that in ten woman university graduates, 7 were

[17] *The Privacy Infringement in the application for Jobs.* http://news.sohu.com/65/92/news148099265.shtml.

asked questions like "do you have a boyfriend" and other questions relating to privacy information. Six of them said they felt embarrassed and uneasy. [18]

Such questions often embarrass interviewees and infringe their rights to privacy. Although attorneys suggest that interviewees could take a recorder in an interview and use the recording for evidence to protect the right of privacy and sue the interviewers and their companies, the suits against interviewers for the violation of privacy protection seldom happen in China due to multiple reasons, which would be introduced later.

An interviewer of an employer explains that the questions are for the interests of enterprises because an employer hopes the staff needs to be stable. If a woman applicant has a boyfriend in another city, the possibility for her leaving the enterprises would be greater and the enterprise would have to recruit another one to start from the beginning to train the new employee, which would result in loss of the enterprises.[19] Actually, this explanation only partly explains one aspect of the personal information collections, more other economic reasons would be discussed later.

With the purpose of acquiring more information that job applicants do not want others to know or do not want to disclose, including drug-taking, sexual orientation and aids, some enterprises start to use high-tech electrical testing methods, such as polygraph, psychological stress evaluation and integrity test. The use of such equipments furthers the infringements of the privacy rights of the employees, because, facing such equipments, employees have to tell the truth even concerning the questions that will infringe their rights.[20] However, no concrete rules are established on whether or when such equipments could be used.

B. Medical check

Usually, after the interview, employer will pick up the prospective employees and have them medically checked. Usually, the hospitals where the medical checks are carried out are arranged by employers. Since there are no special regulations for the contents of the medical check for non-governmental organization and companies[21], the checking items are usually decided by hospitals or employers, or both of them. The fees of the medical checks are usually paid by job applicants themselves. Also, the medical checks tend to be thorough and detailed because hospitals also want to make more money. The purpose of the medical check is to collect the health information of job applicants, which would be of great help for the employer to avoid certain risks in the following several aspects.

First, if an employee gets ill and asks for sick leave during employment, an employer shall pay the sick employee in accordance with the standard that is not less than 80% of the local minimum wage[22]. Also, an employer needs to hire someone else to replace the sick employee, which will increase the cost of an employer. According to total working years of an employee in the current working unit and other working units, the sick leave period may vary from 3 to 24 months.[23]

Second, if an employee is seriously ill or injured out of job and could not get back to

[18] *Privay Inquiery in the Process of Job Application of University Woman Graduates*, South Metroplis, March 9, 2002. http://finance.sina.com.cn/g/20020309/178492.html

[19] *The Privacy Infringement in the application for Jobs.* http://news.sohu.com/65/92/news148099265.shtml.

[20] Jinlong Wang, *Privacy Protection of Employees from the Perspective of Harmonious Organization*, Journal of Human Resourse Development in China, No. 7, 2006.

[21] As for the recruitment of public servants, there is *Unified Standards for Recruitment of Public Servants (trial implementation) 2005*.

[22] See article 9 of *Rules on Wage Payment of Enterprises in Shanghai*.

[23] Article 3 of *Rules on Medical Periods of Ill and Injured Employees of Enterprises*.

work after the sick leave period expires, an employer is entitled to terminate the labor contract on the condition that (1) it shall notify the sick employee of the termination one month earlier[24]; (2) it pays the sick employee severance fee according to the standard of one month's average wage for a year's working; (3) it pays medical subsidy no less than 6 month's wage, if an employee is fatally ill, the medical subsidy shall be another no less than 6 month's wage.[25]

Third, according to *Regulations on Industrial Injury Insurance of China*, if an employee has sudden illness in the workplace and he/she dies within 48 hours from the time the illness occurs, it shall be deemed a death resulting from work.[26] Also, if an employer does not pay the industrial injury premium, the employer shall pay all the compensation, which would be a big sum of money.[27] If an employer has paid the premium, it still needs to pay wage and nursing fees during the period when an injured employee could not work and the wages paid by an employer, normally shall be less than one year.[28] Due to the risks mentioned above, an employer has very strong motives to have the health of job applicants checked thoroughly in order to prevent the subsequent risks.

The former analyses are based on the assumption that an employer abides the law and pays the social insurance premium as required by the laws. But actually, according to the past investigation, lots of employers did not pay social insurance premium. Statistics shows that after the enforcement of *Labor Contract Law in 2008*, the income of social insurance premium has increase a lot, from 1081.23 Billion in 2007 to 2404.32 billion in 2011.[29]

The problem of an employer refusing to pay social insurance premium is deeply rooted in the current social security system. Most of the social insurance funds are operating in the county level. There are over 2000 counties in China and there are five kinds of social insurances, including pension, medical care, industrial, unemployment and birth. All together, there are over 10,000 individual social insurance funds.

Currently, the social insurance premium is quite high in China. For example, in Hefei, capital city of Anhui Province, whose economic status is in the middle in China, its monthly minimum wage in 2013 is 1260 CNY. However, employers and employees are required to pay the social insurance premium according to the local social average wage, which is 2,305 CNY monthly. According to this standard, an employer shall pay 736.47 CNY monthly and an employee shall pay 253.55 monthly for the social premium, even if an employer pays the employee minimum wage.[30] The monthly the social insurance premium is about 60% of the minimum wage, which may be the highest in the world.

In the developed areas along the southeastern coast areas, the workers mostly migrate from the countryside of other cities, and mostly from other provinces. Because the workers often migrate from one city to another, the labor inspections do not enforce the social insurance law very strictly so as to create more relaxed environment for the enterprises, which is of benefits to improve the enterprises' principle positions in the market. Also the profitable operation of the enterprises will bring tax income for the local government, while the strict enforcement may kill enterprises or force them to move to other places

[24] Article 6 of *Rules on Medical Periods of Ill and Injured Employees of Enterprises*.
[25] Article 6 of *Regulations on Economic Compensations for Breaching and Terminating Labor Contracts.*
[26] Article 15(1) of *Regulations on Industrial Insurance.*
[27] Article 62 of *Regulations on Industrial Insurance.*
[28] Article 33 of *Regulations on Industrial Insurance.*
[29] See: *Yearbook of Labor Statistics of China*, p.359.
[30] See: *Some Regulations on Improving the Rapid and Steady Economic Development* by Hefei Municipal City on July 3.

where the law enforcements are loose. Therefore, local governments have impetus, and local enterprises have the interests and needs in enforcing social insurance regulations loosely.

However, the employers would take the risks for not paying social insurance premiums. According to the current regulations, an employer needs to reimburse the money if the social insurance expense occurs and an employer has not paid the premium. If an employee becomes ill, his employer needs to reimburse the medical expense according to the standards of the medical insurance regulations. If an industrial injury occurs, an employer shall compensate the injured worker according to the standards of the industrial compensation laws. Now the industrial compensation standards are quite high. If a worker dies in the process of work or resulting from work, an employer shall pay over 518,000 CYN in 2013 according to the standard. The high compensation standards and high social insurances fees have put great burden on employers, which force them, especially those who do not pay social insurance premiums, to screen out applicants who are potentially of great risks for employers based on the personal information collection and medical check.

C. Discrimination in the process of hiring

Because of the risks and pressures employers are facing and the relaxed environments of getting the personal information or even privacy of the workers, an employer has chance to abuse the situation and maximize their interests. Thus, lots of discrimination problems occur in present China. Also, lots of bias exists towards a certain type of people which aggravates the situation of discrimination because the general public is not well educated.

1. Discriminations relating to sex and age

For the reason of worrying about the cost resulting from hiring women of childbearing age, especially married or unmarried women who have no children, the employers would try their best not to hire women of childbearing age. An investigation conducted by Women Legal Research and Service Center of Beijing University showed that 23.6% of the women university graduates investigated had the experience of being refused of the job opportunities for the reason of being women; 16% had the experiences of being refused even if they had better academic performances in the university than men graduates.[31] The existing problems result from the imbalance between the protection of women employees[32] and the insufficiency in the protection of personal information and privacy in civil and labor laws.

Another common discrimination relating to it is age discrimination. Because an elderly worker has more chances of getting ill or suffering from the dangerous disease of high blood pressure and heart attack. Therefore, applicants who have potential possibilities of disease occurrence, for example, those who have high blood pressure, heart disease, etc., would be difficult to get employed. Often it could be seen that the job advertisements in which specific age period is listed as a requirement.

[31] Hong Liu, Serious Sex Discrimination in the Applications for Jobs of Females, http://www.legaldaily.com.cn/bm/content/2009-06/15/content_1104870.htm

[32] *Labor Contract Law of China* and *Special Protections of Woman Workers of China of 2012* provides detailed and extensive protections for woman employees, including training (article 3), scope of work (article 4), wage & labor contract (article 5), workload (article 6), leaves (article 7), maternity subsidies (article 8), baby nursing time (article 9), facilities (article 10), which would greatly increase the expense of employers.

2. Discriminations relating to diseases

All employers would like to create a safe environment for employees. However, employers would screen out some job applicants because of bias. A common discrimination in China is hepatitis B discrimination. After the medical check, if job applicants are identified as carriers of hepatitis B, many employers, including government agencies, would refuse to employ them. Some lawyers of non-profit organizations having been devoting to fighting this kind of discrimination. In 2005 Ministry of Personnel and Ministry of Health in 2004 issued *Unified Standards for Recruitment of Public Servant (trial implementation)*, which makes clear that hepatitis B carriers could be recruited as civil servants. However, this regulation does not apply to the employer of non-government agencies. Often, this kind of discrimination occurred. For example, in *Sheng Lei v. Nokia Guangzhou Company*, Lei was denied of the job because he was a hepatitis B carrier.[33]

Another group of people that are greatly biased are HIV carriers. In current situation in China, there is nearly no chance for a person with HIV positive to get a job. Although we have had some pioneering suits concerning anti-discrimination for aids patients and advocating equal employment opportunities for them, the suits are doomed to fail. For example, in a lawsuit against an employer for aids discrimination in Anqing City, one of major cities in Anhui Province, the court of the last appeal holds that HIV positive is a contagious disease, that the job applicant is denied of the job is justified.

3. Genetic discrimination

According to the research, genetic test includes genetic screening and genetic monitoring. Genetic screening is mainly done to job applicants so as to find out the tendency of getting a specific disease, while genetic monitoring is done to find out the possibility of getting a certain type of industrial disease.[34] The genetic information is possibly misused and resulted in genetic discrimination without proper regulation. There is no regulation regarding genetic discrimination in labor law or other laws. However, genetic discrimination has already occurred in China. In the medical check arranged by governmental agency during civil servant recruitment, an applicant was identified to have thalassemia and was eventually refused of the job. The applicant brought a lawsuit and still lost the case. The court of the final appeal held that the employer did not disclose the information to the public and therefore no right of privacy was infringed. [35]

At present, the genetic test is used for the interests of employers to screen out the job applicants for the reasons including: health of employees would influence their work performance; the sick leave of employees would cause the problems of work arrangement; the illness of employees would increase the cost of employers; the resignation of employees would increase the cost of recruitment and training; employers would suffer great loss if employees get industrial injuries due to the reason of genetic problems.[36]

Of course, genetic test and monitoring has several advantages: management efficiency could be improved; the possibility of get occupational diseases could be greatly

[33] Ten Famous Labor Disputes in 2007 Ranked by Legal Daily, http://news.ifeng.com/mainland/200801/0120_17_371631.shtml

[34] Shenghua Luo, *Legal Protection of Genetic Privacy Rights*, Science Press, first ed. July, 2010, p. 184-185.

[35] Yong Wei, *Some Questions and Thinking on the First Case concerning Genetic Discrimination of China,* Journal of Medical Science and Philosophy (Humanistic & Social Medicine Edition), No. 8. 2011.

[36] Shenghua Luo, *Legal Protection of Genetic Privacy Rights*, Science Press, first ed. July, 2010, p.185.

reduced; the efficiency of human resources management could be advanced.[37] However, in order to prevent the abuse of genetic information, it is suggested by academics that the following rules should be enforced: the genetic test should be legal; the extents of getting genetic information of employers should be limited; employees should be notified that the genetic testing would be taken when applying for the jobs; the genetic information should be only used for safety and health of workers and strictly controlled; employees are entitled to check their own genetic information and to rectify it if wrong.[38]

There is no systematical investigation to show how serious the situation of all form of the discriminations is because only individual cases are repeatedly reported. Generally speaking, two factors will influence the whole situation. The first is whether employers know how to make full use of the current legal environment and willingly to take advantage of the favorable situations. The second is that how many employees clearly know their rights in personal information and privacy and fight for the rights willingly and bravely. Though we do not know the exact situation, from the repeated reports, it could be concluded the whole situation could be serious.

IV. The protection of personal information and privacy during employment

A. Personal information collection during employment

1. Annual medical check

During the period when the labor relations exist, many employers would demand that the employees take annual medical check arranged by employers. Different employers take different attitude towards the medical check, and the requirement and operation modes are also different according to ownership, scale and social insurance backgrounds of the companies.

In the state-owned enterprises, the core employees usually enjoy permanent employment. The annual medical check is a welfare provided to them by the companies. Generally, the time used for the medical check is considered the working time. For the companies, the information obtained from the medical check is also very useful for the human resource management. Also, if an employee is found to be ill of some specific diseases, the employee could take medical treatment earlier, which would help to save money for the companies. Of course, the results of medical checks could be an element for the promotion decisions. However, no disputes concerning this have been reported to public so far.

However, for the non-core employees, especially for the dispatched employees, annual medical check may become a method of screening out some unhealthy employees. The relationship between the health of employees and the cost risk of employers has been discussed in detail previously. A dispatched employee who suffers from serious illness or fatal illness, or suffered from some form of seizure and is pronounced dead, will greatly increase the expenditure for an employer.

As for the private enterprises, especially small enterprises that do not pay social premium, annual medical check could be an important way to screen out the employees whose health could bring risks to companies. Otherwise, a serious industrial injuries or death could bring down small enterprises that have not been covered by social insurance

[37] *Ibid.,* 186.
[38] *Ibid.,* 191.

for they do not pay the social premium.

There are frequent privacy infringements and unfair dismissals resulting from annual medical checks. For examples, one case is about the protection of privacy of medical check reports, in which a company put all the unclosed medical check reports in the office and asked employees to go to the office to take their own reports. Therefore, employees had chances to read and spread the health information of others.[39] In *Wen Wang v. Guangzhou Baiyun International Conference Center,* the company even publicized the results of the medical check by putting the names of who were checked out to be hepatitis B carriers on a blackboard in the company. [40] Those cases show in some degree that the legal conception of protection of personal information and privacy are quite limited in some companies.

There are many other reports on the internet concerning unfair dismissals because of hepatitis B found out in medical checks arranged by the company. Because there are no systematic studies and wide investigation, we do not have detailed statistics as far as the medical check and infringements to personal information and privacy are concerned. But from the great economic interest of employers relating to such information and the situation that employees are not adequately protected, it could be concluded that the situation could be very serious throughout the whole China.

2. The collection of other information

Apart from the collection of health information, in the period when the employment relationship exists, employers also collect other information of the employees. A very common practice in China is that employees are required to fill out an Annual Employee Evaluation Form every year. Usually, the form is designed very carefully, which requires employees to refresh their personal information, such as mailing address, residence, telephone number, email, family information, work accomplished, comments of the leaders, contributions and evaluation.

There are justifications for the collection of the information. First, the information, especially those regarding to the work evaluation and comments of the leaders are very important basic information for rewarding, promoting and arranging the positions of the employees. Also, the mailing addresses of employees are of importance in dismissing the employees. In accordance with *Some Interpretations Regarding the Applications of Laws in the Trials of Labor Dispute Cases* issued by People's Supreme Court of China（II）, for the labor disputes arising from terminating or ending an employment, if an employer cannot prove the time when an employee receive the notice of such termination or ending, the date on which an employee claims his/her rights shall be deemed the date on which the labor dispute occurs. If the employer terminates the contract but the employee refuses to sign on the notice, the employer needs to post the letter of notice so as to meet the requirement of the law.

B. Surveillance in workplaces

1. Surveillance

In the workplace, many employers put the employees under surveillance. According

[39] *Employers Should Pay Attention to the Protection of Privacy of Employees in Distributing Medical Check Reports*, Yanzhao Metropolis, http://roll.sohu.com/20110918/n319692955.shtml

[40] *Sunling Wu & Yinyue Li, Court Held that Company Infringed the Rights of Employees by Putting the Names hepatitis B carriers on Public Blackboard*, Southern Metropolis, August, 27, 2013. http://news.sina.com.cn/s/2013-08-27/033928054266.shtml

to an investigation conducted by sina.com, a famous website of internet service, the answers to the question—"According to your knowledge, are you under surveillance of the employers you work for?" are collected. 23.35% answered that they were under surveillance but not including the surveillance activities on the internet. 30.61 % answered that they were under surveillance, including the email and communication tools. 46.04% answered that they were not sure whether that they are under surveillance.[41] For those employees who work outside of the premises of employers, some employers also try to put them under surveillance. For example, it is reported that an express delivery company equips employees with cell phones and tries to monitor the employees by stocking the positions and time of stops of them.[42] The other surveillance methods also include wiretapping and recording, which are very common for the on-line service industries.

2. Reasons for controlling

According to the research of a Chinese scholar, in the process of work, employer needs to observe the work process of the workers for many reasons: preventing the theft (including invisible property like trade secrets); finding out malfeasance or self-profiting of employees by take advantage of their positions so as to protect the economic interests of the employers; finding out the behaviors like being lazy, going slow, or even sabotaging so as to improve the efficiency and ensuring the quality of products, finding out the unsafe elements with the purpose of improving work safety; finding out the unreasonable arrangements of work so as to improve the managements; finding out unreasonable and unsafe operation for the improvement of the future training.[43]

Another researcher points out that there are four aspects for the justification of personal information collection and surveillance. First, it is for the efficiency of the workplace. [44] Due to some unfavorable elements, such lack of skills, psychological problems or physical defects, workers' ability to accomplish the jobs will be influenced. Therefore, an employer has justifications to get relevant information. Second, it is for the avoidance of vicarious liability. If an employer puts an employee under surveillance, it will actively watch over the behaviors so as to control employees in the prevention of infringements. Third, it is for the protection of the property of employers. Employers provide jobs for employees. However, the properties of employers are under control or management of employees. Therefore, employers need to keep a close look at workplaces by the use of advanced apparatus. Fourth, it is for the abidance by law. For example, article 19 (4) of Prevention and Control Law of Occupational Diseases of the PRC stipulates that the employer shall keep files on occupational health and files on monitoring and protecting the workers' health, and improve the practice for the prevention and control of occupational diseases.

