PRIVACY IN THE WORKPLACE

FINAL (COMPARATIVE) REPORT ON HUNGARY AND GERMANY

AUTHORS

Dr. Gergely László Szőke

Dr. Zsolt György Balogh

Dipl.-Jur. Falk Hagedorn

Dr. Attila Kiss

Dr. Gábor Polyák

Dr. Balázs Rátai

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

APRIL, 2012

CONTENT

1. INTRODUCTION AND BACKGROUND

1.1. Purpose and methodology

Nowadays, due to the rapid development of digital technology, employers can resort to a comprehensive repertoire of measures for monitoring employees. At the same time the new achievements of the Information Age face rigorous scrutiny under operating data protection measures and from demands for increased efforts by data protectionists. In the light of a variety of so-called data scandals in multinational and German companies, public discussion on employee's data protection has finally moved into the focus of legal policy. Science, jurisprudence and also the legislator are all trying hard to accommodate themselves to the new circumstances and to develop possible solutions to setting an adequate (in respect of potential conflict within the employment relationship) and appropriate level of well-balanced protection in the field of employee data security.

We search for the depiction of the potential conflicts of interest between employer and employee, as employers treads a narrow path between enforcing his legitimate interests and encroaching on the personal rights of his employees. Within this project we cannot take into consideration every single matter regarding data protection in connection to employment relationships. Our research focuses just on one of the key issues in the EU, the regulation of technical surveillance, in order to differentiate between what is allowed and what is not – legal and illegal monitoring of the employees – as in practice there is just a low threshold between them. The goal of the research is to frame and describe the current situation and draw the legal consequences in the respective fields; however writing of new proposals is scheduled for another phase of the project.

The main objective of the Comparative Country Report is to map and compare the current national legal frameworks of Hungary and Germany on Privacy in the Workplace, and besides, to show the European context of the regulation.

Firstly an inventory of essential background information is shown which contains, beside the basic concept of privacy issues, a summary of the relevant EU and international legislation, the national Acts, and also their constitutional-juridical context. To show a more practical aspect, case law on different surveillance technologies, frequently used in workplaces is presented. Therefore the relevant court decisions, as well as the position of the data protection authorities are examined, with particular reference to a more responsible handling of employee's data. Finally, the related legal literature and the insufficient sources of self-regulation are also summarized, and the possible sanctions are shown in this Report before a closing statement follows on the legal situation.

It can to be stated in general, that there is a lack of specific legislation on the means of surveillance technologies, and the national data protection regulations, typically, does not distinguish between or among technologies, and so, for the most part, the same rules apply. Even though, our choice of 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 data protection supervisory bodies and of the courts also focuses on different technologies.

1.2. Overview of the relevant legal sources

1.2.1. International and EU sources

1.2.1.1. The ILO code of practice

Regulatory aspects of personal data protection in relation to monitoring and surveillance in the workplace have been specifically addressed for the first time at international level by the International Labour Organization (ILO). Around the mid 1990s ILO initiated and supported the development of a code of practice,[1] which also set specific rules in a comprehensive way for the processing of workers' personal data in case of monitoring and surveillance.

ILOC, containing also an authorised, integral commentary, was approved for publication and distribution by the ILO Governing Body in November 1996. The code was actually developed and adopted by a group of experts, selected by ILO based on the consultation with governments, Employers' and Workers' Groups of the ILO Governing Body. It has been a deliberate decision of the expert group to give the name of "code of practice" to the document. The choice intended to express that ILOC is not a compulsory "codes of conduct" or "codes of practice", which are foreseen e.g. by the EU data protection directive. According to point 2 of ILOC it only intends to provide guidance and has no binding force. It is also stated that ILOC "does not replace national laws, regulations, international 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 ILOC covers both private and public sector and manual and automatic personal data processing of workers. The term 'worker' covers current and former workers and also job applicants.

1.2.1.1.1. Approach and guiding principles of ILOC

According to the preamble of ILOC, several reasons necessitate the development of data protection provisions, which specifically address the use of workers' personal data. Among these reasons electronic monitoring is also specifically mentioned. ILOC rules relating to the ways of processing personal data are divided into 5 sections. These sections address the following issues:

1. data collection
   - All data should be obtained from the individual worker.
   - Worker should be informed about the collection of data from a third person.
   - Sensible data should not be processed. (sex life; political, religious or other beliefs; criminal convictions)
2. data security
3. data storage
4. use of data

[1] ILO Code of Practice (Hereinafter: ILOC)

5. communication of data

Besides the specific rules relating to the processing of personal data, ILOC defines 12 principles:

1. fair and lawful data processing; direct relevance to employment of data processing
2. no deviation from the original purpose of data collection during data processing – In case of deviation the employer is charged to ensure the processing in a manner compatible with the original purpose and make the necessary measures to avoid the misinterpretation caused by the changed context.
3. prohibition of controlling the behavior of workers
4. prohibition of decisions on the sole ground of automated data processing
5. data acquired through monitoring can only be used for evaluation of performance of workers
6. regular assessment of data processing practices in order to reduce the amount of data collected and to improve privacy protection
7. informing workers on data processing
8. regular training of personal participating in data processing
9. avoidance of unlawful discrimination
10. co-operation between employers and workers in creating privacy policies
11. confidentiality of data collected
12. no waiver for privacy rights of workers

1.2.1.1.2. Rules of ILOC related to monitoring and surveillance

Monitoring according to ILOC "includes, but is not limited to, the use of devices such as computers, cameras, video equipment, sound devices, telephones and other communication equipment, various methods of establishing identity and location, or any other method of surveillance." It is clear from the definition that monitoring and surveillance are used as synonyms, and both considered as a form of data collection by the ILOC.

ILOC point 6.14 contains the rules relating to monitoring of workers. The code states that workers "should be informed in advance of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers." Secret monitoring is not allowed as a general rule, however it provides that secret monitoring is permitted if criminal activity or other serious wrongdoing is suspected on reasonable grounds. Similarly to this rule, "continuous monitoring should be permitted only if required for health and safety or the protection of property." The permission of secret monitoring on the ground of suspicion of criminal activity or other serious wrongdoing provides in practice a clear ground for secret monitoring without limitations, additionally continuous monitoring can also be easily justified in any situation on the ground of property protection. These rules of ILOC clearly favour employee monitoring,

thus completely nullify the intentions set out in the principles and the general rules on monitoring of ILOC.

In addition to point 6.14 examined above, there is a rule relating to monitoring in point 5.6, which states that "personal data collected by electronic monitoring should not be the only factors in evaluating worker performance."

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. Charter of Fundamental Rights of the European Union

With the entry into force of the Treaty of Lisbon[2] the Charter of Fundamental Rights of the European Union[3] acquired a binding legal force.[4] The European fundamental rights protection, which was created by the European Court of Justice as the source of fundamental legal principle based on the constitutional traditions common to the Member States, as well as the ECHR,[5] was extended by a written catalogue of fundamental human rights through Article 6 Paragraph 1 Sub-par. 1 of TEU.[6] The Charter of Fundamental Rights of the EU deals explicitly with the protection of personal data in Article 8.

1.2.1.4. EU initiatives

First of all the "general" data protection directive, Directive 95/46/EC[7] has to be highlighted, what was obligatory 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[8] applies.

---

[2] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007

[3] The Charter of Fundamental Rights of the EU was adopted in December 2000 at the Nice Summit. For the significance of this for Labour Law cf. Däubler, 2001a, p. 380.

[4] Calliess, 2011, § 6 EUV mgn. 1.

[5] Cf. Art. 6 par. 3 TEU. Calliess, 2011, § 6 EUV mgn. 1.

[6] Cf. Art. 6 par. 1 TEU.

[7] 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. Also referred to as DPD.

[8] 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)

At EU level the first specific consultation about the personal data protection in the employment context was initiated by the European Commission.[9] The consultation was launched for two reasons:

1. the issue of creating a personal data protection directive in the field of working relationships has been on the policy agenda since 1997;
2. the Art. 29 Data Protection Working Party stated in his opinion in 2001,[10] that personal data processing raise specific concerns in the employment context, which problems are not addressed adequately by the Directive 95/46/EC;[11]

The Commission proposed that action at community level in relation to the protection of workers' personal data would be advantageous in the areas of consent; medical data; drug and genetic testing; and monitoring and surveillance. The proposals, which were submitted for consultation, were mainly based on the content of the ILOC.[12] The reaction of social partners (employer and employee associations) to the proposal also referenced the ILOC. EUROCADRES (Council of European Professional and Managerial Staff)[13] 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.[14] UEAPME (European Association of Craft, Small and Medium-sized Enterprises)[15] expressed its view that a non-binding code of conduct developed along the lines of the ILOC would be useful.[16]

During this consultation the possibility and necessity of an employment related data protection directive was discussed, yet it had been decided there is no need for EU level regulation. However, the Article 29 Data Protection Working Party[17] issued several opinions and working documents, in which directly addressed the question of privacy in the workplace during the last 10 years, and recently the discussion about an employment related data protection directive has been reopened.[18]

[9] European Commission: Second stage consultation, p. 1. It also has to be mentioned, that European Labour Law Network (ELLN) advises the European Commission on labour law related issues.
[10] Opinion 8/2001 on the processing of personal data in the employment context
[11] Communication from the Commission – First stage consultation of social partners on the protection of workers' personal data, pp. 2-3.
[12] European Commission: Second stage consultation, p. 6, footnote 10.
[13] www.eurocadres.org [18.01.2012]
[14] European Commission: Second stage consultation, p. 20.
[15] www.ueapme.com [18.01.2012]
[16] European Commission: Second stage consultation, p. 3.
[17] Article 29 Data Protection Working Party is often referred as WP.
[18] WP raised again the possibility of sector specific EU level personal data protection regulation in its 2009 contribution to the consultation on the personal data protection. Cf. in The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, p. 8, point 19.

1.2.1.5. Opinions and working papers of the Article 29 Data Protection Working Party

The approach of the European Union is best reflected by the opinions and working papers of the Working Party. In the most relevant ones WP directly addressed the question of personal data protection in the employment context.[19]

1.2.1.5.1. Opinion on Employee Evaluation Data[20]

In the opinion the WP concludes that the definition of personal data in Article 2(a) of the DPD includes not only information results from objective factors, but "also any other element, information or circumstance having an information content such as to add to the knowledge of an identified or identifiable person."

It further states that "Personal data can be therefore found in subjective judgments and evaluations which can actually include elements specific to the physical, physiological, psychical, economic, cultural or social identity of data subjects. This is equally true if a judgment or a evaluation is summarized by a score or rank or is expressed by means of other evaluation criteria."

Thus employee evaluation data is considered to be personal data according to the DPD.

1.2.1.5.2. Opinion on the processing of personal data in the employment context[21]

This opinion had been prepared for the consultation of the Commission on personal data protection in the employment context in 2001. The opinion states that „Any collection, use or storage of information about workers by electronic means will almost certainly fall within the scope of the data protection legislation." The WP specifically highlighted that monitoring of email and internet usage and video surveillance of workers fall within the scope of data protection regulation. The WP has drawn the attention to seven data protection principles that has special significance in the employment context:

1. finality
2. transparency
3. legitimacy
4. proportionality
5. accuracy and retention of data
6. security
7. awareness of the staff

The WP expressed its opinion regarding that consent can only be the ground of processing of personal data if "the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment."

[19] Further relevant opinions and relevant details are cited in Chapter 2 in connection to the surveillance technologies examined within the scope of the research.
[20] WP42
[21] WP48

Additionally the WP opinion addresses the question of interaction between data protection regulation and labour law, surveillance and monitoring in the workplace and transfer of workers data to third countries.

The document provides also an overview of the relevant regulations, and the practice of member states relating to personal data protection in the employment context.

1.2.1.5.3. Working document on the surveillance of electronic communications in the workplace[22]

This working document had been envisioned in the WP opinion on the processing of personal data in the employment context. The document complements WP48. The approach of the Working Party in this matter is best summarized as "in considering the question of surveillance, it must always be borne in mind that while workers have a right to a certain degree of privacy in the workplace, this right must be balanced against the right of the employer to control the functioning of his business and defend himself against workers' action likely to harm employers' legitimate interests, for example the employer's liability for the action of their workers."[23]

The Working document provides guidance and examples about the application of the principles that have a high importance in the employment context according to WP48. Additionally it provides detailed analysis about e-mail monitoring and monitoring of internet access.

1.2.1.5.4. Opinion on the Processing of Personal Data by means of Video Surveillance[24]

Point 8 of the opinion specifically addresses the use of video surveillance in the employment context.[25] The opinion draw a distinction between general purpose video surveillance and video surveillance allowing distance monitoring and systems "that are deployed, subject to appropriate safeguards, to meet production and/or occupational safety requirements and also entail distance monitoring - albeit indirectly."

The opinion also highlights that "surveillance should not include premises that either are reserved for employees' private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation areas; that the images collected exclusively to safeguard property and/or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches; and that employees should always be allowed to lodge their counterclaims by using the contents of the images collected."

WP states here that "information must be given to employees and every other person working on the premises." It also defines the minimum content of the information that should be provided:

[22] WP55
[23] WP55, p. 6.
[24] WP89
[25] WP89, p. 25.

- the identity of the controller
- the purpose of the surveillance and
- other information necessary to guarantee fair processing in respect of the data subject (in which cases the recordings would be examined by the management of the company, the recording period and when the recording would be disclosed to the law enforcement authorities).

1.2.1.5.5. The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data[26]

The WP draws attention in point 19 to specific sectoral regulations, what could be envisaged in the field of employment relationships beside a general comprehensive personal data protection framework.

Furthermore the WP states in point 66 that in employment context the consent cannot be given freely, because there is a clear unbalance between the data subject and the data controller. It is concluded that consent in these cases is an inappropriate ground for processing personal data. It recommends to change the existing regulation in a way, which provides a proper solution to this problem.

1.2.1.5.6. Opinion on the Industry Proposal for Privacy and Data Protection Impact Assessment Framework for RFID Applications[27]

The WP opinion does not contain analysis and evaluation of specifically employment related issues, but since RFID applications will dominantly used in workplaces they will have an obvious impact on the workplace privacy. Therefore it is not surprising that European workers' associations are specifically concerned about the use of RFID applications in the workplace as it is demonstrated by the UNI-Europe policy opinion.

