PRIVACY IN THE WORKPLACE

NATIONAL REPORT ON HUNGARY

AUTHORS

Dr. Gergely László Szőke

Dr. Zsolt György Balogh

Dr. Gábor Polyák

Dr. Balázs Rátai

The Project is co-funded by the European Union's Fundamental Rights and Citizenship Programme

JANUARY, 2012

CONTENT

1. INTRODUCTION AND BACKGROUND

1.1. Purpose and methodology

The main objective of the Country Report is to map current national Hungarian regulations on Privacy in the Workplace and to show the European context of the regulation. We shall also compare Hungarian and German law – based on the two National Reports. Our main objective is to map and describe the current situation; detailing the consequences and making proposals are scheduled for another phase of the project. We will not deal with every single issue regarding data protection in employment: our research will focus on the regulation of technical surveillance in order to differentiate between legal and illegal monitoring or surveillance of an employee, which is a key issue both in Hungary and in the EU.

Besides the relevant Acts we also summarise case law in the respective fields. We search for the recommendations of the Hungarian Data Protection Commissioner (DPC) as well as for the relevant court decisions. The legal literature and the (possible) sources of self-regulation are also examined in our research.

After chapters which summarise the basic concept of privacy issues, we analyse Hungarian regulations on different surveillance technologies which may be used in the workplace. The regulation, typically, does not distinguish between or among technologies, and so, for the most part, the same rules apply. This means that some subchapters will simply refer to another subchapter – but this is in order to avoid repetition. However, our choice of this technology-based structure is based on the fact that the practical problems usually arise concerning a single technology – and so the case law of the DPC and of the courts also focuses on different technologies. It seems that a future code of conduct worked out within the framework of our project will also contain technology-specific rules.

1.2. Overview of the relevant legal sources

In this chapter we look at the relevant international, European and Hungarian regulation on privacy in the workplace.

1.2.1. International and EU sources

1.2.1.1. The ILO code of practice

The International Labour Organisation (ILO) initiated and supported the development of a code of practice[1] which deals in a comprehensive way with the protection of workers' personal data. The code also contains an authorised, integral commentary.[2] This ILOC was approved for publication and distribution by the ILO's governing body in November 1996.

According to Point 2 of the ILOC, it is only intended to provide guidance and has no binding force. It is also stated that the ILOC "does not replace national laws, regulations, international

[1] ILO Code of Practice (Hereinafter: ILOC)
[2] Hereinafter referred to as: ILOCCom

labour standards or other accepted standards. It can be used in the development of legislation, regulations, collective agreements, work rules, policies and practical measures." The scope of the ILOC covers both the private and public sectors and both the manual and automatic personal data processing of workers. The term 'worker' covers current and former workers and also job applicants.

1.2.1.2. The Council of Europe's approach

The Council of Europe was, during the 1980s, a vanguard of international regulation on data protection. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (hereinafter "the Convention") is an early and comprehensive document in this field. The CoE also issued many recommendations in specific fields, and, concerning our research, "Recommendation No. R (89) 2 on the Protection of Personal Data used for Employment Purposes" is relevant. This early document affects many issues and had a strong effect on later national legislation.

1.2.1.3. EU initiatives

First of all we should mention the "general" Data Protection Directive: Directive 95/46/EC[3] which needed to be implemented in all EU member states. The harmonisation of the law means that basic principles are the same in the field of data protection throughout the EU. In the field of data protection in the telecommunication area, Directive 2002/58/EC[4] applies.

We should also mention that the European Commission initiated consultation in 1999 on the development of an EU-level regulatory framework for the protection of workers' personal data. The proposals, which were submitted for consultation, were mainly based on the content of the ILOC.[5] The reaction of social partners (employer and employee associations) to the proposal also referenced the ILOC. EUROCADRES (Council of European Professional and Managerial Staff)[6] emphasised that EU regulation should not be based on workers' consent, but that co-operation between employers, workers and workers' representatives was necessary – as proposed in the ILOC.[7] UEAPME (European Association of Craft, Small and Medium-sized Enterprises)[8] expressed its view that a non-binding code of conduct developed along the lines of the ILOC would be useful.[9]

We also have to mention, that the Article 29 Working Party issues several documents on workplace privacy. The statements and opinion of the working party may affect the national regulation in this field.

---

[3] 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

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[5] European Commission: Second stage consultation, p. 6, footnote 10.

[6] www.eurocadres.org

[7] European Commission: Second stage consultation, p. 20.

[8] www.ueapme.com

[9] European Commission: Second stage consultation, p. 3.

1.2.2. National legislation

Privacy in the Workplace is a complex issue and many Acts contain provisions which are relevant in the field. The legal background is now changing in Hungary: many relevant Acts have been renewed or will be changed in 2011, taking effect on the 1st of January 2012 and on the 1st of July 2012. We try – as far as possible – to analyse the new regulation also.

Regarding the legal framework of Privacy in the Workplace, firstly, there are some fundamental rights in both the current Hungarian Constitution[10] and in the new Constitution[11] which affect the issue of privacy. The main code in the field of privacy protection is the Data Protection Act.[12] The Hungarian Parliament adopted a brand new Data Protection Act[13] on the 11th June 2011, which contains relevant changes in some fields. The Act CXII of 2011 on Informational Self-determination and Freedom of Information abrogates and replaces Data Protection Act of 1992 from 1st January 2012.[14]

Another relevant code is, of course, the Labour Code.[15] The preparation of a new regulation in this field started in summer 2011, and a totally new Labour Code[16] was adopted on 13th December 2011. The new Labour Code will take effect on 1st July 2012.

There are other provisions which regulate data processing concerning employees in the public sector, but none contains any provisions on surveillance and so we do not examine them.

Finally, we should mention that means of privacy protection other than the protection of personal data, such as the Right to Ones Own Image or the Right of Private Correspondence are regulated by both the Hungarian Civil[17] and Criminal Codes.[18]

1.2.3. Self-regulation[19]

In many cases, academic papers refer to the possibility of arranging privacy in the workplace issues in the framework of self-regulation (by collective agreement, by-laws, by codes of conduct or by other internal regulations.)[20] Our research in this field shows that this is more theoretical than everyday practice.

Employers and trade unions have the ability to regulate the procedure and circumstances of the supervision of workers by the employer, and especially the use of personal data, in the collective agreement, specifically in its normative section. This right arises from Art 30. a) of the Labour Code. A collective agreement can regulate rights and obligations relating to the

[10] Act XX of 1949 The Constitution of the Republic of Hungary, (hereinafter: Constitution)
[11] Constitution of Hungary (2011. April 25) (hereinafter: New Constitution)
[12] Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest, hereinafter: Data Protection Act, DPA)
[13] Act CXII of 2011 on information self-determination and freedom of information (hereinafter: New Data Protection Act, New DPA)
[14] About the analysis of the new DPA see more Polyák/Szőke, 2011
[15] Act XXII of 1992 on the Labour Code (hereinafter: Labour Code)
[16] Act I of 2012 on the Labour Code (hereinafter New Labour Code)
[17] Act IV of 1959 on the Civil Code of the Republic of Hungary (hereinafter: Civil Code)
[18] Act IV of 1978 on the Criminal Code (hereinafter: Criminal Code)
[19] This chapter is written with the help of Erika Kovács
[20] Arany Tóth, 2008b, p. 170.

personal data protection of the workers, and it can also regulate the method of supervising workers by technology. The advantage of regulation by collective agreement is that this permits general regulations of the Labour Code and the Data Protection Act to be specified, taking into account any special features of the workplace.[21]

One significant limitation of data protection regulation is that it cannot run counter to the Labour Code, to the Data Protection Act and to the Civil Code. Moreover, it may differ from the regulations of the Labour Code only insofar as it provides more favourable conditions for the worker.[22] However, the Labour Code does not contain any regulation on the supervision of the worker's use of technical tools, apart from tele-workers, and so it is difficult to interpret the main principle, namely regulation which is more favourable for the workers.

As a result of the survey which included 30 collective agreements from different fields and different industries, we can offer some summary in these: collective agreements do not contain any provision for the use or monitoring of the use of e-mail, GPS, internet or phone by the worker or on their supervision by CCTV. The collective agreements examined do not include any regulation on the use or supervision of the use of modern technological tools.

Collective agreements often declare, in general, that a violation of the personal rights of the worker by the employer can be grounds for the worker claiming constructive dismissal. We found the following examples:

1) The collective agreement of MOL (Point 22.2.) specifies that a worker can claim constructive dismissal if the employer violates his or her personal data. This statement can obviously refer to a case when the employer looks at the worker's e-mails, monitors his/her internet use or observes him/her by camera without his/her consent and permission.
2) The collective agreement of Dunaferr specifies, as grounds for constructive dismissal by the worker, a case when the employer humiliates the worker. (3.8.1. point)
3) The collective agreement of Agrow GP states that the worker can claim constructive dismissal if the employer humiliates him/her in public. (37.3. pt c)
4) The collective agreement of Hungarian Post states that the worker can use constructive dismissal if the employer violates his or her dignity or personal rights. (§ 13(3) b) point)
5) The collective agreement of the MTI states the right of the worker to constructive dismissal if the employer humiliates or harasses him/her. (IV. chapter, 1. b)

A recent, comprehensive analysis of collective agreements was conducted in 2008 for the Ministry of Social and Employment Affairs.[23] The study analysed 304 such agreements in 20 sectors. The study examined them in every sector and also summarised them by sector. The study does not include any reference to issues under examination by us, proving that the issues of our research are not the topic of collective agreements.

[21] Cf. Arany Tóth, 2008a pp. 307-308.
[22] Labour Code § 13(3)
[23] Fodor/Nacsa/Neumann, 2008.

It is possible that some company has internal, one-sided guidelines elaborated by the employer laying down regulations on the use of technology by the worker. This can possibly include, even indirectly, provisions for data protection. This practice was indicated informally by one company for us. These internal guidelines are typically for internal use only and are not public. Workers cannot usually participate in drawing up such guidelines and so these can only suggest the way of exercising rights, but cannot limit the rights set in the Labour Code or in other Acts.

1.3. The basic concept of privacy protection in Hungary[24]

1.3.1. Constitutional background

The Hungarian Constitution defines the right to the protection of personal data as a Fundamental Right, and an Act on Data Protection needs a two-thirds majority in Parliament.[25] The new Constitution adopted by Parliament on 18th April, 2011 also lists the right to the Protection of Personal Rights as a fundamental right – in the same article as Freedom of Information. According to the new Constitution, an independent authority monitors these two fundamental rights; the Act concerning the authority (but not the whole Act on Data Protection and Freedom of Information) must be adopted by a two-thirds majority.[26] The new Constitution takes effect on 1st January 2012.

The Constitutional Court declared that the Right to the Protection of Personal Data is interpreted as a right of self-determination in an active sense and not as a traditional right of defence.[27] "Therefore, the content of the Right to the Protection of Personal Data ensured in the Constitution's Article 59 is that the processing and use of personal data is at the discretion of the individuals themselves. The collecting and use of personal data is only allowed with the consent of the data subject; the whole path of data processing has to be transparent and visible for everyone, that is, individuals have the right to know who uses their personal data, when, and for what purpose. As an exception, the law can order compulsory data processing and can also decide the mode of use. Such law limits the right of self-determination but is constitutional if appropriate to the requirements of the Constitution".[28]

Besides the Right to the Protection of Personal Data there are certain other fundamental rights in the Constitution which serve as a means of privacy, namely, the right to the integrity of an individual's reputation, privacy in the individual's home and the right to the protection of secrecy in private affairs. In the new Constitution the right of respecting someone's private

[24] The chapter is based on Szőke, 2010
[25] Constitution, § 59
[26] New Constitution, Article VI.
[27] Majtényi, 2003, pp. 577-637.
[28] Constitutional Court, 15/1991. (IV. 13.); as translated by the author. This concept is based on the famous decision of the German constitutional court in 1983 on the Act on National Census. The decision is cited by Jóri, 2005, p. 25.

and family life, home, communication and good reputation are named as privacy rights in addition to the rights regarding data protection.[29]

1.3.2. General and sector-specific data protection regulation and regulation of other privacy rights

The protection of personal data, as already mentioned, was legally regulated in Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest. The Act was modified several times, including modifications harmonising Hungarian law with the 95/46/EC Directive. The Hungarian Parliament adopted a brand new Data Protection Act on 11th June 2011 which came into effect on 1st January 2012. The new Act changes some fundamental regulations concerning the processing of personal data and establishes a brand-new authority responsible for Data Protection and Freedom of Information. The new authority replaces the current one in which the monitoring and supervision of these issues were entrusted to the Parliamentary Commissioner for Data Protection and Freedom of Information.