The purpose of investing to operate enterprises and organizing managements of employers is to make profits, which is of justice and should be protected. Therefore, the employers are entitled to install video cameras so as to protect their own property and to improve the management. However, the personality of the employees should be respected

[41] Yulang Hu, *Email Monitoring and the Legal Protection of Privacy of Employees*, No. 3, Legality Research, 2009.
[42] Guangcan Li, *A Company Provides Employees with Cell Phones Used for Employee Tracking*, http://www.daynews.com.cn/stock/193604.html.
[43] Xinbao Zhang, *The Protection and Limitation of the Privacy Right Protection of Employees*, Journal of Modern Law, No.5, 1996.
[44] Feng Pan, *On the Protection of the Right of Privacy of Employees: An Analytical Frame*, Hebei Law Review, July, 2008.

and protected at anytime at anywhere, including the workplaces. At the workplace, employees need some privacy: they need feel safe when they use toilets as they are at home. They maybe need feel at ease to talk with colleagues about their own family matters; they need feel secure to keep some personal things, such as mails and photos; they need feel free to make or receive private telephone calls in their spare time[45].

3. Balance of interests

It is true that employers have justification to watch over the workplace. However, if their rights are not properly limited, the rights of employees will be infringed. In China, there are already some reports regarding it. In the lawsuit of *Xiaoyan Chen v. Donghai Co.*, Jinhuang Lin and Chunning Chen, Xiaoyan Chen and Yingfang Jiang are employees in Accounting Department of Donghai Company Ltd. At the end of April, 1996, general manager Chunning Chen bought wiretapping equipments and installed in the office of Xiaoyan Chen and Yingfang Jiang with the purpose of finding out whether the two employees were loyal to the company. General Manager Chunning Chen wiretapped the talks between Xiaoyan Chen and Yingfang Jiang in his own office. Later, vice general manager Jinhuang Lin participated in the wiretapping. When Xiaoyan Chen got to know that she had been wire tapped, she became very depressed and then sued the company and the two managers. The trial court held that Xiaoyan Chen's rights of personality were protected by law, and Donghai Company should apologize to Xiaoyan Chen in the company and compensate 3000 CNY for damages. Xiaoyan Chen was not satisfied with the damages and appealed to the Intermediate Court, which affirmed the judgment of the trial court. [46] In another case in Shenzhen, Guangdong Province, there occurred several thefts in a private watch factory, a strongbox was broken with more 600,000 CNY stolen, and also watches were often reported stolen. In the prevention of future thefts, surveillance cameras were installed in the workshops, canteens, on the road in the premise of the factory, and even in men's toilets. The workers felt insulted and some workers called to tell the mass media. After that the cameras were removed under the pressure of reports.[47]

As to the justice of video surveillance, there are different opinions. Some thinks the private property owners are entitled to protect their own property. Other believes that the rights of the privacy of the workers are infringed by installing video surveillance in the toilets. [48] As to the balance between the protection of the properties of the owners and the privacy of the workers, a researcher summarizes several points. First, the purpose of video surveillance must be legal, such as protecting the property, increasing the work efficiency, ensuring work safety. Second, the employers should notice the workers of the installment of video surveillance. Third, the premise of the employers should be divided into public area and privacy areas, it should be prohibited that surveillance cameras are installed in privacy districts, such as toilets in above cases. Fourth, the video records should be kept in safe place out of the reach of irrelevant persons.[49]

Generally, in China, there is no more surveillance after the working time. However, the off-work activities of employees are still related to employment. An employee can get

---

[45] *Ibid.*

[46] He Huang, *On the Conflicts and Coordination Between the Rights of Privacy of Employees and the Right to be informed of employers: the lawsuit of Xiaoyan Chen v. Donghai Co., Lin Jinhuang and Chen Chunning,* Journal of Yunnan University (Law Research Versrion), Volume 18, No. 2, 2005.

[47] Surveillance in the Toilets and Workers Sued for the Protection of Privacy, http://news.sohu.com/34/01/news148300134.shtml

[48] Daqing Liu, *Legal Rules of the Protection and Limitation of the Privacy rights of Enterprise Emloyees*, Journal of Liaoning Business Institute (Social Science Version), No. 3. 2003.

[49] *Ibid.*

disciplined if he/she is committed to immoral activities after working time. There are some reports concerning that. For examples, there are two cases in 2013. One is concerned with that a head of Health Bureau of a city had an affair with a head of a local public hospital, and the video record of the two going into a hotel room was put on the internet, and later both of them were removed from the administrative position. [50] In another case, a chief judge in a supreme court has an affair with a lady and the video record of the two going into in a hotel a room was also put on the internet, and then he was discharged of from the position of chief justice. An article criticized that the punishment was too light. As a judge, he should be further punished in accordance with *Law of Judges of China*.[51] It should be noted that the persons involved in that above cases are public servants. The results may be different as for private employees. However, no relevant cases have been reported for private employees.

V. Personal information and privacy protection in post termination period

In China the protection of personal information and privacy is closely connected with personnel file management and the liabilities of employers to protect the private information of the employees.

A. Personal information protection

During the planned economy period, strict rules regarding personnel file administration were practiced. However, in nowadays, under the market economy, employers' attitudes towards records management are quite different. The government agencies, along with public non-profit organization, such as schools, universities, research institute and hospitals, still enforce very strict personnel file management rules. In the state-owned enterprises, the management of personal files of employees is still very strict. The annual results of evaluation of individual employees are kept in the personal individual files as record as basic information for future rewards, grade classification, promotion and social insurance, etc. But in the private enterprises, the personal file management system would be quite loose, especially in small enterprises, which usually do not keep the detailed records of employees because of that employees turn round quickly in such working units.

In practice, in some employer unit, especially the public non-profit organization and some state-owned enterprises, the personnel files are very important to employees. In transferring from one employer to another, an individual employee shall have his/her personal file record transferred to the new employer. The new employer could not accept the transferring without the personnel file coming together with the employee. Therefore, some employers would try to refuse the transferring of the personal files so as to stop the employees from leaving.

But market economy demands that all resources be allocated through markets, including human resource market. To block the transferring of personnel file is an action against the mechanism of market mechanism. In order to deal with this abnormal phenomenon in the transferring of personnel files, *Labor Contract Law of China* stipulates

[50] *Weekly Figure, Exposure of the Video of Hotel Room Renting by A Bureau Leader and Head of A Hospital,* http://hjsb.hj.cn/Read.asp?NewsID=891841

[51] Editorial: *Hotel Room Renting by Chief Judge May Be not a Private Business*, The Beijing News, December 11, 2013.

that within 15 days from the termination or end of labor contract, the employers should transfer the personal files to the employee's new employers (article 50).

Another problem about personnel file administration is that no individual has the rights to check the information of his personnel file and knows nothing of the information in the file.[52] This problem often causes disputes when workers argue that information in the file are not correct and influence their pensions.[53] Therefore, the protection for rights concerning personal information in the personnel files need to be improved.

B. Privacy protection

Some employees have the obligation of non-competition after employment relationship ends. In practice, employers always expect employees to abide such an obligation and in order to meet the expectation they sometimes maybe infringe the privacy of employees. For example, it was reported Gamigo Online Entertainment in Shanghai published the names, identity numbers and photos of six former employees who were bound by non-competition agreements with the purpose of protecting their own interests, and notified the public that companies who would employ the employees would bear legal liabilities.[54] Undoubtedly, Gamigo Online Entertainment infringed the privacy of the six employees.

New prospective employers would often like to get information about the job applicants from their former employers. However, there are no regulations on what former employers should provide to new employers; whether the former employers should provide all the information, including the punishments by former employers; whether a job applicant has the right to know what information the former employer has provided to the new prospect employer. Undoubtedly, the negative evaluation by former employers would greatly influence the chances of job application. However, in China there are no regulations regarding it.

VI. Comments and foresights

A. Comments on the current protection of personal information and privacy

From the current legislations, it could be concluded that China has already had initial systems on personal information and privacy protection. The regulation for the protection of personality of citizens in Constitution lays a foundation for the construction of the protection system, which could be applied when the rights of personal information and privacy are infringed. Also, criminal punishments have been provided where personal information or privacy is very seriously infringed or serious consequences are resulted from the infringements. However, from the wide-spread infringements of personal information and privacy rights introduced above, it could be said that the current regulatory scheme in China has not provided effective regulations and remedies. As discussed above, the essential regulations for the protection of rights of personal information and privacy of the employees are in the civil laws. But the current situation makes it clear that the civil law protections are not enough. The limitations of the civil law protections are in the following aspects:

---

[52] Jinsong Sheng, *The Protection of the Right to Know the Information in Personnel File and Legislation Improvements,* Social Science Forum, No. 2, 2006.

[53] Jinrong Li, *Who Changed My Personnel Files,* Sichuan Labor Security, December, 2006.

[54] Shuiyuan Luo, *Gamigo Online Entertainment Company Published the Information of Employees Leaving Office and Accused of Infringements by Employees*, Newspaper of News, September 1, 2006.

First, the remedies for the infringements of personal information and privacy are far from enough for the awards of damages. The judgments of the lawsuits showed that the employees who had won the cases of suing for the infringements of personal information and privacy and could only get very limited awards. For example, in *an applicant v. Decang Dynamo (Shenzhen) Co. Ltd*., the applicant entered into the defendant's company after graduating from a university. In a medical check arranged by defendant, the applicant was found to be carrier of hepatitis B and thus was fired by defendants. The applicant brought a civil litigation and only won 3000 thousand CNY for spiritual distress. In most of the cases, the applicants could only get apologies from employers and less than 10000 CNY for damages and mental distress. Sometimes, the damages are less than the attorney fees, not to mention the waste of time and mental suffering in the process of trials.

Second, the procedures are long and the cost is high for the civil lawsuits. Generally, it needs at least one year to finish the lawsuits of two trials, and the attorney fee cost would be over 10000 CNY for a simple common case. Even, an employee wins the case; the attorney fees he/she pays could not be recovered. Considering the limited rewards and the long high cost of the lawsuits that are usually full of hardship. Nearly all employees will choose to eat the humble pies and give up the legal efforts to claim for remedies when thinking of the difficulties and high cost of lawsuit in the protection of personal information and privacies. Such situations would in return encourage the employers to abuse the favorable situations.

Third, the protection of personal information and privacy has not been paid its due attention by the governmental agencies. In the current social background it would be quite difficult if an employee turns for help from the labor inspections for the infringement of personal information or privacy. Normally, the labor inspections pay more attentions to the material interest protection like back pay problems.

Forth, the cases that have been won have not produced great social influence due to the civil litigation structure. In China, normally a civil law case ends at the intermediate court and the judgments are not open to the public because they are related to privacy. Therefore, outside the jurisdiction of the intermediate court, the public would not know the case and the results. Such a system has greatly limited the influence of the cases, making it difficult for improving the consciousness of rights of personal information and privacy.

The current situations of personal information and privacy protection are decided by several factors.

First, current Chinese labor law system started from 1995 and it could not be comprehensive in such a short time. China maybe needs another 30 year to accomplish industrialization, during which the labor law protection for employees would be gradually improved.

Second, it is quite normal that the legislation focuses more on the material interests than personality interests at such a development stage. From the damages awarded by court, it could be inferred, personality interests including personal information and privacy is now despised.

Third, the existing problems are partly resulted from the imbalance between the protection of employees, especially for the ill, industrially injured and women workers, along with the problems existing in the social insurance mechanism and district interest conflicts. All of the above factors combine together to result in the current situations.

B. The future legislation and directions

1. Protection would be strengthened in civil laws.

At present, the protection for personal information and privacy has not been paid enough attention. But the civil scholars have been studying this field and advocating new legislations on it. The Draft of Civil Code of China (DCCC) prepared by scholars suggests more clear regulations on privacy, which provides that "natural person is entitled to enjoy the right of privacy, and privacy is prohibited to be stolen, wiretapped, recorded or filmed secretly. It is prohibited to publicize or make use of the life secrets of others or act in other ways which would infringe personal privacy without consent unless otherwise provided by law. Also, Article 376 of DCCC provides that an employee's right of privacy in the workplace shall be protected by law, and an employer shall take actions to control workplaces which would not do damages to the privacy of employees by using video-taking, recording, surveillance, testing or other measures, and such measures should be limited to necessity. Base on the researches and advocates, personal information and privacy protection would be strengthened in the future.

2. Labor law protections would get more attentions.

Some Chinese scholars have studied the specialty of employment relations and pointed out that labor relation is different from the civil relation. Labor relations contain social elements in which the employees are subordinated to the employers economically and personally.[55] Therefore, special rules need to be set up for the protection. It has been suggested that more and clearer regulations on the collection of personal information and workplace surveillance should be put into practice in order to stop the abuse of personal information and the improper work surveillance.

With more and more cases and researches coming out in the future, the legislators would pay more and more attention to the imbalance of the interests between the protection of women and senior workers and the risks and costs of employers, from which they would try every possible means to avoid. Also with the development of economy, the courts would be paying more attention to the personality rights of employees. As for the problems existing in the social insurance systems, China has just proposed to establish nationally unified social insurance system which covers all the farmers and employees.

In all, China is a big country that has been in the process of rapid transformation. In the process of quick economic, social, political development, the existing problems including the problems in the protection of personal information and privacy could be hopefully solved gradually along with the deepening of political reforms and development of labor laws, social security laws and the reforms of judicial system.

[55] Feng Pan, *On the Protection of the Right of Privacy of Employees: An Analytical Frame*, Hebei Law Review, July, 2008.

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

Sung-Wook Lee*
Ewha Womans University

I. Introduction

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

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

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

---

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

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

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

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

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

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

---

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

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

A. The Constitution

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

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

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

1. Purpose and Scope of the Law

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

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

2. Scope

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

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

---

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

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

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

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

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

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

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

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

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

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

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

3. Principle of Personal Information Management

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

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

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

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

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

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

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

4. Relief Procedure in Case of Violation

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

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

---

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

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

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

C. The Protection of Communications Secrets Act

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

F. The National Human Rights Commission Act

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

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

---

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

leakage of personal information.[66]

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

G. The Labor Legislations

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

IV. Personal Information Protection in Recruitment Process

A. Consent from Applicant

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

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

---

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

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

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

B. Scope of Collectable Personal Information

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

V. Protection of Personal Information and Privacy in Employment

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

1. Installation of CCTV, etc. in the Workplace

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

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

---

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

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

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

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

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

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

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

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

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

2. Surveillance by Monitoring Internet and E-mail

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

VI. Conclusion

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

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

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

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

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

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

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

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

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

---

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

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

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.

Protection of Employees' Personal Information and Privacy in Taiwan

Shih-Hao Liu[1]
Ming-Chuan University

I. Introduction

1. New Tools Change the World

Historically, employees have been disadvantaged in the context of employment relations, and their rights of freedom and personality have been relatively restricted. The protection of legal personality and, particularly, privacy has undergone substantial changes in modern society following the development of novel technologies that can be used in the workplace, including monitoring equipment, hidden cameras, and devices for monitoring computer networks or telephones. Consequently, employee rights of personality can be affected by a new crisis.[2]

Moreover, through activities associated with employment relations, employers can easily acquire private information about employees. Even before an employment contract has been formalised, employers can collect personal information from job applicants. During the hiring process, employers or human resource managers can request personal information from applicants, including their address, health, marital status, age, ability, and educational background.[3] Through employment relations activities, employees may be required to perform or undergo various tests, such as personality tests and health examinations, which can be used to acquire private information from employees. Thus, protecting the personal information and privacy of employees is crucial in modern society.

2. Historical Background of Taiwan

Taiwan's laws for protecting personal information and privacy were established relatively later than those of most other countries, undoubtedly as a result of the relatively recent transition to democracy and social freedom that manifested following the lifting of martial law in 1987. Taiwan began developing its legal system for protecting personal information, data, and privacy in 1990s. The promulgation of the Computer-Processed Personal Data Protection Act on August 11, 1995 was a milestone in developing laws for protecting personal information.[4] Before 1990, Taiwan's Civil Code protected private

---

[1] Professor, Law School, Ming-Chuan University, Taiwan.

[2] See Liu, Shih-Hao, Protection of employees' personality in the network society, Cheng-Chi University Labor Journal, Vol. 12, 2002, PP. 187.

[3] See Zhan, Sheng-Lin, The right of employers to ask the jobseekers, Formosa Law Review, Vol. 63, 1992, PP.2-12; Liu, Shih-Hao, Protection of employees' personality in the network society, Cheng-Chi University Labor Journal, Vol. 12, 2002, PP. 204.

[4] Wang, Zhe-Zhien, Subject and Development of Protection for Personality, Taiwan Law Journal, Part III,

interests mainly in the form property, but not in the form of legal personality, although Article 18 of the 1929 Civil Code provided declaratory protection of these rights.[5] The right of privacy was not regulated specifically for legal personality until the Civil Code was amended in 1999 (Article 195). Following the rapid development and diffusion of information technologies, personal information and privacy have become prominent legal concerns in Taiwan. As democracy and the rule of law have progressed, the people of Taiwan have increasingly emphasised the importance of protecting privacy and personal information. Furthermore, several notable legal cases involving the abuse of personal data have emerged, and recent cases have typically involved the fraudulent misuse of personal information. The Computer-Processed Personal Data Protection Act was replaced with the Personal Data Protection Act (PDPA), which was amended in 2010 and promulgated in 2012; moreover, its coverage for protecting privacy is broader and more assertive.[6]

Protecting the personal information of employees has gradually received a greater attention in Taiwan. The courts in Taiwan have heard only a few cases involving the violation of employees' personal information, primarily because the PDPA has been implemented for only one and a half years. In particular, some cases have been crucial in setting a precedence for future judgements.