The WP opinion was a formal evaluation and response to an industry proposal for a privacy impact assessment framework in the field of RFID applications. The most important element of the opinion is that privacy impact assessment by definition includes the uncovering of privacy risks, because without identifying the risks, the adequacy of the privacy protection measures cannot be judged.

1.2.1.5.7. Monitoring and surveillance related rules

The WP first addressed the issue of surveillance in its opinion on the processing of personal data in the employment context. It states that "Data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, Internet access, video cameras or location data. Any monitoring must be a proportionate response by an employer to the risks it faces taking into accounts the legitimate privacy and other interests of workers. Any personal data held or used in the course of monitoring must be adequate, relevant and not

[26] WP168
[27] WP175; cf. also the revised opinion: WP180.

excessive for the purpose for which the monitoring is justified. Any monitoring must be carried out in the least intrusive way possible." [28]

WP55 also provides detailed guidance relating to email and internet access monitoring. The Working Party took the view that the most important data protection principle is transparency in relation to surveillance and monitoring. According to the working document transparency can be achieved if the employer:

1. provides information about the monitoring and surveillance to the employees,
2. notifies supervisory authorities before carrying out any wholly or partly automatic processing operation or set of such processing operations,
3. access to employers' files without constraint at reasonable intervals and without excessive delay or expense.

Regarding e-mail monitoring the WP took the view that Article 7 point f) of the DPD does not provide a suitable basis for accessing email accounts. It pointed out that "that where a worker is given an e-mail account for purely personal use or is allowed access to web-mail account, opening of e-mails in this account by his employer (apart from scanning viruses) can only be justified in very limited circumstances and cannot under normal circumstances be justified on the basis of Article 7 (f) because it is not in the legitimate interests of the employer to have access to such data. Instead the fundamental right to secrecy of correspondence prevails."

The WP suggested addressing the following questions in privacy policies in order to satisfy the transparency principle:

- "Whether a worker is entitled to have an e-mail account for purely personal use, whether use of web-mail accounts is permitted at work and whether the employer recommends the use, by workers, of a private web-mail account for the purpose of using e-mail for purely personal use
- The arrangements in place with workers to access the contents of an e-mail, i.e. when the worker is unexpectantly absent, and the specific purposes for such access.
- When a backup copy of messages are made, the storage period of it.
- Information as to when e-mails are definitively deleted from the server.
- Security issues
- The involvement of representative of workers in formulating the policy."[29]

Regarding the internet access monitoring the WP took the opinion that prevention of the internet misuse must be the general rule instead of the detection of misuse through monitoring. Secondly it emphasized that monitoring should be proportionate to the risk faced by the employer. Thirdly it emphasized that in case of detection of misuse the employees should be given full opportunity to contest the misuse. The WP suggested including specific rules into the employer's internet policy relating to the following issues:

[28] WP55, p. 4.
[29] WP55, p. 22.

- "The employer must set out clearly to workers the conditions on which private use of the Internet is permitted as well as specifying material, which cannot be viewed or copied. These conditions and limitations have to be explained to the workers.
- Workers need to be informed about the systems implemented both to prevent access to certain sites and to detect misuse. The extent of such monitoring should be specified, for instance, whether such monitoring may relate to individuals or particular sections of the company or whether the content of the sites visited is viewed or recorded by the employer in particular circumstances. Furthermore, the policy should specify what use, if any, will be made of any data collected in relation to who visited what sites.
- Inform workers about the involvement of their representatives, both in the implementation of this policy and in the investigation of alleged breaches."[30]

1.2.2. The basic concept of privacy protection and the detailed legal framework in Hungary[31]

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 should also try – as far as possible – to analyse the new regulation.

Regarding the legal framework of Privacy in the Workplace, firstly, there are some fundamental rights in both the current Hungarian Constitution[32] and in the new Constitution[33] which affect the issue of privacy. The main code in the field of privacy protection is the Data Protection Act.[34] The Hungarian Parliament adopted a brand new Data Protection Act[35] 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.[36]

Another relevant code is, of course, the Labour Code.[37] The preparation of a new regulation in this field started in summer 2011, and a totally new Labour Code[38] 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.

[30] WP55, p. 25.
[31] This chapter is based on Szőke, 2010
[32] Act XX of 1949 The Constitution of the Republic of Hungary, (hereinafter: Constitution)
[33] Constitution of Hungary (2011. April 25) (hereinafter: New Constitution)
[34] Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest, hereinafter: Data Protection Act, DPA)
[35] Act CXII of 2011 on information self-determination and freedom of information (hereinafter: New Data Protection Act, New DPA)
[36] About the analysis of the new DPA see more Polyák/Szőke, 2011
[37] Act XXII of 1992 on the Labour Code (hereinafter: Labour Code)
[38] Act I of 2012 on the Labour Code (hereinafter New Labour Code)

Finally, we should mention that means of privacy protection other than the protection of personal data, such as the Right to One's Own Image or the Right of Private Correspondence are regulated by both the Hungarian Civil[39] and Criminal Codes.[40]

1.2.2.1. 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.[41] 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.[42] 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.[43] "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."[44]

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 and family life, home, communication and good reputation are named as privacy rights in addition to the rights regarding data protection.[45]

1.2.2.2. 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

[39] Act IV of 1959 on the Civil Code of the Republic of Hungary (hereinafter: Civil Code)
[40] Act IV of 1978 on the Criminal Code (hereinafter: Criminal Code)
[41] Constitution, § 59
[42] New Constitution, Article VI.
[43] Majtényi, 2003, pp. 577-637.
[44] 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.
[45] New Constitution, Article VI.

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.

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.[46]

There are also regulations connected to this issue in the Criminal Code, containing sanctions in the event of a breach of privacy rights.[47]

1.2.2.3. The basic concept of the Data Protection Act

1.2.2.3.1. 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.[48] 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[49] – even with the involvement of more checks or controllers and with more

[46] Civil Code, §§ 78-81.
[47] Cf. in details in Chapter 3.
[48] DPA § 2(1)
[49] 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.

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.[50] The actual interpretation of this provisions is not clear so far,[51] it will be the task of the new Data Protection Authority to work out the details of this issue.[52]

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.[53]

The Act orders stricter conditions concerning sensitive data. These involve – according to the closed listing of the Act[54] – 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.

1.2.2.3.2. 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.[55]

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'.[56]

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.

1.2.2.3.3. The legal basis of data processing

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.[57] The Act on Data Protection did not recognise any other legal ground.[58]

---

[50] New DPA § 4(3)
[51] Mostly because of the fact that the definition of personal data still contains the phrase "indirectly identifiable", and the European Directive also follows the
[52] About relative and absolute interpretation of personal data see Majtényi, 2006, pp. 109-111.
[53] Gálik/Polyák, 2005 p. 217.
[54] DPA § 2. 2. New DPA § 3. 3.
[55] DPA § 2. 9; New DPA § 3. 10.
[56] DPA § 2. 8; New DPA § 3. 9.

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).

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,[59] 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.[60] 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.[61] According to our view, the different regulation of the legal basis for processing personal data may infringe the free movement of such data.[62]

[57] DPA § 3(1)
[58] 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)
[59] Jóri, 2005, p. 81.
[60] Case C-101/01
[61] Case C-101/01, 97-98.
[62] The brand new decision of the ECJ strengthens our opinion. See C- 468/10 and C-469/10 cases

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.[63]

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.

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

- 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.[64]

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.

1.2.2.3.4. 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.[65] 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.[66]

[63] New DPA § 6(1)
[64] New DPA § 6(5)
[65] DPA § 2(6), New DPA § 3(7)
[66] 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.

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.[67] Similarly, consent to processing his data to the extent necessary is considered as granted in connection with any proceedings requested by the data subject.[68]

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).[69] 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.[70]

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 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.[71]

[67] DPA § 3(5), New DPA § 6(7)
[68] DPA § 3(6), New DPA § 6(6)
[69] DPA, § 3(1), § 5(3), New DPA § 5(1) b)
[70] Jóri, 2005, p. 165.
[71] DPA § 3(6), (7)

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.[72] 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."[73]

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 and according to the interpretation of the DPA. This (which is the predominant interpretation still) is far from unambiguous[74] 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

[72] This is the general view in the literature, ld. Arany Tóth, 2004b, pp. 15-17; Majtényi, 2006, p. 332; Hartai, 2003, p. 46; etc.
[73] Majtényi, 2006, p. 333.
[74] Jóri, 2005, pp. 187-188.

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.[75] 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 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,[76] 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.

[75] New DPA § 6(5)
[76] Arany Tóth, 2004b, pp. 18-19; Arany Tóth, 2008b

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.)"[77]

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.

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.[78] 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 seem to be answered once the new Labour Code comes into effect on 1st July 2012.

1.2.2.3.5. Other rules of data processing

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

[77] Majtényi 2006, p. 336.
[78] Jóri, 2005, pp. 164-165.

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.[79]

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.[80]

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.[81] Some of these purposes are also mentioned in the Data Protection Directive, but as a legal basis for data processing.

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.[82]

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.[83]

The rights of the data subject

The Act on Data Protection ensures special rights to data subjects for validating information-related self-determination.[84] 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

[79] DPA § 5(1), (2), § 14(2) d); New DPA § 4(1)-(2)
[80] Cf. DPC, 1472/A/2003. and Gálik/Polyák, 2005, p. 221.
[81] DPA § 5(4)
[82] DPA § 7(1), New DPA § 4(4)
[83] DPA § 10, New DPA § 7
[84] DPA §§ 11-17, New DPA §§ 14-18, § 21.

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.[85] 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.[86] 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 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.[87]

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. [88] 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.[89] 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.

1.2.2.4. 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" [90] 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

[85] DPA § 2. 12; New DPA § 3. 13.
[86] Gálik/Polyák, 2005, p. 223
[87] Jóri, 2005, p. 266
[88] DPA § 2. 12.; New DPA § 3. 13.
[89] 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)]
[90] Sólyom, 2001, pp. 89-90.

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.

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

1.2.2.5.1. 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 has the effect that the same rules and principles apply to both sectors. Neither case law nor academic papers differentiate.[91]

1.2.2.5.2. 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:[92] 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.[93] 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.'[94] §104 (1) says that 'employees shall perform their work in accordance with the employer's instructions.'[95] GYÖRGY KISS says, that the right to monitor is strongly connected to the right to instruct, which is based on these provisions.[96] The employer also has the right to monitor the equipment which he provided for the employee.

1.2.2.5.3. Data protection provisions in the Labour Codes

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

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

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.

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 the employee's consent.[97] 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.[98]

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.[99] 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.

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.[100]

[97] Labour Code § 3(4);
[98] Labour Code § 77(1);
[99] Labour Code § 192/G(3), (6);
[100] New Labour Code § 11(1)

The employer has to inform the employees about the technical measures that is used to control/monitor the employees activity (work).[101]

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 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,[102] 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've already shown it, 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[103] and on the details of the data processing concerning the control and monitoring,[104] the new Law may strengthen the tendencies towards adoption of internal norms. It seems to be worth, at least for bigger employers, to adopt Codes of Conduct or by-laws to regulate and clarify the details of the employee's monitoring.

1.2.3. Basic concept of data protection in Germany and the dogmatic bases of the general protection of personality rights

In Germany, data protection law is arranged as a special personality right[105] whose constitutional-juridical roots lie especially in the fundamental rights of the free development of the personality (Art. 2 par. 1 GG) as well as in the protection of human dignity (Art. 1 par. 1 GG).[106] The law has been the subject of numerous court decisions,[107] and it is and will remain so. Deriving from Art. 2 par. 1 GG, in conjunction with Art. 1 par. 1 GG,[108] the general right to privacy grants a comprehensive right of respect for the individual and for his personal development.[109] The reference point of this protection is the privacy of the basic legal entity, the person, as such.[110] From this there emerges the obligation of the "fundamental

[101] New Labour Code § 11(2)
[102] After 1st July, 2012, when the Code comes into effect.
[103] New Labour Code, § 11(2)
[104] New Data Protection Act § 20
[105] Gola, 2010a, mgn. 45. On the historical development of the personality right protection, cf. Gola/Wronka, 2010, mgn. 1 ff.
[106] Kerstin Orantek, 2008, p. 51.
[107] Cf. BVerfGE 27, 1 ff. (Microcensus); 34, 238 ff. (Tonband); 65, 1 ff. (Population count); 80, 367 ff. (Diary) or, from more recent past the verdict on online investigation of computers of 27 February 2008 (NJW 2008, 822). Cf. with regard to the Supreme Court Jurisdiction on the handling of employee data Gola/Wronka, 2010, p. 575 ff.
[108] Constant jurisdiction of BVerfG, Cf. just: BVerfGE, 35, 202, 219; 72, 155; 82, 236, 269; 90, 263, 270.
[109] BGHZ 13, 334, 338; 26, 349, 354.
[110] BVerfGE 27, 1; Ehmann, 1997, p. 196; Schmidt, 1974, p. 243.

right (…) to guarantee elements of the personality which are not in themselves objects of the special freedom guarantees of the GG, but neither do they take second place to these in terms of the constituted meaning of personality."[111] The Federal Constitutional Court stresses that the need for such loophole-closing[112] exists in particular "also in view of modern developments and with them to related new dangers for the protection of the human personality".[113] Thereby we arrive at the essential significance of the general right to privacy with respect to the effectiveness of a fundamental right with which it must be fully harmonised.[114] It goes without question that this personal protection must be also be applied in the workplace.

1.2.3.1. Taking stock of protection of personality rights at the workplace

By virtue of the power of the state and the private economy to exercise widespread control over almost all domains of work, employees face the danger that they are unable to protect their private sphere to the required extent. Concerning technological innovation in recent years, there has been a constant increase in the level of danger of the misuse of personnel-related data. Starting from access to email correspondence to the possibility of creating and evaluating relevant movement and personality profiles of colleagues, there are almost no fields where even a single movement or action could not be – at least theoretically – monitored. It is, therefore, totally clear that the working environment is precisely where many different facets of the personal rights of the employee can be affected.[115]

1.2.3.1.1. The needs of the employee in respect of personality rights

If we talk in terms of monitoring levels in the workplace, employees are not helpless under the law, and they are able to challenge their employer legally in respect of the right to privacy. Concerning the direct involvement of the fundamental right as a third component, the constitutional right is involved not only from the point of view of the state[116] but the fundamental right as an objective value-system prevails over the general clauses[117] in the domain of the private economy.[118] In this sense the personality rights of the employee are in danger of violation in several ways, and such violations can appear in the working environment in many forms.