The Acts on Data Protection (both the new and the former Acts) prescribe general rules. There are special regulations (lex specialis) concerning personal data processing in certain fields, such as in public administration, in banking, insurance and the telecommunications industry, or concerning direct marketing or scientific research. These provisions (whether as an Act or as part of another Act) concretise the rules of the DPA and permit data processing.

One of the biggest problems in the field of privacy in the workplace is the lack of lex specialis in Hungary. There are no specific rules in the Labour Code which regulate any privacy issues in connection with surveillance, and so the general regulation of the DPA and certain other, very specifically focused rules apply in such cases.

This situation will be changed once the new Labour Code comes into effect on 1st July 2012. The new Labour Code contains some very general provisions on the possibility and boundaries of employee's control and monitoring, which is shown in chapter 1.4.3.2.1. of this essay.

We should also mention that, besides data protection, there are other forms or aspects of privacy protection. The Hungarian Civil Code protects the right to a good reputation (protection against defamation), the right to protect one's image or recorded voice and the protection of mail and personal secrets.[30]

There are also some Criminal Code rules and sanctions in the event of a breach of privacy rights – we shall detail these in the third chapter ('Sanctions').

[29] New Constitution, Article VI.
[30] Civil Code, §§ 78-81.

1.3.3. The basic concept of the Data Protection Act

1.3.3.1. The definition of personal data

The Act on Data Protection defines 'personal data' widely. Personal data means any defined information – relating to an identified or identifiable – natural person and any reference drawn from such information that refers to the given natural person. According to the "old" DPA the personal data preserves this quality during its processing until its relation to the data subject can be restored.[31] The personal factor of the information still remains if the identification is only indirect. In Hungarian law practice, the prevailing view is that the personal factor remains until the relation between the data subject and the information can in some way be reconstructed[32] – even with the involvement of more checks or controllers and with more steps. We have to mention, that the New DPA takes clear step towards the relative interpretation, since it says, that "a data is a personal data as far as the data controller has technical conditions to relate the data to the data subject.[33] The actual interpretation of this provisions is not clear so far,[34] it will be the task of the new Data Protection Authority to work out the details of this issue.[35]

According to the Act, only natural persons can have personal data; legal persons and other institutions are not covered by the Protection of Personal Data.[36]

The Act orders stricter conditions concerning sensitive data. These involve – according to the closed listing of the Act[37] – racial origin, belonging to a national or ethnic minority, political opinions and any affiliation with political parties, religious or other beliefs, trade-union membership, information concerning health, addictions, sex life or criminal records.

1.3.3.2. Data processing, data controller, data processor

'Data processing' means any operation or set of operations that is performed upon data, irrespective of the method of operation (automatic or manual), such as data collection, recording, organisation, storage, alteration, use, transmission, disclosure, alignment or combination, blocking, deletion and destruction, and blocking for further use. The Act unambiguously considers photographing, sound and video recording as data processing.[38]

---

[31] DPA § 2(1)
[32] In detail see the cases DPC, 917/K/1998. and DPC, 127/K/2003. at the same time, viewpoints opposing this can also be found in Judge's law practice (BH 2001.269). The cases are referred to by Jóri, 2005, pp. 109-111., 118.
[33] New DPA § 4(3)
[34] Mostly because of the fact that the definition of personal data still contains the phrase "indirectly identifiable", and the European Directive also follows the
[35] About relative and absolute interpretation of personal data see Majtényi, 2006, pp. 109-111.
[36] Gálik/Polyák, 2005 p. 217.
[37] DPA § 2. 2. New DPA § 3. 3.
[38] DPA § 2. 9., New DPA § 3. 10.

The natural or legal person, and unincorporated organisation that determines the purpose of the processing of data, makes decisions regarding data processing and implements such decisions – itself or engages a data processor to implement them – is a 'controller'.[39]

The new legislation preserved the formal distinction of the "old" Data Protection Act between the data processing activity performed by data controller (as data processing) and processing by the data processor (as technical data processing). Notably, the new legislation also kept the general prohibition of sub-processing of processing operations by processors. Although according to certain opinions this was a fairly outdated provision of the "old" Data Protection Act, §10 (2) of the new legislation still generally prohibits sub-contracting by a data processor of processing services to other processors. This prohibition is considered to be a technical guarantee of the transparent course of data processing.

1.3.3.3. The legal basis of data processing

1.3.3.3.1. Regulation of the DPA of 1992

According to the DPA of 1992, personal data could only be processed if the data subject gives his consent or it is ordered by an Act.[40] The Act on Data Protection did not recognise any other legal ground.[41]

It should be noted that the Directive on the Protection of Personal Data defines the legal basis of data processing more widely. According to Article 7 of the Directive, a legal basis for data processing can be that:

1) The data subject has clearly given his consent; or
2) 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
3) processing is necessary to comply with a legal obligations to which the controller is subject; or
4) processing is necessary in order to protect the vital interests of the data subject; or
5) data 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
6) 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 of the fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

[39] DPA § 2. 8., New DPA § 3. 9.
[40] DPA § 3(1)
[41] Except in those quite rare cases, when the data subject is physically unable to or legally incapable of giving his consent for processing – in this case the processing of his personal data is allowed to the extent necessary to protect the vital interests of himself or of another person or in order to prevent or avert a catastrophe or emergency, cf. DPA § 3(8)

The Act on Data Protection enabled data processing in a still tighter circle. The legal basis based on consideration of the interests of the controller and of the data subject, explained in Article 7 (f) of the Directive, did not exist in Hungarian law before 2012. The requirements included in the Directive only appeared as possible purposes of data processing, even though it is one of the most important safeguards in processing personal data, but the consent of the data subject or legal authorisation could not be substituted by the lawful purpose in itself. According to relevant legal literature,[42] this strict regulation of the Data Protection Act did not run counter to the Directive, since the European Court of Justice declared the possibility of wider protection in the well-known Lindqvist case.[43] We think that conformity is not at all obvious. The ECJ admits the possibility of wider protection outside the scope of the Directive; otherwise it is only acceptable if the balance between the free movement of personal data and the protection of one's private life is maintained.[44] According to our view, the different regulation of the legal basis for processing personal data may infringe the free movement of such data.[45]

1.3.3.3.1. Regulation of the DPA of 2011

The new Data Protection Act changes this situation and also enacts the regulation of article 7 (f) of the Directive – although not as a general legal basis, but as a special legal basis on which data processing may be based.

First, personal data may be processed without the consent of the individual, provided that obtaining the consent is impossible or the expenses involved are disproportionate and

- the processing is necessary for the compliance with a legal obligation of data controller or
- the processing is necessary for the purpose of legitimate interests pursued by the controller or by the third party and such necessity is proportionate to the restriction of privacy.[46]

For one thing, initial indications are that the drafting around the legitimate interest condition actually requires a higher test than set out in the Directive. The data controller must be able to demonstrate that obtaining consent from individuals is impossible or disproportionally expensive before he can rely on the legitimate interest condition.

Notably that the New Data Protection Act does not provide for any interpretation of the above section, therefore, the exact meaning of "impossible" and "disproportionate expenses" will be clarified by the case-law of the Authority and the Court.

Second, if the collection of the personal data was based on the consent of the data subject, the data processing may be continued, if

[42] Jóri, 2005, p. 81.
[43] Case C-101/01
[44] Case C-101/01, 97-98.
[45] The brand new decision of the ECJ strengthen our opinion. See C- 468/10 and C-469/10 cases
[46] New DPA § 6(1)

- the processing is necessary for the compliance with a legal obligation of data controller, or
- the processing is necessary for the purpose of legitimate interests pursued by the controller or by the third party and such necessity is proportionate to the restriction of privacy.[47]

In this case, this legal basis may be used to process personal data for other purposes than the purposes for which it was originally collected.

1.3.3.3.2. Consent to data processing

Consent is a data subject's statement which unambiguously signifies his agreement to personal data related to him being managed – without limitation or with regard to specific operations.[48] The data subject's consent can only be considered valid if it is freely given and determined, and also if it is based on proper information. Therefore, the data subject has to be informed before the data is collected about the most important features of data processing.[49] Consent is generally not dependent on formalities, and so can be given by written or oral means and even by means of some physical movement (for example, by answering a reporter's question). Sensitive data processing requires written consent.

Consent to data processing is considered as given when the data subject himself gives the information either during or for the purpose of his public appearance.[50] Similarly, consent to processing his data to the extent necessary is considered as granted in connection with any proceedings requested by the data subject.[51]

1.3.3.3.3. Data processing based on legal regulation

Personal data processing, even without the consent of the data subject, can be ordered by law in the public interest or by regulation of a local authority based on authorisation (obligatory data processing).[52] The Data Protection Act uses the expression "data processing is ordered by law" and "compulsory data processing"; it does not necessarily mean that the data processing based on law is always obligatory. The interpretation in practice is that data processing may be legal if a legal regulation allows it.[53]

1.3.3.3.4. The legal basis concerning data processing in the workplace

According to the Data Protection Act of 1992 the legal ground for processing personal data in the employment context, as under any other circumstances, could only be the consent of the data subject or authorisation by law. However, this seemingly simple system cannot work in

[47] New DPA § 6(5)
[48] DPA § 2(6), New DPA § 3(7)
[49] Cf. DPA § 6(2); New DPA § 20. The given information has to cover the issue of processing as voluntary or compulsory, the purpose for which his data is required and the legal ground, the person entitled to carry out the management and processing, the duration of the proposed processing operation, the persons to whom his data may be disclosed, and the data subject's rights and remedies.
[50] DPA § 3(5), New DPA § 6(7)
[51] DPA § 3(6), New DPA § 6(6)
[52] DPA, § 3(1), § 5(3), New DPA § 5(1) b)
[53] Jóri, 2005, p. 165.

practice, since the Labour Code and other laws applicable to employment relationships did not contain explicit authorisation for the processing of employees' personal data. At first sight, it may seem from the above that only the consent of the data subject could provide a legitimate ground for processing employees' data. This, however, cannot work in practice.

According to both the old and the new Data Protection Law, consent is the voluntary and determined declaration of the data subject, based on appropriate information, whereby the data subject unambiguously agrees to the processing of personal data relating to him or her with respect to every or merely certain types of data. In case of proceedings initiated by the data subject, consent to the processing of the required data has to be presumed, but the data subject has to be informed about this in advance. Consent can also be given in written form as part of the contract concluded with the data controller – so as to ensure fulfilment of the contract. In this case, the contract has to contain all information needed by the data subject in relation to the processing of personal data, most notably the clear determination of the data to be processed, the time and purpose of processing and transferring data and the use of entities other than the data controller for technical management of the data. The contract must contain the data subject's clear consent to the processing of his personal data as described in the contract by means of his signature.[54]

In many situations the voluntary nature of consent can be questioned due to the existentially dependent position of the employee, or the information and economic power imbalance in favour of the employer. It can be assumed that, during the recruitment process, consent is often voluntary, but the excess of labour on the job market is one form of defencelessness, and this makes it likely not to be the case.[55] On the other hand – and this becomes relevant when monitoring employees – inverted defencelessness is also becoming more common in that various employers' data are not secure due to the use of modern technology, and employees can cause considerable damage to the employer by disclosing confidential information to unauthorised persons. This situation has special importance in relation to the monitoring of employees. "The defencelessness of the employer is increasing in the information age with new, highly significant factors. Employers experience the 'enemy attacking from within' and the fear is justified under the circumstances of wide-scale access to information technology."[56]

In the domain of labour law the questions of the legitimacy of data processing before and during employment is distinguished in legal literature.

The voluntary nature of the data subject's consent before the establishment of an employment relationship is generally accepted in the literature. The legal basis of data processing in these cases is the consent of the data subject, which can be expressed in writing, orally or as a clear, conclusive act. In cases of presumed consent, when the data subject initiated the proceedings, the rules of the Data Protection Law relating to 'proceedings' need to be understood broadly

[54] DPA § 3(6), (7)
[55] This is the general view in the literature, ld. Arany Tóth, 2004b, pp. 15-17., Majtényi, 2006, p. 332., Hartai, 2003, p. 46., etc.
[56] Majtényi, 2006, p. 333.

and according to the interpretation of the DPA. This (which is the predominant interpretation still) is far from unambiguous[57] and so the term 'proceedings' means not only formal legal proceedings, but any type of transaction initiated by the data subject. Accordingly, in our opinion, these rules also apply to job applications.