II. Regulatory Schemes for Protecting Employees' Personal Information and Privacy

Over the past 27 years since martial law was lifted, Taiwan has undergone rapid economic development and considerable development in consolidating democratic constitutionalism. Consequently, social structures and values have emerged based on ethical foundations for promoting human dignity.[7] The following section details the regulatory schemes protecting legal personality.

1. Taiwan's Constitution

The Constitutional Court of Taiwan declared that the maintenance of personal dignity and protection of personal safety are two fundamental concepts underlying the constitutional protection of the people's freedoms and rights[8]; thus, the protection of legal personality is currently a primary objective of the Taiwanese legal system. Although the right of privacy is not specifically enumerated in the Constitution, it should nonetheless be considered an indispensable and fundamental right and, thus, be protected under Article 22 of the Constitution, which focuses on preserving human dignity, individuality, and moral integrity, as well as preventing the invasion of privacy and maintaining self-control of personal information.[9] Article 22 of the Constitution, which is called the right of general freedom, states that all civil freedoms and rights that are not detrimental to social order or public welfare are guaranteed under the Constitution.

Privacy (2), Taiwan Law Journal , Vol. 97, Aug.. 2008, P. 38.

[5] Shi, Chi-Yang, The General Principle of Civil Code, 2012, P. 35.

[6] Lu, Ding-Wang, Interpretation and Practice of Personal Data Protection Act- Part I, Parliament Monthly, Nov. 2010, P.20.

[7] Wang, Zhe-Zhien, Subject and Development of Protection for Personality, Part I, Personality in Constitution and civil law, Vol. 80, Taiwan Law Journal, Mar. 2006, P. 105.

[8] The Interpretation of Justices (Constitutional Court) No. 372, Feb. 24. 1995.

[9] The Interpretation of Justices (Constitutional Court) No. 585, Dec. 15. 2004.

The protection of personal information in the constitutional rights includes the rights of information privacy and self-determination.[10] These rights, which emphasise the importance of self-control in managing personal information, are designed to guarantee the right for people to decide whether to disclose their personal information, and, if so, to what extent, at what time, in what manner, and to whom it is disclosed. Furthermore, they are designed to guarantee the right to know and control how personal information is used, as well as the right to correct inaccuracies.[11]

2. International Law

In 1971, Taiwan lost its United Nations member status and withdrew from the International Labour Organisation. However, on April 22, 2009, the Taiwanese government announced the Act to Implement the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights, which was designed as a platform for implementing the International Covenant on Civil and Political Rights as well as the International Covenant on Economic, Social, and Cultural Rights (both of which were adopted by the United Nations in 1966), and to strengthen Taiwan's human rights protection system. Article 17 of the International Covenant on Civil and Political Rights provides a general framework for the right of privacy; specifically, Article 17 states the following:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

However, the political implications of the act for implementing the two aforementioned international covenants are far greater than its legal scope.

3. Criminal Code

A. Offenses against Reputation

An employer who infringes upon an employee's privacy or misuses an employee's personal data may be guilty of damaging their reputation. Article 310 of Taiwan's Criminal Code states that a person identifying or disseminating a fact that damages the reputation of another person by communicating it to the public is committing slander, and, if found guilty, could be sentenced to minimal imprisonment term of up to one year, short-term imprisonment, or a maximal fine of NT$500. Moreover, a person who proves the truth of a defamatory fact is exempt from punishment unless the fact concerns the defamed person's private life, and it is of no public concern.[12]

B. Offenses against Privacy

An employer who infringes upon an employee's privacy or misuses an employee's personal data could particularly compliance with prejudice against privacy in the criminal code. For example, an employer who uses concealed cameras to monitor employee

[10] Chiew, Wen-Chung, The Concept's Difference between the information self-determination and information privacy, The Taiwan Law Review, Vol. 168, May. 2009, P. 174; Shiao, YI-Hong, The Problems of the Personal Data Protection Act, Cheng-Gong University Law Review, Vol. 23, June 2012, PP.146-149.
[11] The Interpretation of Justices (Constitutional Court) No. 603, Sep. 25. 2005.
[12] Article 310, Paragraphs 1 and 3, Criminal Code.

behaviour could violate Article 315-1, which states that a person who commits an offense under one of the following circumstances could be sentenced to up to 3 years imprisonment, short-term imprisonment, or a maximal fine of NT$30,000:
1. Instruments or equipment is used without good reason to observe or eavesdrop on another person's private activities, speeches, conversations, or private body parts.
2. Audio recording devices, photography, visual taping, or electromagnetic means are used without good reason to record another person's private activities, speeches, conversations, or private body parts.

An employer who uses a computer to collect, use, or process an employee's personal data and discloses that information without good reason could violate Article 318-1, which states that a person who, without good reason, discloses the secrets of another person that are known or acquired by using a computer (or related equipment) could be sentenced to imprisonment for up to 2 years, short-term imprisonment, or fined up to NT$5,000.

4. Civil Code

Taiwan's Civil Code has protected the right of personality for many years. Since the 1929 Nationalist Government (Kuo-Ming-Tang)[13] formulated Article 18 in mainland China, "When a person's personality is infringed, they can apply to the courts for removing. When a person's personality is in danger of being infringed, a person may apply to the courts for prevention. In the preceding paragraphs, an action for damages for emotional distress may be brought only when it is otherwise provided by the act." This article provides the right of "general personality". Privacy has been considered a "particular personality" in the 1999 amendment of Taiwan's Civil Code. According to Article 195 of the Civil Code, if a person wrongfully violates the privacy of another person, the injured party may claim reasonable monetary compensation, even when the injury is not a purely pecuniary loss.

Because employment contracts are binding agreements between employees and their employers, disputes can be resolved under both tort and contract law in Taiwan. The employer's primary duty in accruing information from an employment contract is the duty of remuneration (i.e., wages or salary). In addition, based on the principle of good faith, the employer has a secondary duty to protect the life, body, health, and personality of employees.[14,15] Thus, an employer who violates an employee's privacy or misuses their personal data is in breach of this secondary duty; consequently, the employee may be entitled to compensation under the debt of contract,[16] or they may refuse to work without losing their entitlement to receive payment.[17]

5. Personal Data Protection Act

Promulgated on August 11, 1995, the Computer-Processed Personal Data Protection Act was the first law in Taiwan specifically designed for protecting personal information. It was replaced by the PDPA in 2012.

[13] Nationalist Government (Kuo-Ming-Tang) took over Taiwan after the Second War in 1945, and then the laws of Republic of China (ROC) implemented in Taiwan.
[14] Article 423-1 and Article 148 Civil Code.
[15] Liu, Shih-Hao, The main duty and secondary duty of employment relation, in Taiwan Labor Law Association edit., Interpretation of the Labor Standards Law, 2009, PP.38-40.
[16] Article 227-1 and Article 427-1Civil Code.
[17] Analogy of Article 264 Civil Code and Article 427 Civil Code.

A. Coverage of Protection

a. Personal Data

The PDPA is a general framework that is applicable to both employment and nonemployment relationships. Although it does not specifically address employees, it offers clear and specific protection of their personal data in the context of employment relationships, including their name, date of birth, national identification card number, passport number, characteristics, fingerprints, marital status, family details, education, occupation, medical records, medical history, genetic records, sex life, health examination results, criminal record, contact information, financial conditions, social activities, and other information that could be used to identify them directly or indirectly as a natural person.[18] The PDPA can protect employees from damage resulting from the collection, processing, and use of their personal information by either government or nongovernment agencies.[19] In this context, "government agency" typically refers to a public-service-based employment agency, whereas "nongovernment agency" refers to private enterprises.

b. Special Personal Data

Special personal data refer specifically to personal information such as medical records, medical history, genetic records, sex life, health examination results, and criminal records.[20] Article 67 (Paragraph 2) of the Medical Care Act defines personal information relating to "medical records" (1) a medical record produced by a physician in accordance with the Physicians Act, (2) an examination or inspection report, and (3) other records produced by medical personnel during practice. Moreover, the Medical Care Act defines "medical history" as medical records and other examination- or treatment-related information produced by doctors or medical personnel for treating, correcting, or preventing disease, harm, or disability, or for other medically due reasons. Medical history also refers to personal information produced through prescription, medication, operation, or disposition based on examination results.

In addition, according to the Medical Care Act, "genetic records" is defined as the message of a heredity unit (comprising a segment of DNA from a human body) for controlling the specific functions of the human body; "sex life" refers to sexual orientation or sexual habits; "health examination results" refer to any information produced from a medical examination for purposes other than diagnosing or treating a specific disease; and "criminal records" is defined as the records of decisions to defer prosecution or not to prosecute *ex officio*, as well as a final guilty judgement or its enforcement.

c. Normal Personal Data

Normal personal data include a person's name, date of birth, national identification card number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical records, contact information, financial conditions, social activities, or other information that can directly or indirectly identify a natural person.

B. Liability for Damage and Compensation

a. Liability Doctrine

An employer may be liable to pay compensation for damages resulting from the

[18] Article 2 Paragraph 2 PDPA.
[19] Chapters 2 and 3 PDPA.
[20] Article 6 PDPA.

illegal collection, processing, or use of an employee's personal information, or for other infringements on employee rights that are in violation of the PDPA. However, the type of liability depends on whether an offense is committed by a government or nongovernment agency[21]; specifically, strict liability applies to government agencies, whereas fault applies to nongovernment agencies.[22]

b. Compensation Systems

Regarding damages, Taiwan's Civil Law states that compensation coverage should be comprehensive. However, the amount and range of damages payable in cases involving personal information can be difficult to calculate and prove. Therefore, the PDPA adopts both comprehensive and fixed compensation systems.[23] If a victim provides evidence justifying the claimed amount of damages, comprehensive compensation may be applicable. However, in cases in which the victims may not or cannot provide evidence justifying the actual amount of damages, the compensation for each case of damages for each person is NT$500–NT$20,000 (approximately US$16.50–US$662). When damages are caused to multiple parties by the same cause and fact, the maximal total amount of compensation is NT$200 million (approximately US$6.62 million). However, if the involved interest exceeds the amount involved in the preceding sentence, the amount of interest should be set as the limit.[24]

c. Altruistic Class Action System

Some cases can have involved numerous victims whose personal data have been infringed, although an individual victim might receive only minor compensation; therefore, the PDPA adopts an altruistic class action system.[25] For cases caused by the same cause and fact involving multiple infringed parties, a charitable juridical person or entity may file a lawsuit to the court in its name after obtaining a written authorisation of litigation rights from 20 or more parties. Trade unions are a suitable example of charitable juridical entities that can act when employees are victims. Employers who violate the PDPA are liable to pay compensation for any damages, and they may be punished with criminal or administrative penalties.

C. Limitations on the Collection, Processing, and Use of Special Personal Data

Special personal data is sensitive personal information that requires considerable privacy; thus, strict protection measures are necessary. Although these data should not be collected, processed, or used, the following situations are exceptions to these limits:

1. The information is collected, processed, or used in accordance with the law.
2. A government agency must collect, process, or use the information to perform its duties or a nongovernment agency must collect, process, or use the information to fulfil its legal obligations (provided that appropriate security measures are in place.
3. An affected party has disclosed the information by himself or herself, or the information

[21] Article 28 PDPA.

[22] See Ministry of Justice, The Explanation of Draft "Personal Data Protection Act", May 26. 2010, in Ministry of Justice, The Compilation of the Legislation and Reference of "Personal Data Protection Act" Aug. 2013, P.54.

[23] See Lu, Ding-Wang, An Introduction of the Personal Data Protection Act, The Taiwan Law Review, Vol. 183, Aug. 2010, P. 142.

[24] Article 28 PDPA.

[25] Lu, Ding-Wang, Interpretation and Practice of Personal Data Protection Act- Part II, Parliament Monthly, Dec. 2010, PP.39,40.

has been publicised legally.
4. A government agency or academic research institution employs specific methods to collect, process, or use the information for the purpose of medical treatment, personal hygiene, or for calculating crime prevention statistics or conducting research.

Although the infringement of privacy or misuse of personal data could be offenses against reputation, or offenses against privacy in according to the Criminal Code, the PDPA addresses the shortfall of the Criminal Code by ensuring the protection of personal data and privacy.[26] An employer who violates an employee's rights by collecting, processing, or using special personal data without good cause is subject to a maximal sentence of 2 years imprisonment or custody, a maximal fine of NT$200,000 (approximately US$6,620), or both. A person who intends to unlawfully profit by committing such a violation can be sentenced for up to 5 years imprisonment and fined up to NT$1,000,000 (approximately US$33,100).[27]

D. Limitations on Collecting, Processing, and Using Normal Personal Data

An employer should not collect or process normal personal data unless it is collected or processed for a specific purpose and should comply with one of the following conditions[28]:
1. The information is collected, processed, or used in accordance with the law.
2. A contract or quasicontract is binding between the employer and the employee.
3.The employee has disclosed such information or the information has been publicised legally.
4. Collecting or processing normal personal data is necessary for the public interest, specifically relating to statistical information, or for the purpose of academic research conducted by a research institution. However, the information may not lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector.
5. The employee has provided written consent.
6. The public interest is involved.
7. The information is obtained from publicly available resources. However, an exception applies if the information is limited by the employee regarding the processing or use of the information. Furthermore, the interests of the employees should be protected.

A violation committed by collecting or processing employees' normal personal data, or an order or disciplinary action of the limitation on international transmission made by the government authority in charge of a subject industry at the central government level in accordance with Article 21 of the PDPA that might violate the rights of other employees is subject to a maximal sentence or custody of 2 years, a maximal fine of NT$200,000 (approximately US$6,620), or both. An employer intending to commit an offense in the aforementioned situation is subject to a maximal sentence of 5 years and a maximal fine NT$1,000,000 (approximately US$33,100).[29]

A violation committed by collecting, processing, or using employees' normal personal data which may not harm other employees' rights without good cause is subject to

[26] Lu, Ding-Wang, Interpretation and Practice of Personal Data Protection Act- Part II, Parliament Monthly, Dec. 2010, P.42.
[27] Article 41 PDPA.
[28] Article 19 PDPA.
[29] Article 41 PDPA.

an administrative fine of NT$50,000–NT$500,00 (approximately US$1,655–US$16,550). Furthermore, if the employer fails to take corrective measures within a specific period, a fine is imposed each time the violation occurs.[30]

E. Duty to Inform before Collecting, Processing, or Using Personal Data

Regarding the self-determination of personal information, in which an employer collects, processes, or uses an employee's personal information with good cause and in accordance with the PDPA, they must inform the employee of the following items:
1. the employer's name (particularly in situations involving dispatch work),
2. the purpose for collecting, processing, or using the information,
3. the classification of the information being collected,
4. the time, area, target, and manner in which the employer intends to use the information,
5. the rights of the employer in this act and how they are exercised, and
6. the effect that not sharing the information may have on the employee's rights and interests.

However, the following situations may be exceptions for providing notice:
1. The information is collected in accordance with the law;
2. Collecting the information is necessary for the employer to fulfil their legal obligations.
3. Such notice would impair the interests of a third party.
4. An employee should already know the content of the notification.

When an employer violates these duties, the appropriate government authority responsible for the subject industry at the central government level, municipality level (directly under the central government), or county or city government level orders the employer to take corrective measures within a specified time. Employers who fail to comply with such an order are subject to an administrative fine of NT$20,000–NT$200,000 (approximately US$662–US$6,620) that is imposed each time the employer violates these duties.

6. Employment Services Act

An employer can violate the privacy of employees or job seekers during employment or the recruitment process, respectively. The Employment Service Act protects both job seekers and employees. Article 5 of that act states that employers can neither withhold an identification card, work certificate, or other certified document of any job applicant or employee nor request job applicants or employees to surrender any unrelated personal documents against his or her free will. Items containing personal information include the following[31]:
1. Physiological information: genetic, drug, medical treatment, HIV, or intelligence quotient test results, or fingerprints.
2. Psychological information: psychiatric, loyalty, or polygraph test results.
3. Personal lifestyle information: financial or criminal records, family plans, and background checks.

When requesting job seekers or employees to present the aforementioned information, an employer must respect the personal interests of the people concerned, and no boundary should be crossed beyond the mandatory and specific confinements upon

[30] Article 47 PDPA.
[31] Article 1-1, Enforcement rule of Employment Services Act.

economic demands or public interest protection. In addition, appropriate and decent relations with the intended purposes must be satisfied.

III. Balance between Business Necessity and Employees' privacy

Employers may attempt to obtain personal information from employees and to monitor them for various reasons, many of which would be considered appropriate and reasonable. Taiwan's legal mechanisms for protecting personal data were designed to maintain a reasonable balance between the necessities for conducting business and the protection of employee privacy.

Special personal data are strictly protected by the PDPA. However, these data can be collected, processed, or used if one of four exceptions detailed in Section II-5-C are met. Similarly, normal personal data can be collected, processed, or used if any of the seven exceptions listed in Section II-5-D are met. In the context of employment relationships, the first two exceptions (i.e., when acting in accordance with the law or fulfilling legal obligations) are typical justifications for collecting, processing, and using special personal data and normal personal data. In addition, employment contracts and written employee consent are typical reasons for collecting, processing, and using normal personal data. Finally, criminal records are a type of special personal data; thus, the common rule "clean work, clean people" can be strictly challenged. These concerns are addressed in the following sections.

1. Exception in Accordance with the Law

A. Occupational Safety and Health Act

a. General

For occupational health and safety, employer necessity and employee privacy should be balanced. Article 20 of the Occupational Safety and Health Act states that employers should conduct preemployment physical examinations for labourers at the time employment commences; for currently employed labourers, the following health examinations should be conducted[32]:

1. general health examination
2. special health examinations for employees involved in tasks with specific health hazards.
3. health examinations testing for specific conditions in certain professions, as designated by the central competent authority.