[111] BVerfGE 54, 148, 153; 95, 220, 241; 99, 185, 193; 101, 361, 380.
[112] BVerfGE 106, 28, 39.
[113] BVerfGE 54, 148, 152; 65, 1, 41.
[114] Di Fabio, 2011, Art. 2 GG mgn. 127.
[115] Naturally the range of potentially violable employee rights in labour law is not limited to violations of personal rights, although within the private sphere in the field of employment, treatises currently tend to concentrate on this area.
[116] According to Art. 20. Sec. 3 GG the legislative, executive und judicature are bound to the fundamental rights.
[117] As e.g. the general clauses of BDSG and BGB, Thüsing, 2010, mgn. 342.
[118] Roloff, 2009, § 5 mgn. 2; cf. basically with the classification of fundamental rights as objective valuem BVerfGE 7, 198, 203 ff. as well as specially to the indirect third-party effect of the general personality right BVerfGE 35, 202, 219 ff.

The protection of personality rights over the right of informational self-determination[119]

As far as the area of working conditions is concerned[120] it is not only the state that needs data in order to be able to carry out its duties, but the private sector also – e.g., if it is to decide on contractual conditions.[121] Without regard to the form of monitoring as well as to the data processing procedures to be carried out, the employer is obliged to respect his employee's demand for the protection of his personal rights in the form of the right of informational self-determination (the so-called fundamental right of data protection).[122] The Federal Constitutional Court explained that "under the conditions of modern data processing (…) the protection of the individual against unlimited inquiry, storage, application and transmission of his personal data is embedded in his general personality right (…). The fundamental right guarantees the individual's authority to the extent that he himself can basically decide about the omission or use of his personal data."[123] He can basically decide himself when and within what framework he is prepared to reveal his personal circumstances. Thus "there are no more irrelevant data among the conditions of automatic data processing"[124] since all data relevant to an individual date enjoys the protection of the fundamental law – regardless of whether or not it contains a sensitive item of information.[125] Hence, not only is an individual protected against new technology in respect of private and intimate data, but the employer is also required to comply with various basic requirements.[126] Data must be collected directly from the person concerned (the principle of direct collection).[127] Extensive computer-assisted profiling and complete data collection is forbidden, insofar as this allows a complete picture of the individual involved to be created.[128] According to the principle of necessity, the handling of personal data is limited to the extent actually required, and data are to be used only for defined and legitimate purposes.[129] The core issue of private life is inviolable;[130] unreasonable intimacies pertaining to the employee or self-accusations may not be collected. An additional requirement is for the open handling of data – the principle of transparency. In this respect, the individual has the right to check information, to examine records and to be

[119] Fundamental right to data protection, Tinnefeld/Petri/Brink, 2010, p. 727. Cf. further Schaar, 2008. and also the brochure of the Federal Agency for Data Protection and Freedom of Information, accessible from: http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/Dokumentation25JahreVolkszaehlungsurteil.pdf?__blob=publicationFile [05.05.2011.]

[120] Concerning the vulnerability of the fundamental rights within employments cf. e.g. Müller-Glöge, 2009, mgn. 278-293.

[121] Gola/Wronka, 2010, mgn. 7.

[122] Gola, 2010a, mgn. 45. Thus, for instance, according to § 75 par. 2 s. 1 BetrVG employers and works councils have the duty to protect and promote the free development of the personality of the employees. Further they have to promote the independency and the initiatives of the employees. The right to informational self-determination was developed by the Federal Constitutional Court in its so-called census adjudication (BVerfGE 65, 1).

[123] BVerfGE 65, 1, 44.

[124] BVerfGE 65, 1, 44.

[125] BVerfGE 65, 1, 45.

[126] Tinnefeld/Petri/Brink, 2010, p. 727.

[127] Cf. to this aspect Gola/Wronka, 2010, mgn. 454 ff.

[128] BVerfG, NJW 2010, p. 839; 1 BvR 370/07 with reference to BVerfGE 65, 1, 42.

[129] BVerfGE 65, 1, 44-45.

[130] BVerfGE 109, 279, 291.

notified of relevant matters, to correct data, to block or even delete it.[131] The person involved has also the opportunity to find legal remedies and turn to the data protection authority.[132]

The precedence of the personality right protection over the right to ensure the integrity and confidentiality of information technology systems[133]

Of recent rulings, that of the Federal Constitutional Court in its decision in respect of online searches has developed the fundamental right to guarantee the confidentiality and integrity of information technology systems should be mentioned.[134] This expands the guarantees derived from constitutional rights and from the rights to informational self-determination.[135] In this case the personal and material areas of the life of the individual are protected from access in the IT area if it is the information technology system as a whole which is accessed and not only the individual communication processes.[136] Secret access to the information technology system that an employee uses or can use are, according to this, not allowed.[137] In this case it is not only the confidentiality of saved data but also the ability to control the data in the processing that has to be protected.[138] The IT law is subsidiary and comes after, e.g., telecommunication privacy (Art. 10 Paragraph 1 GG) or the right to informational self-determination.[139] As a 'catch-all' fundamental right, it has the function to close loopholes in protection and, in this way, to broaden and unify the protection of the private sphere.[140] The new dangers, which can occur due to technical development and to new life-circumstances, can, in this way, be avoided.[141]

Further features of the personality right protection

The protection of the personality rights of employees can also be achieved in many cases in respect of their own word and image.[142]

The right to the spoken word[143]

The protection of the spoken word gives the individual the power to decide basically whether the content of a communication should be open only to his partner in conversation or to a wider circle also.[144] Spontaneous speech has to be protected against recording and subsequent replay at any time, and in this way the right of self-determination in connection with the

[131] Cf. BVerfGE 65, 1, 46; Tinnefeld/Petri/ Brink, 2010, p. 727.
[132] Cf. BVerfGE 65, 1, 46.
[133] So-called fundamental right to IT, Tinnefeld/Petri/ Brink, 2010, p. 727.
[134] NJW 2008, p. 822.
[135] Tinnefeld/Petri/ Brink, 2010, p. 727.
[136] BVerfG – 1 BvR 370/07, 1 BvR 595/07 (clause 201).
[137] Tinnefeld/Petri/Brink, 2010, pp. 727-728. on the problem of how far employees may use the IT-systems of the employer as their own, cf. BVerfG, NJW 2008, p. 822 as well as the case study by Petri, 2009, p. 55 ff.
[138] BVerfG, NJW 2008, p. 824.
[139] BVerfGE 120, 274, 302.
[140] Durner, 2011, Art. 10 GG mgn. 59.
[141] BVerfG, NJW 2008, p. 824 with reference to BVerfGE 54, 148, 153; 65, 1, 41; 118, 168.
[142] Cf. to this BVerfG – 1 BvR 1611/96; E 106, 28; BAG – 2 AZR 51/02, NZA 2003, 1193, 1194; 1 ABR 16/07, NZA 2008, p. 1189; Dieterich, 2011, Art. 2 GG mgn. 43.
[143] Concerning the right of the spoken word cf. BVerfGE 34, 238, 246 f.; 54, 148, 154.
[144] BVerfGE 54, 148, 153; BGHZ 27, 284, 286; BAGE 80, 366, 376; Dieterich, 2011, Art. 2 GG mgn. 43.

spoken word is also protected.[145] This relates to categories such as secret voice-recordings[146] or listening with the help of monitoring equipment.[147] Concerning the level of protection, there is no congruity with the right to privacy.[148] The right to the spoken word protects in general the self-determination of certain sensitive conversation contents on the one hand and, on the other, it restricts the place of the conversation from the domain of the private sphere.[149]

The right to the written word

As one part of the personality rights, right to the written word include the right to not to publish certain private notes – the so-called privacy of correspondence.[150] In particular, right to the written word have increased significance in an individual's working life, where they may involve documents, such as letters relating to job applications.[151]

The right to an individual's own picture

By the right to one's own picture, the individual is protected from all forms of unauthorised copies, the circulating either in a material way or by means of technical equipment directly transmitting images of his personal appearance.[152] In this way, the person concerned has the kind of self-determination right which means that it is basically his decision as to if, how and when he would like to present himself to third parties or to the public[153] and, further, who may save, use and transmit the data in the form of a picture.[154] We can exemplify such a violation of a right in the field of video-monitoring measurements. The legal regulations of the right to one's own image are §§ 22 ff. KUG and § 201a StGB (Penalty Law Code).[155]

The protection of the confidentiality of communication in Art. 10 GG

A further matter to be protected, belonging to the category of personality rights, includes Art. 10 GG – for the individual the guarantee of the confidentiality of communication.[156]

According to the postulation of Art. 10 Abs. 1 GG, the confidentiality of both correspondence and of the post and telegraph-services are inviolable. Art. 10 GG includes an important guarantee of freedom which supersedes the general guarantee of Art. 2 Abs. 1 i.V.m. Art. 1 Abs. GG.[157] Art. 10 GG is applied independently of the content and method of sending a letter or of sending a message via telecommunication.[158] All forms of transmission of information by means of telecommunication equipment belong to the field.[159] An important connection for

[145] BGHZ 80, 25, 42; BVerfG, NJW 1992, p. 816.
[146] BVerfG 1992, 815, 816; BAG, NJW 1998, 1331, 1332.
[147] Gola, 2010a, mgn. 48.
[148] BVerfGE 106, 28, 41.
[149] Gola, 2010a, mgn. 49. Cf. further BGH, NJW 2003, p. 1728.
[150] Gola, 2010a, mgn. 51.
[151] Cf. further BVerfGE 80, 367.
[152] Gola, 2010a, mgn. 58.
[153] BVerfGE 63, 131 and 142; constant jurisdiction of the BGH, cf. NJW 1996, p. 986 with further references.
[154] Gola, 2010a, mgn. 58.
[155] Seitz, 2011, part 8 mgn. 6.
[156] BVerfGE 85, 386, 398; 100, 313, 366; 115, 166, 183; Gola, 2010a, mgn. 94.
[157] BVerfGE 67, 157, 171; 100, 313, 358.
[158] Gola, 2010a, mgn. 94.
[159] BVerfGE 85, 386, 396; 100, 313, 358.

the confidentiality of telecommunication is the actual medium of communication used and the dangers of confidentiality which result from the use of the medium.[160] The protection involves the whole process of communication as such – that is, the time from the beginning to the end of the transmission.[161] When the protection actually starts has so far not been discussed either by the jurisdiction nor by the literature,[162] but, according to the BVerfGe (Federal Constitutional Court), protection ceases "at the moment when the message has arrived at the addressee and the transmission process is over".[163] Besides its preventive-legal nature (protection against learning the contents and the more detailed circumstances of the telecommunication through the state) there is included the secrecy of the telecommunication and at the same time the requirement that the state must protect the individual insofar as there are third parties who run telecommunications[164] operations.

The limitation of the secrecy of telecommunication to the right to information self-determination applies depending on whether or not the data are outside the sphere of the person involved.[165] Data connected with communications which are retained in the domain of a participant in the communication no longer enjoy the protection of Art. 10 Abs. 1 GG, but they are protected by the right to informational self-determination. The protection of the secrecy of telecommunications ends when the process of the transfer of the information is over and the addressee has actual possession of the data.[166] The specific dangers of distance-(i.e. tele)communication no longer exist for the addressee, since he has the power to take appropriate precautions against unwanted data-access.[167]

1.2.3.1.2. Limitations of the personality rights of the employee

As is the case with other fundamental rights, the personal rights of the employee do not require absolute protection.[168] When examining a breach of personal rights we must also take into consideration the relevant personal rights of the employer.[169] Personal protection is, hence, limited by the valid (company) interests of the employer.[170] Breaches of the personal rights of the employee can, therefore, be justified by accepting the greater validity of the interests of the employer.[171]

This conflict of fundamental rights is to be harmonised in such a way that the conflicting rights can be harmonised most reasonably.[172] In respect of the employer, the fundamental rights in addition to economic freedom of action (Art. 2 Abs. 2 GG), the freedom to exercise his profession (Art. 12 Abs. 1 GG) and his rights in respect of ownership (Art. 14 Abs. 1 GG)

[160] BVerfGE 124, 43, 54 f.
[161] Gerhards, 2010, p. 192.
[162] De Wolf, 2010, p. 1209.
[163] BVerfGE 115, 166, 184.
[164] BVerfG, NJW 2002, p. 3620; Gola, 2010a, mgn. 95.
[165] BVerfG, NJW 2006, p. 976.
[166] BVerfG, NJW 2006, p. 978. Gerhards, 2010, p. 193; de Wolf, 2010, p. 1209; Vietmeyer/Byers, 2010, p. 809.
[167] BVerfGE 115, 166, 184; BVerfG, NJW 2008, p. 825.
[168] Tinnefeld/Petri/Brink, 2010, p.728.
[169] Or the related interests of the colleagues of the employee, Moll, 2009, § 32 BDSG mgn. 45.
[170] Tinnefeld/Petri/Brink, 2010, p. 728. Moll, 2009, § 32 BDSG mgn. 45.
[171] BAG – 2 AZR 485/08 remark 36.
[172] Dieterich, 2011, introd. mgn. 71.

should be considered.[173] Even in respect of important interests of the employer (such as issues of legal compliance)[174] the principles of data protection must also be taken into consideration to an appropriate degree.[175] This assessment mechanism is incorporated also in the level of simple law, such as in the BDSG, where the weighing of the interests of the persons involved and those of the data-processors plays a central role in connection with the admissibility of the data processing.