By contrast, it is our firm opinion that the legitimate ground for data processing during employment cannot be the employee's consent. Although consent can be given as part of the employment contract, it is unlikely that employment contracts can cover all aspects of data processing and provide all necessary information. Moreover during an employment relationship a need for further data processing may arise which could not have been foreseen by the parties at the time when the employment contract was concluded. Therefore, it is unlikely in respect of long-term employment relationships that the employment contract in itself can provide sufficient legal grounds for data processing.

However, there may be exceptions where consent may prove to be a firm basis for data processing during employment relationships, but the validity of consent will always be subject to debate in cases of controversy, and this factor should always be carefully evaluated.

The legal basis of data processing can be the legitimate interest of the controller or of the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for the fundamental rights and freedoms of the data subject" according to Article 7 point f) of the EU Data Protection Directive. This rule requires the balancing of the interests of the data controller and the data subject and provides the legal basis for data processing in cases where the interests of the data controller outweigh those of the subject.

The previous Data Protection Act did not contain this general rule of authorisation, but the new one does, although with a different wording and meaning.[58] It states that the data controller can process the data without the consent of the data subject – and also in case of the withdrawal of consent, for the purpose of

- fulfilling its legal duties, or
- enforcing the lawful interests of the data controller or third parties, if the enforcement of these interests is proportionate to the restriction of the data subject's right to protection of personal data;

if the data subject originally agreed to the recording of the data. This wording raises the possibility of different interpretations. First of all, it is unclear whether the balancing of interests of data controller and data subject is allowed only in cases when the data subject originally consented to the recording of the data or whether it is allowed in other cases as well. It is also unclear whether third parties can process the data based on this rule or whether only the original data controller has this right. In our view these rules provide the possibility for balancing the interest of subject and controller if the data were processed by the data controller on the basis of the consent of the data subject. However, the wording also gives

[57] Jóri, 2005, pp. 187-188.
[58] New DPA § 6(5)

room for the possible interpretation that third parties may process the data on the basis of the balancing of interests without the consent of the data subject.

Similarly to the Directive, the Hungarian regulation requires the balancing of interests, which provides room for manoeuvre, but also places a great responsibility on the data controller.

These rules also provide for the possibility of processing the data without time limitation. They may also provide the basis for the processing of data without an explicit and legitimate purpose if the data subject once consented to the recording of the data. Thus these rules provide exemption from the finality principle. The risk is that it may allow the collection of data for a certain purpose at the time of recording and the further processing of this data at a later time for another purpose. The future will show how this rule will be interpreted in practice, but it seems to us that one consequence of this new rule is that the level of protection is much lower than under the previous Data Protection Law.

Although the previous DPL did not provide the explicit possibility for the balancing of interests, some scholars, such as MARIANN ARANY TÓTH, argued that there did exist such a possibility in respect of employment relationships,[59] although this could not have served as a legal ground on the basis of the legal regulation. In practice, however, there had been room for balancing interests on the basis of certain rules of the Labour Code and the data processing purposes listed.

The new Data Protection Law seemingly provides the possibility for employers to process data which they collected with the consent of the employee, for any kinds of purpose. However, it does not allow them to process those data which they collected without the consent of the data subject. For example, authorisation in an employment contract does not provide sufficient ground for the processing of computer usage data or accessing and reading emails if the authorisation in the contract of employment did not refer to this.

A different approach – seemingly independent on the question of legitimacy – was suggested by LÁSZLÓ MAJTÉNYI. He argues that the right to the protection of privacy also has to be enforced at the workplace, but the necessary rational condition for this protection (although it is hard to support this with the wording of the regulation) is that the activity to be protected is private in nature and not related to the activity of the company, […] privacy protection in the workplace must relate to the private life of the employee and not to obvious, direct work activities. (With an absurdly wide interpretation it would be possible to conclude that the product manufactured by the worker is also his or her personal data.)"[60]

MAJTÉNYI's argument suggests that it would be useful to restrict the scope of personal data protection, and, maybe, the definition of personal data, in the context of employment to activities of a private nature – although the author acknowledges that it is difficult to deduce such an interpretation from the existing rules. Despite the potential difficulties in such an approach, it would seem a good solution to create sectoral data protection rules in relation to employment on the principle of separating private and job-related activities.

[59] Arany Tóth, 2004b, pp. 18-19., Arany Tóth, 2008b
[60] Majtényi 2006, p. 336.

We would also assert that, to maintain total clarity in Data Protection Law, the different rules of the Labour Code can provide the most suitable legal basis for processing personal data by the employer. We agree with the approach of ANDRÁS JÓRI, who claims, that those legal rules which empower or oblige legal subjects to act in certain ways and which implicitly require the processing of personal data, can be interpreted as also providing legitimate grounds for the processing of personal data.[61] Many Labour Code provisions are certainly such rules, and this interpretation may provide an adequate basis for personal data processing. This approach does not always lead to clear solutions, however, since many of these types of rule are very general by nature, and so interpretation is nearly always required.

It seems, that the new Labour Code make these debates outdated, since the § 11 of the new Law may be the legal ground for the monitoring of employees. So the questions regarding the legal base seems to be answered once the new Labour Code comes into effect on 1st July 2012.

1.3.3.4. Other rules of data processing

1.3.3.4.1. The purpose of data processing

According to the Data Protection Act, personal data may be processed only for specified and explicit purposes, where it is necessary for carrying out certain rights or obligations. This purpose must be satisfied at all stages of the operation of data processing and data processing. The personal data processed must be essential for the purpose for which it was collected, it must be suitable to achieve that purpose, and it may be processed to the extent and for the length of time necessary to achieve that purpose. Personal data must be erased if the purpose of processing no longer exists or the legal time limit for storage has expired.[62]

The criteria for a legal purpose apply to public personal data also, and so published personal data can only legally be processed for a purpose other than that for which it was originally published if there is a new legal basis for this.[63]

The (old) Data Protection Act listed some potential purposes of data processing. Personal data could be processed for the performance of a task carried out in the public interest or in the exercise of official authority, in the fulfilment of the official tasks of the controller or of a recipient third party, for the protection of the data subject's vital interest, for the performance of a contract between the data subject and the controller, in the legitimate interests of the controller or a third party, or in the legitimate operation of a charitable organisation.[64] Some of these purposes are also mentioned in the Data Protection Directive, but as a legal basis for data processing.

[61] Jóri, 2005, pp. 164-165.
[62] DPA § 5(1), (2), § 14(2) d); New DPA § 4(1)-(2)
[63] Cf. DPC, 1472/A/2003. and Gálik/Polyák, 2005, p. 221.
[64] DPA § 5(4)

1.3.3.4.2. Data quality and requirements for data security

The Act on Data Protection directs, in respect of the requirements relating to the quality of data collected, that the conditions and their management must be fair and lawful. As a requirement of data quality, the law orders that personal data processing must be accurate, complete, and, where necessary, kept up to date.[65]

Data processing must be legal and fair, and the requirements of data protection can only be implemented if the technical and structural background of the data processing makes it possible. Therefore, the law demands that there should be total data security. According to law, the controller – and the processor working within the controller's area – must ensure the security of information, and also he must take those technical and structural actions and apply that adjective (procedural) law, necessary for the validation of the Data Protection Act and of other Acts of protection of data and secrets. Data must be protected against unauthorised access, alteration, transfer, disclosure, transmission or deletion as well as damage and accidental destruction.[66]

1.3.3.4.3. The rights of the data subject

The Act on Data Protection ensures special rights to data subjects for validating information-related self-determination.[67] The rights of the data subject can be summarised as follows:

The data subject should not only be informed at the time when data are collected about the important features of processing, but he can also request information during processing which the controller must give - in writing and within the shortest time, counting from the day when the request was handed in, but at most within 30 days. Recompense can be demanded if the person requesting the information had already handed in a similar request within the given year concerning the same matters.

The data subject can ask for the data to be corrected if his data are not correct. If incomplete or erroneous data cannot be corrected, then it must be deleted in the absence of any other order in the Act.

Aside from obligatory data processing, the data subject can ask for the deletion of his personal data at any time, and, with that, the cancellation of data processing. Data deletion means the elimination of data in so that it is irretrievable.[68] Data misappropriation is not a necessary condition of requesting data deletion. The Data Protection Commissioner confirmed in his comments reacting to the reasons appearing in the media that the controller has no right of decision in relation to this request.[69] On the right of deletion, the controller can request, apart from his own interest (not defined by Act) the deletion of information on the data subject, which may cause a problem in that the signing of a contract is not a legal basis in itself, and so

[65] DPA § 7(1), New DPA § 4(4)
[66] DPA § 10, New DPA § 7
[67] DPA §§ 11-17, New DPA §§ 14-18, § 21.
[68] DPA § 2. 12., New DPA § 3. 13.
[69] Gálik/Polyák, 2005, p. 223

the necessary data processing is based on the consent of the data subject. In theory, therefore, the abuse of the right of deletion may also be considered.[70]

The Act on Data Protection ensures the right of objection for the data subject. The objection is a declaration by the data subject that he refuses the processing of his information and asks for the processing to be cancelled and the information deleted. [71] The data subject can, in particular, use this right if, with the exception of obligatory data processing, the processing of the data subject is exclusively necessary for the validation or based on the validation of the rights of the controller, and if the processing of personal data and its transmission are aimed at an indirect matter, for a public questionnaire or for academic purposes. The controller must consider the objection within 15 days at most and inform the applicant in writing. If the objection is justified, then the controller must cancel data processing and block the information.[72] Personal data must not be deleted if the data processing was ordered by law, but, if the objection is upheld, the information cannot be transferred to other data processors.

1.3.4. The special role of the Data Protection Commissioner in case law

We have to mention the special role of the Data Protection Commissioner. The Commissioner had the competence to make recommendations in general, or to specific controllers. Since the recommendations of the commissioner often contain "rules", the cases of the Commissioner became real "law" [73] which is actually followed by employers.

This means that, in the field of privacy in the workplace, case law is based much more on the summary of the Commissioner's cases and recommendations than on the summary of court cases. Judicial case law in this field is not essential, simply due to the very small number of court cases, or, in some fields, a total lack of court cases.

We will show and analyse the supervision regime of data protection and the competences of the Data Protection Commissioner and of the new National Data Protection and Freedom of Information Authority, in detail in the third chapter.

1.4. Definitions of the area – basic background information regarding the issue of privacy in the workplace

1.4.1. Different regulation of the public and private sectors

Although in Hungary there are different laws concerning private and public bodies' data processing, the lack of specific regulation on the use and monitoring of technical equipment

[70] Jóri, 2005, p. 266
[71] DPA § 2. 12.; New DPA § 3. 13.
[72] The practice of the 'objection law' can offend the rights or fair interest of those who receive personal data through data transmission from the processor (recipient) Therefore, the Data Protection Act ensures that the recipient can turn to a jury to obtain the data. [DPA § 16/A(4)]
[73] Sólyom, 2001, pp. 89-90.

has the effect that the same rules and principles apply to both sectors. Neither case law nor academic papers differentiate.[74]

1.4.2. The employer' interest in monitoring the employee

Generally there is a legitimate interest on the employer's side to monitor the employee's work and there are many rules in the Labour Code which relate to this issue.

Although we must mention that the right to monitor is not expressly written in the Labour Code, it is widely accepted by labour law experts:[75] the right to supervise means the right to monitor the employee's conduct and activity in connection with the employment, to state facts, to assess the employee's performance and compare it with the performance expected. The employee has to accept and tolerate the exercising of this right.[76] Academic papers deduce this right from §102(3) a) and b) and §104 (1) of the Labour Code, which state the obligation on both employer and employee. §102(3) a) and b) state that employers shall organise work so as to allow the employees to exercise the rights and fulfil the obligations arising out of their employment and shall provide the employees with the information and guidance necessary for carrying out their work.'[77] §104(1) says that 'employees shall perform their work in accordance with the employer's instructions.'[78] GYÖRGY KISS says, that the right to monitor is strongly connected to the right to instruct, which is based on these provisions.[79] The employer also has the right to monitor the equipment which he provided for the employee.

1.4.3. The boundaries of monitoring

1.4.3.1. The line between legal monitoring and illegal surveillance

At this point, if we wished to summarise the aim of our research, we could say that we wished to draw a line between the legal monitoring of employees and illegal surveillance. As we have already said, the employer has a legitimate interest in monitoring an employee's work and to check whether a task has been completed or not, but the employer does not have the right to breach privacy by means of continuous (technical) monitoring. As we will see, the main problem is that it is hard to distinguish clearly between the official and private use of different technological equipment and between an employee's official and private conduct.