Under law, employees are obligated to undergo these health examinations. Based on the results, an employer cannot employ a labourer in a role for which they would be unsuitable. When the results identify an abnormal condition, medical personnel must provide appropriate health guidance for the employee. When the results of a physician's health assessment indicate that an employee is unsuitable for his or her original work, the physician's recommendations are referred to for transferring the employee to another workplace, reassigning them to other duties, shortening their work hours, and adopting appropriate health management measures. Employers are within their rights to know the

[32] Article 20 Occupational Safety and Health Act.

results of an employee's health examination; moreover, they require such knowledge to provide adequate occupational health and safety. When necessary, the employer must understand whether the employee is expected to recover to full health, and they require knowledge on any medical treatments affecting employees.

b. Employers' Authority and Attendant Legal Duties

The preceding subsection outlines employee and employer obligations regarding mandatory health examinations. Regarding the results of those examinations, Article 16 of the Protection Rule for Labour Health states that employers must take the following measures:

1. Reassign the employee to a suitable workplace in accordance with the official examination results from a doctor.
2. Health examination results should be given to the employees.
3. The employer must protect employee privacy when handling and reviewing examination records.

Furthermore, employers cannot collect, process, or use special personal data, except when it is necessary for them to fulfil legal obligations, and only when appropriate security measures are taken.[33] Appropriate security measures are technical or organisational measures for preventing personal information from being stolen, modified, damaged, destroyed, or disclosed.[34]

c. Employers' Right to Refuse Employment and to Transfer or Dismiss Employees

When medical examination or test results indicate that a job seeker is unfit for the job for which they have applied, an employer might not have the capacity to employ them. In such circumstances, employers must comply with certain rules when deciding whether to refuse to hire a job seeker, transfer an employee to another workplace, or terminate an employment contract. First, based on the examination results and a physician's recommendation, an employer may assign a job seeker to another workplace that is suitable for his or her condition. However, if no suitable job is available, then the employer can refuse to hire them. Second, when an employee is unsuitable for continuing their employment because of medical reasons, the employer could transfer them to a more suitable workplace. However, the transference must comply with certain principles.[35] Specifically, transfers that fail to comply with the following principles are illegal, except when employee consent is obtained:

1. The transfer should be based on the business's necessities.
2. The transfer must not violate the employment contract.
3. Employers cannot offer less favourable wages and other working conditions at the new workplace.
4. The new role must be appropriate for the skill and the physical fitness of the employee.
5. The employer must provide adequate assistance if the new workplace is too far for the employee to travel to.

---

[33] Article 6 PDPA.

[34] Article 12 Enforcement Rules of the Personal Information Protection Act.

[35] 1985.9.5 The administrative explanation of the Ministry of Interior,1985 Tai-Nei-Zhe No. 328433. The Ministry of Labor was stetted in 1987. Before 1987 the authority of central level for labor affairs is the Ministry of Interior.

Finally, when the employer genuinely has no other work opportunity for the employee, the employer can terminate the employment contract (*ultima ratio*), although they must provide severance pay in accordance with Article 11 (Paragraph 5) of Taiwan's Labour Standard Law. Taiwan does not have employment at will, but only employment in justice.

B. Labour Insurance Act and National Health Insurance Act

Taiwan's Labour Insurance Act states that labourers between the ages of 15 and 65 years must be insured as insured persons, with their employers, or the organisations (e.g., craft union) or institutes (e.g., vocational training institution) to which they belong as the insured units.[36] Each insured unit is responsible for managing the processes and affairs involved in providing labour insurance for its employees, and preparing a roll list of the employees or members. Thus, an employer, craft union, or vocational training institution may collect, process, and use its employees' personal information. Furthermore, the National Health Insurance Act states that employers must provide health insurance for their employees.[37] Furthermore, they must organise and manage their labour-insurance-related affairs. Thus, employers could acquire personal information from their employees through this process.

C. Teacher Law

In Taiwan, the Teacher Law has strict requirements for the hiring of teachers; one of these requirements is related criminal records. When teachers are involved in any of the following situations while tenured, they can be dismissed, suspended, or denied renewal of employment[38]:

1. A teacher is sentenced to a prison term of one year or more without probation.
2. A teacher is convicted of corruption or malfeasance, or they are issued a warrant of arrest for a case that it is not settled during their term of civil service.
3. A teacher is charged and convicted of a crime under Paragraph 1 (Article 2) of the Sexual Assault Crime Prevention Act.

Furthermore, the Gender Equity Education Act states that a school or competent authority must establish a database of incidents involving sexual assault, harassment, or bullying on campus, and offender profile information should be recorded.[39] If an offender transfers to another school for either study or employment purposes, then the former competent authority or school is obligated to notify the new school within one month from the date of knowing of the transfer. Subsequently, the new school must monitor the offender and provide counselling as necessary. The new school must not, without legitimate reason, reveal the offender's name or other personal information that may lead to his or her identification.

Provisions of the Sexual Assault Crime Prevention Act state that, before a school appoints an educator or hires a full-time or part-time staff member, it must review whether potential candidates have a criminal record of sexual assault, or whether they have been dismissed or denied renewal of employment after being investigated by competent authorities or the school's Gender Equity Education Committee. The school must

[36] Article 6 Labor Insurance Act.
[37] Article 15 National Health Insurance Act.
[38] Article 14 Teacher Law.
[39] Article 27 Gender Equity Education Act.

determine whether any alleged incidents of sexual assault, harassment, or bullying were perpetrated by the candidate in question.

D. Company Law

To ensure that businesses are ethical, Company Law in Taiwan states that managers must not have a criminal record. When applying for a managerial position, job applicants must provide proof of no criminal conviction. Moreover, any currently appointed manager who is determined to have been convicted for a criminal offence must be discharged. The following conditions render a person ineligible for employment as the manager of a company:

1. Having been adjudicated guilty according to a final judgment of any offence specified in the Statute for the Prevention of Organisational Crimes, and the time elapsed since serving the full sentence term is less than 5 years;
2. Having been imprisoned for a term of more than one year for committing fraud, breach of trust, or misappropriation, and the time elapsed since serving the full sentence term is less than 2 years;
3. Having been adjudicated guilty according to a final judgement for misappropriating public funds during a tenure of public service, and the time elapsed since serving the full sentence term is less than 2 years.

2. Exception for Employers to Fulfil the Legal Obligation

A. Prevention of Communicable Disease

Taiwan's Labour Standards Law states that an employee may terminate an employment contract without providing advance notice to their employer when a coworker contracts a harmful contagious disease and the employee is at risk of contracting that disease. However, if the employer has hospitalised the infected person or the infected person has been discharged, then the employee may not terminate the employment contract without notice. Thus, employers have the right and obligation to know the health status of employees with infectious diseases.[40]

In addition, some jobs have serious implications regarding the health of workers (e.g., cooks and kitchen staff). All local governments in Taiwan have announced health management rules for public eating places.[41]These rules generally require kitchen staff to undergo a health inspection. Typical inspection items involved in a qualified health examination include a chest X-ray, hepatitis test, and serum, skin, and stool samples.[42] Any person who violates these rules is subject to a fine of NT$30,000–NT$3,000,000. In severe circumstances, violators may be ordered to terminate or suspend business operations for a certain period. Furthermore, relevant authorities may revoke all or part of the items registered to a company, business, or factory, and food businesses may have their registration revoked, in which case reregistration is not permitted within one year.[43]

[40] Article 14 Labor Standards Law.
[41] According to Article 14 Act of Governing Food Sanitation.
[42] For example, Taipei public eating places health management rules.
[43] Article 47 Act of Governing Food Sanitation.

B. Indigenous Peoples Employment Rights Protection Act and People with Disabilities Rights Protection Act

Indigenous people and people with disabilities are considered disadvantaged in the employment market. Consequently, the Indigenous Peoples Employment Rights Protection Act and People with Disabilities Rights Protection Act contain provisions that specifically address the ratio of employed minorities.

According to the Government Procurement Act, any company that wins a government contract and employs more than 100 staff must hire indigenous people while bound to that contract. Specifically, the minimal number of indigenous employees must account for 1% of the total number of staff members.[44]

Any government department, public school, or public business entity employing at least 34 people is obligated to employ people with disabilities who have the capacity to work. Specifically, the number of employees with disabilities must account for at least 3% of the total number of staff. Any private school, association, or private business entity employing at least 67 staff members must employ people with disabilities who have the capacity to work. Moreover, the number of employees with disabilities must account for at least 1% of the total number of staff members (no less than one person).[45]

The job application forms used by most companies may contain questions about ethnicity and health status. This information assists companies in fulfilling their legal obligation to hire a specific number of indigenous people and people with disabilities.

However, in 2010, the Taipei High Administrative Court judged a case involving an employee with a mental disorder. When applying for the position, this employee indicated that his health status was "good", and then signed an affidavit stating "I confirm that all of the completed information is true. If any information is false, I agree that the Company may terminate the employment contract." When the employer became aware of the employee's condition, the employment relationship was terminated. The Court ruled that, although the employee had a mental disorder, his disability did not interfere with his capacity to work. To ensure equal employment opportunities nationwide, Article 5 of the Employment Services Act[46] states that employers are prohibited from discriminating against job applicants or employees on the basis of race, class, language, thought, religion, political orientation, place of origin or birth, gender, gender orientation, age, marital status, appearance, facial features, disability, or past membership in any labour union. Thus, that employer could have been charged with discrimination.

The Ministry offered an administrative explanation[47] that refers to the legality of the questionnaire of application's formula. The function of a resume or application formula is designed to facilitate the conclusion of an employment contract. Employers or employment agencies that discriminate against job applicants or employees through the fulfilment of an application formula violate Article 5 of the Employment Services Act.

3. Exceptions in the Cases of Employment Contracts or Written Consent Provided by Employees

Employment contracts and written employee consent are other exceptions for an

[44] Article 12 Indigenous Peoples Employment Rights Protection Act.
[45] Article 38 of People with Disabilities Rights Protection Act.
[46] Taipei High Administrative Court , Gian-Zhe, No. 648, 2010.
[47] The administrative explanation of Ministry of Labor, Lao-Zhe-Ye-Zhe No. 0980013235, May 25. 2009.

employer to collect, process, and use an employee's personal data. However, this exception has limited applicability for normal personal data. The most crucial example involves monitoring employees based on an agreement stipulated in an employment contract; work rules, which are considered a part of the employment contract[48]; and written consent. According to the PDPA, because a person's image or voice can be used to identify them directly or indirectly identify as a natural person, they can be considered types of personal data.[49]

However, the monitoring of employees should be limited. When an employer continually monitors employees, particularly when surveillance cameras are involved, the employer is simultaneously supervising the work of labour and monitoring the behaviour of employees, potentially causing persistent psychological pressure for the employees and violating the employees' right of personality.[50] In other words, monitoring should be considered in the context of necessity and compliance with the principle of proportionality.

A renowned case heard by Taiwan's Supreme Court involving a manager who was dismissed for monitoring employee telephone calls can explain the necessity and the principle of proportionality to monitor. The manager of a hotel grievance unit abused his position by secretly installing recording equipment in the office telephones. When employees discovered the manager's actions, 523 hotel staff requested the employer to dismiss the manager. The manager argued that the dismissal was illegal and filed a lawsuit. The Supreme Court judged against the manager on the basis that the manager's behaviour was against the necessity and principle of proportionality of monitoring the employees.[51]

4. Clean Work, Clean People?

Generally, several jobs require workers who have a clean criminal record. Whether financial work is considered "clean" or "dirty" intellectually or theoretically, it must be executed by people who have no criminal record in Taiwan. In Taiwan's private sector, a record of no prior conviction is necessary for teachers, managers, and financial workers, such as employees of banks, insurance companies, stock market traders, and accounting firms. Employers in this sector typically request job applicants to provide proof of no criminal conviction specifically related to finance.

In Taiwan, rehabilitated criminals typically experience considerable difficulty acquiring employment that offers favourable remuneration. Even relatively low-skilled employment positions (e.g., cleaning) in both cities and counties favour employees with no prior criminal convictions. For example, in Taichung, which is Taiwan's third-largest city, the cleaning staff working at the Environmental Protection Bureau must provide proof of no criminal record when applying for a job. These requirements are general provisions in community-based public services. However, the PDPA is expected to challenge employer requirements such as these, primarily because the PDPA categorises criminal records as a type of special personal data. These sensitive data are under strict protection, as detailed in Section II-5-C; consequently, the requirement of providing proof of no criminal record is

[48] See Wang, Neng-Jiun, Work Rules, in Taiwan Labor Law Association edit., Interpretation of the Labor Standards Law, 2009, PP.404-409.

[49] Liu, Ding-Chi, The Definition, Principle of Protection of the Personal Data and it's Exception – the Monitoring, Part 1, Taiwan Jurist, Vol. 115, May 2012, P. 50.

[50] See Liu, Shih-Hao, Protection of employees' personality in the network society, Cheng-Chi University Labor Journal, Vol. 12, 2002, PP. 199.

[51] The Supreme Court, Civil Judgment of Year 2000, Tai-Shang-Zhe No.2267.

considered illegal if employers cannot justify such a request based on the four exceptions.

IV. Protection of the Privacy of Off-Duty Employees

The activities of off-duty employees must be considered based on the principle of personal privacy alone. Employers have no right to monitor the behaviour of off-duty employees. In 1993, the Supreme Court stated that "employment relations are based on the labour force. The binding relationships between employers and employees are limited by space and time; they do not a form a completely binding relationship between the personalities of employers and employees. Therefore, employer conduct should not intrude on the lives of employees while they are off duty. The private behaviour of employees outside of working hours is a part of their private lives. Employers have only the right to judge employee at such times when their behaviour directly relating to business activities could harm the social evaluation of the business' undertakings."[52]

The Supreme Court restated the concept in the aforementioned case involving a married manager who had an affair with a female coworker. Subsequently, he was dismissed on the basis that his actions harmed the social evaluation of the employer's undertakings. The Supreme Court determined that the affair had no effect on his work or the work of other employees. Furthermore, the work rules applied by his employer did not expressly forbid employees from engaging in affairs with coworkers. Therefore, the Supreme Court ruled against the employer, and the dismissal was judged illegal.

To provide an example for the sake of contrast, pilots may not drink alcohol within a certain period before flying. Another contrasting example involves undertakings with special tendencies, such as political parties or religious undertakings.[53] The Kuo-Ming-Tang, the incumbent nationalist party in Taiwan, forbids employees from participating in activities hosted by the opposition, the Democratic Progressive Party, even when employees are off duty.

V. Conclusion

Compared with personal privacy protection laws in other countries, the protection of personal data and privacy has emerged relatively later in Taiwan because of historical reasons. As democracy and law have advanced during the past 27 years, Taiwan has increasingly emphasised human rights, including the protection of personality, privacy, and personal data. The milestone in protecting personal information was the Computer-Processed Personal Data Protection Act, although its coverage of protection was considerably narrow. Until 1990, Taiwan underwent substantial progress in protecting personality and privacy according to the Civil Code as well as the interpretation of the Constitutional Court and Judgements of the Supreme Court and other courts.

The PDPA amendments are the most crucial reforms for protecting personal information and privacy. These reforms were designed based on European Union directives, Germany's Federal Data Protection Act, Japan's Personal Information Protection Law, and

[52] The Supreme Court, Civil Judgment of Year 1993, Tai-Shang-Zhe No.1786.

[53] See Liu, Shih-Hao, Protection of employees' personality in the network society, Cheng-Chi University Labor Journal, Vol. 12, 2002, PP. 206.

various laws of the United States.[54] However, the PDPA has been criticised for being too weak in protecting special personal data[55] and for the failure of the exception of written consent to reflect reality.[56] This discussion indicates that the protection of personal data and privacy should be successful. The PDPA does not specifically address employees, although it could offer clear and specific protection for employee data in the context of employment relationships. However, the PDPA has been implemented for only one and a half years; thus, Taiwanese lawmakers can continue referring to the experiences of various advanced countries to improve the implementation of this act.

[54] Fang Chiang, Zheng-May, Foreign- discipline and Self-discipline structure of Personal Data Protection Law System, Dong-Wu University Law Review, Jul. 2009, PP. 166-169.
[55] See Liu, Gin-Yi, It's not progressive Legislation- The Personal Data Protection Act., The Taiwan Law Review, Vol. 183, Aug. 2010, PP. 152,153.
[56] See Liu, Ding-Chi, The Idea of Written Consent in Personal Data Protection Act, The Taiwan Law Review, Vol. 218, Jul. 2013, PP. 151-153.

A Thin Wall of Privacy Protection, with Gaps and Cracks: Regulation of Employees' Personal Information and Workplace Privacy in Australia

Anthony Forsyth[*]
RMIT University

1. Introduction

The protection of employees' personal information and workplace privacy is once again becoming a significant employment law issue in Australia. Rapid technological change in the 1990s resulted in legislative and policy responses in several Australian jurisdictions, amid concerns about growing intrusion upon employees' personal lives. These developments also generated a considerable volume of academic literature.[1] The pace of legal change, and the extent of academic consideration of workplace privacy, slowed to some degree in the 2000s. However the evolution of newer technologies – and their adaptation by employers for purposes including recruitment, surveillance and monitoring of employees, and their (mis)use by employees themselves – has seen renewed attention to these issues in the last five years. This is particularly evident in the growing number of court and tribunal decisions examining various aspects of the delicate balance between employer interests in control over the workforce and employees' privacy rights.

Australians have enthusiastically embraced all forms of information and communication technology. One positive effect of this has been to bridge the distance between our 'geographically far-flung nation' and 'the centers of global capital in North America, Europe and Japan'.[2] The use of social media by private citizens in Australia had increased to 62% of the population by 2012 – with much of this access to forums such as Facebook, Twitter and LinkedIn occurring at the workplace and/or using work-provided devices.[3] The interface between social media and the workplace has given rise to a number

[*] Professor, Graduate School of Business & Law, RMIT University, Melbourne, Australia; Consultant, Corrs Chambers Westgarth, Lawyers. Thanks to Alannah Hogan of Corrs Chambers Westgarth for research assistance.