The different regulations in the public and private sectors

Within the public and the private sectors there are a large number of regulations at both federal and provincial (Land) level that can be of importance in connection with breaches of personal rights in the workplace. In the public sphere we can find sector-specific regulations on reporting and archiving systems in the field of social-data protection or in education, in the medical sphere or in relation to the security (i.e. police) authorities. Within the private sector there are, among others, regulations introduced for the handling of multimedia in the field of ICT in Telecommunications Act or in Telemedia Act.[176] It should be emphasised that in the usually relevant field of regulation of the federal data protection law § 12 Abs. 4 BDSG, in the case of the legal relations of employees in the public sector there is frequent reference to regulations applicable to the private sector.[177] The purpose of this norm is, on the one hand, to provide for those working for the public sector a uniform data protection right.[178] On the other hand it ensures the principle of equal treatment in public and non-public working-relations.[179] Beyond §§ 2 Abs. 4, 1 Abs. 2 Nr. 3 BDSG the application field of the BDSG relates to all private employers, so that also personnel-relevant data enjoy uniform protection.[180]

The interest of the employer in monitoring the employee

There can be several sound motives on the part of the employer for carrying out monitoring. Basically, the employer may be interested in observing by video some process, department or the personnel located there, perhaps, for example, in a dangerous location such as a nuclear power-station.[181] In the telecommunication field several factors may play a role such as checking the loss of working time by employees using telecommunication services, the risk of damage to the firm's electronic-data-processing by viruses or spam via the internet and e-mail, the committing of a crime at the workplace,[182] unauthorised access to the e-mails of

[173] Tinnefeld/Petri/Brink, 2010, p.728.
[174] The concept of "compliance" is more commonly understood than the totality of organisational measures which are necessary for a business to conform wholly with the law. Tinnefeld/Petri/Brink, 2010, p. 728.
[175] Cf. to this aspect e.g. Petri, 2010, p. 305 ff.
[176] Gola/Wronka, 2010, mgn. 31.
[177] For a critique of the regulation cf. Heckmann, 2010, § 12 BDSG mgn. 29 by reference to e.g. Dammann, 2011, § 12 mgn. 22 and Simitis, 1989, pp.52-53. Cf. also Gola/Wronka, 2010, mgn. 216 ff. In spite of the change in EC data protection law, the basic separation between public and non-public areas has been maintained.
[178] Gola/Schomerus, 2010, § 12 BDSG mgn. 7.
[179] Wedde, 2009, § 12 BDSG mgn. 14.
[180] Cf. Weißnicht, 2003, p. 450; Mengel, 2004b, p. 2015.
[181] Gola/Wronka, 2010, mgn. 833.
[182] With the accompanying danger of damage to the reputation of the employer cf. Tinnefeld/Petri/Brink, 2010, p. 728. with reference to the ruling of the Federal Labour Court (NJW 2006, 2939 ; E 111, 291) as an example: the downloading of pornography.

employees in their absence[183] as well as generally doing everything possible to ensure smooth running[184] and avoiding the responsibility for criminal or for civil offences and obligations to provide information to the security authority[185] could play the role.[186] For example, committing an offence in relation to the employer-employee relationship may well lead to a loss of reputation by the employer.[187] In general, taking the side of the employee too early, without careful thought and without considering the interests of the employer is something to be avoided.

The limits of supervision: the line between legal and illegal monitoring

Deciding the permitted limits to the monitoring of employees is currently a rather difficult problem for employers. A major factor in the question of whether the employer has such a right and, if he has, then to what extent, must, in the light of the conflicting legal interests of employer and of employee, be considered in terms of proportionality.[188] There may actually be situations in which an overriding and justified interest of the employer is present if we for the moment ignore the purpose of a working relationship (the exchange of labour for remuneration).[189] Taking technical developments into account, there is, for example, a justified interest of the employer concerning the right of information self-determination of the employee through the use of technical equipment "to seek the information for which he has a valid need in an economically rational way, rapidly and at a reasonable cost."[190] It is expressly forbidden to formulate general answers in defining the border-line between legal and illegal monitoring. Any evaluation and analysis of the data protection law context must be individual case-dependent and should be carried out in the light of the overall situation.[191]

1.2.4. Legal sources of national data protection law in Germany

In addition to the constitutional principles[192] a number of various legal sources have gained increasing significance in terms of privacy at the workplace.[193]

1.2.4.1. BDSG and field-specific data protection regulations

When it comes to field-specific sets of facts in the field of employee data protection, the German law offers – in the absence of a field-specific employee data protection law – a number of statutes and statutory orders to cover this topic.[194] According to the subsidiarity

[183] Vietmeyer/Byers, 2010, p. 808.
[184] Cf. Pauly/Osnabrügge, 2009, § 6 mgn. 128.
[185] Gola, 2010a, mgn. 28, 29, 198.
[186] Cf. to this aspect Holzner, 2011, p. 13 which opposes cost-risk analysis and also working time argumentation.
[187] Pauly/Osnabrügge, 2009, § 6 mgn. 127.
[188] In several decisions the Federal Labour Law has addressed this problem (cf. e.g. NJW 1984, p. 2910; NJW 1986, p. 2724 or recently NZA 2011, p. 571).
[189] BAG, NJW 1986, 2724, 2726; Pauly/Osnabrügge, 2009, § 6 mgn. 43.
[190] BAG, NJW 1986, 2724, 2726.
[191] BVerfG NJW 2002, 3619, 3624 by reference to E 34, 238, 248; 367, 373 ff.
[192] Cf. in details in the following chapter.
[193] To the question of whether the private data protection should be integrated into the Civil Code (BGB), cf. the controversy between Steffen and Weichert, 2009, p. 95.
[194] E.g. AEntG, AFBG, AGG, AktG, AltZG, AO, ArbMedV, ArbSchG, ArbSiG, ArbZG, AÜG, AufenthG, AWG, BbiG, BetrVG, BGB, BildscharbV, BKV, DEÜV, EntgFG, EStG, FeV, FreizügG/EU, GenG, GenDG, GewO, GGBefG, GefStoffV, HeimarbeitsG, HGB, IfSG, JArbSchG, KUrhG, LadSchlG, LuftSiG, SGB 2-7, 9-

clause of § 1 par. 3 s. 1 of the Federal Data Protection Act the federal legislation has priority, which provide for the processing of personal data including the disclosure thereof.[195] The obligation to observe the legal confidentiality obligations or the professional and special administrative confidentiality, which are not based on legal regulations, remains unchanged according to § 1 par. 3 s. 1 of the BDSG. The relation between the special data protection law and the German National Data Protection Act[196] is the consequence of the principle included in Article 31 of the Constitution (federal law takes precedence over state law), according to which the federal special data protection law enjoys primacy of application.[197]

1.2.4.2. Data protection in scope of the federal data protection law

Frequently there are no field-specific regulations, thus the processing[198] of employees' data should be assessed against the provisions of the Federal Data Protection Act.

1.2.4.2.1. § 32 of the BDSG as the basic regulation for employee data protection

Up till now, within the Federal Data Protection Act labour law issues have not been taken seriously. Within the scope of preventive prohibition with the obligation to seek permission of § 4 par. 1 of the Federal Data Protection Act,[199] § 32 of the BDSG includes as basic regulation for employee data protection in par. 1 diverse permissions regarding the data processing in the employment relationship.[200]

1.2.4.2.2. Fundamental facts, and § 32 par. 1 s. 1. of BDSG

§ 32 par. 1 s. 1 of Federal Data Protection Act includes three different permissions, pursuant to which it is possible to derogate the prohibition with § 4 par. 1 of the BDSG. In order to open up the personal scope of application of § 32 par. 1 s. 1 of the Federal Data Protection Act, in the case of those affected it must be an employed person pursuant to § 3 par. 11 of the Act. The concept is defined broadly and is not in compliance with the social security concept of the employed person, which in relates only to employees.[201] It rather embraces also among others persons employed for vocational training, personnel with the same status as employees, applicants and persons whose employment relationship has terminated.[202] Pursuant to § 32 par. 1. s. 1. of the Federal Data Protection Act the admissibility of the processing of employee

---

10, SÜG, StGB, StPO, StVG, TKG, TMG, UrhG, VVG, ZPO, cf. Tinnefeld/Petri/Brink, 2010, p. 728 mgn. 27. Cf. also the enumeration in Thon, 2006, p. 137. Regarding details, these are impossible to review due to their enormous scale. In this respect their follows merely a simple outline example, which cannot claim to be at all complete.

[195] Schmidt, 2010, § 1 BDSG mgn. 32.

[196] Däubler, 2010, mgn. 49. Cf. also http://www.datenschutz.de

[197] Schmidt, 2010, § 1 BDSG mgn. 32.

[198] Regarding the terminology see § 3 para 1. of the BDSG and Zöll, 2010, § 32 BDSG, mgn. 1.

[199] In general the admissibility of the handling of personal data can be proved, apart from any agreement by the concerned party, by the legal permission deriving from the BDSG according to the merits of the case, or legal provisions which permit or order the specific handling of data (among which are found perhaps in-house wage agreements) is not dealt with separately. Cf. also Franzen, 2010, pp. 259-260; §§ 227 BGB, §§ 32, 34 StGB which, inter alia, should also produce legal provisions in this sense (cf. e.g. BAG, NJW 2005, 313, 316 as well as Richardi/Korstock, 2005, p. 382; doubting Bayreuther, 2005, p. 1040; in the outcome also Grosjean, 2003, p. 2651).

[200] Zöll, 2010, § 32 BDSG mgn. 1. Concerning the historical background cf. Schmidt, 2009a, p. 200.

[201] Zöll, 2010, § 32 BDSG mgn. 13.

[202] Bundestag, 2009a, p. 27; cf. § 3 par. 11 BDSG.

data may arise for the purpose of the employment relationship. In this sense, permitted employment purposes may arise from the legislative requirements, collective agreements as well as from the labour contract.[203] In contrast to the wording, besides the purposes precisely defined in the law[204] all other purposes of the employment relationship should be permitted.[205] Having regard to the wording of § 32 par. 1 s. 1 of the BDSG, the requirements of data processing must meet the necessity criterion.[206] According to the will of the legislature[207] the characteristic of necessity is understood to the largest extent in a sense that a proportionality check must be performed.[208] During this it must be first checked whether the processing of personal data can be abandoned or at least there are means available that are although a less intensive but equally suitable for achieving the objective. Subsequently, in a second step it must be asked whether, after due consideration of the interests of employers and employees, the processing of employee data is appropriate for the purpose of employment. The necessity test takes thereby a subjective benchmark as basis, consequently, it must be performed regarding a specific individual situation and by assessing the specific facts.[209]

1.2.4.2.3. Identification of offences, § 32 par. 1 s. 2 BDSG

In relation to the basic offence § 32 par. 1 s. 2 BDSG [210] imposes stricter requirements, in case the admissibility of data processing is considered for disclosure of criminal offences.[211] Pursuant to the wording of the legislation, in addition to offences committed in connection with the work item, those are also embraced which are committed only the occasion of employment.[212] Purely defaulting or unlawful conduct falls on the other hand within the scope of § 32 par. 1 s. 1 BDSG, which governs other violations of the law.[213] Having regard to the final half-sentence of the norm, within the scope of weighing up of interests, in particular the nature and extent in relation to the reason must not to be disproportionately. According to the explanatory memorandum, by the reason of data collection on the one hand the nature and severity of the offence and on the other hand the intensity of suspicion is meant.[214] The greater the weight of suspicion and the more severe the damage to or threat to the legally protected interest, the more intense can be the intervention in the personality rights of employees. However, intrusive measures must only be the last resort (ultima ratio).[215] Regarding the weighting of conflicting interests it is recommended, as far as possible to

[203] Gola/Schomerus, 2010, § 28 BDSG mgn. 14 f.; Simitis, 2010, § 28 BDSG mgn. 101 ff.; Lembke, 2010, intr. BDSG mgn. 41; Zöll, 2010, § 32 BDSG mgn. 15.
[204] That is, establishing, implementing and terminating the employment relationship
[205] Zöll, 2010, § 32 BDSG mgn. 17, Thüsing, 2009, p. 867.
[206] Cf. to this criterion the critique mentioned by Thüsing, 2009, p. 867.
[207] Bundestag, 2009a, pp. 35-36. With reference to the decision of the BAG (BAGE 46, 98 = NZA, 1984, 321; BAG, NZA 1985, 57; BAGE, 81, 15 = NZA 1996, 536, 528; BAGE 53, 226 = DB 1987, 1048).
[208] Schmidt, 2009a, pp. 198-199.
[209] Zöll, 2010, § 32 BDSG mgn. 17.
[210] The wording of this provision corresponds with § 100 par. 3 s. 1 TKG, Cf. Thüsing, 2009, p. 868 by reference to BAG, NZA 2003, 1193 and NZA 2008, 1187.
[211] E.g. theft and corruption, Bundestag, printed matter 16/13657, p. 36. Regarding the question as to the relationship between § 32 Para. 1 S. 1 and S.2 BDSG, see cf. Franzen, 2010, pp. 260-261.
[212] Deutsch/Diller, 2009, p. 1462.
[213] Bundestag, 2009a, p. 36; Schmidt, 2009a, p. 195; regarding the problematic features of the regulation.
[214] Bundestag, 2009a, p. 36.
[215] Zöll, 2010, § 32 BDSG mgn. 46.

recourse[216] to the jurisprudence of the Federal Constitutional Court.[217] In case of information-related fundamental right interventions by the government the weight of the curtailment depends among others upon which content is covered by the curtailment, in particular the degree of personal relevance of the information concerned each have on their own and in their connection with others and the means by which these contents were acquired.[218] Furthermore, the extent of impairment of the right to informational self-determination depends on the threat or not groundless fears of consequences of data collection for those concerned.[219] The secrecy of an action leads thereby to increase of its intensity.[220]

1.2.4.2.4. § 32 par. 2 BDSG as extension for manual data processing

Pursuant to § 32 par. 2 of the Federal Data Protection Act paragraph 1 shall be applied also regarding the manual data processing.[221] According to the explanatory memorandum, in this respect the principles of data protection in employment relationship are dealt with.[222] Thus any employee-related data collections (e.g. records of managers and interviewers from job interviews and annual management discussions, as well as any notes taken about the personal performance) are subject to the scope of § 32 par. 1 BDSG.[223]