1.4.3.2. Data protection provisions in the Labour Code

1.4.3.2.1. The Labour Code of 1992

The Labour Code [§ 3(4)] says that employers shall be only permitted to disclose facts, data and opinions concerning an employee to third persons in the cases specified by law or with

[74] There is one important exception: the regulation of 'snail-mail'. We will discuss this issue in the chapter concerning the regulation of normal mail.
[75] Kiss, 2005, p. 180., Bankó/Berke/Kiss, 2004., p. 89, Arany Tóth, 2008a, p. 235.
[76] Bankó/Berke/Kiss, 2004, pp. 89-90.
[77] Labour Code § 102(3) a), b);
[78] Labour Code § 104(1);
[79] Kiss, 2005, p. 180.

the employee's consent.[80] Another provision regulates data processing during the hiring process: the Code prescribes that an employee shall only be required to make a statement, fill out a data sheet, or take an aptitude test if it does not violate his personal rights and if it essentially provides information considered substantive for the purposes of entering into an employment relationship.[81]

There is little to be said about these provisions in connection with the legality of surveillance.

We should mention, however, that the Labour Code contains some rules on the possible surveillance of employees in the field of teleworking. The Act says that the employer shall have the right to restrict the use of any computer and information technology hardware, and electronic equipment which it has provided to the person employed in teleworking. In justified cases the employer shall be entitled to monitor the completion of the work, but the employer shall not inspect any information stored on the computer or other information technology equipment which is not related to the rights and obligations arising from the employment relationship. As regards the employer's right of access, the data necessary for monitoring the restriction prescribed in the Act shall be considered to be related to obligations originating from the employment relationship.[82] Although we agree with the general principles laid down in these provisions, we have to bear in mind that these rules apply only to teleworking.

In total, there are not many data protection provisions in the Labour Code, which means that, in most cases, the general rules laid down in the Data Protection Act apply.

1.4.3.2.2. The Labour Code of 2012

The new Labour Code changes the former regulation on privacy protection in employment significantly only in one important field: regarding the possibility of employer's control/monitoring. The § 11. of the Code prescribes, that the employer may only control the employee's activity in connection with his employment. As a limitation, the Code also prescribes, that

- the means measures and methods of the control cannot breach the employees right to dignity, and
- the control/monitoring cannot affects the private life of the employees.[83]

The employer has to inform the employees about the technical measures that is used to control/monitor the employees activity (work).[84]

The new Labour Code does not contain any detailed rules in this field, so there is still no 'real' sectoral data protection regulation in this filed. Since the Labour Code of 1992 has not contain any provision on the possibility of monitoring, the new Labour Code has one strong

[80] Labour Code § 3(4);
[81] Labour Code § 77(1);
[82] Labour Code § 192/G(3), (6);
[83] New Labour Code § 11(1)
[84] New Labour Code § 11(2)

effect on data protection regulation: the data processing in connection with control or monitoring of the employee shall not be based on the 'voluntary' consent of the employee's any more,[85] but, in our view, it will be clearly a data processing based on the provisions of an Act, namely on the § 11 of the new Labour Code.

On one hand, as we show it in chapter 1.3.3.3.4, we think that the doctrine of consent-based data processing is a mistaken in the field of workplace privacy, therefore, at least from the aspect of the legal ground of data processing, the new Labour Code clarifies this question.

On the other hand the new Labour Code does not contain detailed provisions on the limitation of data processing. The lack of these guaranties is quite problematic. It may results, that the details shall be worked out by case law of the new Data Protection Authority (which will take time, of course) and by legal experts. Since the employer has to provide detailed information to the employee both on the technical measures[86] and on the details of the data processing concerning the control and monitoring,[87] the new Law may strengthen the tendencies towards adoption of internal norms. It seems to be worth, at least for bigger employers, to adopt Code of Conducts or by-laws to regulate and clarify the details of the employee's monitoring.

1.4.4. Mutual dependence

1.4.4.1. The dependent position of the employee: can his consent be regarded as voluntary consent?

As already mentioned in another chapter, one of the most important general problems is the voluntary nature of the consent to data processing. In many situations the voluntary nature can be questioned due to the existentially dependent position of the employee, or the information and economic power imbalance in favour of the employer. It can be assumed that, during recruitment procedures, consent is more often voluntary, but the excess of labour on the job market is a form of defencelessness which makes that unlikely to be so.[88]

1.4.4.2. The 'dependent' employer: can the employer prevent an employee from stealing valuable data without strong monitoring?

On the other hand – and this becomes relevant when monitoring employees – 'inverted defencelessness' is also becoming more common: various employers' data are not safe as a result of the use of modern technologies and employees can cause considerable damage to the employer by disclosing confidential information to unauthorised persons. This has special importance in relation to the monitoring of employees. 'The defencelessness of the employers is increasing in the information age with novel and significant factors. Employers are

[85] After 1st July, 2012, when the Code comes into effect.
[86] New Labour Code, § 11(2)
[87] New Data Protection Act § 20
[88] This is the general view in the literature. Cf. Arany Tóth, 2004b, pp. 15-17., Majtényi, 2006, p. 332., Hartai, 2003, p. 46., etc.

experiencing ‘the enemy attacking from within’, and the fear of this is justified under the circumstances of the widespread possession of information technology.”[89]

[89] Majtényi, 2006, p. 333.

2. THE LEGAL REGULATION CONCERNING SURVEILLANCE IN THE WORKPLACE

We have to mention, that the summary of the regulation and case law of the different surveillance technologies is based on the actual legal framework, and the new Labour Code may change many statements of this chapter. One of the most important changes concerns the legal base of the monitoring of employee's activity. As it will be clear from this chapter the Data Protection Commissioner's case law is based so far on the 'consent-doctrine': any monitoring shall based on the employees consent. This 'starting point' will be changed once the New Labour Code comes into effect on 1st July 2012. The other statements of the Data Protection Commissioners mostly worked out the conditions of a fair control by the employers. These conditions may be still valid under the new regulation framework too.

2.1. The regulation of 'snail-mail'

The content of the mail, and the circumstances of writing, sending and receiving it (the name of the sender and recipient, the date of sending, of receiving, the place of posting) are personal data according to the Data Protection Act, and so the monitoring of traditional mail ('snail-mail') may raise privacy issues. We should also mention that mail which is sent from or received at a workplace is not only connected to the employee but also to a third party, who probably has no legal relationship with the employer. Another problematic issue is to distinguish in practice between official and private mail: the first may be subject to the employer's monitoring and the latter not.

2.1.1. Legislation

The possible monitoring of mail is also limited by civil law rules and criminal law provisions. According to the Civil Code, any person who has violated the integrity of the mails or has come into the possession of a private or business secret and publishes such secret without authorisation or abuses it in any other manner shall be construed as having violated an inherent right.[90] Once the content of a (closed) mail is known without consent, the inherent right is breached, even if the content was not misused. This protection also covers electronic mail.[91]

The Criminal Code also contains provisions on this issue. The crime of "violation of the privacy of correspondence" is committed by any person who opens or obtains a sealed package containing a communication which belongs to another person for the purpose of gaining knowledge of the contents, or conveys such to an unauthorised person for this purpose, as well as by any person who 'taps' or 'hacks' into correspondence forwarded through telecommunications equipment.[92] Telecommunications equipment is equipment

[90] Civil Code § 81(1)
[91] Gálik/Polyák, 2005, p. 212
[92] Criminal Code § 178

which enables the transmission of electronic signals. Tapping or hacking mean any activity which is intended to illegally access the content of the correspondence.[93] The Criminal Code prescribes stricter sanctions if the crime is committed in a professional or official capacity or is the source of serious loss.[94]

There is a special regulation in this field for public bodies. Government Decree 335/2005. (XII. 29.) on the General Requirements of Document Management Systems in Public Sector Bodies with reference to the opening and registration of consignments sent by post declares that the consignment can be opened

- by the addressee or
- by a person licensed in writing by the head of the central documentation system or
- by an employee of the unit designated for this task in the statute of the body or
- by the electronic mail processing system designated in the Code on the documentation management of the body.

The consignment shall be registered and delivered to the addressee without opening if

- marked as 'private and confidential',
- this was ordered by an authorised person.

In the case of a) and b) the addressee should register the delivered consignment as stipulated in the Code of the documentation management of the body. Before its amendment, the Decree also designated the addressee as the exclusively authorised person for opening the letter if the letter was addressed to a personal name and was obviously private. The amended Decree authorises the employer to make a local regulation on processing letters addressed to an employee. This mode of regulation may infringe certain constitutional principles, but, nevertheless, the case law of the Commissioner should influence local codification.

2.1.2. Case law of the Data Protection Commissioner

The case law of the Commissioner follows a restricted interpretation in respect of differentiation between private and official letters. Accordingly, 'insofar as a presumably private letter is delivered to an office, the addressee is supposed to open it for the sake of legal guarantees. As soon as the letter is opened it can be decided whether it is official or private and, consequently, whether it should be registered or not." Another resolution of the Commissioner confirms this interpretation. 'The letter addressed to an employee shall not be opened by officials of the employer unless the official character and content of communication can be clearly proven on the basis of the address or other indication.' According to the consistent opinion of the Commissioner, the official character of the letter should be proved, and, in case of uncertainty, the private character shall be presumed. If the official of the employer casually opens a private message, the letter must be resealed and the addressee informed of who had opened the letter and when.

[93] Gálik/Polyák, 2005, pp. 213-213
[94] Criminal Code § 178(2),(3)

The Commissioner also stated that the employer has full legal right to monitor the letters sent from the office as the letter was written during office hours and using the employer's tools.[95]

2.1.3. Judicial case law

There is no judicial case law in this specific field.

2.1.4. Academic papers, scientific opinions

Referring to the case law of the Commissioner BULCSÚ HEGEDŰS remarks that the prohibition of private correspondence does not support the opening of private letters by the employer since the sender of the letter is not expected to know and respect this restriction.[96]

2.1.5. Self-regulation

No sources were found in this field.

2.2. Regulations regarding the monitoring of e-mail

Writing an e-mail at a workplace is usually a part of normal workflow, and the form and content of an official communication is an important element of the function. However, email is also personal data – regardless of the private or official character of the communication - and it is not only personal data in respect of the employee, but also of the receiver or sender who is outside the employer's organisation, and for whom the application of the employer's regulation is at least questionable. Moreover, in practice, it is typical that the conditions of using electronic equipment and email for private purposes are unclear.

2.2.1. Legislation

There is no special regulation in this field, and so the general rules of the Civil Code, Data Protection Act and Labour Code are applicable.

2.2.2. Case law of the Data Protection Commissioner

The case law of the Data Protection Commissioner covers the issue of monitoring email, and although numerous recommendations were issued, their content was not totally consistent.

The case law of the Data Protection Commissioner distinguishes between emails sent and received. The commissioner says, generally, that the employer has greater rights to monitor e-mails sent by the employee since he has given consent to this by writing the email.[97]

Later this distinction was repeated, and the issue of consent was also re-emphasised: if the employee is informed of possible monitoring by the employer, then consent is given by the very act of writing the email.[98]

[95] DPC, 120/A/2004.
[96] Hegedűs, 2006a, p. 48.
[97] DPC, 120/A/2004, DPC, 1543/A/2004
[98] DPC, 1722/A/2004

In another case, in 2006, the Commissioner stated that an employer may look into an official e-mail sent or received in accordance with the employee's duties, based on the employer's instructions. In this case the privacy rights of the third person have to be protected. The document does not refer to any necessity for the employee's consent.[99]

Later, the Commissioner strengthened the need for consent and stated that, in order to 'process [including monitor] e-mails, both the sender's and receiver's consent had to be obtained".[100] The statement is based on the assumption that there is no special legal provision for processing such data, and so the legal basis can only be consent. We should stress that, on one hand, the voluntary nature of the consent is questioned in an employment relation, and, on the other hand, once we accept that the consent is voluntary, consent would probably not be given by the employee if he had anything to hide and if monitoring might have serious consequences.

The recommendation also declares that the employer must inform all employees of the rules of monitoring, and then, once the employer writes an email, he must accept the possibility of monitoring. The commissioner does not expressly state this in this recommendation, but alludes to the fact that consent is regarded as having been given in this case by the writing of the e-mail.