[1] See for example Ronald McCallum and Greg McCarry, 'Worker Privacy in Australia' (1996) 17 *Comparative Labor Law and Policy Journal* 13; Richard Johnstone, 'Pre-employment Health Screening: The Legal Framework' (1988) 1 *Australian Journal of Labour Law* 115; Anna Chapman and Joo-Cheong Tham, 'The Legal Regulation of Information in Australian Labor Markets: Disclosure to Employers of Information about Employees' (2000) 21 *Comparative Labor Law and Policy Journal* 613; Ronald McCallum, *Employer Controls over Private Life*, UNSW Press, Sydney, 2000; Julian Sempill, 'Under the Lens: Electronic Workplace Surveillance' (2001) 14 *Australian Journal of Labour Law* 111; Ronald McCallum and Andrew Stewart, 'The Impact of Electronic Technology on Workplace Disputes in Australia' (2002) 24 *Comparative Labor Law and Policy Journal* 19; Margaret Otlowski, 'Employers' Use of Genetic Test Information: Is there a Need for Regulation?' (2002) 15 *Australian Journal of Labour Law* 1.

[2] McCallum and Stewart, *supra* note 1, 19.

[3] M Watkins et al, *State of Australian Social Media 2012*, quoted in Andrew Bland and Sarah Waterhouse, 'Social Media in the workplace: practical tips for best practice policies' (June 2013) *Internet Law Bulletin* 45.

of employment law issues, including the extent of employers' rights to monitor the activities of employees; and the blurring of 'work' and 'private' life.[4]

Under the Australian federal system of government, regulation of workplace privacy and related employment issues occurs through a complex web of Federal, State and Territory laws. In general terms, the employment of almost all private sector employees is covered by Federal legislation: the *Fair Work Act 2009* (Cth) (*FW Act*). This includes regulation of minimum wages and other employment conditions such as working hours and leave entitlements, either directly (through the National Employment Standards)[5] or indirectly through modern awards and/or enterprise agreements made under the *FW Act*.[6] Federal public sector employees and those in Victoria, the Australian Capital Territory and Northern Territory are also covered by the national system of workplace regulation under the *FW Act.* The employment of public service employees in the remaining five States (New South Wales, Queensland, South Australia, Tasmania and Western Australia) is regulated by specific legislation in each State.[7]

Privacy is the subject of specific Federal legislation applicable to both the private and public sectors nationally: the *Privacy Act 1988* (Cth) (*Privacy Act*). Similar legislation also applies in most Australian States and Territories, regulating the privacy practices of State/Territory public sector organisations in those jurisdictions.[8] In addition, the common law offers some measure of protection of the privacy rights of individuals; and in some States, further legislation regulates the handling of personal health information.[9] There are also laws in each Australian jurisdiction dealing with prohibitions on illegitimate or unauthorised telecommunications interception and monitoring.[10] Some of these statutes specifically regulate surveillance in the workplace context.[11]

In relation to three specific areas of employment law in which issues of protection of employees' personal information, or breach by employees of their own workplace obligations, commonly arise:

- Unfair dismissal protections are provided by the *FW Act*,[12] and each of the State industrial statutes (although the vast number of unfair dismissal claims are brought under the Federal legislation). An increasing number of unfair dismissal cases involve

---

See further Geoffry Holland, Kathryn Crossley and Wenee Yap, *Social Media Law and Marketing: Fans, Followers and Online Infamy*, Thomson Reuters Lawbook Co, Sydney, 2014.

[4] Louise Thornthwaite, 'Social Media, Unfair Dismissal and the Regulation of Employees' Conduct outside Work' (2013) 26 *Australian Journal of Labour Law* 164.

[5] *FW Act*, Part 2-2.

[6] *FW Act*, Parts 2-3 and 2-4 respectively.

[7] For example, *Industrial Relations Act 1996* (NSW) and *Public Sector Employment and Management Act 2002* (NSW).

[8] *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2009* (Qld); *Personal Information Protection Act 2004* (Tas); *Information Privacy Act 2000* (Vic); *Information Act 2002* (NT). South Australia and Western Australia do not have specific privacy legislation, although some privacy protections are provided by other laws. The Federal *Privacy Act* applies in the Australian Capital Territory.

[9] *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

[10] For example *Telecommunications (Interception and Access) Act 1979* (Cth); *Surveillance Devices Act 2004* (Cth); *Invasion of Privacy Act 1971* (Qld); *Listening and Surveillance Devices Act 1972* (SA); *Listening Devices Act 1991* (Tas); *Surveillance Devices Act 1998* (WA); *Surveillance Devices Act 2007* (NT).

[11] *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices (Workplace Privacy) Act 2006* (Vic), inserting Part 2A in the *Surveillance Devices Act 1999* (Vic); *Workplace Privacy Act 2011* (ACT).

[12] *FW Act*, Part 3-2.

alleged misconduct by employees using various forms of employer-provided or personally-owned technology (for example, to access social media sites) – often outside the workplace or regular work hours. These cases have raised questions as to the reach of express and implied duties of employees under the contract of employment.[13]

- Protections against employment discrimination and sexual harassment apply under Federal, State and Territory legislation.[14] These laws impose restrictions on employers around the acquisition and use of individuals' personal information as part of recruitment and management processes. Some of the statutes also operate to prevent certain types of discriminatory information requests in the hiring of employees.
- Workplace health and safety (WHS) and workers' compensation for illness or injury are also the subject of Federal, State and Territory laws. Various privacy issues arise in the operation of WHS and workers' compensation legislation, for example in relation to employers' handling of employees' sensitive health information. Although hitherto regulated mainly by WHS laws, workplace bullying has recently become subject to new Federal provisions enabling bullying claims to be initiated by individual employees in the Fair Work Commission (FWC).[15] The management of bullying cases raises privacy issues for employers including the need to maintain the privacy of information provided by the complainant and the alleged 'bully' once a complaint has been made.

In light of the above, it is apparent that larger Australian employers with operations across State/Territory boundaries face an array of overlapping – and at times conflicting – laws imposing obligations in relation to employees' personal information. The absence of uniform regulation in this area across Australia also means that individual employees' expectations of the level of privacy protection in the workplace do not accord with the actual legal position.[16]

---

[13] Thornthwaite, *supra* note 4.

[14] For example, *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Disability Discrimination Act 1992* (Cth); *Age Discrimination Act 2004* (Cth); *FW Act*, Part 3-1 (sections 351-352); *Equal Opportunity Act 2010* (Vic); *Discrimination Act 1991* (ACT).

[15] FW Act, Part 6-4B, operative from 1 January 2014. For background see Caroline Kelly, 'An Inquiry into Workplace Bullying in Australia: Report of the Standing Committee on Education and Employment – *Workplace Bullying: We Just Want It to Stop*' (2013) 26:2 *Australian Journal of Labour Law* 224; Sarah Oxenbridge and Justine Evesson, *Bullying Jurisdiction Strategies: An Analysis of Acas' Experience and its Application in the Australian Context*, Report for the Fair Work Commission, Employment Research Australia, July 2013.

[16] See for example Australian Government, Office of the Australian Information Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy* (March 2000), at: http://www.oaic.gov.au/privacy/privacy-archive/privacy-guidelines-archive/guidelines-on-workplace-email-web-browsing-and-privacy (accessed 8 January 2014); and see further Section 6 of this paper (Conclusion). On workplace privacy protections in Australia in comparative terms see for example Anne O'Rourke, Amanda Pyman and Julian Teicher, 'The Right to Privacy and the Conceptualisation of the Person in the Workplace: A Comparative Examination of EU, US and Australian Approaches' (2007) 23 *International Journal of Comparative Labour Law and Industrial Relations* 161.

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

Australian Constitution and State/Territory Human Rights Charters

There is no constitutional or other general right to privacy in Australia. The protection of individual rights under the *Australian Constitution* is quite limited and does not extend to privacy.[17] There is no separate Bill of Rights at the Federal level. Two Australian jurisdictions have enacted human rights charters which include the right to privacy and protection of reputation: *Charter of Human Rights and Responsibilities Act 2006* (Victoria), section 13;[18] and *Human Rights Act 2004* (ACT), section 12.[19] However, the privacy protections offered by both these instruments are restricted in nature. For example, the Victorian Charter:

> … does not create any new cause of action for individuals who believe their privacy has been interfered with. Instead, the Charter requires that any bill (new legislation) introduced into the Victorian Parliament must be accompanied by a statement of compatibility with the human rights protected by the Charter. Where the bill is incompatible with one or more of the rights in the Charter, reasons for this must be provided.
>
> The Charter also requires that existing [State] laws are interpreted, as far as is possible, in a way that is compatible with human rights. Further, the Charter imposes an obligation on public authorities [in Victoria] to consider human rights in their decision making and makes it unlawful, in most circumstances, for a public authority to act in a way that is incompatible with a human right.[20]

Common Law Protection of Privacy

While the High Court of Australia affirmed in 1937 that there is no general right to privacy under Australian law,[21] the common law of tort and equitable principles relating to use of confidential information do provide some protection for individuals against privacy breaches. The High Court's more recent decision in *Australian Broadcasting Corporation v*

---

[17] Some of the rights protected include the right to vote (*Australian Constitution*, section 41), the right to trial by jury (section 80) and freedom of religion (section 116): see George Williams, *A Charter of Rights for Australia*, UNSW Press, Sydney, 3rd edition, 2007, Chapter 3.

[18] This provision states that: 'Everyone has the right—
(a) not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
(b) not to have his or her reputation unlawfully attacked.'

[19] Stated in almost identical terms to section 13 of the Victorian Charter, *supra*.

[20] Office of the Victorian Information Privacy Commissioner, *Privacy and the Charter of Human Rights and Responsibilities*, Info Sheet 03.08 (June 2008), at: http://www.privacy.vic.gov.au/privacy/web2.nsf/files/privacy-and-the-charter-of-human-rights-and-responsibilities/$file/info_sheet_03_08.pdf (accessed 14 January 2014). Similar limitations apply in the ACT; see Gilbert and Tobin Centre of Public Law, University of NSW, 'The ACT Human Rights Act', at: http://www.gtcentre.unsw.edu.au/node/3074 (accessed 14 January 2014). In relation to the ACT and Victorian human rights charters generally, see Williams, *supra* note 17, Chapter 5; Simon Evans and Carolyn Evans, 'Legal Redress under the Victorian Charter of Human Rights and Responsibilities' (2006) 17 *Public Law Review* 264.

[21] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 (owner of racecourse not able to prevent defendants from broadcasting race information from a viewing platform on adjacent land).

Lenah Game Meats Pty Ltd[22] is thought by some to provide a stronger basis for equitable actions in particular, and has contributed to debate over the need for a statutory action for breach of privacy in Australia[23] (this debate has been given momentum by the media phone-hacking scandal which led to the Leveson Inquiry in the United Kingdom).[24]

Privacy Protection under Federal Law: the Privacy Act

The *Privacy Act* came into operation in 1988, initially imposing privacy requirements only on Federal public sector departments and agencies in the handling of personal information.[25] In 2001, this framework of privacy regulation was extended to the private sector (although small businesses with an annual turnover under A$3 million were exempted).[26] Until March 2014, the *Privacy Act* set down a number of Information Privacy Principles (IPPs) applicable to public sector bodies, and National Privacy Principles (NPPs) for the private sector. The IPPs and NPPs imposed similar obligations in relation to the collection, use, storage and disclosure of 'personal information' by organisations – i.e. information about an individual whose identity was apparent or reasonably ascertainable from that information.[27] In general terms,[28] the IPPs and NPPs required that personal information about an individual:

- could only be collected for a lawful purpose;
- could only be used for that purpose (with some limited exceptions);
- had to be kept in accurate and current records, accessible to the individual concerned (who must also have had the ability to correct their record);
- had to be securely stored;
- could not be disclosed to a third party without the individual's consent (or on certain limited public interest grounds).

Under amendments to the *Privacy Act* which took effect in March 2014, the IPPs and NPPs were replaced by one set of Australian Privacy Principles (APPs) that now apply to Federal government departments/agencies and private businesses (see further *infra*).

Additional protections apply under the APPs in relation to 'sensitive information' – i.e. information about an individual's racial or ethnic origin, political opinions or affiliations, religious or philosophical beliefs, membership of a professional body or trade

[22] (2001) 208 CLR 199 (although plaintiff unsuccessful in action seeking to prevent broadcast of film showing its slaughtering practices for meat export, obtained by animal rights campaigners, judgments indicated openness to recognition of tort of invasion of privacy).

[23] See for example Barbara McDonald, 'A Statutory Action for Breach of Privacy: Would it Make a (Beneficial) Difference?' (2013) 36 *Australian Bar Review* 241, 243-50; Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice*, ALRC Report No 108, 2008, discussed in McDonald, *supra*, 254-255, 262-268; ALRC, *Serious Invasions of Privacy in the Digital Era*, Issues Paper 43, October 2013.

[24] The events in the UK partly precipitated the recent Finkelstein Inquiry into Media and Media Regulation in Australia.

[25] Unless otherwise stated, the following discussion of the *Privacy Act* (prior to the 2012 amendments which took effect in March 2014) draws upon McCallum and Stewart, *supra* note 1, 32-34; and Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia*, Federation Press, Sydney, 2005, 99, 119-129, 153-155. Note also relevant State and Territory privacy legislation, *supra* note 8; Doyle and Bagaric, *supra*, 100-102.

[26] *Privacy Amendment (Private Sector) Act 2000* (Cth).

[27] *Privacy Act*, section 6(1) (definition of 'personal information').

[28] For further detail see Jeremy Douglas-Stewart, *Annotated National Privacy Principles*, Presidian Legal Publications, Adelaide, 4th edition, 2009.

union, sexual preference, criminal record, health information and genetic information.[29]

Employee Records Exemption from the Privacy Act

Importantly, any act or practice directly related to an 'employee record' was excluded from the operation of the NPPs – and this exclusion remains in place under the new APPs.[30] This means that private sector employers are *not* subject to the limits on the collection, use, storage and disclosure imposed by the APPs, in respect of any 'record of personal information relating to the employment of [an] employee'.[31] This includes an employee's health information, and personal information relating to the employee's:[32]

- engagement, training, discipline or resignation;
- termination of employment;
- terms and conditions of employment;
- personal and emergency contact details;
- performance or conduct;
- hours of work, salary or wages;
- membership of a professional body or trade union;
- recreation, long service, sick, personal, maternity, paternity or other leave;
- taxation, banking or superannuation (i.e. pension) affairs.

The employee records exemption from the *Privacy Act*, and its application in a number of specific employment contexts (for example, monitoring of employee emails and internet use) are discussed further in the remainder of this paper. For now, it should be noted that the exemption has long been a controversial aspect of Australia's privacy regime.[33] The main justification for exempting employee records from the *Privacy Act* was that privacy protection for employees 'is more properly a matter for workplace relations legislation'.[34] However, several reviews and inquiries over the last 15 years have identified significant limitations in the privacy protections provided to employees under Federal, State and Territory workplace laws.[35] According to Otlowski:

> Inclusion of the broad exemption in the [*Privacy Act*] for employee records consequently leaves employees vulnerable to breaches of privacy at the hands of their employers, in respect of which they would not necessarily have a remedy.[36]

---

[29] *Privacy Act*, section 6(1) (definition of 'sensitive information').
[30] *Privacy Act*, section 7B(3).
[31] *Privacy Act*, section 6(1) (definition of 'employee record'). However, the employee records exclusion does not apply in the public sector; therefore, Federal government departments and agencies must observe the requirements of the APPs in their handling of employees' personal information.
[32] *Ibid*.
[33] See for example the criticism in Senate Legal and Constitutional References Committee, *Privacy in the Private Sector: Inquiring into Privacy Issues, including the Privacy Amendment Bill 1998*, 1999, discussed in Margaret Jackson, *Hughes on Data Protection in Australia*, Lawbook Co, Sydney, 2nd edition, 2001, 109.
[34] Margaret Otlowski, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law* 169, 172 (see also 174).
[35] See for example House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000*, 2000, discussed in Otlowski, *supra* note 34, 172-175; Victorian Law Reform Commission, *Workplace Privacy: Final Report*, Victorian Government Printer, Melbourne, 2005, Chapter 2; ALRC (2008), *supra* note 23 (discussed further *infra*).
[36] Otlowski, *supra* note 34, 175. See also Doyle and Bagaric, *supra* note 25, 153-154.

A wide-ranging review of the *Privacy Act* by the ALRC in 2008 included recommendations for the removal of the employee records exclusion on the following grounds:

> While public sector agencies are required to treat employee records in accordance with the *Privacy Act*, private organisations generally are exempt in relation to current and past employees (with some limited exceptions). There seems little justification in principle for the differential approach—which does not feature in the law of comparable jurisdictions.
>
> The ALRC recommends that this exemption be removed. This would create consistent rules for personal information about employees, regardless of whether they are public or private sector employees.
>
> The ALRC acknowledges that there may be circumstances in which it is undesirable to allow employees to have access to all of the information contained in their files—such as referees' reports and other similarly confidential material. It would be much better practice to deal with such exceptions on the basis of the general law of confidentiality, however, rather than wholly exempting private sector employers from the normal requirements of the *Privacy Act*.[37]

2012 Amendments to the Privacy Act

The ALRC's 2008 Review of the *Privacy Act* ultimately lead to passage of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (*Privacy Amendment Act*). This legislation made extensive changes to the *Privacy Act* , which took effect on 12 March 2014. The most significant aspects of the *Privacy Amendment Act* for present purposes are:[38]

- enhancement of the Federal Privacy Commissioner's powers to ensure compliance with the *Privacy Act*, including civil penalties of up to A$340,000 for individuals and A$1.7 million for organisations (in instances of serious or repeated breach of an individual's privacy); and
- as indicated *supra*, adoption of the APPs for both the public and private sectors. In terms of content, the APPs impose very similar privacy obligations to those which previously applied under the IPPs and NPPs.

[37] ALRC (2008), *supra* note 23, Executive Summary; note also the following Recommendations in the ALRC's Report:
'Recommendation 40–1 The *Privacy Act* should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.
Recommendation 40–2 The Office of the Privacy Commissioner should develop and publish guidance on the application of the model Unified Privacy Principles to employee records, including when it is and is not appropriate to disclose to an employee concerns or complaints by third parties about the employee.'