1.2.4.2.5. Competition with Article 28 of Federal Data Protection Act[224]

So far the relationship between Article 32 and Article 28 of the BDSG has been clarified insufficiently. According to the explanatory memorandum, through the revision of Article 32 of the Federal Data Protection Act the principles of employment data protection developed by the jurisprudence should not be changed, but only summarized.[225] In this respect, some suggested, to recourse mainly to the principles developed for Article 28 of the Federal Data Protection Act.[226] According to the explanatory memorandum for employment purposes Article 32 of the Federal Data Protection Act substantiates[227] and rules out Article 28 para 1 sentence 1 No. 1 of the Federal Data Protection Act[228] and thus represents a special rule (lex specialis).[229] Similarly, § 28 par. 1 s. 2 BDSG shall also be ruled out.[230] Furthermore, in addition to Article 32 also Article 28 paragraph 3 sentence 1 No. 1 and Article 28 paragraph 1

---

[216] BVerfGE 115, 320.
[217] Thüsing, 2009, p. 868, who approaches the reciprocal relationships of the parties in a contract of employment from a central perspective, and, further Hillgruber, 2007, p. 209 and Bausback, 2006, p. 1922.
[218] BVerfGE 115, 320, 347 by reference to E 100, 313, 376; 107, 299, 318 ff.; 109, 279, 353.
[219] BVerfGE 115, 320, 347 by reference to E 100, 313, 376; 109, 279, 353.
[220] BVerfGE 115, 320, 353 by reference to E 107, 299, 321; NJW 2006, 976, 981.
[221] Cf. re the extension of the scope of the BDSG also § 8 Para. 1 BewachV.
[222] Bundestag, 2009a, p. 37 with reference to BAGE 54, 365; 119, 238.
[223] Wank, 2010, § 32 BDSG mgn. 2.
[224] Insofar as, under point 2, a permissible form of legal surveillance takes place, the reader is required to recall in its entirety the relationship of § 32 BDSG to § 28 BDSG.
[225] Bundestag, 2009a, p. 35.
[226] Wellhöner/Byers, 2009, p. 2311. Critical: Thüsing, 2010, mgn. 58 ff.
[227] In contradiction: Thüsing, 2009, p. 867.
[228] Bundestag, 2009a, p. 34.
[229] Zöll, 2010, § 32 BDSG mgn. 5.
[230] Bundestag, 2009a, p. 34; This criticises somewhat Vogel/Glas, 2009, pp. 1750-1751. Thüsing, (2009, p. 869) speaking even of an 'error of legislative motivation' and assumes that § 28 Para. 1 S. 2 BDSG applies (v Däubler, 2010, marginal no. 186). Other (Deutsch/Diller, 2009, p. 1465) feared, specific applications in connection with labour relations cannot be implemented in the future as problems arise with handling the law in practice.

sentence 1 No. 2 shall be applicable.[231] However, in individual cases here are many questions open, so that there is no legal clarity.[232]

1.2.4.3. Outlook: Revision of employee data protection, §§ 32-32l in the new BDSG

Since the introduction of § 32 of the Federal Data Protection Act, the literature often deals with the analysis of this provision.[233] In connection with the criticism voiced, people were even talking about an "ad-hoc, symbolic legislation", "which reacts too hastily and therefore it follows a political rather than a factual logic".[234] Following the frequently expressed desire for a comprehensive codification of a separate employee data protection law[235] the federal government has decided[236] on the 25th October 2010 to "draft a law regulating the employment data protection".[237] Concerning the opinion of the Federal Council of 11th May 2010,[238] the federal government adopted position then again on 15th December 2010.[239] Recently, in the 25th February 2011 the Bundestag discussed the bill of the federal government in the first reading.[240] On the 23th May 2011 within the scope of a public hearing of experts in the Interior Committee of the Bundestag the government draft bill was controversially discussed. In addition to the bill provided by the Federal Government, there were two additional bills of the SPD fraction[241] as well as of the Alliance 90/The Greens,[242] whom was also granted a hearing on the 23th May 2011.

The bill provided by the federal government provides for not adopting an own employee data protection law, but to codify the treatment of personal data of employees merely in the BDSG.[243] Thus, the current Article 32 of the Federal Data Protection Act shall be replaced by Articles 32-32l of the new version of the Federal Data Protection Act as follows:

- Article 32 Data collection before the establishment of an employment relationship
- Article 32a Medical examinations and aptitude tests before the establishment of an employment relationship
- Article 32b Data processing before the establishment of an employment relationship
- Article 32c Data collection during the employment relationship

---

[231] At least according to the legislator's will, Bundestag, 2009a, p. 35. This is controversial, cf. Thüsing, 2009, p. 869; as well as Grentzenberg/Schreibauer/Schuppert, 2009, pp.539-540. and Zöll, 2010, § 32 BDSG mgn. 6.
[232] Thüsing, 2009, p. 869.
[233] Cf. the contributions of Albrecht/Maisch, 2010, p. 11.; Behling, 2010, p. 892.; Beisenherz/Tinnefeld, 2010, p. 221.; Forst, 2010, p. 8.; Kamp/Körffer, 2010, p. 72.; Kramer, 2010, p. 14.; Salvenmoser/Hauschka, 2010, p. 331.; Kort, 2011, p. 294; and also the papers of Däubler, 2010, mgn.183. and Gola/Wronka, 2010, mgn. 847. ff.
[234] Thüsing, 2010, mgn. 77.
[235] So the academic debate goes backwards cf. e.g. Simitis, 1981 or Zöllner, 1983. Cf. further Fleck, 2003, p. 306 as well as Grobys, 2003, p. 682 and Simitis, 2003, p. 43.
[236] Bundestag, 2010a.
[237] In its approach the Federal Ministry of the Interior (BMI) has already published several drafts (cf. Bundesministerium des Innern, 2010.) which met the critics.
[238] Bundesrat, 2010.
[239] Bundestag, 2010b.
[240] Re the opinions of a speaker in the Bundestag cf. Wybitul, 2011, 315091.
[241] Bundestag, 2009b.
[242] Bundestag, 2011.
[243] Here is the implementation of the agreement of the Government Coalition Parties cf. CDU/CSU/FDP, 2009, p. 106.

- Article 32d Data processing and usage during the employment relationship
- Article 32e Data collection without the knowledge of employees to detect and prevent offences and other serious violation of obligations during the employment relationship
- Article 32f Observation of publicly not accessible business establishments with optical-electronic devices
- Article 32g Positioning systems
- Article 32h Biometric processes
- Article 32i Use of telecommunication services
- Article 32j Obligation to inform
- Article 32k Amendments
- Article 32l Consent, scope for third parties, rights of interest group organisations, right to appeal, mandatory provisions

1.2.5. Self-regulation in Hungary[244]

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.)[245] 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 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.[246]

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.[247] However, the Labour Code does not contain any regulation on the supervision of the worker's use of technical tools, apart from teleworkers, 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

[244] This chapter was written with the respectable and honoured help of Dr. Erika Kovács.
[245] Arany Tóth, 2008b, p. 170.
[246] Cf. Arany Tóth, 2008a pp. 307-308.
[247] Labour Code § 13(3)

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.[248] 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.

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.

1.2.6. The concept of self-regulation in Germany

Self-regulation[249] may serve as the means of the safeguards of data protection interests.[250] Thus Article 27 of the European Data Protection Directive[251] determines the framework for a code of conduct for places to be processed by associations, which was implemented with the introduction of Article 38a of the Federal Data Protection Act.[252] The objective of § 38a of the BDSG is, among others, to standardize the internal codes of conduct in order to promote and

[248] Fodor/Nacsa/Neumann, 2008.
[249] Self-regulation is argued by Franzen 2010, pp. 260-261.
[250] Weichert/Kilian, 2011, part 13 ch. 5.1 mgn. 46.
[251] Directive 95/46/EC
[252] Weichert/Kilian, 2010, part 13 ch. 5.1 mgn. 48.

implement data protection regulations.[253] The code of conduct is examined by the supervisory authorities (principle of self-regulation).[254] Codes of conduct are not on the same level as legal norms, and are therefore, in principle, not binding. However, if they are approved by the supervisory authorities, they have a binding effect in accordance with the principle of self-commitment of the administration.[255] Although the establishment of a code of conduct would create on the one hand legal certainty and industry-specific data flows,[256] and on the other hand, the transparency of the type of data treatment would increase for those concerned,[257] the model of self-regulation concerning employee data protection could not be realised so far in Germany to the extent as this was sometimes required by the BITKOM.[258][259] In his theses drafted for the foundations of a common network policy of the future, the then Federal Minister THOMAS DE MAIZIERE declared himself in favour of strengthening self-regulation.[260] This trend is followed by his successor in office, DR. HANS-PETER FRIEDRICH and stressed in particular that "the way of self-regulation (...) (should) be continued".[261] On the part of the data protection commissioner the development of self-regulation tends to take place with concern and the mere conception of a regulated self-regulation is to be considered as insufficient.[262] In this respect we must wait to see how the regulated framework of self-regulation will be developed in the future in the area of employee data protection.

1.3. Mutual dependence

The employment relationship is, in general, a continuing account of mutual indebtedness.[263] This relationship is typically marked by a higher degree of obligation between the parties.[264] For these parties the employment contract means that they must be highly dependent on each other within the relationship. This leads us again to the question as to whether the employee has any effective possibility to disagree to the use of his personal data. At the same time it is questionable if the employer is able to block the misuse of data by the employee.

1.3.1. 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

[253] Bundestag, 2000a, p. 30.
[254] Roßnagel, 2003, ch. 3.6, mgn. 47 f; 68 ff.
[255] Weichert/Kilian, 2010, part 13 ch. 5.1 mgn. 49.
[256] State parliament Schleswig-Holstein, 2009, p. 89.
[257] Kinast, 2010, § 38a BDSG mgn. 3.
[258] Federal Association for Information Technology, Telecommunications and New Media.
[259] Cf. in detail the Internet page of BITKOM (http://www.bitkom.org). Most recent example of the framework for self-regulation of Data Protection re RFID (cf. the previous detailed sub-sections 2.5.1.3) endorsed, which was welcomed by Heinz Paul Bonn, Vice-President of BITKOM, cf. Bonn, 2011. and Kempf, 2011.
[260] Cf. de Mazière, 2010.
[261] Friedrich, 2011.
[262] Cf. just the critical statement of the Federal Commissioner for Data Protection and Freedom of Information Peter Schaar (2011) as well as the statement of the Commissioner for Data Protection and Freedom of Information of Hamburg Prof. Dr. Johannes Caspar within the scope of an interview with the author (2011).
[263] Müller-Glöge, 2009, § 611 BGB mgn. 16.
[264] Kramer, 2007, book 2 introd. mgn. 97.

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.[265]

In the directive on data protection the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed[266] in respect of a specific case and with knowledge of the facts of the case, through which the person involved accepts that person-relevant data concerning him can be processed.[267] The possibility that parity in a contact may be disturbed and, hence, the negotiating balance between the two[268] could mean that a situation involving compulsion might arise to the disadvantage of the employee.[269] Therefore one of the main features of consent in work-practice is the criterion of voluntariness.[270] It is a matter of dispute whether, under the circumstances of an employer-employee relationship, consent can be given effectively at all. Some of the literature rejects the possibility of consent in general[271] with, among other reasons, the explanation that illegal intrusions in the person rights of the employee cannot be legitimised by consent,[272] as the employee would lack the necessary independence.[273] In this way there could be the permanent danger that consent was the result of the abuse f the employer's position of power.[274] Neither can it be prevented that the employer provides a clause according to which the employee declares that, when making his decision to consent, he was under no form of pressure.[275] The situation would be different if there were a works council and if outline conditions had been negotiated with them.[276] Others are of the opinion that a general and unlimited refusal of voluntary consent would not be possible,[277] and it is recommended that a free decision by the employee should not be refused since this might allow for effective consent in cases where consent has neither been forced nor obtained by deception.[278] Very often, however, the individual has practically no right of choice concerning the erasure of his data[279] This is only

[265] This is the general view in the literature. Cf. Arany Tóth, 2004b, pp. 15-17; Majtényi, 2006, p. 332; Hartai, 2003, p. 46.
[266] On the requirements for voluntariness within the meaning of § 4a par. 1 s. 1 BDSG cf. BGHZ 177, 253, 254 as well as Maties, 2008, p. 2220.
[267] 95/46/EC Art. 2. In German Law the term consent is also defined as prior agreement, § 183 BGB, Gola/Schumerus, 2010, § 4a BDSG mgn. 2.
[268] Gola/Schomerus, 2010, § 4a BDSG mgn.6 f.
[269] Büllesbach, 2003, ch. 6.1, mgn. 14; Gola, 2002, p. 110; Simitis, 2011, § 4a BDSG mgn. 64 f.; Backes/Eul/Guthmann/Martwich/Schmidt, 2004, p. 159; Schmidt, 2009b, p. 1298;
[270] Cf. to this Wedde, 2009, § 28 BDSG mgn. 24; Richardi/Kortstock, 2005, p. 384; Maties, 2008, p. 2220.
[271] E.g. Simitis, 1999, p. 628; Simitis, 2001, p. 431; Meyer, 2008, p. 372; Meyer, 2009, p.16; Trittin/Fischer, 2009, p. 344.
[272] Kunst, 2003, p. 77.
[273] Schrader, 2002, p. 197; similar Meyer, 2009, p. 17.
[274] Däubler, 2005, p. 770; Gola/Schomerus, 2010, § 4a BDSG mgn. 7.
[275] Meyer, 2009, p. 17.
[276] Gola/Schomerus, 2010, § 4a BDSG mgn. 9. on the relationship between consent and in-house agreement. On questions of industrial constitutional law cf. in detail Roloff, 2009, § 5 mgn. 53 ff.
[277] Taeger, 2010, § 4a mgn. 60; Hilber, 2005, p. 147; Hold, 2006, p. 252; Schuster, 2009, pp. 135-136; Müller, 2008, p. 36.
[278] Grimm/Schiefer, 2009, p. 337.
[279] Wohlgemuth, 1988, mgn. 12; Gola, 2010a, mgn. 324.

true in the context that practising his profession ultimately serves shaping and maintaining his livelihood.[280] Besides this financial factor, his standing in relation to his superiors or colleagues may also play a role. It is advisable however to obtain consent independently of the contract of employment, as linking the contract to consent might well suggest a possible lack of willingness or give the impression of compulsion.[281] Further, it should also be remembered that any restraint on free consent is a breach of European law, as Art 7 lit. a. of the Data Protection Directive declares consent as a basis of justification.[282]

1.3.2. 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. Therefore employers should have a legitimate interest in the protection of their data. The unauthorised disclosure of data to third parties threatens with serious disadvantages both in intangible and in economic terms.[283] This has special importance in relation to the monitoring of employees. Due to this, employers try to mitigate the loss through the involvement of internal security departments or investigation activities combined with preventive and detection measures.[284] This is actual almost impossible to the extent the employer intends to do. He has at least the possibility to protect his data against unauthorized access, perhaps through the implementation of effective security systems. However, the employer will eventually have to prepare himself to repressively sanction the abuse of data, in the course of which he takes action against the employee.[285] 'The defencelessness of the employers is increasing in the information age with novel and significant factors. Employers are experiencing 'the enemy attacking from within', and the fear of this is justified under the circumstances of the widespread possession of information technology."[286]

[280] Cf. fundamental BVerfGE 7, 377, 397 to the definition of job which enjoys protection under constitutional law (Art. 12 par. 1 GG, so-called freedom of profession.
[281] Maties, 2008, p. 2221.
[282] Forst, 2010, p. 1044.
[283] Regarding the prevention of economic crime by business enterprises cf. Langrock/Samson, 2007, p. 1684.
[284] Gastell, 2008, p. 2945.
[285] E.g. according to § 17 UWG (Unfair Competition Act) under German law.
[286] Majtényi, 2006, p. 333.