The very same recommendation also states that 'the employer has the right to ask the employee to print out the sent or received official e-mails. […] If the e-mail address is allowed for use solely for official purposes, the employer also has the right to monitor the heading of the e-mails […] and ask for a specific e-mail to look into'.[101] The employee can only refuse to show this email if it breaches a third party's privacy rights, but, if the employee still refuses to show the e-mail written by him referring to the third party's right of privacy, the employer may impose labour law sanctions – states the recommendation.

In our opinion, for monitoring and examining an official email written by the employee no consent is needed; it is based on the labour law rules on the right to monitor and so derives from the employment relationship of the parties. Once the monitoring of email is based on the employee's consent, this consent can be withdrawn without sanction – although in practice this would not work.

2.2.3. Judicial case law

There is no judicial case law in the specific field of monitoring e-mails in the workplace.

2.2.4. Academic papers, scientific opinion

Firstly, the relevant academic sources point out that the e-mail is also a subject of the protection of correspondence, similarly to the traditional mail,[102] and also a subject of the data

[99] DPC, 1393/K/2006
[100] DPC, 40/K/2006
[101] DPC, 40/K/2006
[102] Gálik/Polyák, 2005, p. 212., Arany Tóth, 2008, p. 267, Hegedűs, 2006a, p. 47.

protection regime if the e-mail address and/or the content can be attached to a natural person – as, in practice, it normally can.

Secondly, the relevant legal literature also emphasises that the content of the e-mail belongs to two parties and so is the personal data of both sender and receiver, one of whom may be a person outside the workplace. Hence the required legal basis for processing such personal data may be the consent of both parties.[103] We should add that, in practice, it would not be easy to obtain the third party's consent, which would need to be based on proper information provided about the data processing.

Thirdly, the official or private character of the email is also a key issue. Private emails cannot be monitored by the employer unless the employer and the third party give consent.[104] We think that, besides consent, a further requirement has also to be met: a legitimate reason to monitor private emails. In practice it is quite rare that the employer would have any legitimate interest and purpose in monitoring private email, except for one clear case: to separate the private from official e-mails in order to examine the latter. According to academic papers, the right to read the content of emails by the employer is still restricted even if it is an official e-mail address; it also has to be based on the consent of both the employer and the third party – consent is regarded as given if the employer knows of possible monitoring.[105]

Fourthly, academic papers also distinguish according to whether the e-mail was written by the employee or was received from a third party.[106] This distinction is based on the Data Protection Commissioner, and some authors agree,[107] whilst others do not: ARANY TÓTH expresses the view that e-mails should have been granted the same, or very similar, legal protection regardless of the parties.[108] Although we admit that the same principles apply to both categories of e-mail, we agree with the distinction since the legal basis is different in the case of e-mails written by the employee compared to those written by a third party. In practice, however, it is hard to realise this distinction.

Finally, MARIANN ARANY TÓTH mentions the issue of the traffic data of an email, and she suggests that, for processing these data, the principles of the Electronic Communications Act[109] should apply.[110] Although we agree that it is useful to use the provisions of the ECA, we should mention that an employer is not subject to the ECA even if he acts as a special 'service provider' of the Internet, e-mail, or as a host-provider. This is quite problematic, since the data processing attached directly to these services (e.g., traffic data) is not derived from the employment relationship, and so the legal basis of this data processing is at least questionable. Generally, the issue of the employer's legal position as a service provider is

[103] Arany Tóth, 2008, p. 268., Hegedűs, 2006a, p. 48.
[104] Arany Tóth, 2008, p. 271., Hegedűs, 2006a, pp. 48-49., Majtényi, 2006, pp. 345-346.
[105] Arany Tóth, 2008, pp. 269-270., Hegedűs, 2006a, pp. 48-49.
[106] In other words, whether is it internal correspondence or communication between the workplace and a third party.
[107] Hegedűs, 2006a, p. 48.
[108] Arany Tóth, 2008, p. 270
[109] Act C of 2003 on Electronic Communications
[110] Arany Tóth, 2008, pp. 272-273.

something of a black hole: neither the Data Protection Commissioner nor academic papers[111] deal with this issue at all.

By way of summary, it would seem that the issue of monitoring an employer's e-mails is quite contradictory both in respect of the Data Protection Commissioner and of academic papers, which are mostly based on the fact that the legal basis for such data processing are unclear.

2.2.5. Self-regulation

No sources were found in this field.

2.3. Regulation of computer-usage

The regular use of an electronic computer generates a great deal of personal data. A set of electronic personal data comprises – beyond the personal files stored on the hard disk of the computer – several technical records such as a list of installed computer programs or data related to the use of particular files and programs. Monitoring and supervision by the employer may cover all the tools, implements and equipment and their use – casually for the sake of protection of confidential knowledge and information. Beyond the determination of the personal character of certain data and the extent of monitoring rights, the mode of supervision also poses problems in the field of data protection regulation.

2.3.1. Legislation

There is no special regulation in this field, and so the general rules of the Civil Code, Data Protection Act and Labour Code are applicable.

2.3.2. Case law of the Data Protection Commissioner

Seeing that there is no substantive legal regulation on the monitoring of Internet and computer access we can only consider the Commissioner's case law. On this basis the employer is not authorised to monitor the use of the personal computer made available to the employee without the consent of the individual concerned.

Case law in this sector also affirms that program and data files installed and/or stored on the computer and made available to an employee may not be monitored or supervised by the employer unless the computer was rendered exclusively for the aim of work and the employer was prohibited from installing programs for his/her own initiative. Beyond information and consultation the consent of employee is also inevitable requirement. The notion of "monitoring" covers access to and inspection of records stored on the computer. The enumeration and listing of programs installed on a computer itself can be a processing of personal data and the result of this monitoring cannot be transferred or published without the informed consent of the concerned subject.[112]

If the employee gives the computer back to the employer, he should either delete the personal and confidential files or, otherwise, the consent of the data subject shall be considered granted

[111] Except the one mentioned by Arany Tóth
[112] DPC, 866/A/2006

as it was he/she who transferred or made accessible the data for another subject.[113] The principle of finality or purpose specification also should be taken into consideration. If the data controller found non-official or non-work-related data on the computer he/she should call the employee to remove them all. Monitoring itself can extend to the detection of forbidden and/or unlawful files – e.g., voice records, sound tracks and video records stored there. Beyond detection, however, the controller is not allowed to inspect the content of these files. Watching the video records or listening to the music files should be well outside the legal competence of monitoring.[114] The right to monitor does not entitle the employer to gain access to and knowledge of any private document stored on the computer used by the employee.[115]

The employer is prohibited from monitoring the use of the computer by spyware installed without the informed consent of the employee. As the Commissioner stated in 2005, this should be deemed that form of covert information-gathering operation which can be legally pursued only by leave of the court.[116] The Commissioner's statement also declared that there are pragmatic solutions for the monitoring of computer use, Internet browsing and workplace behaviour of employees which should respect the dignity and personal rights of the concerned subjects. Accordingly, the use of spyware constitutes disproportionate restriction.

A specific problem of monitoring computers has been revealed in a consultative case when an employee of a Hungarian affiliate of a German company turned to the Commissioner. The German parent company had ordered that the computers of employees should be fitted with a spyware program that enabled the central company management sitting in Germany to monitor literally all data: every file, record and transaction on the computers. This arrangement was objected to by employees and one of them asked the Commissioner about the legality of the company spyware. The Commissioner pointed out that, by this measure, the employer – in this case the head of the Hungarian affiliate – would become the data processor and the German parent company the data controller. Consequently, the rights of the employer would be transferred to the German company from the Hungarian subsidiary. This would infringe the rights of employees as Hungarian jurisdiction does not extend to Germany and has no influence on the decisions of the German parent company. This switching of responsibility for monitored data infringes the interests of Hungarian employees irrespective of the formal granting of their consent. It is important to stress that the Constitutional Court formulated the requirement of transparency in the context of data processing and declared that the concerned subject is qualified to assert his/her rights. In this case both requirements were infringed.[117]

2.3.3. Judicial case law

There is no judicial case law in this specific field.

[113] DPC, 772/A/2000, DPC, 841/K/2002
[114] DPC, 866/A/2006
[115] DPC, 531/A/2004
[116] DPC, 1012/K/2005
[117] DPC, 2511/K/2007

2.3.4. Academic papers, scientific opinions

After analysing the case law of the Commissioner, BULCSÚ HEGEDŰS added some comments:

- In the case of private files, not only inspection but also copying and erasure are unlawful. The employer is not allowed to remove these files unless he unsuccessfully called upon the employee to carry out the deletion.
- As far as possible, the monitor of the computer shall not be carried out manually but by automated means.[118]

2.3.5. Self-regulation

No sources were found in this field.

2.4. Regulation of Internet use and use of social networks

The use of the Internet is essential for many employees to do their job and the information gained through the Internet is very helpful in many workplaces. On the other hand, there is a rather high risk that employees use the Internet for private purposes in working hours, and so monitoring usage may be important for the employer, but may also breach the employee's privacy.[119]

We should add that the use of social networks such as Facebook may also raise data protection and labour law issues. A negative message sent on a social network may affect the loyalty of the employee or even damage the reputation of the employer. Besides this, the timing of a comment or any other activity may reveal the fact that the employee was using Facebook during working hours. Generally, this problem is not commonly met in Hungarian legal practice and legal literature – except in one new paper which focuses on the labour law issues of social networks.[120]

2.4.1. Legislation

There is no special regulation in this field, and so the general rules of the Civil Code, Data Protection Act and Labour Code are applicable.

2.4.2. Case law of the Data Protection Commissioner

There are some relevant cases of the Data Protection Commissioner which concern the monitoring of internet use by the employer.

[118] Hegedűs, 2006b, pp. 82-83.
[119] Arany Tóth, 2008b, p 170, Hegedűs, 2006b, p. 81.
[120] Horváth/Gelányi, 2011. The general privacy issues of social networks are discussed also in Hungary, of course (Cf. Polefkó, 2010) but workplace privacy issues are not.

Firstly, Data Protection has made it clear in several recommendations that the IP address and opened websites, the timing of a visit to a website etc. are personal data, since they can be attached to a natural person.[121]

The Commissioner also emphasises that monitoring Internet usage should be based on the employee's consent, consent which is based on accurate information.[122] Later, the Commissioner stresses the need for these conditions.[123] If private Internet use is forbidden and the employee was informed of the possibility of monitoring, then the employee's action in opening a website is regarded as consent to monitoring.[124] Monitoring internet usage is not allowed if the employer allows it to be used for private purposes. If it is only allowed to be used for official purposes, then monitoring usage is only legal if the employer gives information about this possibility to the employee. It is forbidden to monitor the visited website in secret.[125]

2.4.3. Judicial case law

There is no judicial case law concerning the privacy issues of monitoring Internet usage, but there was a notable case in which the court had to decide whether the private use of the computer and Internet may be legal grounds for the unusual termination of the contract of employment or not. In this case, the employee visited – among others – erotic websites on the Internet, using both his own and a colleague's computer. The Supreme Court says that this behaviour can be regarded as a serious breach of the contract of employment, since private use was forbidden, and so this activity was a legal ground for terminating the contract of employment.[126] We should, however, mention that the judgement did not refer to how the employer obtained the information about the websites visited, and whether collecting this information was lawful or not.[127]

2.4.4. Academic papers, scientific opinions

Academic papers firstly distinguish between the official and the private use of the Internet in the workplace. Generally it is the employers right to determine the conditions of Internet use: he may allow or prohibit it. The main problem is that, in practice, it is usually unclear and the employee may use the Internet for private purposes with the tacit consent of the employer.[128]

If the employee may use the Internet for private purposes, the employer cannot monitor the websites opened.[129] If Internet use is only allowed for official purposes, then the employer

[121] DPC, 693/K/1998, DPC, 750/A/2004, DPC, 1598/K/2004. We have to mention that it sometimes it is not possible to attach dates to a natural person, but both the Hungarian Data Protection Commissioner, and the general European approach to IP addresses are based on the assumption that normally they can be.
[122] DPC, 531/A/2004
[123] DPC, 800/K/2008
[124] DPC, 1767/K/2006
[125] DPC, 570/A/2001
[126] BH2006.64
[127] The employee admitted that he visited erotic websites – which is why the court did not need to deal with the circumstances of acquiring the information.
[128] Arany Tóth, 2008b, pp. 170-171.
[129] Arany Tóth, 2008b, p. 172.

may monitor usage, but only if the employer gives his consent, and only if the employee was informed about potential monitoring. Other data protection principles, such as proportionality, should also be borne in mind.[130]

Besides the content of the websites visited, the monitoring of other relevant traffic data may also be important (e.g., too much traffic may mean illegal downloading and copyright infringement). There are no general rules concerning traffic data. Although ARANY TÓTH refers to the applicability of the provisions of the Electronic Communications Act,[131] we still think that the employer is not a subject of this regulation.[132]

Academic papers generally suggest other methods of restricting the private use of the Internet such as filtering some websites by keywords, or only allowing certain (listed) web pages to open.[133] Although these are privacy-friendly methods, we think that, in practice, they are complicated and rarely work well. Another way may be 'Anonym filtering' with which a message can be sent to all employees to stop private use[134] – this can work in practice.