[38] See Norman Witzleb, 'Halfway or Half-hearted? An Overview of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)' (2013) 41 *Australian Business Law Review* 55; Alec Christie, 'The Australian Privacy Act amendments will significantly impact federal government agencies' (December 2013) *Privacy Law Bulletin* 49.

Summary of the Australian Privacy Principles (effective 12 March 2014)[39]

APP1	Organisations must maintain a clear policy on management of personal information
APP2	Individuals may interact with organisations anonymously or using a pseudonym
APP3	Organisations may collect sensitive information only where an individual consents and the information is reasonably necessary for the agency's activities/functions, or collection is authorised by law
APP4	Obligations of organisations in relation to unsolicited personal information
APP5	Organisations must notify individuals about collection of personal information
APP6	Sensitive information must only be used for the primary purpose for which it was collected (although use for some secondary purposes is permitted)
APP7	Prohibition of use of personal information for direct marketing
APP8	Requirements relating to cross-border disclosure of personal information by organisations
APP9	Restrictions on use of government related identifiers of individuals
APP10	Organisations must ensure that personal information collected is accurate, up to date and complete
APP11	Obligations of organisations to ensure security of personal information (i.e. prevent misuse, interference, unauthorised access, etc)
APP12	Right of individuals to access personal information about them held by an organisation
APP13	Obligation of organisations to correct personal information which is inaccurate, out of date, misleading, etc

However, as mentioned earlier, no change has been made to the employee records exemption from the *Privacy Act* (although the former Labor Federal Government indicated that this could arise from a second stage legislative response to the ALRC's 2008 privacy law review).[40]

Remedies under the Privacy Act

In addition to the new civil penalties for serious breaches (*supra*), the remedies available under the *Privacy Act* include:

- a right for individuals to lodge a complaint with the Privacy Commissioner, which has investigatory and evidence-gathering powers;[41]

[39] For the full text of the APPs see Australian Government, Office of the Australian Information Commissioner, *Australian Privacy Principles*, Privacy Fact Sheet 17, January 2014, at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles (accessed 8 January 2014).

[40] See Witzleb, *supra* note 38, 55; Helen Lewin, 'Australian Law Reform Commission's Report on Australian Privacy Law – *For Your Information: Australian Privacy Law and Practice*' (October 2008) *Keeping Good Companies* 543. Note however that the prospect of amendment to the current employee records exemption has most likely narrowed, following the election to office of the (conservative) Coalition Government in September 2013.

[41] *Privacy Act*, sections 36 and 40. Since 12 March 2014, the Privacy Commissioner also has the power to initiate investigations on its own motion: Charles Alexander, Elizabeth Koster and Helen Paterson, 'Punitive

- the availability of compensation and other declaratory remedies (e.g. a declaration that conduct constituting an interference with an individual's privacy has occurred and should not be repeated, or that the respondent take any reasonable action to redress the loss or damage suffered by the complainant), as part of a determination issued by the Privacy Commissioner following an investigation into an alleged privacy breach;[42]
- an injunction to restrain a privacy breach, following an application to the Federal Court or Federal Circuit Court by the aggrieved party or the Privacy Commissioner.[43]

3. Personal information protection in the hiring process

Overview

A range of restrictions apply to Australian employers' ability to request, use and retain information about prospective employees in the recruitment process. These limits derive from several different sources, including anti-discrimination laws, spent convictions legislation and the *Privacy Act*.

Employers are permitted to request a job applicant's address, telephone number and e-mail address when he/she applies for a position. There is no legal basis for an employer to insist that a prospective employee provide his/her social network password in the recruitment process. However, many employers now carry out searches of job applicants' publicly accessible social media presence to identify any negative personal activities or behaviour.[44] A recent ALRC Issues Paper canvasses the idea of prohibiting employer requests for access to job applicants'/employees' private social media accounts, noting that a number of United States jurisdictions have passed legislation to that effect.[45]

Application of the Privacy Act to Recruitment/Hiring

The collection of the above or any other types of personal information in the course of an individual's employment application *is* subject to the protections in the *Privacy Act*, including the requirements of the APPs. This is because the employee records exemption from the *Privacy Act* (*supra*) does not apply in the pre-employment context[46] – it only applies to current and former employment relationships[47] (see further *infra*). As a result, employers must ensure compliance with the *Privacy Act* during the hiring process, for

Powers Guided by Ambiguity: The Australian Federal Privacy Commissioner's New Powers in the Context of a Principles-based Privacy Regime' (January 2013) *Privacy Law Bulletin* 66, 67-68.

[42] *Privacy Act*, section 52; see e.g. *Rummery v Federal Privacy Commissioner* [2004] AATA 1221. Enforcement of determinations issued by the Privacy Commissioner requires proceedings to be brought in the Federal Court of Australia or the Federal Circuit Court.

[43] *Privacy Act*, section 98.

[44] See for example CCH, *Australian Privacy Reporter*, CCH Australia Ltd, 2012, [20-216]; Lucille Keen, '#bored at work means #yourefired', *The Australian Financial Review*, 13 January 2014, 1, 6; Thornthwaite, *supra* note 3, 168.

[45] ALRC (2013), *supra* note 23; 'ALRC to consider ban on employer request for Facebook passwords', *Workforce*, No 18912, 29 October 2013.

[46] Doyle and Bagaric, *supra* note 25, 155; note also *Privacy Act,* section 6(1) (definition of 'employee record'), *supra* note 31, referring to records 'relating to the employment of the employee'.

[47] *Privacy Act,* section 7B(3), *supra* note 30.

example by:[48]

- telling job applicants how their personal information (for example, in their curriculum vitae) will be collected from them, and from third parties such as referees;
- collecting that information in a fair and non-intrusive manner;
- only collecting information that is relevant to the individual's application for the particular position;
- allowing the applicant access to their personal information on request (this can also extend to the employer's files relating to the application, including interview notes although not third party references[49]).

Anti-Discrimination Law Provisions

Legislation in every Australian jurisdiction prohibits discrimination against individuals in the advertising and offering of employment.[50] Some Federal and State anti-discrimination statutes contain further provisions precluding employers from making certain kinds of requests for information from prospective employees.[51] At the Federal level, such requests are prohibited where the information requested is in connection with, or for the purposes of, unlawful discrimination on the basis of a person's sex, disability or age; and persons without that attribute would not be asked to provide the same information.[52] These provisions would therefore prevent an employer from making verbal requests (e.g. at a job interview) for information about an applicant's:

- gender, sexual orientation, gender identity, intersex status, marital or relationship status, pregnancy or potential pregnancy, breastfeeding or family responsibilities;[53]
- age or age group;
- disability (including a physical or mental disease, disorder or illness), although questions may be asked about a person's ability to perform the inherent or reasonable requirements of the position he/she is seeking;[54] in turn, this may inform the employer's consideration of the reasonable adjustments that may be necessary to accommodate the individual in the workplace.[55]

The above prohibitions would also apply to requests for information of this nature in written form, for example on a job application or medical form (on the latter, see further *infra*).

---

[48] CCH, *supra* note 44, [20-210].
[49] See *O v Automotive Company* [2009] PrivCmrA 18.
[50] See for example *supra* note 14.
[51] See Chapman and Tham, *supra* note 1, 629-634; Neil Rees, Katherine Lindsay and Simon Rice, *Australian Anti-discrimination Law: Text, Cases and Materials*, Federation Press, Sydney, 2008, 443-444.
[52] *Sex Discrimination Act 1984* (Cth), section 27; *Disability Discrimination Act 1992* (Cth), section 30; *Age Discrimination Act 2004* (Cth), section 32.
[53] See for example *Smith v Commonwealth of Australia* (2000) EOC 93-077. However, under section 27(2) of the *Sex Discrimination Act 1984* (Cth), job applicants may be asked about medical information concerning their pregnancy; or any gender-specific medical conditions.
[54] See Rees, Lindsay and Rice, *supra* note 51, 283-287, including extract from *X v Commonwealth* (1999) 200 CLR 177 (Australian Army soldier discharged after positive HIV test during training; High Court upheld Army's argument re inherent requirement that soldier not pose risk of HIV transmission to other soldiers).
[55] Chapman and Tham, *supra* note 1, 634; Otlowski, *supra* note 1, 14.

In Queensland and Victoria, employer requests from job applicants for information that would form the basis of unlawful discrimination are prohibited.[56] This would cover information relating to a prospective employee's sex, age or disability (as per the Federal statutes, *supra*); as well as information about the individual's race, physical features, political/religious belief or activity, or industrial activity (e.g. union membership).

Health Screening

Employers commonly request prospective employees to answer questions about their health, or even undergo a medical examination, as part of the recruitment process. Such requests are lawful; however, a job applicant cannot be compelled to provide health information, and his/her participation in any health screening (including genetic testing, such as for susceptibility to workplace hazards) must be voluntary.[57] In contrast, employers have the power at common law to direct an existing employee to undergo a medical examination to determine the employee's fitness for duties (as long as the direction is reasonable in the circumstances).[58]

Employers also need to be mindful of anti-discrimination laws when conducting pre-employment medical checks.[59] For example, if a check is being conducted to establish whether an individual has a higher propensity to make workers' compensation claims, employers must exercise caution as this could indicate an intention to make a decision not to employ the person which constitutes unlawful discrimination on the grounds of disability or impairment (*supra*).[60] However, legislation in Queensland specifically allows employers to require a prospective employee to disclose a pre-existing injury or medical condition upon request by an employer; and to access the prospective employee's workers' compensation claim history (where the individual consents).[61]

Under the *Privacy Act*, as any 'health information'[62] provided by a job applicant is considered sensitive personal information, and the employee records exemption from the *Privacy Act* does not apply in the pre-employment context (*supra*), that information must

---

[56] *Equal Opportunity Act 2010* (Vic), section 107; *Anti-Discrimination Act 1991* (Qld), section 124. See e.g. *Bair v Goldpath* [2010] QCAT 483 (job applicant was unlawfully asked questions about his age, parental leave status and sick leave history at previous employer; however, only a written apology was ordered rather than compensation or damages).

[57] Otlowski, *supra* note 1, 3-9. See further David Keays, 'The Legal Implications of Genetic Testing: Insurance, Employment and Privacy' (1999) 6 *Journal of Law and Medicine* 357; and the reform proposals outlined in ALRC, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC Report 96, March 2013.

[58] Breen Creighton and Andrew Stewart, *Labour Law*, Federation Press, Sydney, 5th edition, 2010, 407 referring to *Blackadder v Ramsey Butchering Services Pty Ltd* (2002) 113 IR 461; see also *Schoeman v Director-General, Department of Attorney-General and Justice* [2013] NSWIR Comm 108.

[59] See further Otlowski, *supra* note 1, 9-20; Wendy Zukerman, 'Genetic Discrimination in the Workplace: Towards Legal Certainty in Uncertain Times' (2009) 16 *Journal of Law and Medicine* 770.

[60] Andrew Stewart, *Stewart's Guide to Employment Law*, Federation Press, Sydney, 4th edition, 2013, 86. See for example *Own Motion Investigation v Australian Government Agency* [2007] PrivCmr A 4 (government body which sought information about work-related injuries/illness in recruitment process, settled Privacy Commissioner's investigation by agreement to review selection process and remove offending questions).

[61] *Workers' Compensation and Rehabilitation and Other Legislation Amendment Act 2013* (Qld), amending the *Workers' Compensation and Rehabilitation Act 2003* (Qld).

[62] As defined in section 6(1), including information about an individual's health or disability; information about a health service provided to an individual; and other personal information about an individual collected in connection with donation by the individual of his/her body parts, organs or substances.

be handled by the employer in accordance with the APPs (noting the stronger protections which they provide for sensitive information).[63]

Criminal Records

Having become widespread over the last 15 years,[64] criminal record checks on prospective employees are regulated by the *Privacy Act* and spent convictions legislation operating in all Australian jurisdictions except Victoria. Under the *Privacy Act*, information relating to a person's criminal record is considered sensitive information to which the APPs and additional protections apply. An employer can run a criminal record check on an individual through the official authorities (e.g. Australian Federal Police), if the individual consents.[65] In practice, an individual him/herself will usually request a criminal record report from the relevant authority, then provide it to the prospective employer.

Where a prior criminal conviction constitutes a 'spent conviction' under the terms of applicable Federal, State or Territory legislation,[66] it does not have to be disclosed by a prospective employee. Further, these laws 'forbid employers … from taking into account spent convictions in making assessments about [the] character and fitness' of a job applicant.[67] The definition of a spent (or lapsed) conviction varies across jurisdictions. Generally, however, offences that are more than 10 years old (or 5 years old for young offenders) – and carry low maximum jail terms (e.g. 6 months in NSW, Tasmania, ACT and NT; 30 months in Queensland and federally) – will be considered spent convictions for purposes of the applicable legislation.[68] A number of exclusions apply, for example requiring persons convicted of violent/sex offences to disclose these when seeking employment involving children (in fact 'working with children checks' are mandatory for such employment across Australia).[69]

Discrimination on the basis of an irrelevant criminal record (i.e. not relevant to a person's ability to perform a particular job) is also unlawful under Federal, Tasmanian and NT legislation.[70] Allegations of unlawful discrimination on the basis of a person's criminal

---

[63] See further Doyle and Bagaric, *supra* note 25, 157-160.

[64] Criminal record checks in Australia increased seven-fold in the decade to 2007: see Bronwyn Naylor, Moira Paterson and Marilyn Pittard, 'In the Shadow of a Criminal Record: Proposing a Just Model of Criminal Record Employment Checks' (2008) 32 *Melbourne University Law Review* 171, 172. See also Moira Paterson and Bronwyn Naylor, 'Australian Spent Convictions Reform: A Contextual Analysis' (2011) 34 *UNSW Law Journal* 938.

[65] Private organisations offering criminal record check services can also be used only with the prospective employee's consent: Moira Paterson, 'Restrictions on Employers' Handling of Criminal Records Information: Privacy and Confidentiality Issues' (2012) 18:8 *Employment Law Bulletin* 120, 121.

[66] *Crimes Act 1914* (Cth), Part VIIC; *Criminal Records Act 1991* (NSW); *Criminal Law (Rehabilitation of Offenders) Act 1986* (Qld); *Spent Convictions Act 2011* (SA); *Annulled Convictions Act 2003* (Tas); *Spent Convictions Act 1988* (WA); *Spent Convictions Act 2000* (ACT); *Criminal Records (Spent Convictions) Act 1992* (NT).

[67] Paterson, *supra* note 65, 121.

[68] *Ibid*.

[69] See for example Department of Justice, Victoria, 'Working with Children Check' at: http://www.workingwithchildren.vic.gov.au/home/applications/the+application+process/what+is+checked/ (accessed 20 January 2014); CCH, *Australian Human Resource Management*, CCH Australia Ltd, 2012, [5-890].

[70] *Australian Human Rights Commission Act 1986* (Cth) (*AHRC Act*), section 3(1) and *Australian Human Rights Commission Regulations 1989* (Cth), regulation 4; *Anti-Discrimination Act 1998* (Tas), section 50; *Anti-Discrimination Act 1992* (NT), section 4.

record are fairly common, making up 23% of complaints to the Federal Human Rights and Equal Opportunity Commission (HREOC) under the *AHRC Act* in 2010-2011.[71] In response, the HREOC has issued guidelines indicating that employers should not ask job applicants or employees about any past criminal convictions, unless this information is relevant to the individual's ability to perform the inherent requirements of the particular position (for example, a prior driving offence may be relevant where a driver's licence is required to perform the job; a prior offence involving dishonesty may be relevant where the job involves responsibility for financial matters).[72]

Finally, even where spent convictions or anti-discrimination laws would otherwise apply, licensing and registration requirements in certain industries/occupations require employers both to ask prospective employees about prior criminal activity; and to take that information into account when deciding whether to employ the person. Areas of employment where these specific regulatory arrangements apply include teaching, nursing, policing, correctional and security services, taxis/transport, casinos/gaming/racing, and the legal profession.[73]

4. Personal information and privacy protection during the employment relations

Overview

Australian employers are entitled to obtain a range of personal information relating to their employees, given the employee records exclusion from the *Privacy Act* (*supra*). However, it is important to understand the limitations of that exclusion and the questions that arise about its application to the monitoring of employee emails, internet use, social media activity, etc (both while on-duty and outside the workplace/work hours). Legislation regulating various forms of surveillance of employees is also relevant in this context, along with the law impacting on workplace drug and alcohol testing. Misuse by employees of social media – and employers' rights to discipline and dismiss employees on this basis – has become a major issue in Australian employment law recently, giving rise to increasing numbers of unfair dismissal claims. Finally, under the *FW Act*, employers are required to maintain records of employees' pay and other employment conditions for compliance purposes.

Operation of the Privacy Act Employee Records Exemption during Employment

As indicated earlier in this paper, any act or practice directly related to an employee record is exempt from the requirements of the *Privacy Act* (in relation to private sector

[71] HREOC, 'Discrimination in Employment on the basis of Criminal Record' at: http://www.humanrights.gov.au/discrimination-employment-basis-criminal-record (accessed 20 January 2014).

[72] HREOC, *On the Record: Guidelines for the Prevention of Discrimination in Employment on the basis of Criminal Record*, 2012, at: http://www.humanrights.gov.au/sites/default/files/content/human_rights/criminalrecord/on_the_record/download/otr_guidelines.pdf (accessed 20 January 2014), pages 5, 14-19, including discussion of *Christensen v Adelaide Casino Pty Ltd*, unreported (casino's rejection of application for employment as a bar attendant from individual with prior conviction for stealing alcohol 7-8 years previously, found not sufficiently connected to inherent requirements of particular position including requirement of trustworthiness).