2. THE LEGAL REGULATION CONCERNING SELECTED MONITORING MEASURES

2.1. The regulation of correspondence monitoring

The content of the mail, and also 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 Directive 95/46/EC, therefore the monitoring of traditional mail (often referred to as 'snail-mail') may raise privacy issues. It has to be highlighted that mail which is sent from or received at a workplace is not only connected to the employee but 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. Hungarian regulation

2.1.1.1. Legislation

The content and other details of a mail should generally be regarded as personal data according to the Data Protection Act, similarly to the EU Directive. 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.[287] 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.[288]

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.[289] Telecommunications equipment is equipment which enables the transmission of electronic signals. Tapping or hacking shall mean any activity which is intended to illegally access the content of the correspondence.[290] The Criminal Code prescribes stricter sanctions if the crime is committed in a professional or official capacity or is the source of serious loss.[291]

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

[287] Civil Code § 81(1)
[288] Gálik/Polyák, 2005, p. 212.
[289] Criminal Code § 178
[290] Gálik/Polyák, 2005, pp. 213-213
[291] Criminal Code § 178(2),(3)

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 first and second case 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.

2.1.1.2. 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.

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.[292]

2.1.1.3. Judicial case law

There is no relevant judicial case law in this specific field.

2.1.1.4. Academic papers, scientific opinions

Referring to the case law of the Commissioner 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.[293]

[292] DPC, 120/A/2004.

2.1.2. German regulation

2.1.2.1. Legislation

When the issue concerns the monitoring of the correspondence of the employee, the question arises of whether this constitutes unjustifiable interference with the right to the written word.[294] Based on the *ratio legis* of Article 10 paragraph 1 old 1 GG, in order to protect the confidentiality of written communication, the term 'letter' covers all written messages between the sender and individual recipient in the form of individual communication. According to prevailing opinion, it does not matter whether the letter is closed or not, and so protection also extends to postcards.[295]

2.1.2.2. Cases from the jurisdiction

The jurisdiction has had to deal with the question of whether official mail may be opened by the employer. In this regard, it was stated that it does not mean a violation of the secrecy of correspondence if, within the scope of office rules, a department opens, stamps with the date of receipt and forwards to the employee concerned the mails addressed to employees and at the same time also to the given department if these are not marked as private or confidential.[296]

2.1.2.3. Academic debate

In the literature, the explanations of case law on the handling of official mail are drawn upon. Therefore, the criterion of marking as private or confidential is ignored and, on this basis, the personal rights granted to the employee are given priority.[297] Unlike business post, which may be accessed by the employer,[298] written messages that are apparently destined for the employee personally must be delivered sealed.[299]

2.1.3. Conclusion

We have to underline that the main goal of the research is to draw attention to the means of surveillance using new technologies in the workplace. Therefore on the regulation of correspondence monitoring only a summary can be given, as it can serve as a basis for the detailed analysis of email correspondence monitoring. We are concerned that the concept of legislation and jurisdiction is clear, dating back before the new technological equipments spread. As to conclude it, in both countries the employer can legally monitor the letters sent from the workplace as the letter was written during office hours and using the employer's

---

[293] Hegedűs, 2006a, p. 48.
[294] Protection of written correspondence is – apart from the constitutional law dimension – secured in particular by § 202 StGB.
[295] Durner, 2011, Art. 10 GG mgn. 68. Contrary view e.g. *Evers*, 1965, p. 662; *Marxen*, 1958, p. 22 ff.; *Groß, 2011, Art.* 10 GG mgn. 21; *Pagenkopf*, 2009, Art. 10 GG mgn. 12 and *Oehler*, 1954, p. 608 which demands merely that communication be closed.
[296] LAG Hamm, NZA-RR 2003, 346, 347. Cf. also BAG, NZA-RR 2011, 15 (extraordinary dismissal of an employee); RDV 2000, 23 (providing forenames in business letters) and BVerwG, RDV 2006, 124 (LS) on the use of handwritten records concerning an employee.
[297] Sassenberg/Bamberg, 2006, pp. 228-229; Gola/Wronka, 2010, mgn. 17.
[298] Pröpper/Römermann, 2008, p. 514; Wolf/Mulert, 2008, p. 443. (with further references).
[299] Gola/Wronka, 2010, mgn. 17.

tools. Contrary, letters addressed to an employee (especially if marked as private or confidential) shall not be opened by the employer unless the official character and content of communication can be clearly proven.

2.2. The monitoring of the use of computer, Internet and email in the workplace

The use of personal computers and notebooks (including the related accessories such as screen, software or printer) are nowadays indispensable at work for carrying out all the office work which is needed. Electronic monitoring refers to the use of computer technology and various tools and equipment in order to protect confidential knowledge and information related to the workplace, or to evaluate the speed, efficiency and effectiveness characteristics of an employee.[300] The regular use of devices like monitoring of keyboard input, use of computer applications, internet activities, and email or telephone communication generates a great deal of personal data.[301] 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. 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. Computer surveillance may also have a separating effect between workers and executives through the use of one-way monitoring that provides data to the executive that are not available to the worker.

Access to the organization's networked computers allows the employees to use Internet in working hours for a variety of legitimate purposes, what can be essential for many workers to carry out their tasks. Information gained through browsing the web can support the work; however monitoring can be important for the employer, as there is a rather high risk that employees use the Internet for private or illegitimate purposes in working hours. Downloading copyrighted or offensive materials; slowing down the flow of legitimate work-related traffic; and making the organization's networks and computers vulnerable to attacks needs the use of controlling measures in the workplace,[302] but may also breach the employee's privacy.[303]

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. Several tools and applications are available nowadays allowing for hidden email forwarding, mail analysis and reporting the communication of employees in the workplace.[304] However, email is also personal data – regardless of the private or official character of the communication - and it is

[300] Electronic Performance Monitoring takes many forms, such as access surveillance for monitoring entries and exits, the keystroke logging to monitor activities on individual computers, the tracking of an employee throughout a complex, including trips to the washroom. With computer surveillance a complete record of every employer's movements is now theoretically possible. Petersen, 2007, p. 957.
[301] Petersen, 2007, p. 966.
[302] Stanton/Stam, 2006, pp. 30-31.
[303] Arany Tóth, 2008b, p 170, Hegedűs, 2006b, p. 81.
[304] Leopold/Meints, 2010, p. 222.

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. NILS and MEINTS argues that an overall internet and email policy should be defined in workplaces in order to give transparent advice to the employees and set limits on their possible use, while employers should strictly discriminate between email accounts that are used for private email at or from the workplace and those that are used for email on behalf of the employer only.[305]

2.2.1. Hungarian regulation

2.2.1.1. Legislation

There is no special regulation in connection to the monitoring of the use of computers, emails and Internet connections in the workplace, therefore the general rules of the Civil Code, Data Protection Act and Labour Code are applicable.

2.2.1.2. 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.

2.2.1.2.1. Cases on the monitoring of computers

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.[306]

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 as it was he/she who transferred or made accessible the data for another subject.[307] 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

[305] Leopold /Meints, 2010, p. 226.
[306] DPC, 866/A/2006
[307] DPC, 772/A/2000, DPC, 841/K/2002

competence of monitoring.[308] 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.[309]

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.[310] 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.[311]

2.2.1.2.2. Cases on the monitoring of Internet use by the employer

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.[312]

The Commissioner also emphasises that monitoring Internet usage should be based on the employee's consent, consent which is based on accurate information.[313] Later, the Commissioner stresses the need for these conditions.[314] If private Internet use is forbidden and

[308] DPC, 866/A/2006
[309] DPC, 531/A/2004
[310] DPC, 1012/K/2005
[311] DPC, 2511/K/2007
[312] 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.
[313] DPC, 531/A/2004
[314] DPC, 800/K/2008

the employee was informed of the possibility of monitoring, then the employee's action in opening a website is regarded as consent to monitoring.[315] 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.[316]

2.2.1.2.3. Cases on the monitoring of emails

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.[317]

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.[318]

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.[319]

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".[320] 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

[315] DPC, 1767/K/2006
[316] DPC, 570/A/2001
[317] DPC, 120/A/2004, DPC, 1543/A/2004
[318] DPC, 1722/A/2004
[319] DPC, 1393/K/2006
[320] DPC, 40/K/2006

heading of the e-mails […] and ask for a specific e-mail to look into'.[321] 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.

2.2.1.3. Judicial case law

There is no judicial case law in connection to the use of computers and emails by the employees or the privacy issues of monitoring Internet usage, however 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.[322] 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.[323]

2.2.1.4. Academic papers, scientific opinions

2.2.1.4.1. Issues connected to the monitoring of computers

After analysing the case law of the Commissioner, HEGEDŰS adds 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.[324]

2.2.1.4.2. Issues connected to the monitoring of Internet use by the employees

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.[325]

[321] DPC, 40/K/2006
[322] BH2006.64
[323] 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.
[324] Hegedűs, 2006b, pp. 82-83.
[325] Arany Tóth, 2008b, pp. 170-171.

If the employee may use the Internet for private purposes, the employer cannot monitor the websites opened.[326] If Internet use is only allowed for official purposes, then the employer 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.[327]

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,[328] we still think that the employer is not a subject of this regulation.[329]

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.[330] 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[331] – this can work in practice.

2.2.1.4.3. Issues connected to the monitoring of email communications

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,[332] and also a subject of the data 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.[333] 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.[334] 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-

[326] Arany Tóth, 2008b, p. 172.
[327] Hegedűs, 2006b, pp. 82-83.
[328] Arany Tóth, 2008b, p. 173.
[329] Cf. with the same opinion in chapter 2.2.4. on e-mail
[330] Arany Tóth, 2008b, p. 173, Hegedűs, 2006b, pp. 82-83, Jóri/Hegedűs/Kerekes, 2010, p. 288.
[331] Arany Tóth, 2008b, p. 173
[332] Gálik/Polyák, 2005, p. 212., Arany Tóth, 2008, p. 267, Hegedűs, 2006a, p. 47.
[333] Arany Tóth, 2008, p. 268., Hegedűs, 2006a, p. 48.
[334] Arany Tóth, 2008, p. 271., Hegedűs, 2006a, pp. 48-49., Majtényi, 2006, pp. 345-346.

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.[335]

Fourthly, academic papers also distinguish according to whether the e-mail was written by the employee or was received from a third party.[336] This distinction is based on the Data Protection Commissioner, and some authors agree,[337] 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.[338] 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, 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[339] should apply.[340] 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 something of a black hole: neither the Data Protection Commissioner nor academic papers[341] 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 is unclear.

2.2.2. German regulation

2.2.2.1. The employer's right to monitor personal computers or notebooks, internet and email usage

As a rule, there are no separate regulations in contracts of employment regarding the use of personal computers and notebooks. The activity of the employee is often described only generally and reference is made to workplace or job descriptions only rarely.[342] The use of PCs and notebooks is regulated individually on the basis of the right to manage of the employer, as the owner of the operational means and whose legal norm is the economy of operation in accordance with Article 315 of the Civil Code.[343] The common result of this is

[335] Arany Tóth, 2008, pp. 269-270., Hegedűs, 2006a, pp. 48-49; Szabó/Székely, 2005, pp. 263-265.
[336] In other words, whether is it internal correspondence or communication between the workplace and a third party.
[337] Hegedűs, 2006a, p. 48.
[338] Arany Tóth, 2008, p. 270
[339] Act C of 2003 on Electronic Communications
[340] Arany Tóth, 2008, pp. 272-273.
[341] Except the one mentioned by Arany Tóth
[342] Pauly/Osnabrügge, 2009, § 6 mgn. 120.
[343] Cf. also § 106 GewO.

that the duty of the employee is to use the equipped workplace for official purposes.[344] In exceptional cases, in accordance with the provisions of Article 315 of the Civil Code, individual colleagues may be released from this obligation, which can often be the case with older colleagues who are rather afraid of using technology.[345] Regarding this, it should be noted that certain work conditions may not consolidate over a longer period of time either to the extent that they would become unilaterally unchangeable components of the contract.[346] In addition, the general principle of equal treatment set out in Art. 3 Sec. 1 of the basic constitutional law[347] requires the employer to equip all comparable work places with computers.[348] There is the duty not to treat individual employees or groups of employees for irrelevant reasons more unfavourably than other colleagues in a comparable situation.[349] Regarding the transfer of a PC/notebook, in the case of notice to quit or exemption, the obligation to return it must be provided for in the employment contract.[350] By this the employer can assert different claims concerning the return, as he deems appropriate.[351]