2.4.5. Self-regulation

No sources were found in this field.

2.5. Regulations concerning the use of voice telephony technology

It is usually necessary for the employer to be able to monitor the use of voice telephony (mobile or fixed) by employees, especially in cases where the cost of telephone usage is covered by the employer.

2.5.1. Legislation

There is no specific regulation concerning usage of the telephone by employees, although it is indirectly regulated by: a) the Civil Code; b) by the Law on Electronic Communications;[135] c) the Labour Code; d) the Law on Personal Data Protection.

The Civil Code gives protection to personal secrets, including the secrecy of communication, and it also provides protection against the voice recording of individuals as one element of general personal rights.[136]

Voice telephony services are regulated within electronic communications regulation, although there are no employment-specific rules. Service providers are obliged not to disclose traffic and location data without the consent of the user.[137]

[130] Hegedűs, 2006b, pp. 82-83.
[131] Arany Tóth, 2008b, p. 173.
[132] Cf. with the same opinion in chapter 2.2.4. on e-mail
[133] Arany Tóth, 2008b, p. 173, Hegedűs, 2006b, pp. 82-83, Jóri/Hegedűs/Kerekes, 2010, p. 288.
[134] Arany Tóth, 2008b, p. 173
[135] Act C of 2003 on Electronic Communications (hereinafter: Act on Electronic Communications)
[136] Civil Code, §§ 75-85.
[137] Law on Electronic Communications, § 156(14)

The Labour Code provides the possibility for employers to limit the use of equipment provided for work purposes - which includes the possibility of defining the conditions for telephone usage.[138]

Telephone usage always involves the processing of personal data and so the rules laid down in the Law on Personal Data Protection also apply to the use of telephones by employees.

2.5.2. Case law of the Data Protection Commissioner

The processing of the personal data of employees relating to the use of voice telephony technology is a recurring issue for the Commissioner, and his most important recent recommendations are:

- Monitoring telephone and internet use by employees;[139]
- Monitoring the use of the telephone in the workplace in respect of personal income tax regulations;[140]
- Recommendation on accessing data on telephone calls made by public servants;[141]

The approach of the Commissioner can be summarised by the following factors:

1. Employers have the right to monitor the telephone usage of employees, although they do not have the right to access call history or to request service providers to provide data concerning the numbers of called and received telephone calls and their duration, since data concerning telephone calls are also the personal data of the employee and of the other party to the individual calls.
2. The same rule applies to cases when personal income tax-related rules handle in different ways the expenditure on personal and official calls.
3. The Commissioner recommended sharing the cost of telephone usage between the employer and the employee at a pre-arranged rate, or by defining the maximal cost which an employer should pay, rather than by means of an item-by-item checking of all calls.
4. If an item-by-item review of official and private calls cannot be avoided, then the selection of private and official calls can only be done by the employee. In this case the employer shall be provided with the list of calls in a sealed envelope and the employee should mark the official calls, simultaneously making the numbers illegible.

2.5.3. Judicial case law

There is no judicial case law in this specific field.

2.5.4. Academic papers, scientific opinions

In the legal literature further summaries of the recommendations of the Commissioner can be found.[142]

[138] Labour Code, § 103(1)
[139] DPC, 1767/K/2006
[140] DPC, 1672/K/2006
[141] DPC, 3362/P/2009

ARANY-TÓTH suggests the creation of specific Rules of Electronic Surveillance (e.g.: 'phone, GSM, camera, internet usage etc.) of employees within the framework of regulations relating to the employment relationship. ARANY-TÓTH argues that there is a need for such a regulation, since the current rules of law on Data Protection do not provide sufficient guidance as to the situations in which the processing of the personal data of employees is possible, and since, in employment relationships, the consent of the employee as the basis for personal data processing is always questionable.[143]

2.5.5. Self-regulation

No sources were found in this field.

2.6. Regulation of CCTV use

The installation and large-scale use of CCTV systems is a very common phenomenon in several fields of daily life such as business activity, crime prevention, traffic monitoring, transport safety and public or private security. The hardware and software of these systems are increasingly intelligent and the proliferation of these systems poses a major threat to the privacy of the inhabitants of industrialised countries. CCTV cameras are often regarded as Big Brother's electronic eyes.

The regular use of CCTV systems generates a great deal of personal data. This can be used to produce a personality profile of the employee. Monitoring and supervision by the employer may cover all the tools, implements and equipment (and their use) for the sake of protecting confidential knowledge and information, but, beyond determining the personal nature of certain data and the extent of monitoring rights, the actual mode of supervision also poses awkward problems in the field of data protection regulation.

2.6.1. Legislation

There are no specific rules in the Labour Code on the installation and use of CCTV systems in the workplace,[144] and so we can only refer to the general rules and try to draw rational conclusions for particular cases. The basic principles of data protection are interpreted by Data Protection Commissioners.

2.6.2. Case law of the Data Protection Commissioner

The crucial point of debate on the legitimate use of CCTV systems is the aim of surveillance. In business life and in the working world, the main purposes are the protection of property and the monitoring of employees. A further critical point, however, is the fate of video images. In real time systems, technical or security staff follow the images produced by the cameras, but nowadays this is relatively rare. Current CCTV systems are equipped with a mass storage device and video records are stored for a shorter or longer period. This mode of use implies a major threat to privacy.

---

[142] Cf. Székely/Szabó, 2005 pp. 129-130; Hartai, 2003 p. 48; Hajdú, 2005 pp. 172-173.
[143] Arany Tóth, 2008a pp. 305-306.
[144] Arany Tóth, 2008. p. 277.

Video surveillance in the workplace is admissible only for legitimate purposes and no departure from this rule is lawful. The Commissioner stresses that the current practice of unlimited recording and storing of video images does not comply with the Act on Data Protection. Employees should be informed of the installation of any such system and its purpose must also be declared. The Commissioner stressed that the information must also reveal whether or not the video images are recorded and stored. The employee is also authorised to see and examine any records made of him/her.[145]

Surveillance and video recording is legitimate if the employee has been informed and has consented. This also refers to the processing of personal data connected to this activity.[146] Consequently the operation of a hidden camera is a serious and extreme infringement of Employee Privacy.[147]

2.6.3. Judicial case law (Employment Tribunals)

In the Official List of Court Decisions we find total of 8 cases since 2007 in which the use of a CCTV system in the workplace had any relevance. These cases were disputes concerned with unfair dismissal and employment discrimination.

To date no employee has filed a suit against an employer because of the installation and use of such a system in the office, workshop or in any other place of work. Consequently we have no explicit court decision on the conditions of the legitimate use of video surveillance.

A common feature of these cases was that the video record was not a matter of dispute but merely a piece of evidence; both the court and the parties involved invariably accepted the record as proof.[148]

2.6.4. Academic papers, scientific opinions

In the legal literature mainly summaries of the practice of the Data Protection Commissioner can be found, with some further explanations of his recommendations and positions concerning the camera surveillance. MAJTÉNYI identifies monitoring with the use of CCTV systems as the core problem of privacy protection in the place of work. He draws attention to the fact, that camera surveillance in these places can only be justified if the extent of invasion to privacy is proportional with the rights to be protected by applying the monitoring system, and data subject were properly informed about all the circumstances of the surveillance.[149] On the accurate consideration of interests of parties concerned CCTV monitoring ARANY TÓTH argues that the duration of operating cameras, the time of the day when the system is used, and in some cases also the number of the data subjects observed have to be taken into consideration, as these details can reasonably affect the legitimacy of the surveillance. She

[145] DPC, 461/A/1998
[146] DPC, 475/H/2000
[147] Arany Tóth, 2008, p. 289.
[148] The list of the relevant cases: Fővárosi Munkaügyi Bíróság, 5.M. 394/2007/12.; Veszprémi Munkaügyi Bíróság, 2.M.341./2006./8.; Miskolci Munkaügyi Bíróság, 8.M.1286/2005/19.; Fővárosi Munkaügyi Bíróság, 31.M.3189/2002/55.; Pécsi Munkaügyi Bíróság, 3.M.1763/2005/15.; Nyíregyházi Munkaügyi Bíróság, 1.M.687/2005/12.
[149] Majtényi, 2006, pp. 347-348.

highlights that the individualized observation of a given employee, as well as monitoring with the use of hidden cameras are unlawful acts.[150] In her point of view the data subjects have to be informed in details about the monitoring, which includes also the role of the recordings in connection to the decision-making process of the employer, and the possible legal remedies. She points out the interest groups of the employees should have more important roles and functions concerning the operating of CCTV systems.[151]

HEGEDŰS shows that setting up camera surveillance, in some cases even independently from their legality, is a common practice in workplaces, as these can be operated easily, and their price is affordable. CCTV systems are frequently used not just for security reasons, but for labour inspections, despite that none of the interests of the employer could serve as a lawful reason for it, coming from the fact that continuous surveillance of the subjects could lead to the distortion of the personality.[152] On the effect of the camera surveillance of the citizens, it has to be stated, that notwithstanding the numerous research projects and publications on the topic, no clear tendencies can be driven up describing the personal outcomes of the subjects after constant monitoring with CCTV.[153]

2.6.5. Self-regulation

One collective agreement of the Budapest Transport Company mentions the importance of complying with data protection regulation: Point 3 of the 2nd Annex to the collective agreement of the company has the title 'Description of the regulation regarding monitoring f drivers'. Point 3.1. describes the general guidelines which have to be followed during monitoring. This is contained in the following general and short text: 'During monitoring conducted by camera and video camera, it is necessary to pay special attention to the protection of personal data and the regulation of the Act on the Protection of Personal Rights. Recordings can be used only for documenting the monitoring of the worker and with due consideration to the Protection of Personal Data in materials aiming to prevent accidents."

2.7. Regulation of RFID usage

Radio-frequency identification (RFID) is a technology that uses radio waves to transfer data from an electronic tag, called an RFID tag or label, attached to an object, through a reader for the purpose of identifying and tracking the object.

The use of RFID technology has engendered considerable controversy and criticism by privacy advocates. The two main privacy concerns regarding RFID are:

- Since the owner of an item will not necessarily be aware of the presence of an RFID tag and the tag can be read at a distance without the knowledge of the individual, it is possible to gather sensitive data about an individual without his consent.

[150] Arany Tóth, 2008, pp. 287-289.
[151] Arany Tóth, 2008, pp. 294., 311.
[152] Jóri/Hegedűs/Kerekes, 2010, p. 286. Cf. also 35/2002. (VII.19.) AB decision.
[153] Szőke, 2011, p. 204.

- If a tagged item is paid for by credit card or in conjunction with use of a loyalty card then it would be possible to indirectly deduce the identity of the purchaser by reading the globally unique ID of that item (contained in the RFID tag). This is only true if the person undertaking the watching also had access to the loyalty card data and the credit card data, and the person with the equipment knows where you are going to be.

The European Commission released a recommendation on May 12th 2009 on the principles of guarantees of privacy in the field of radio frequency identification.[154] The recommendation prescribes that member states should ensure that RFID operators carry out a comprehensive privacy test before the installation of these systems. The RFID operators are obliged to make and release a report on the results of the test to the competent authorities.

2.7.1. Legislation

In Hungary there are only two legal documents which relate to RFID technology. Both Government Decree 346/2004. (XII. 22) on the National Allocation of Radio Frequencies and Decree No. 35/2004. (XII. 28.) IHM of the Minister of Information and Communication Technologies on the Use of Radio Frequencies refers to RFID only in a technological context and makes no reference to privacy regulations concerning the technology.

2.7.2. Case law of the Data Protection Commissioner

The present case law of the Data Protection Commissioner does not cover the use or misuse of RFID technology.

2.7.3. Judicial case law

There is no relevant judicial case law.