[73] *Ibid*, 13, 32-33.

employers with an annual turnover of at least A$3 million). It has also been shown that this exclusion only applies in the context of a current or former employment relationship (therefore, it does not apply in respect of job applicants, *supra*; nor does it apply in relation to persons engaged as contractors or subcontractors).[74]

There are two further requirements that must be satisfied for the exemption in section 7B(3) to apply:

- the act or practice must be directly related to the employment relationship – therefore, use by an employer of personal information contained in an employee record for a purpose extraneous to the employee's employment would not be covered by the exclusion (for example, the employer's provision of the personal information to a direct marketing firm or debt collection agency; or disclosure of an employee's status as a client of the employer, a charity, without the employee's consent);[75]
- the act or practice must be directly related to the employee record held by the employer – so, for example, if personal information in an employee record is provided by the employer to its workers' compensation insurer, the information does not retain its exempt status in the hands of the insurance company (i.e. the insurer's handling of that information is subject to the APPs in the *Privacy Act*).[76]

The application of the *Privacy Act* (and the employee records exemption) to employers' monitoring of employee email and internet use is discussed in the next section.

Workplace Surveillance/Monitoring of Employees

Australian employers (like employers elsewhere) have a strong interest in monitoring their employees' use of workplace email and the internet, for example 'to ensure that employees are not wasting time or their employer's resources, or harassing co-workers, or even engaging in unlawful activities …'.[77] However, the lawfulness of such monitoring is a complex issue, involving the potential application of the *Privacy Act* and Federal, State and Territory surveillance legislation.[78]

(i) Privacy Act Regulation of Monitoring

In relation to the *Privacy Act*, the first issue to consider is whether an employee's work emails or records of their internet activity constitute 'personal information' which is covered by the protections in the legislation – i.e. do the emails or web records contain information which could in some way enable identification of the individual? This will often be the case, for example where an employee's name forms part of their email

[74] On the privacy rights of workplace contractors see Leanne Nickels and Rachael Smith, 'The legal risks arising from electronic storage of work information in the construction industry', *Mondaq Business Briefing*, 7 June 2012, at: http://www.mondaq.com/ (accessed 7 January 2014).

[75] CCH, *supra* note 44, [20-200]-[20-205], including discussion of *B v Cleaning Company* [2009] PrivCmrA 2 and *C v Charity* [2011] PrivCmrA 3.

[76] CCH, *supra* note 44, [20-200]*;* see also [20-205] noting that this principle applies in respect of the full range of third parties to which an employer may provide employees' personal information for HR management purposes, including payroll processing, medical checks/health services, remuneration consultants, superannuation funds, etc.

[77] Creighton and Stewart, *supra* note 58, 577.

[78] See generally Anne O'Rourke, Julian Teicher and Amanda Pyman, 'Internet and Email Monitoring in the Workplace: Time for an Alternate Approach' (2011) 53 *Journal of Industrial Relations* 522.

address.[79]

Secondly, it must be determined whether the employee's emails or web history form part of an employee record and are therefore subject to the *Privacy Act* exemption (*supra*). This will not always be straightforward. In Creighton and Stewart's view: 'Arguably … information gathered by or accessible to an employer regarding personal e-mails sent on work computers would fall outside the exemption, as would records on internet browsing.'[80] If the contents of an email are not relevant to the employee's employment, then the exemption will not apply.[81] However, according to Banks et al, the *Privacy Act* definition of 'employee record' is broad enough to cover 'many matters of interest to an employer when conducting email surveillance, so as to exclude such emails … from any protection under the legislation' (including information that may ultimately be relevant to disciplinary matters).[82]

In *Griffiths v Rose*,[83] an employer's monitoring of an employee's use of a work-provided laptop was found not to be inconsistent with the *Privacy Act*. The employee was dismissed by a Federal government department for viewing pornography on the laptop at his home, in breach of the department's IT policy. This followed monitoring by the department using 'Spector 360' technology, which is:

> a utility … known as a "desktop logging system". It performed a number of functions including logging the occurrence of particular keywords and taking a precise snapshot of the user's desktop every 30 seconds. … Spector360 also collected all emails, attachments, internet searches and instant messages performed by a user and sent them to [a] dedicated server.[84]

Perram J of the Federal Court found that the department was entitled to insist on the employee's compliance with its IT policy; and its monitoring of his computer use (even at home) to ensure compliance was for a lawful purpose under the *Privacy Act*. The employee's argument that it was unfair for the department to monitor his private use of the laptop was dismissed by Perram J:

> Unlike the circumstance where Spector360 gratuitously collects personal banking information or credit card details during periods of personal use (which may very well involve a breach of privacy) what it collected from Mr Griffiths was the very thing it was intended to collect, namely, evidence of breaches of the Code of Conduct. It was also the very thing the Department had warned Mr Griffiths that it was going to monitor his use to detect. In those circumstances, I conclude that the collection of this particular information was not unfair within the meaning of [IPP] 1(2). It is not unfair to warn a person that their computer use will be monitored in order to detect any accessing of pornography and then

[79] CCH, *Australian Labour Law Reporter*, CCH Australia Ltd, 2012, 31-700.
[80] Creighton and Stewart, *supra* note 58, 577. See also Dan Svantesson, 'Can you read an employee's private email? Addressing the legal concerns' (2009) 12:7 *Internet Law Bulletin* 98; and Australian Government, Office of the Australian Information Commissioner, *supra* note 16, asserting that the *Privacy Act*: ' … applies to staff e-mails that contain personal information other than "employee records" in certain circumstances. [It] also applies to logs of staff web browsing activities.'
[81] CCH, *supra* note 78, 31-700.
[82] Dianne Banks, Peter Leonard, James Pomeroy, Grace Keesing and Kim McGuren, 'Employer surveillance of employee emails: what are the rules?' (April/May 2013) *Internet Law Bulletin* 8, 11; see also Des Butler and Vanessa Mellis, 'Email: Do Employees have a Right to Privacy?' (2002) 23 *The Queensland Lawyer* 78, 82.
[83] (2011) 192 FCR 130.
[84] *Ibid*, [3].

to do so.[85]

However given the risk that monitoring of employees' emails, in particular, will likely result in some private information being viewed, private sector employers are often counseled to err on the side of compliance with the APPs in the handling of such material (for example, by keeping access to it within reasonable limits and not using it for ulterior purposes).[86]

Another response to the legal minefield for employers in this area is the widespread adoption of workplace policies on email and internet use, to ensure that employees are aware of an organisation's rules and expectations and the consequences of any misuse (including disciplinary action or dismissal). These policies should also clearly indicate to employees the nature of any monitoring conducted by the employer, and identify relevant personnel who may access staff email and internet records.[87]

(ii) Monitoring and Surveillance Legislation

In addition to the *Privacy Act*, email and internet monitoring is subject to the operation of various surveillance legislation in place around Australia, which also regulate other forms of surveillance including telephone monitoring and GPS tracking.

As indicated earlier in this paper, each Australian jurisdiction has legislation prohibiting unlawful telecommunications interception and monitoring, with some of these laws dealing specifically with workplace surveillance.[88] Many of these statutes were introduced in response to technological developments such as tape recorders and other listening devices (from the 1970s), CCTV cameras (1980s-1990s) and mobile phones (1990s-2000s) – although mostly they pre-date newer technologies like smart phones, tablets and GPS tracking.[89] Employers increasingly deploy these different types of technology for reasons including protecting the business from theft or damage, ensuring compliance with regulatory requirements (e.g. under WHS legislation), monitoring employee performance and observing any misconduct by employees.[90]

Federal legislation, the *Telecommunications (Interception and Access) Act 1979* (Cth), will apply in most instances to require that employers notify employees of any interception (i.e. listening or recording) of communications in the workplace such as phone calls or emails.[91] Failure to comply with the requirements of this legislation, for example where an employer intercepts a communication without an employee's knowledge, constitutes a

[85] *Ibid*, [30]. See also *Queensland Rail v Wake* (2006) 156 IR 393; *B, C and D v Australian Postal Corporation* [2013] FWCFB 6191.

[86] McCallum and Stewart, *supra* note 1, 37; see also Margaret Jackson, *A Practical Guide to Protecting Confidential Business Information*, Thomson Lawbook Co, Sydney, 2003, 81.

[87] Australian Government, Office of the Australian Information Commissioner, *supra* note 16. See also Dean Ellinson, 'Employees' Personal Use of Their Employer's E-mail System' (2001) 29 *Australian Business Law Review* 165; and *Australian Municipal, Administrative, Clerical and Services Union v Ansett Australia Limited* (2000) 175 ALR 173, urging employers to adopt policies on acceptable email and IT use.

[88] See *supra* notes 10 - 11.

[89] See Sempill, *supra* note 1, 111-115; Chapman and Tham, *supra* note 1, 634; Anna Johnston and Myra Cheng, 'Electronic workplace surveillance, Part 2: responses to electronic surveillance – resistance and regulation' [2003] *Privacy Law and Policy Reporter* 7; Suzanne Cusack, 'Employee privacy in the modern workplace' (2010) 7:3 *Privacy Law Bulletin* 38.

[90] Chapman and Tham, *supra* note 1, 634-635.

[91] CCH, *supra* note 44, [20-300]; see also [20-440] for a detailed discussion of the *Telecommunications (Interception and Access) Act 1979* (Cth).

criminal offence.[92] Employers usually seek to ensure compliance with the *Telecommunications (Interception and Access) Act* by informing employees of any intended surveillance of emails or other communications in a workplace policy.[93]

State and Territory statutes also apply to prohibit the use of various types of 'devices' to listen in on private conversations and activities, although some legislation permits a person to record a conversation which he/she is party to or where necessary to protect his/her lawful interests.[94] These laws (some of which also cover video surveillance and GPS tracking) are increasingly coming into play in workplace disputes, with employees covertly recording disciplinary meetings or conflicts with other workers and seeking to rely on the 'evidence' obtained in subsequent legal proceedings.[95] In one recent case, an employee's alleged use of a listening device to record unfair dismissal conciliation proceedings in the FWC led to a police investigation.[96] In another case, the employer's surveillance of an employee was called into question although found to be lawful.[97] The potential for unlawful surveillance has also arisen in the context of FWC's role in approving proposed enterprise agreements.[98]

---

[92] Banks et al, *supra* note 81, 10.

[93] *Ibid*.

[94] For a detailed explanation of the relevant statutes see Doyle and Bagaric, *supra* note 25, 142-148; CCH, *supra* note 44, [20-440].

[95] William Houston, 'Covert recordings? – there's an app for that!', Baker & McKenzie, *HReSource*, 7 November 2013, discussing *Thomas v Newland Food Company* [2013] FWC 8220 (employee's secret recording of discussions with management, although legal under Queensland statute, breached trust between parties such that employee not entitled to reinstatement following finding of unfair dismissal: 'there could hardly be an act which strikes at the heart of the employment relationship, such as to shatter any chance of re-establishing the trust and confidence necessary to maintain that relationship, than the secret recording by an employee of conversations he or she has with management'); *Thompson v John Holland Group Pty Ltd* [2012] FWA 10362 (dismissal of employee for covertly recording discussion about duties, in breach of WA legislation, upheld as breach of company's Code of Ethics requiring employees to protect individuals' privacy); *Hazlam v Fasche Pty Ltd* [2013] FWC 5593 (recording potentially illegally obtained by employee not admitted in evidence in unfair dismissal case); and *Wintle v RUC Cementation Mining Contractors Pty Ltd* [2013] FCCA 694 (evidence inadvertently recorded admitted in general protections claim). Note also the observation of Drake DP in *Lever v Australian Nuclear Science and Technology Organisation* [2009] AIRC 784 [103]: 'Applying ordinary Australian community standards I do not accept that any employee or any employer would be content to have any meeting they were attending secretly tape recorded. The ordinary conduct of personal, business and working relationships in our community is predicated on the basis that if there is to be any record of a meeting it will be agreed in advance**.** Anything else is quite properly described as sneaky**.** It's [sic] very sneakiness makes it abhorrent to ordinary persons dealing with each other in a proper fashion.'

[96] 'Worker ordered to pay $10,000 costs, as employer alleges proceedings bugged', *Workplace Express*, 13 December 2013; Matthew Stevens, 'Qube, Lunt and a little black box', *The Australian Financial Review*, 13 December 2013, 28.

[97] *Diehm v Toll Transport Pty Ltd* [2012] FWA 8818 (employer's video surveillance of employee undertaking private activities to ascertain veracity of worker's compensation claim, held legitimate because employee was on paid leave, although dismissal of employee found unfair on other grounds). See also *Claypole v BlueScope Steel Ltd, JKC v BlueScope Steel Ltd* [2008] AIRC 276 and 354; *Gervasoni v Rand Transport (1986) Pty Ltd* [2010] FWAFB 2526.

[98] See e.g. *City of Joondalup* [2013] FWCA 7977 (agreement approved despite including clause permitting installation of GPS tracking devices on work vehicles or equipment; FWC rejected argument that by breaching WA surveillance devices legislation, the agreement could not be approved; FWC held section 192, FW Act only precludes approval of agreements inconsistent with Federal (not State) laws). See also *CPSU v VicForests* [2011] FWA 3079 (FWC conciliation assisted parties to reach agreement on implementation of GPS-based surveillance).

Specific workplace surveillance legislation in several States and the ACT goes further in protecting employees' privacy than the telecommunications interception and listening devices laws discussed *supra*. The most comprehensive statute is the *Workplace Surveillance Act 2005* (NSW), which applies to computer surveillance (including employees' email and internet usage, at work or at any other place where work is being performed); video surveillance; and location tracking.[99] Generally, employees must be informed at least 14 days in advance of any proposed surveillance, including the kind of surveillance that will be carried out; the method to be used; when it will commence; and whether it will be for a fixed period, intermittent or ongoing. Additional notice requirements apply to camera surveillance (e.g. clearly visible signs and cameras), and tracking surveillance (e.g. clearly visible notice on a vehicle). Certain types of surveillance are completely prohibited (e.g. in change rooms, toilets or showers at a workplace; or computer use outside the workplace, unless an employee is using employer-provided equipment). Any records obtained by an employer through any of the types of surveillance permitted by the NSW legislation can only be used for a legitimate purpose related to the employment of employees; the employer's legitimate business activities; or law enforcement purposes. The legislation also includes some restrictions on employers' blocking of employees' email or access to internet sites (e.g. this must be consistent with the employer's workplace surveillance policy).

In Cusack's view, the NSW *Workplace Surveillance Act* has been 'a great step forward in recognising that surveillance in an employment context is very different to surveillance outside of work'; and bridges the gap left by the telecommunications interception and listening devices laws which 'largely rely on … protecting "private conversations" … [but fail] to take into account the employer/employee relationship, and the tension between the need and desire for business to harness technology and the need for reasonable employee privacy.'[100]

Drug and Alcohol Testing

Testing of employees for the presence of drugs, alcohol or other substances that have a capacity to impair performance is another fairly widespread practice in Australia, usually justified on the basis of the employers' obligations under WHS legislation.[101] The legality of such testing is reasonably clear: although there is no statutory basis for it (apart from mandatory testing requirements in certain industries, e.g. public transport, mining), at common law employers can direct employees to undergo a drug or alcohol test as long as the request is reasonable.[102] Further, industrial tribunals tend to support the prerogative of

[99] CCH, *supra* note 44, [20-310] and [20-400]-[20-430]. Under the NSW legislation, 'overt' surveillance is permitted subject to compliance with the statute's requirements, while 'covert' surveillance usually requires a warrant to be issued by a magistrate (on the basis that unlawful activity is suspected).

[100] Cusack, *supra* note 89.

[101] See generally Jim Nolan, 'Employee privacy in the electronic workplace Pt 2: drug testing, out of hours conduct and references' [2000] *Privacy Law and Policy Reporter* 61; Peter Holland, Amanda Pyman and Julian Teicher, 'Negotiating the Contested Terrain of Drug Testing in the Australian Workplace' (2005) 47 *Journal of Industrial Relations* 326; Creighton and Stewart, *supra* note 58, 438. Mandatory drug and alcohol testing on construction sites is soon likely to become a requirement for tenderers seeking to obtain Victorian government-funded building work: see 'Victorian building workers face drug and alcohol testing plus monitoring', *Workplace Express*, 6 February 2014.

[102] *Australian Federated Union of Locomotive Engineers v State Rail Authority of New South Wales* (1984) 295 CAR 188 at 188-193; *Anderson v Sullivan* (1997) 148 CLR 633 at 647-648; discussed in CCH, *supra*

management to implement testing as part of a workplace drug and alcohol policy with appropriate safeguards of employees' interests.[103] The terms of any applicable employment contract, modern award or enterprise agreement may also be relevant to whether an employer has a right to insist on drug or alcohol testing.[104] In numerous decisions, workers have been found to have been lawfully dismissed for failing a drug/alcohol test; and/or for dishonesty associated with drug/alcohol-related activity or the testing itself.[105]

It was noted in 2012 that: 'Typically [drug and alcohol testing] can occur through the taking of blood, urine, saliva, and hair samples as well as breath tests'.[106] Recently, however, there has been some controversy surrounding the testing of oral fluid, with the National Association of Testing Authorities, Australia withdrawing accreditation for on-site drug testing of oral fluid due to questions over its reliability as a basis for determining cannabis use (among other factors).[107] Despite this, the FWC has since declined an employer's request to allow it to conduct urine testing (rather than saliva-based swab tests).[108]

It is likely that the employee records exemption from the *Privacy Act* would apply to information about an employee acquired through drug or alcohol testing, as this information would clearly be relevant to the employee's employment.[109] However, any external agencies involved in the testing would be subject to the requirements of the *Privacy Act*.[110]

Dismissal of Employees for Social Media-related Misconduct

As mentioned a number of times in this chapter, employee use of social media has become a major employment issue in Australia recently,[111] with a rise since 2010 in unfair dismissal cases involving alleged serious misconduct by employees for social media activity.[112] The general trend in these decisions has been to uphold the dismissal where the

note 44, [20-460].

[103] CCH, *supra* note 44, [20-460] including reference to *Caltex Australia Limited v Australian Institute of Marine and Power Engineers, Sydney Branch; Australian Workers Union* [2009] FWA 424.

[104] CCH, *supra* note 44, [20-460].