As the owner of the means of operation,[352] the employer basically has the right to decide freely about whether and to what extent he would like to allow his employees the use of internet and e-mail-services.[353] Thereby the employee may basically neither claim permission for private use,[354] nor may the internet be used for private purposes in the absence of the employer's permission (no matter whether *expressis verbis* or implied).[355] In emergencies or in urgent cases,[356] private use is exceptionally permitted, irrespective of the type of communication means used.[357] Generally, on the other hand, such use is forbidden which violates the law or is obviously contrary to business interests.[358]

---

[344] Pauly/Osnabrügge, 2009, § 6 mgn. 120. Whether the Computer may be used only for official or also for private purposes depends on permission from the employer, which can be arranged in relation to the employment contract by a Works Council agreement, Pauly/Osnabrügge, 2009, § 6 mgn. 122.
[345] Pauly/Osnabrügge, 2009, § 6 mgn. 120.
[346] BAG, NZA 1993, 89, 91.
[347] Cf. Küttner/Kania, 2011, Gleichbehandlung, mgn. 9 ff.
[348] Pauly/Osnabrügge, 2009, § 6 mgn. 120.
[349] BAG, NZA 1984, 201, 202.
[350] Pauly/Osnabrügge, 2009, § 6 mgn. 121.
[351] Cf. for details Pauly/Osnabrügge, 2009, § 6 mgn. 11 ff.
[352] *BAG*, NZA 2006, 98.
[353] *Beckschulze*, 2003, p. 2779; *Beckschulze/Henkel*, 2001, p. 1491, 1494; Däubler, 2000, p. 323, 324. This is valid also for the use of private smart phones belonging to the employee, who can be connected with on the Internet, LAG Rheinland-Pfalz, BeckRS 2010, 66924 (cf. also the note by Stück, 2010, p. 432). For the limitations in permission for private use cf. Gola, 2010a, mgn. 193 ff. With reference to the implementation of operational regulations for IT usage see Kramer, 2010, p. 164.
[354] Bloesinger, 2007, p. 2177; Mengel, 2004a, p. 1446 (with further references); Vietmeyer/Byers, 2010, p. 808; Beckschulze/Natzel, 2010, p. 2373; Mengel, 2004b, pp. 2014-2015; Weißnicht, 2003 p. 448.
[355] Rath/Karner, 2007, p. 449. Re definitive granting of permission cf. Gola, 2010a, mgn. 185.
[356] Hanau/Hoeren, 2003, p. 20.
[357] Holzner, 2011, p. 12; cf. further BAG, NZA 1986, 643 (telephone use) and also, Ernst, 2002 p. 588 (Organisation of communication via e-mail or VoIP).
[358] Gola, 2010a, mgn. 197, which apart from libellous, racist, sexist, violence promoting and unconstitutional content also includes that which runs counter to those laws concerning personal rights, copyright or penal regulations.

2.2.2.2. Cases from the jurisdiction[359]

The jurisdiction has already dealt on several occasions with the use of computers and the corresponding control over them.[360] The question of the extent to which the employer may monitor official internet communication has not so far been the subject of the highest judicial jurisprudence.[361]

2.2.2.3. Academic debate

The private use of e-mail and internet is often neither specifically forbidden nor explicitly permitted by the employer.[362] The question arises how to consider this situation in legal terms. Even if no general answers can be given in this context, there are some principles that could develop concerning the private use of e-mail and internet in the workplace, which should be described in the following.

2.2.2.3.1. In the absence of an explicit regulation the private use is not allowed

Partially the position is that in the absence of an explicit regulation, private use can be allowed.[363] The employee could assume that such actions are tolerated, because the use of operational technical equipment to an appropriate extent could be a socially acceptable gesture by today's standards.[364] This view, however, misjudges the fact that, due to lost working hours, the employer suffers considerable damage from his employees.[365] On the other hand, the employer is still the one who decides on the use and application of operational means, and so the employee must not assume that he is entitled to private use.[366] In this respect private use is principally to be excluded without explicit authorisation or toleration by the employer.[367]

2.2.2.3.2. Explicit and implied regulations of use

Private use can be explicitly regulated by means of mailing circulars to the entire personnel (total commitment), by individual contractual clauses or in-house agreements.[368] Furthermore,

---

[359] Cf. in general to the most relevant Supreme Court decisions Gola/Wronka, 2010, p. 575 ff.

[360] Cf. by way of example Pauly/Osnabrügge, 2009, § 6 mgn. 120. ff.: named decision: BAG, NZA 1993, 89 (Organisation of workplaces), NZA 1984, 201 (Principle of Equal Treatment); LAG Köln, NZA 2006, 106; ArbG Düsseldorf – 4 Ca 3437/01 (not published; most extreme transfer of the principles of private telephone calls to private Internet use); ArbG Frankfurt a.M. 2.1.2002 – 2 Ca 5340/01 (not published; Toleration of private use); BAGE 115, 195 (Internet use with inadequately clear permission or toleration); LAG Köln, NZA 2006, 106; ArbG Düsseldorf 1.8.2001 – 4 Ca 3437/01 (not published); BAG, NJW 2006, 540.; LAG Rheinland-Pfalz 9.5.2005 – 7 Sa 68/05 (not published); NZA-RR 2005, 303 (Notice and written warning; cf. further BAGE 115, 195; NZA 2007, 922, 924 and also LAG Rheinland-Pfalz, NZA-RR 2010, 297, 299).

[361] Gola, 2010a, mgn. 206.

[362] Rath/Karner, 2007, p. 448.

[363] LAG Köln, NZA 2006, 106; *ArbG Wesel* NJW 2001, 2490; *ArbG Frankfurt a.M.*, NZA 2002, 1093.

[364] *AG Köln*, NZA 2006, 106; *ArbG Frankfurt a.M.*, NZA 2002, 1093; *LAG Rheinland-Pfalz* , NZA-RR 2005, 303.

[365] Pauly/Osnabrügge, 2009, § 6 mgn. 123. with reference to Dickmann, 2003, p. 1009 Fn. 4, who has calculated the annual loss for companies in Germany merely on the basis of unauthorised Internet use at 50 billion EUR.

[366] Kratz/Gubbels, 2009, p. 652; also as a result: Gola, 2010a, mgn. 181.

[367] Cf. BAGE 115, 195 and also Beckschulze, 2003, p. 2377; Ernst, 2002, p. 586; Dickmann, 2003, p. 1009; Kramer, 2004, p. 461; Mengel, 2005, p. 753.

[368] *Nägele/Meyer*, 2004, p. 313; *Beckschulze*, 2003, p. 2777; Gola, 2010a, mgn. 183. In in-house agreements between the employer and the works council, from the legal standpoints of both the assessment of the basic law, mandatory law (ius cogens) and also of the general principles of the Labour Law, special attention must be paid.

the set up of a private e-mail address through the employer is to be considered as implied authorisation of private use.[369] The mere provision of internet access, however, is to be considered differently.[370] In addition, tacit authorisation could be the case where, despite having knowledge of the private use of the operational means of communication, the employer does not intervene, and consequently the practice is apparently tolerated by him.[371]

2.2.2.3.3. Operational practice

It is debatable, in the absence of a specific agreement, whether or not the employee may claim private use according to the principles of operational practice and due to the implied behaviour of the employer. This would be conceivable if, the simple toleration of private use by the employer over a longer period of time would have such explanatory value on which the employee could sufficiently rely.[372] This is rejected by the view whereby,[373] among other things, it is argued from the position of the employer as the owner of the equipment. Therefore, the principle should be applied that all acts by the employee which are not explicitly permitted are forbidden.[374] Through private use, or by overriding the scope of permission specified by the employer, the employee commits a breach of duty which the employer does not have to accept.[375] This view, however, misjudges the qualitative difference between simple omission and toleration.[376] Whilst in the case of omission it is the behaviour of the employer that does not allow the creation of a situation of confidence, the situation is different in the case of toleration. Here the employer has knowledge of private use and accepts this over a longer period of time[377] without complaint.[378] The extent of toleration in accordance with Articles 133 and 157 of the Civil Code is to be interpreted with an objective onlooker's vision, and so from the perspective of an employee with common sense - and by taking into consideration mutual work contract interests.[379] Consequently, the contractual primary and ancillary obligations of the employee comprise the standard to be used to determine where one stands.[380] This is maintained within the scope of his primary obligations, while the former is primarily to fulfil his work responsibilities in such a way that neither the

---

Above all else with respect to § 75 Abs. 2 Satz 1 BetrVG such agreements more frequently produce a just effect in respect of infringement of the individual rights of the employee on informational self-determination, Brink/Schmidt, 2010, p. 593.

[369] Erler, 2003, p. 18; as well Kratz/Gubbels, 2009, p. 652.

[370] *Mengel*, 2004a, p. 1446; also Mengel, 2004b, p. 2015; Ernst, 2002, p. 586; Kratz/Gubbels, 2009, p. 652. Whether in the clear or definitive organisation of private telephone calls a final clarification has been given by the employer, also private Internet and E-Mail use is to be allowed, is a matter of dispute. This, for example, is affirmed by Ernst, 2002, 585 also Däubler, 2004, mgn. 184a; *Hanau/Hoeren*, 2003, p. 22. But opposed by Uecker, 2003, p. 158; Kratz/Gubbels, 2009, p. 652 (with further references).

[371] Gola, 2010a, mgn. 185.

[372] Kratz/Gubbels, 2009, p. 652.

[373] Cf. Beckschulze, 2009, p. 2097; Koch, 2008, p. 911; Waltermann, 2007, p. 531.

[374] Bissels/Lützeler/Wisskirchen, 2010, p. 2433. with reference to BAG, NJW 2006, 540; LAG Hamm, BeckRS 2010, 67373; Beckschulze, 2009, p. 2097.

[375] Bissels/Lützeler/Wisskirchen, 2010, p. 2433.

[376] In this direction argue also Kratz/Gubbels, 2009, p. 652. as does Gola, 2010a, mgn. 186.

[377] The time limits are laid down differently in the academic debate (Beckschulze/Henkel, 2001, p. 1492 and also Ernst, 2002, p. 586; Däubler, 2004, mgn. 180 a half year in Kramer, 2004, p. 457 as opposed to a year.)

[378] Gola, 2010a, mgn. 186.

[379] BAG, NZA 2006, 107, 108.

[380] Kratz/Gubbels, 2009, p. 653. Likewise Gola, 2010a, mgn. 193. regarding the legal responsibilities for safeguarding the IT security of the business see Trappehl/Schmidl, 2009, p. 987.

quality of the results of his work nor his productivity is disproportionately negatively affected. In this context, the implied authorisation of use is limited by excess prohibition,[381] whereby the individual cases must be considered individually by taking particularly into account the existing work load on the employee. Therefore, the extent of use is regularly limited to times when operational interests are not impaired.[382] These are periods where the employee does not have to fulfil duties or – as in the case of a lack of work – can do his job with breaks and time to spare.[383] Likewise, within the scope of their contractual ancillary obligations, employees must respect the operational and financial interest of the employer.[384] In addition, the employer subsequently cannot merely specify the limits of the permission for use,[385] but he can also prevent the development of operational practice in advance, by specifying adequate regulations in the bylaws and service agreements[386] for reasons of legal certainty[387] - and by enforcing and monitoring compliance with the prohibition of private use by means of monitoring [388]and also by formally sanctioning the offences.[389]

2.2.2.3.4. Restriction and withdrawal of permission

Restrictions of the permission for private use can be imposed in terms of time, place and content.[390] Also, the employer has the possibility to withdraw permission for use as long as the private use was permitted as a voluntary service without intent to enter into a commitment.[391] On the other hand, on the basis of the labour contract, or if permitted, on operational practice, the employee has already claimed private use, the withdrawal of permission must be preceded by notice of termination pending a change of contract.[392]

2.2.2.3.5. Allowed extent of monitoring e-mails and internet use

The question arises as to whether, and to what extent, monitoring of employer-provided e-mail and internet use is permitted.[393]

Limits of purely official and private internet communication[394] as the starting point for the extent of the employer's surveillance power

Basically, it should be noted that the extent of the employer's powers over private e-mail and internet use is significantly lower than in the case of purely official use, and so a clear

[381] ArbG Wesel, NJW 2001, 2490, 2492; Mattl, 2008, p. 49; Kliemt, 2001, p. 534; Ernst, 2002, p. 586; Mengel, 2004b, p. 2015; Kramer, 2004, p. 460.
[382] Kratz/Gubbels, 2009, p. 653.
[383] Kratz/Gubbels, 2009, p. 653, with reference to *Ernst*, 2002, p. 586 (The practice of trust-based working time) and Däubler, 2004, mgn. 170.
[384] Cf. the examples given by Kratz/Gubbels, 2009, p. 653 on the damage to the resources and other legal assets of the employer (with further references).
[385] Gola, 2010a, mgn. 188.
[386] Vietmeyer/Byers, 2010, p. 808.
[387] LAG Rheinland-Pfalz, NZA-RR 2005, 303, 306.; Rath/Karner, 2007, p. 449.
[388] Rath/Karner, 2007, p. 449.
[389] Gola, 2010a, mgn. 188.
[390] For details cf. Dickmann, 2003, p. 1009.
[391] Gola, 2010a, mgn. 189.
[392] BAG, RDV 2010, 68.
[393] Full controlling is already prohibited for reasons of proportionality, Gola, 2010a, mgn. 291.
[394] If apart from purely official use, private use is permitted, we speak of so-called mixed use, Rath/Karner, 2007, p. 450.

distinction must be made.[395] Use, basically, always has an official character if it is designed to promote the work.[396] Such exists if the internet communication shows some reference to the official tasks of the employee and corresponds to the objective interests of the employer. These also include private use for official reasons, which, for whatever reason, are performed from the sphere of the employer. Such use is permitted due to the employer's duty of care in accordance with Articles 611, 242 of the Civil Code.[397] Further, the social exchange at work can be assigned, even through e-mail traffic, to the sphere of official use.[398] In fact, the employer cannot prevent this totally.[399] All other forms of external communication are to be assigned to the private sphere.[400]

Monitoring of official internet communication (banning of private use)