2.7.4. Academic papers, scientific opinions

There is no relevant academic papers.

2.7.5. Self-regulation

No sources were found in this field.

2.8. Regulation of biometric identification devices

Biometrics involves techniques used to identify individuals based on a particular trait or physical characteristic unique to that individual. Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- Universality: each person should have the characteristic;
- Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;
- Permanence: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;

[154] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 2011, p. 3.

- Collectability: the characteristic can be measured quantitatively.[155]

A biometric system is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. These systems acquire and use biometric information in four steps:

- a physical characteristic is scanned,
- the characteristic is converted into digital code,
- the code is stored in a database, and
- the database and digital code are accessed to identify the individual at a later time.

Biometrics systems can operate in two modes: a verification mode or an identification mode.

In verification mode, the biometric system validates a person's identity by comparing the person's biometric data with the stored biometric data previously collected and stored in the system database. Common non-biometric verification mode systems include the use of a PIN number, a user name, or a password. For example, when a person enters a password to log on to his or her computer, the computer conducts a one-to-one comparison to determine whether the claimed user is the correct person. The verification mode is usually used for positive recognition, where the goal is to prevent multiple people from using the same identity.[156]

A biometric system that functions in identification mode recognizes a person by searching all the users in the database for a match. In this case, the system conducts a one-to-many comparison to establish a person's identity. The identification mode is generally used for negative recognition, where the goal is to prevent a person from using multiple identities. Unlike systems that function in verification mode, which can use non-biometric data to meet its goals, negative recognition can only be established through systems that use biometric data.[157]

2.8.1. Legislation

The basic regulation on processing of biometric data is the act XLVII. of 2009. on crime registration, and on national registration of sentences passed by courts of EU member states against Hungarian citizens and on registration of criminal and policy biometric data.

Other regulations of the Hungarian legal system refer to this Act and do not lay down any further rules. There is no particular regulation on collecting and processing biometric data in the field of work.

2.8.2. Case law of the Data Protection Commissioner

During recent years the Commissioner has had very few cases on processing biometric data and these mostly refer to Criminal Records, which is not relevant in the scope of our project.

[155] McGuire, 2000, pp. 441, 444.
[156] Jain/Prabhakar/Ross, 2004
[157] Betzel, 2005, p. 520.

On the subject of biometric data, the Commissioner generally affirms the principle of minimal amount of data. He stresses that, out of several equivalent processing methods, what should be chosen is that which involves less infringement or the restriction of self-determination and which results in less personal data collected.[158]

In another case the Commissioner also stressed that appropriate information should always be given to the data subject about the processing of biometric data. According to the Commissioner, the processing of such data can be accepted only under limited special conditions.[159]

2.8.3. Judicial case law

There is no relevant judicial case law.

2.8.4. Academic papers, scientific opinions

No significant academic essays on this matter.

2.8.5. Self-regulation

No sources were found in this field.

2.9. Regulations for using GPS and GSM technology for tracking the location of employees

GPS and GSM technology can be used for tracking the movement of employees, and the most common data protection problems relate to the use of GPS devices installed in cars or other vehicles driven by employees. More recently, the mobile ‘‘phones of employees equipped with GPS devices and the related applications have also raised personal data protection issues. Mobile ‘phone use-related location data processing by the employers also raised similar problems as the use of GPS devices.

2.9.1. Legislation

There is no specifically GPS or GSM technology-related regulation in Hungary. However, the use of location data that can be collected through the use of mobile ‘phone services falls within the scope of electronic communications-related data protection regulation. Section 156 subsection (13) and (14) of the Law on Electronic Communications states that electronic communication service providers (including mobile telephone service providers) can process location data only with the -permission of the subscriber (or user) and only for the purpose of the provision of value-added services.

[158] DPC, 1454/K/2010
[159] DPC, 926/H/2010

2.9.2. Case law of the Data Protection Commissioner

The tracking of employees with the help of GPS or GSM technology (or with the combination of both) is a recurring issue in the Commissioner's practice, and the most important recent recommendations of the Commissioner are:

- Determining the geographical position of employees with the help of GPS;[160]
- Determining the geographical position of employees with the help of GPS;[161]
- Determining a geographical position with the help of SIM-card cell information in respect of employees;[162]
- Recommendation on the use of a position determination system in employees' mobile 'phones;[163]
- Recommendation on monitoring the location of employees on the basis of mobile telephone cell information;[164]
- Recommendation on the use of a GPS-based position-tracking system in employees' vehicles;[165]
- Recommendation on a GPS system installed in the mobile 'phones of employees;[166]
- Recommendation on the GPS system introduced by a multi-national company;[167]
- Personal data protection conditions relating to personnel-tracking systems.[168]

The approach of the Commissioner can be summarised in the following factors:

1. The location of a person is his or her personal data and that of a vehicle is the personal data of the person using it.
2. If an employer installs location-tracking systems in vehicles or mobile 'phones used by employees, then the employer is considered to be a data processor.
3. Processing the location data of employers is not authorised by law. It is a misunderstanding for Section 103 subsection (1) point a) of the Labour Code to be regarded as providing a suitable legal basis for processing such data.[169] Hence, only the consent of the data subject can provide a suitable basis for data processing.
4. Only the location of those employees whose work makes location-tracking necessary (and where there are no other means available to monitor the proper performance of the employee) can be tracked by such systems.
5. Location tracking can only be used during working hours. The Commissioner has recommended on several occasions that it should be possible for the employee to switch off any location-tracking system installed.

[160] DPC, 559/A/2006
[161] DPC, 1664/A/2006
[162] DPC, 920/K/2006
[163] DPC, 663/P/2009
[164] DPC, 1092/P/2009
[165] DPC, 415/K/2009
[166] DPC, 636/K/2009
[167] DPC, 857/K/2009
[168] DPC, 922/2/2010
[169] This section of the Labor Code states that the employee shall appear at the place and time specified and spend the working hours performing work.

2.9.3. Judicial case law

There is no judicial case law in this specific field.

2.9.4. Academic papers, scientific opinions

In the legal literature further summaries of the recommendations of the Commissioner can be found.[170]

2.9.5. Self-regulation

No sources were found in this field.

[170] Székely/Szabó, 2004, p. 130. Jóri/Hegedűs/Kerekes, 2010, pp. 289-290.

3. SUPERVISION REGIME AND SANCTIONS IN THE FIELD OF PRIVACY AT WORKPLACES

3.1. Sanctions according to Data Protection Law

3.1.1. Court action

According to the Act on Data Protection, data subjects may file a court action against the controller for any violation of their rights for information, correction or deletion. The court shall hear such cases immediately, and the burden of proof of compliance with the law lies with the data controller and data processor. This rule concerning the burden of proof clearly gives an advantage to the data subject: if the data controller cannot prove that the data processing and data processing were lawful, he will lose the case. When the decision is in favour of the plaintiff, the court shall order the controller to provide the information, to correct or delete the data in question, to honour the data subject's objection.[171]

If the data processing causes any damage to the data subject as a result of unlawful processing or by breaching the technical requirements of data protection, the data controller shall be liable. The data controller shall also be liable for any damage caused by a data processor acting on his behalf. The data controller may be exempted from liability if he proves that the damage was caused by reasons beyond his monitor.[172]

3.1.2. The Data Protection Commissioner and the National Data Protection and Freedom of Information Authority

3.1.2.1. The Data Protection Commissioner

The previous Data Protection Act established the institution of Data Protection Commissioner. The provisions of the Act on the Ombudsman for Civil Rights also applied to the Data Protection Commissioner, with the exceptions set out in the Data Protection Act. Generally the Data Protection Commissioner had greater powers than, in general, an ombudsman – mostly owing to the provisions of the European Data Protection Directive.

The Data Protection Commissioner was elected by Parliament for six years, and the first Commissioner took office in 1995.

In the case of any violation of the rights of a person in connection with his personal data this was to be reported to the Data Protection Commissioner unless a court action is already pending concerning the case in question. The Data Protection Commissioner had the competence, upon request or ex officio to oversee compliance with the regulations of the Data Protection Act and other legislation related to data protection. He investigated the reports he received, and made recommendations either in general, or to specific controllers.[173]

[171] DPA § 17, new DPA § 22
[172] DPA § 18, new DPA § 23
[173] DPA §§ 24, 27(1)

Publicity was also an important tool for e Data Protection Commissioner. He had the competence to announce to the public the opening of proceedings, and any illegitimate data processing.[174]

If any unlawful data processing operation is detected, the Commissioner could advise the data controller (processor) to cease such operation. In this case the data controller (processor) had to comply within 30 days and report it to the Data Protection Commissioner. If the controller or processor failed to comply and cease the specified unlawful processing of personal data, the Data Protection Commissioner had the competence to order, by resolution, that unlawfully processed data be deleted, or he could prohibit the unauthorised data processing operations and suspend any operation aimed at transferring data abroad. The data controller (processor) could turn to the court within 30 days following the date of receipt of the resolution.[175] Owing to these competences the Data Protection Commissioner has acted since 2003 also as an authority and not only as a traditional ombudsman. The changes have been subject to some criticism in the legal literature, mostly due to a lack of rules concerning the execution and realisation of the resolution.[176] The Data Protection Commissioner did not have the right to impose a fine if illegal data processing is detected.

3.1.2.1. National Data Protection and Freedom of Information Authority

As mentioned earlier, the new Data Protection Act significantly changes the supervision regime of Data Protection (and Freedom of Information). The Act establishes a brand new authority: the National Data Protection and Freedom of Information Authority (NDPFIA) responsible for Data Protection and Freedom of Information. This new authority replaces the current model and so the mandate of the Parliamentary Commissioner for Data Protection and Freedom of Information came to an end at the end of 2011, after three years, instead of the original six years which Parliament adopted. This mode of legislation may infringe the EU's Data Protection Directive's provisions on the independence of national regulatory authorities.[177]

The new Authority is empowered with all the powers that the Commissioner has, except the right to turn to the Constitutional Court. The "ombudsman-like" powers are summarized as 'investigation proceeding'. An investigation conducted by the Authority may have the following main outcomes:

- the Authority calls upon the data controller to remedy unlawful data processing and, respectively, terminate the situation threatening with unlawful data processing;
- the Authority may prepare a report (which is open to the public) if it does not initiate an administrative or court procedure;

[174] DPA § 25(3)
[175] DPA § 25(2), (4)-(5)
[176] Majtényi, 2006, p. 138
[177] According to the current news, the European Commission is now analyzing the situation and considering to start infringement action.
http://www.globallawwatch.com/2011/12/analysis-hungarys-new-data-protection-act-raises-concerns-prompts-call-for-european-commission-infringement-action/

- the Authority may initiate a so-called 'data protection proceedings';
- the Authority may initiate a so-called secret-supervision proceedings';
- the Authority may initiate court proceeding and
- the Authority may decide to terminate the investigation.

So the Authority has new powers, namely the possibility to start different types of public proceedings: 'Data protection proceedings' or so- called 'secret-supervision proceedings'.[178]

The NDPFIA starts data protection proceedings if the illegal data processing affects a wide range of data subjects, affects sensitive data or if it causes significant injury to the data subject's interests.[179]

As sanctions, the Authority may order by resolution the correction of personal data, the deletion or blocking of personal data, it may prohibit the whole data processing or transfer to third countries, it may order the provision of information for the data subject, and – as a totally new feature – it may impose a fine between HUF 100,000 (approx. EUR 330) and HUF 10,000,000 (approx. EUR 33.000 EUR) on the controller of personal data.[180]

Generally the supervision of Data Protection is regarded as a mixed model, since the National Data Protection and Freedom of Information Authority has, on one hand, a number of "ombudsman-like" powers and, on the other hand, public proceedings powers, including the right to impose fines.

3.2. Sanctions based on the Labour Code

First, it is necessary to distinguish if the damage was caused before employment (during the hiring procedure) or during employment. There are special rules governing liability for damages in the Labour Code, but they are only applicable in the course of employment. The hiring process, therefore, falls under the "general" liability rules,[181] which means, in the context of privacy in the workplace, that the regulation of the DPA shall apply, since the employer is still a data processor even if the employment relationship does not, in fact, occur.[182]

For damages caused by any party during employment – including, of course, damages caused by the employer by a breach of privacy – the regulations of the Labour Code are applicable. Under the Labour Code the employer is liable to provide compensation for damages caused in connection with an employment relationship. The employee is relieved of liability if able to prove that the damage occurred in consequence of unforeseen circumstances beyond his control, and there had been no reasonable cause to take action for preventing or mitigating the damage; or that the damage was caused solely by the unavoidable conduct of the aggrieved

[178] New DPA § 55(1) The aim of 'secret-supervision' proceedings is to decide whether classified data are justified or not – which has little to do with powers concerning privacy in the workplace.
[179] New DPA § 60(4)
[180] New DPA § 61(1)
[181] Kiss, 2005, p. 285.
[182] Cf. Arany Tóth, 2004a

party.[183] The regulation of the Labour Code conforms to the regulation of the DPA, as both of the Acts contain the same special liability rule.