[105] See for example *McCarthy v Woolstar Pty Ltd* [2014] FWC 1186 (dismissal of forklift driver upheld following laboratory test for cannabis use); *Pitts v AGC Industries Pty Ltd* [2013] FWCFB 9196 (employee failed to meet drug test deadline because provided unsuitable sample, diluted by drinking two bottles of water immediately prior to test); *Vaughan v Anglo Coal (Drayton Management) Pty Ltd* [2013] FWC 10101 (employee dishonestly claimed had taken cold and flu tablets, rather than methamphetamines, prior to test).

[106] CCH, *supra* note 44, [20-460].

[107] Ashurst Australia, 'To pee or not to pee? Drug testing is the question again', *Employment Alert*, 28 October 2013.

[108] *Endeavour Energy* [2014] FWC 198, reported in 'FWC rejects bid for on-site urine drug-testing regime', *Workplace Express*, 17 January 2014; see also *Maritime Union of Australia v DP World Brisbane Pty Ltd and Others* [2014] FWC 1523, stayed in [2014] FWC 2404 pending an appeal before a Full Bench of the FWC (not concluded at the time of writing).

[109] *Ibid*; although employers should keep such information confidential, see Creighton and Stewart, *supra* note 58, 438.

[110] CCH, *supra* note 44, [20-460].

[111] On privacy issues relating to the use of social media generally see Margaret Jackson and Marita Shelly, *Electronic Information and the Law*, Thomson Reuters Lawbook Co, Sydney, 2012, Chapter 9.

[112] Employees covered by the FW Act may bring a claim for unfair dismissal under Part 3-2 of the legislation (unless they fall within one of the exclusions from eligibility to bring a claim); see further Creighton and Stewart, *supra* note 58, 632-656.

employee's social media posts (even if 'private') are highly offensive or derogatory towards the employer and have (or could) cause serious harm to the business. On the other hand, other factors – such as an employee's inexperience with forums like Facebook, and length of service with an employer – can result in a finding of unfair dismissal in these cases. Space does not permit a complete discussion of this case law.[113] However, some of the more interesting and significant decisions include the following.

Employee's conduct justified dismissal:

- *O'Keefe v Williams Muir's Pty Ltd* [2011] FWA 5311: employee's offensive comments on Facebook about pay discrepancies found to provide grounds for summary dismissal; although privacy settings set to maximum and employer not named, comments were seen by several co-workers and considered to be threatening in nature.
- *Margelis v Alfred Health* [2012] FWA 5390: IT administrator's dismissal for reasons including highly offensive online conversation with co-worker, upheld; such conversations using work computer found to be inherently non-private.
- *Little v Credit Corp Group Limited* [2013] FWC 9642: employee's dismissal for grossly offensive Facebook comments re sexual harassment of a co-worker,[114] and criticism of employer's key stakeholder, upheld; employee's claim that did not know how Facebook worked dismissed as highly implausible (young person, frequent user of Facebook). The social media posts were likely to be deeply offensive and damaging to employer's business.
- *Banerji v Bowles* [2013] FCCA 1052:[115] Federal Circuit Court refused injunction preventing dismissal of public servant in Department of Immigration and Citizenship, who anonymously made comments on Twitter criticising Federal Government's policies on immigration detention. Dismissal found to be consistent with Australian Public Service Code of Conduct, including limits on unofficial public comment. Implied freedom of political expression under *Australian Constitution* does not extend to provide unfettered rights of expression, and did not extend to comments 'tweeted' by employee to her 700 followers.[116]

Employee succeeded in unfair dismissal claim:

- *Fitzgerald v Dianna Smith t/a Escape Hair Design* [2010] FWA 7358, upheld on appeal [2011] FWAFB 1422: employee's Facebook post (read by 'friends' including some of employer's clients), complaining of warning issued by employer and failure to provide holiday pay,[117] found to be a 'foolish and silly' outburst but not so detrimental to employer's business as to justify dismissal.
- *Wilkinson-Reed v Launtoy Pty Ltd* [2014] FWC 644: held, employee unfairly dismissed by principal of car sales business for making critical comments about him

[113] See for example Thornthwaite, *supra* note 4; Louise Floyd and Max Spry, 'Four burgeoning IR issues for 2013: Adverse action; social media & workplace policy; trade union regulation (after the HSU affair); and the QANTAS aftermath' (2013) 37 *Australian Bar Review* 153, 160-164; Bland and Waterhouse, *supra* note 3.

[114] See also Paul O'Halloran, 'Cyber-sexual harassment at work' (October 2012) *Internet Law Bulletin* 123.

[115] This was in fact a general protections/adverse action claim under Part 3-1 of the FW Act, rather than an unfair dismissal claim; on Part 3-1 see further Creighton and Stewart, *supra* note 58, 557-574.

[116] See Stephen Price and Allison Grant 'Social Media: Private Life and Work Life Collides Again', Corrs Chambers Westgarth, 9 September 2013.

[117] Her exact words were: 'Xmas 'bonus' along side a job warning, followed by no holiday pay!!! Whoooooo! The Hairdressing Industry rocks man!!! AWSOME!!! [sic]'.

in private Facebook chat with the principal's wife. Company's social media policy did not extend to preclude such communications, which were in the manner of a private email.

- *Linfox Australia Pty Ltd v Stutsel* [2012] FWAFB 7097, upheld by Full Federal Court in *Linfox Australia Pty Ltd v Fair Work Commission* [2013] FCAFC 157: employee's dismissal for making racially derogatory and sexually offensive comments about managers on Facebook, held to be harsh, unjust and unreasonable; employee reinstated. Relevant factors included employee's lengthy service and good employment record; limited understanding of how Facebook worked (e.g. that comments could be disseminated more broadly than just his 170 'friends'); fact that conduct occurred outside work hours; and that employee did not intend comments to be seen by managers. Also important was the company's failure to have a policy on employees' use of social media.

In a number of these decisions, the FWC has made some general comments about employee social media use that will no doubt be instructive in future cases. For example, in *Fitzgerald v Dianna Smith t/a Escape Hair Design* [2010] FWA 7358 it was stated that ([50]-[51]):

> Postings on Facebook and the general use of social networking sites by individuals to display their displeasure with their employer or a co-worker are becoming more common. What might previously have been a grumble about their employer over a coffee or drinks with friends has turned into a posting on a website that, in some cases, may be seen by an unlimited number of people. Posting comments about an employer on a website (Facebook) that can be seen by an uncontrollable number of people is no longer a private matter but a public comment.
>
> It is well accepted that behaviour outside working hours may have an impact on employment 'to the extent that it can be said to breach an express term of [an employee's] contract of employment'. (*Rose v Telstra*, AIRC Print Q9292 (4 December 1998))[118]

And despite the lenient approach adopted in *Linfox Australia Pty Ltd v Stutsel* [2012] FWAFB 7097, it was also stated that ([26]):

> In the present case, the series of Facebook conversations in which the comments were made were described by the Commissioner as having the flavour of a conversation in a pub or cafe, although conducted in electronic form. We do not agree altogether with this characterisation of the comments. The fact that the conversations were conducted in electronic form and on Facebook gave the comments a different characteristic and a potentially wider circulation than a pub discussion. Even if the comments were only accessible by the 170 Facebook "friends" of the Applicant, this was a wide audience and one which included employees of the Company. Further the nature of Facebook (and other such electronic communication on the internet) means that the comments might easily be forwarded on to others, widening the audience for their publication. Unlike conversations in a pub or cafe, the Facebook conversations leave a permanent written record of statements and comments made by the participants, which can be read at any time into the future until they are taken down by the page owner. Employees should therefore exercise considerable care in using social networking sites in making comments or conducting conversations

[118] See also 'When work and out-of-hours conduct clash: Lessons from the case law', *Workplace Express*, 15 March 2013; and Thornthwaite, *supra* note 4, 170: 'An employer … must be able to show a sufficient, requisite connection between the employee's off-duty conduct and the employment relationship legitimately to terminate them or otherwise adversely affect their employment on the basis of off-duty conduct.'

about their managers and fellow employees.[119]

Thornthwaite concludes, from her summary of the case law, that: '… for employees to comply with their implied contractual duties they cannot safely communicate about their work lives in [social media] forums. Social media does appear to have had the effect that employees are never entirely off-duty.'[120]

Finally, many Australian employers have adopted social media policies and require employees to undertake social media training.[121] In one recent case, an employee's refusal to participate in such training was found to provide lawful grounds for dismissal for serious misconduct.[122] More controversially, the Department of Prime Minister and Cabinet introduced a very restrictive social media policy in April 2014, prohibiting employees from (among other things) engaging in harsh or extreme criticism of the government or its policies; and requiring employees to report social media breaches by their colleagues to the Department.[123]

Employers' Obligations to Maintain Employee Records under the Fair Work Act

Employers covered by the *FW Act* are *required* to maintain various employee records, to ensure that employees receive their correct pay and entitlements under that legislation and any modern awards or enterprise agreements that apply to their employment.[124] Civil penalties of up to A$2,550 apply to breaches of these obligations.

Known colloquially as 'time and wages records', these employee records must be kept for seven years in the form prescribed by the *Fair Work Regulations 2009* (Cth) (*FW Regulations*), and must include the following information:[125]

- names of employer and employee;
- type of employment (full-time, part-time, casual, etc);
- employee's date of commencement;
- Australian Business Number of employer (where applicable);
- employee's rate of remuneration (gross and net pay, any deductions); bonuses; loadings; penalty rates; other monetary allowances;
- overtime hours worked; hours of work for casual/irregular part-time employees;
- leave taken by employee (annual leave, personal/carer's leave, etc); balance of leave entitlements;
- information relating to superannuation contributions made by employer on behalf of employee;
- details of termination of employment (for example, whether by consent, by notice,

[119] See also 'Social media ignorance less likely to get employees off the hook: VECCI director', *Workplace Express*, 10 February 2014.
[120] Thornthwaite, *supra* note 4, 184.
[121] See for example 'Twitter ban at work counterproductive: Telstra', *Workplace Express*, 20 April 2009; 'Unions concerns trigger Commbank rethink on social media', *Workplace Express*, 7 February 2011. Increasingly, enterprise agreements are including workplace social media restrictions: see 'Agreements outlaw Facebook at work and seek to limit after-hours use', *Workplace Express*, 7 December 2012.
[122] *Pearson v Linfox Australia Pty Ltd* [2014] FWC 446; upheld on appeal [2014] FWCFB 1870.
[123] *Social Media Policy of the Department of the Prime Minister and Cabinet*, 8 April 2014; this policy is in part a direct response to *Banerji v Bowles* [2013] FCCA 1052 (*supra*).
[124] *FW Act*, section 535(1).
[125] *FW Act*, section 535(2); *FW Regulations*, Chapter 3, Part 3-6, regulations 3.31-3.41.

summarily or other form of dismissal).

An employee is entitled to inspect and copy his/her employment record, upon request to the employer (former employees may also exercise this right).[126] Employee records may also be accessed by the Fair Work Ombudsman (the Federal agency responsible for enforcement of minimum employment standards),[127] or a trade union representing an employee whose employment rights may have been infringed.[128] Employers must correct any error in an employee record as soon as the employer becomes aware of the error (for example, once it is drawn to the employer's attention by an employee or union).[129] In effect, these provisions give employees some of the rights they would have under the NPPs if the employee records exemption under the *Privacy Act* did not apply.[130]

5. Personal information and privacy protection after the employment relations

As indicated earlier in this paper, the employee records exemption from the *Privacy Act* applies not only to current but also former employment relationships. As a result, any personal information relating to a former employee held within an employee record (*supra*) could be provided by the former employer to another prospective employer – e.g. information about the employee's performance, training, (mis)conduct, any disciplinary action, and reasons for termination.[131] However, such information *would* be subject to the *Privacy Act* in the hands of the prospective employer. Commonly, information about a former employee will be provided in a reference. Although not obliged to provide a reference for a former employee, employers must be careful when they do so not to include any misleading or defamatory material.[132]

Another post-employment issue that has arisen in a number of recent cases is the use by former employees of social media sites such as LinkedIn to solicit business from clients of their former employer (alternatively, this might occur while an employee is still employed but making moves to start out on their own or join another business). Such conduct is likely to breach an employee's implied contractual obligations, or express restraint clauses/restrictive covenants, not to engage in competition with a former employer; not to solicit its customers or staff; and not to misuse the former employer's confidential information.[133]

---

[126] *FW Regulations*, Chapter 3, Part 3-6, regulations 3.42-3.43.

[127] *FW Act*, sections 708, 712, 714; *FW Regulations*, Chapter 3, Part 3-6, regulation 3.31 (records must be kept 'in a form that is readily accessible to an inspector').

[128] *FW Act*, sections 482-483.

[129] *FW Regulations*, Chapter 3, Part 3-6, regulation 3.44.

[130] CCH, *supra* note 44, [20-200].

[131] Carolyn Sappideen, Paul O'Grady, Joellen Riley and Geoff Warburton, *Macken's Law of Employment*, Thomson Reuters Lawbook Co, Sydney, 7th edition, 2011, 202-203.

[132] *Ibid*, 202-206.

[133] See e.g. *Pedley v IPMS Pty Ltd t/a peckvonhartel* [2013] FWC 4282; Chris McLeod and James Neil, 'Employees, social media and confidential information: uneasy bedfellows' (October 2013) *Internet Law Bulletin* 134. On the law relating to the implied duty of fidelity, and the enforceability of express restraint clauses, see Creighton and Stewart, *supra* note 58, 413-416, 423-428.

6. Conclusion

In 2000, the Office of the Australian Information Commissioner stated that: 'It is clear that most staff do not expect to completely sacrifice their privacy while at work.'[134] This sentiment is reflected in data from a 2004 survey commissioned by the Federal Privacy Commissioner, showing that 34% of respondents felt employers should not have any access to employees' work emails; 35% objected to the use of surveillance equipment in the workplace; and 59% opposed random drug testing.[135]

However, as this paper has shown, the actual extent of privacy protection afforded to Australians in the workplace is limited – and inconsistent in different parts of the country. Ironically, workers have more protection of their personal information *before* commencing employment, given that the employee records exemption from the *Privacy Act* does not apply during the recruitment process. Prospective employees are also the subject of discrimination law protections, and safeguards in relation to health screening and the use of information relating to criminal records.

Once in a job, personal information relating to an employee's employment is not covered by the protections provided under the *Privacy Act*. The employee's use of email and internet in the workplace (or outside) may be the subject of monitoring and surveillance, as may his/her phone calls and even movements (through GPS tracking) – with differing levels of safeguards under Federal, State and Territory laws. There is a fairly permissive approach to drug and alcohol testing in Australia, and increasingly the social media activities of employees are being called into question in unfair dismissal cases.

Given the overhaul of the *Privacy Act* through the 2012 amendments, further major legislative change in this area is unlikely. Nor does there seem to be any impetus for uniform national regulation of workplace surveillance. It can be expected, then, that Australian law will continue to provide employees with only 'a thin wall of privacy protection, with gaps and cracks' for some time to come.

[134] Australian Government, Office of the Australian Information Commissioner, *supra* note 16.

[135] Roy Morgan Research, *Community Attitudes Towards Privacy 2004*, discussed in 'Research on Australian attitudes towards privacy – Part 1' (2004) 1: 6 *Privacy Law Bulletin* 93, 95.

List of Participants

I. Coordinators

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

Hiroya Nakakubo
Professor
Graduate School of International Corporate Strategy (ICS)
Hitotsubashi University, Japan

II. Speakers <in order of presentation>

Gregor Thüsing
Professor
Faculty of Law
University of Bonn, Germany

Benjamin Dabosville
Maître de conferences
Institute du Travail
Université de Strasbourg, France

Diego Álvarez Alonso
Lecturer of Labour Law and Social Security
Department of Law
University of Oviedo, Spain

Gillian Morris
Professor
Barrister, Matrix Chambers
University College London, United Kingdom

Benjamin Sachs
Professor
Harvard Law School, U.S.A.

Kungang Li
Professor
Law School
Anhui University, China

Sung-wook Lee
Professor
School of Law
Ewha Womans University, Korea

Ryoko Sakuraba
Associate Professor
Graduate School of Law
Kobe University, Japan

Shih-Hao Liu
Professor
Law School
Ming-Chuan University, Taiwan

Anthony Forsyth
Professor
Graduate School of Business and Law
RMIT University, Australia

III. Discussants **<in alphabetical order>**

Dongwook Cha
International Research Student
Graduate Schools for Law and Politics
The University of Tokyo

Sukhwan Choi
Assistant Professor
College of Law
Myongji University, Korea

Tamako Hasegawa
Associate Professor
Faculty of Administration and Social Sciences
Fukushima University

Yoko Hashimoto
Professor
Faculty of Law
Gakushuin University

Hisashi Ikeda
Associate Professor
Graduate School of Law
Hokkaido University

Masahiko Iwamura
Professor
Graduate Schools for Law and Politics
The University of Tokyo

Natsuki Kohno
Assistant Professor
Graduate Schools for Law and Politics
The University of Tokyo

Yuri Nabeshima
Graduate Student
Graduate Schools for Law and Politics
The University of Tokyo

Yoshiaki Nishigai
Assistant Professor
Graduate Schools for Law and Politics
The University of Tokyo

Hyosook Park
Graduate Student
Graduate Schools for Law and Politics
The University of Tokyo

Ying-Hong Shih
Graduate Student
Graduate Schools for Law and Politics
The University of Tokyo

Nana Takahashi
Assistant Professor
Graduate Schools for Law and Politics
The University of Tokyo

Masahito Toki
Assistant Professor
Graduate Schools for Law and Politics
The University of Tokyo

Koichi Tominaga
Associate Professor
Faculty of Law
Sophia University

Ryuichi Yamakawa
Professor
Graduate Schools for Law and Politics
The University of Tokyo

Qi Zhong
Graduate Student
Graduate Schools for Law and Politics
The University of Tokyo

IV. JILPT

Kotaro Nomura
Executive Director

Mitsuji Amase
Director

International Affairs Department

Hideyuki Oshima
Deputy Director
International Affairs Department

Kayo Amano
International Affairs Department

The Japan Institute for Labour Policy and Training