3.3. Other sanctions

3.3.1. Sanctions based on the Civil Code

Since data protection, the right to ones own image (and recorded voice) and the right to privacy are regarded as inherent rights, the legal consequences of infringing such rights shall also apply, regulated by the Civil Code. According to § 84, a person whose inherent rights have been violated has the following options under civil law, depending on the circumstances of the case:

- to demand a court declaration that an infringement has occurred,
- to demand that the infringement be halted and the perpetrator restrained from further infringement;
- to demand that the perpetrator makes restitution in a statement or by some other suitable means and, if necessary, that the perpetrator, at his own expense, make an appropriate public announcement of this restitution;
- demand the termination of the injurious situation and the restoration of the previous state by and at the expense of the perpetrator and, furthermore, to have the effects of the infringement nullified or deprived of their injurious nature;[184]

These are so-called objective sanctions, which are applicable regardless of any damage caused by the data controller.

3.3.2. Sanctions based on the Criminal Code

In some more serious cases, a breach of privacy, whether in the workplace or in any other location, may be sanctioned by the Criminal Code.

There are criminal law sanctions concerning the misuse of personal data: § 177/A of the Criminal Code states that any person who, in violation of the statutory provisions governing the protection and processing of personal data,

- is engaged in the unauthorised and inappropriate processing of personal data;
- fails to take measures to ensure the security of data;

commits a crime, if he thereby causes significant injury to the interests of another person or commits the crime in order to gain illegal benefit. It is also a crime if anyone fails to provide information to the data subject, as required by law, if it causes significant injury to the interests of the data subject.[185]

[183] New Labour Code § 166
[184] Civil Code § 84
[185] Criminal Code § 177/A

The Criminal Code also names the crime of 'violation of the privacy of correspondence' According to § 178, any person who opens or obtains a sealed package containing a communication which belongs to another person for the purpose of gaining knowledge of its contents, or conveys such to an unauthorised person for this purpose, as well as any person who 'taps' or 'hacks' into correspondence sent through telecommunications equipment commits a crime.[186]

Finally, the Criminal Code regulates the illegal possession of private secrets and says that any person who opens or obtains the sealed package of correspondence of another person and records such by technical means, captures correspondence forwarded by means of communication equipment or computer network to another person and records the contents of such by technical means for the illicit possession of private secret commits a crime.[187]

[186] Criminal Code § 178
[187] Criminal Code § 178/A

4. REFERENCES AND LITERATURE

4.1. Legal literature

Arany Tóth, Mariann (2004a): Munkáltatói felelősség a jogellenes adatkezelésért a munkaerő-felvételi eljárásban, Munkaügyi szemle, Issue 1.

Arany Tóth, Mariann (2004b): Hozzájárulás a munkáltatói adatkezeléshez a munkajogviszonyban, Munkaügyi szemle, Issue 11.

Arany Tóth, Mariann (2008a): A munkavállalók személyes adatainak védelme a magyar munkajogban, Bába és Társai, Budapest

Arany Tóth, Mariann (2008b): A munkavállalók személyes adatainak védelme az internet munkahelyi használatának ellenőrzésekor, Infokommunikáció és Jog, Issue 4.

Bankó, Zoltán – Berke, Gyula – Kiss, György (2004): Bevezetés a munkajogba, JUSTIS, Budapest

Betzel, Margaret (2005): Privacy Year in Review: Recent Changes in the Law of Biometrics, I/S: A Journal of Law and Policy for the Information Society, Issue 2-3.

Fodor T., Gábor – Nacsa, Beáta – Neumann, László (2008): Egy és több munkáltatóra kiterjedő hatályú kollektív szerződések összehasonlító elemzése, Szociális és Munkaügyi Minisztérium, Budapest

Gálik, Mihály – Polyák, Gábor (2005): Médiaszabályozás, KJK-Kerszöv, Budapest

Hajdú, József (2005): A munkavállalók személyiségi jogainak védelme, Pólay Elemér Alapítvány, Szeged

Hartai, Győző (2003): Adatvédelem a munkahelyen, Munkaügyi szemle, Issue 1.

Hegedűs, Bulcsú (2006a): A munkahelyi hagyományos és elektronikus levelezés ellenőrzése, Munkaügyi szemle, Issue 1.

Hegedűs, Bulcsú (2006b): A munkahelyi számítógép és internet ellenőrzésével kapcsolatos gyakorlat, Munkaügyi szemle, Issue 7-8.

Horváth, Linda – Gelányi, Anikó (2011): Lájkolni vagy nem lájkolni? A közösségi oldalak használatának munkajogi kérdései, Infokommunikáció és Jog, Issue 2.

Jain, Anil K. – Prabhakar, Salil – Ross, Arun (2004): An Introduction to Biometric Recognition, 14 IEEE Transactions On Circuits And Systems For Video Technology: Special Issue On Image-And Video-Based Biometrics, Issue 4 http://biometrics.cse.msu.edu/JainRossPrabhakarCSVT-vl5.pdf [27.04.2005].

Jóri, András (2005): Adatvédelmi kézikönyv, Osiris, Budapest

Jóri, András – Hegedűs, Bulcsú – Kerekes, Zsuzsa (eds.) (2010): Adatvédelem és információszabadság a gyakorlatban, Complex, Budapest

Kiss, György (2005): Munkajog, Osiris

Majtényi, László (2003): Az információs jogok. In: Halmai, Gábor – Tóth, Gábor Attila (Eds.): Emberi Jogok, Osiris, Budapest, pp. 577-637.

Majtényi, László (2006): Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága, Complex, Budapest

McGuire, Lisa Jane (2000) Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up You Privacy, Akron Law Review, Issue 3.

Polefkó, Patrik (2010): Barátok és bizonytalanságok közt, avagy a közösségi oldalakról adatvédelmi szemszögből (1. rész), Infokommunikáció és Jog, Issue 3.

Polyák, Gábor – Szőke, Gergely (2011): Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései. In.: Drinóczi, Tímea (ed.): Magyarország új alkotmányossága, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs, pp. 155-178.

Sólyom, László (2001): Az ombudsman „alapjog értelmezése" és „normakontrollja", In.: Az odaátra nyíló ajtó, Adatvédelmi Biztos Irodája, Budapest

Székely, Iván – Szabó, Máté Dániel (eds.) (2005): A privacy védelme a munkahelyen, In.: Szabad adatok, védett adatok, BME GTK Információ és Tudásmenedzsment Tanszék

Szőke, Gergely László (2010): Privacy Protection (Book chapter). In.: Rátai, Balázs – Homoki, Péter – Polyák, Gábor – Schvéger, Judit – Szemes, Balázs – Szőke, Gergely László – Tasnádi, Sándor – Tóth, András: *Cyber Law in Hungary*, Kluwer Law International, The Netherlands

Szőke, Gergely László (2011): Közterületi kamerázás az Európai Unióban, JURA, Issue 2.

4.2. Cases of the Data Protection Commissioner

DPC, 461/A/1998
http://abiweb.obh.hu/abi/index.php?menu=aktualis/archivum/ajanlasok&dok=9278 [10.05.2011.]

DPC, 693/K/1998
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1998/M/1/1&dok=693_K_1998 [10.05.2011.]

DPC, 917/K/1998
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/1999/M/1/1&dok=917_K_1998 [10.05.2011.]

DPC, 475/H/2000
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/M/1/1&dok=475_H_2000 [10.05.2011.]

DPC, 772/A/2000
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2000/III/1/2/1&dok=beszamolok_2000_III_A2 [10.05.2011.]

DPC, 570/A/2001
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2001/M/1/1&dok=570_A_2001 [10.05.2011.]

DPC, 127/K/2003
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/M/1&dok=127_K_2003 [10.05.2011.]

DPC, 1472/A/2003
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2003/II/1/2&dok=beszamolok_2003_IIA3 [10.05.2011.]

DPC, 120/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/2 [27.05.2011]

DPC, 531/A/2004
http://abiweb.obh.hu/abi/index.php?menu=munkaugy&dok=11861 [27.05.2011]

DPC, 750/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/6 [24.05.2011]

DPC, 1543/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/2 [27.05.2011]

DPC, 1598/K/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2004/II/1/3/6 [24.05.2011]

DPC 1722/A/2004
http://abiweb.obh.hu/abi/index.php?menu=beszamolok/2005/M/4/1&dok=1722_A_2004 [27.05.2011]

DPC, 1012/K/2005
http://abiweb.obh.hu/abi/index.php?menu=munkaugy&dok=11866 [24.05.2011]

DPC, 40/K/2006
http://abiweb.obh.hu/abi/index.php?menu=munkaugy&dok=11871 [27.05.2011]

DPC, 559/A/2006
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=559_A_2006-3&nyomtat=1 [15.05.2011]

DPC, 866/A/2006
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=866_A_2006-3 [24.05.2011]

DPC, 920/K/2006
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2006&dok=920_K_2006-2&nyomtat=1 [15.05.2011]

DPC, 1393/K/2006
http://abiweb.obh.hu/abi/index201.php?menu=munkaugy&dok=1393_K_2006-5 [24.05.2011]

DPC, 1664/A/2006
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2007&dok=1664_A_2006-8&nyomtat=1 [15.05.2011]

DPC, 1672/K/2006
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=1672_K_2006-3&nyomtat=1 [15.05.2011]

DPC, 1767/K/2006
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=1767_K_2006-3&nyomtat=1 [15.05.2011]

DPC, 2511/K/2007
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=2511_K_2007-3 [27.05.2011]

DPC, 800/K/2008
http://abiweb.obh.hu/abi/index.php?menu=internet1&dok=800_K_2008-3 [27.05.2011]

DPC, 415/K/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=415_K_2009-3&nyomtat=1 [15.05.2011]

DPC, 636/K/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=636/K/2009-3&nyomtat=1 [15.05.2011]

DPC, 663/P/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=663/P/2009-3&nyomtat=1 [15.05.2011]

DPC, 857/K/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=857/K/2009-3&nyomtat=1 [15.05.2011]

DPC, 1092/P/2009
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2009&dok=1092_P_2009-6&nyomtat=1 [15.05.2011]

DPC, 3362/P/2009
http://abiweb.obh.hu/abi/index.php?menu=Munkaltato&dok=3362/P/2009-3&nyomtat=1 [15.05.2011]

DPC, 922/2/2010
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2010&dok=ABI-922-2_2010_K&nyomtat=1 [15.05.2011]

DPC, 926/H/2010
http://abiweb.obh.hu/abi/index.php?menu=aktualis/allasfoglalasok/2011&dok=ABI-1642-9_2011_H [20.09.2011]

DPC, 1454/K/2010
http://abiweb.obh.hu/abi/beszamolok/2010/beszamolo_2010.pdf [15.05.2011]

4.3. Court cases

4.3.1. Cases of the ECJ

Case C-101/01. – Judgment of the Court of 6 November 2003. Criminal proceedings against Bodil Lindqvist)

Cases C- 468/10 and C-469/10 – Judgment of the Court (Third Chamber) of 24 November 2011. Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado.

4.3.2. Hungarian court cases

35/2002. (VII.19.) AB decision

BH2001.269

BH2006.64

Fővárosi Munkaügyi Bíróság, 5.M. 394/2007/12.;

Fővárosi Munkaügyi Bíróság, 31.M.3189/2002/55.;

Miskolci Munkaügyi Bíróság, 8.M.1286/2005/19.;

Nyíregyházi Munkaügyi Bíróság, 1.M.687/2005/12.

Pécsi Munkaügyi Bíróság, 3.M.1763/2005/15.;

Veszprémi Munkaügyi Bíróság, 2.M.341./2006./8.;

4.4. Other documents

ILO Code of Practice – Protection of workers' personal data, International Labour Office, Geneva, 1997

European Commission: Second stage consultation by social partners on the protection of workers' personal data, http://ec.europa.eu/social/BlobServlet?docId=2504&langId=en [12.03.2011.]

Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12th January 2011, http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf [10.09.2011.]