If there is a ban or prohibition on the private use of e-mail and internet and this is implemented by the employer, the admissibility of storage and the evaluation of the employee's traffic data[401] is to be judged according to the contractual purpose of Article 32 sec. 1 of the Federal Data Protection Act[402] by taking into consideration the employee's right to informational self-determination.[403] External data (e.g. sender and receiver of the e-mails,[404] time of sending) can serve as connection data in relation to the e-mail traffic.[405] Concerning internet use, the time of accessing a site,[406] the duration of the internet use and the protocols of accessed websites,[407] as well as any expenses incurred[408] (for instance for reasons of the control of abuse and cost control),[409] or the prevention and removal of interference with the EDP[410] system can play a role. When making the necessary assessment, the interests of the employer have basic priority regarding purely official use. Thereby, as a rule, regarding at least a regularly monitored prohibition of the private use, it is assumed that the monitoring of the purely official use of e-mail and internet is accepted.[411] The monitoring of e-mail in terms

---

[395] Rath/Karner, 2007, p. 449; Rasmussen-Bonne/Raif, 2011, 80; Hoppe, 2010, p. 388; Vietmeyer/Byers, 2010, p. 807.
[396] Ernst, 2002, p. 588.
[397] Rath/Karner, 2007, p. 449. Cf. further in respect of telephone conversations BAG, NJW 1987, 674, 678.
[398] Ernst, 2002, p. 588.
[399] Rath/Karner, 2007, p. 449.
[400] Däubler, 2000, p. 324.
[401] Traffic data are data which are generated, collected, processed or used by the provision of a Telecommunication services, § 3 Nr. 30 TKG.
[402] Gola, 2010a, mgn. 287. Opinions of the TKG und TMG find no application in the case of purely official use in the employment relationship; Däubler, 2010, mgn. 337, 342; Kratz/Gubbels, 2009, p. 653.
[403] Rath/Karner, 2010, p. 470, with reference to Mengel, 2004b, p. 2015; Ernst, 2002, p. 588; Lindemann/Simon, 2001, p. 1951.
[404] Gola, 2010a, mgn. 288. Cf. Also loc.cit., 2010, mgn. 289 (with further references) re the issue of the storage of details of addressees.
[405] Vehslage, 2001, p. 148; Däubler, 2010, mgn. 351, 354; Naujock, 2002, p. 593; constrictive Ernst, 2002, p. 590.
[406] Gola, 2010a, mgn. 288.
[407] Vietmeyer/Byers, 2010, p. 808.
[408] Gola, 2010a, mgn. 288.
[409] Raffner/Hellich, 1997, p. 867.
[410] Hoppe/Braun, 2010, p. 81; Kramer, 2010, p. 164.
[411] Rath/Karner, 2010, p. 470. Cf. as a result Hoppe/Braun, 2010, p. 81; Jenau, 2010, p. 90; Raif/Bordet, 2010, p. 88; Braun/Spiegl, 2008, p. 394; Schmitt-Rolfes, 2008, p. 391; Wolf/Mulert, 2008, p. 443; Altenburg/v. Reinersdorff/Leister, 2005, p. 136. Often compared with opening and reading official mail through the employer,

of content will then not result in the violation of the employees' right to informational self-determination, since they, considering the prohibition of private use, must accept the fact that the communication takes place not only in the relation to the receiver.[412] Hence, by permitting purely official use, the employer may, in general, only store the employees' data[413] for which he has extensive monitoring possibilities available. In this way, in standard web-browsers he can obtain knowledge of the cache contents and can draw conclusions as to the surfing conduct (e.g., Internet addresses, time of access to a website) of the employees.[414] In addition to this, by means of detailed log files[415] the employee's data traffic can be analysed.[416] It must be noted that the allowed extent of protocol and the scope of data to be analysed must be carefully verified and determined in advance.[417]

Monitoring of private internet communication

Far more complicated is the legal status in the case of the private use allowed in addition to the purely official use (so-called mixed use).[418] If such permission exists, then not only do the provisions of the Federal Data Protection Act apply, but, in accordance with Article 3 No. 6 of the Telecommunication Act[419] and Article 2 Sec. 1 No. 1 of the Telemedia Act, the employer is to be considered as service provider.[420] This has the consequence that he becomes subject to the legal telecommunication restrictions of § 88 et seq. of the Telecommunication Act and § 11 et seq. of the Telemedia Act. The provisions shall apply even if the employer restricts the scope of use in terms of time or in scope and employees exceed these specified terms and conditions of use. Ultimately, by this, monitoring or inspection of the communication data is always *de facto* concealed to the employer.[421] Partly it is believed that, by making a written general declaration, employees release the employer from respecting the telecommunication

---

cf. only Gola, 1999, p. 326; Weißnicht, 2003, p. 451; Lindemann/Simon, 2001, p. 1952; Mengel, 2004b, p. 2017, Rath/Karner, 2007, p. 450.

[412] Gola, 1999, p. 326; Rath/Karner, 2007, p. 450.

[413] Rasmussen-Bonne/Raif, 2011, p. 80.

[414] Besgen/Prinz, 2009, § 1 mgn. 53.

[415] In this context, we also include Protocol Data which gives information about traffic data in Internet communication (e.g. time and duration of the connection to the server, transmission of data involved), Thüsing, 2010, mgn. 198.

[416] Besgen/Prinz, 2009, § 1 mgn. 53.

[417] Gola, 2010a, mgn. 288. Cf. further, assistance with orientation, the protocolisation of 'Technical and organisational data protection questions at the Conference "Datenschutzbeauftragten des Bundes und der Länder", (Arbeitskreis, 2009).

[418] Rath/Karner, 2010, p. 470.

[419] i.e, between the parties to the employment contract and in relation to permitted telecommunications use, there lies a separate telecoms usage arrangement, which applies to the employee as an outside third party (prevailing opinion; Hoppe/Braun, 2010, p. 81; Mengel, 2004a, p. 1450; Gola, 1999, p. 324; Kratz/Gubbels, 2009, pp. 654-655; Vietmeyer/Byers, 2010, p. 808). The employer is, due to the arrangement for private use, already the Access Provider (Rath/Karner, K&R 2007, 446, 450). (Rath/Karner, 2007, p. 450). Thüsing, 2010, mgn. 220 ff. as well as Löwisch, 2009, p. 2783 have a different point of view. Refusing this: de Wolf, 2010, pp. 1208-1209. Regarding the relevant legal terms cf. the statual definitions of § 3 no. 6 TKG (service provider) and § 3 no. 10 TKG (Business-related product of Telecommunication services; business-related here is not synonymous with commercial, and so the question of winning does not arise and the real meaning is simply the long-term provision of access, Weißnicht, 2008, p. 161.).

[420] Busse, 2009, § 10 mgn. 74 ff.; Kramer, 2010, p. 164.

[421] Lembke, 2010, BDSG introd. mgn. 92 (with further references); Kramer, 2010, p. 164.

secrets and could, therefore, have control over authorised private use.[422] An opposing opinion proposes to restrict this possibility, at least to the extent that it would be necessary to determine (depending on each case), whether there is a corresponding written declaration of approval for the respective communication type or for the clearly imminent process.[423]

Monitoring of internet and e-mail use within the scope of application of the Telecommunication Act

From Article 88 Sect. 2 of the TKG there comes, according to the prevailing view that, in compliance with his status as a service provider,[424] the employer has the obligation to protect telecommunication secrets.[425] This has its effect on the extent of the protection of the employee. Hence, the employer may basically note the content of the internet communication if the private use of the internet is permitted.[426] As is clear from Article 88 sec. 3 sentence 1 and sentence 3 of the TKG, the inspection of the content as well as the closer circumstances of telecommunication and the disclosure to third parties is only permitted if this is required for those named purposes and to the extent that it is permitted by the TKG or by another law referring to telecommunication activities. However, first of all, the obligation to notify set out in Article 138 of the German Penal Code must be met (cf. Article 88 sec. 3 sentence 4 of the TKG). In accordance with government reasoning[427] even *de lege ferenda* nothing alters the fact that the employer is classified as telecommunication supplier.[428] The inspection of e-mails by the employer is not only denied when e-mails are stored in an external mailbox and are only accessible via the internet, but, due to the factual possibility of access through the provider despite the user's password, it is, in consequence, beyond his control.[429] Rather, there is a comparable situation, where - as usual - e-mails are downloaded from the e-mail server of the employer into the mailbox of the employee, which is installed as a program on the employee's computer. Since the computers of employees are connected through a corporate network with the employer's e-mail server, the system administrator can technically access the mailbox of the employees, by resetting the password and thus enabling monitoring. In addition, it must be noted that the employer, as owner, may at any time demand that the employees return the relevant terminals (eg. PC, laptop, Smartphone). These reasons speak for the fundamental extension of protection of Article 10 of the Basic Law on E-mails that have already been transmitted and opened, as long as these are in the mailbox of a computer, which can be accessed via the corporate network without the consent of the employee.[430] Additionally, it is to be noted that the employer within the meaning of service provider in accordance with Article 109 Sect. 1 No. 1 of the TKG is required to make appropriate technical arrangements and other measures in order to protect the secrecy of

[422] Hartmann/Pröpper, 2009, p. 1300. Critically: Kramer, 2010, p. 164.
[423] Kramer, 2010, p. 164.
[424] Thüsing, 2010, mgn. 295.
[425] Thüsing, 2010, mgn. 221.
[426] Weißnicht, 2008, p. 164; Rath/Karner, 2010, p. 470.
[427] Background paper to an outline law on the regulation of employee's data protection v. 25.8.2010, S. 6; Beckschulze/Natzel, BB 2010, 2368, 2374.
[428] Vietmeyer/Byers, 2010, p. 807.
[429] De Wolf, 2010, p. 1209. Cf. also BVerfGE 124, 43, 54 with reference to E 120, 274, 341.
[430] De Wolf, 2010, p. 1209.

telecommunications and personal data. In addition to technical and organizational measures, this also includes monitoring measures taken regarding the maintenance of the stipulated principles.[431] Specifically, unauthorized persons must not obtain knowledge of connection of data, for example, those arising from telephone calls or the use a database, and the scope of those eligible to obtain knowledge must be kept as narrow as possible.[432]

Monitoring of internet and e-mail usage within the scope of application of the Telemedia Act

Since the employer either himself offers specific services or, at least, mediated in access to such, the data protection obligations set out in the TMG must be observed regarding the monitoring of private internet communications.[433] In accordance with Article 1 Sect. 1 of the TMG, all electronic information and communication services which are not classified as telecommunication services or broadcasting fall under the concept of telemedia service.[434] The delimitation of scopes of application of the TKG and TMG depends on whether the question concerns the technological transmission process as such (TKG) or the preparation or use of the transmitted content (TMG).[435] Here, Article 11 sec. 3 of the Telemedia Act restricts the scope of application of telemedia, which consist mainly[436] of the transmission of signals over the telecommunication networks and are, therefore, also subject to the TKG.[437] Offering the private use of corporate e-mail and other internet applications to employees is also usually considered as telemedia.[438] For the employer it follows that, as a rule, it is not permitted to resort to the employee's data resulting from private use, by means of monitoring the communications or performance of the employee.[439] Then, according to the TMG only the data protection provisions of Article 15 para. 8 of the TMG (assertion of right), as well as the corresponding penalty provision of § 16 para. 2 No. 4 of the TMG, are applied with respect to the collection and use of the personal data of the user, cf. § 11 sec. 3 of Telemedia Act. There could be deviations but only in the case of the voluntary explicit consent of the employee.[440] In the event that the scope of application of the Telemedia Act, beyond the scope of Article 11 para 3 of the TMG, is broadened, and on the basis of the principle of data avoidance and data economy, care must be taken that, by developing and selecting the technical equipment, no (or as little as possible) personal data is collected, processed or used.[441] Also, the employer must respect the principle of anonymization and pseudonymization laid down in Article 13 para 6 sentence 1 of the TMG, where this is technically possible and reasonable. Concerning this, in

[431] Däubler, 2010, mgn. 370 with reference to the antecessor regulation of § 109 TKG mentioned by Ehmer, 2006, § 87 TKG mgn. 18.
[432] Däubler, 2010, mgn. 370 f.
[433] Däubler, 2010, mgn. 342.
[434] Not within the scope of the TMG are employee portals, in-house-information systems or B2B-services, Gola, 2010a, mgn. 163 f. (re the limitation of § 11 Abs. 3 TMG cf. mgn. 167 f.).
[435] Gola, 2010a, mgn. 166.
[436] Cf. § 3 no. 24 TKG. A major part of transmission is assumed with a share of more than 50%, Wittern/Schuster, 2006, § 3 TKG mgn. 48.
[437] Gola, 2010a, mgn. 166.
[438] Moos, in: Taeger/Gabel, BDSG, § 12 TMG mgn. 32; Heidrich, CR 2009, 168, 173; Gola, 2010a, mgn. 167.
[439] Gola, 2010a, mgn. 167.
[440] Däubler, 2010, mgn. 378.
[441] Däubler, 2010, mgn. 373.

accordance with Article 13 paragraph 6 sentence 2 of the TMG, the user is to be informed. The duration of use must not be recorded. Furthermore, the checking of free services is forbidden.[442] In accordance with Article14 para. 1 of the Federal Data Protection Act, the service provider may collect and use the user's personal data only to the extent that is necessary for the establishment of, is contextual to, or for the modification of a contractual relationship between him and the user concerning the use of telemedia (so-called inventory data). These data relate only to the contract as such, and not to its implementation.[443] In addition, § 15 paragraph 1 of the Telemedia Act stipulates that the service provider may only collect and use the user's personal data to the extent that it is necessary in order to enable and give account of the use of telemedia (so-called usage data).

Preventive control of e-mails in accordance with the Federal Data Protection Act

In addition to the specific telecommunications right of data protection, the regulations of the BDSG also apply. The question is, first, whether Article 32 of the BDSG can be used to permit the preventive monitoring of e-mails. It is conceivable, regarding this, to consider Article 32 Paragraph 1 Sentence 2 of BDSG. As is apparent from the wording, it is necessary to specify basically that the actual evidence should justify the suspicion that the person concerned has committed a criminal offence within the employment relationship. In the preventive monitoring of e-mail-traffic, this may be suspected, but the evidence is not yet strong enough, so that Article 32 paragraph 1 sentence 2 of the BDSG does not constitute valid permission. Valid permission could, however, result from Article 32 paragraph 1 sentence 1 of the BDSG. Preventive controls could then be required to fulfil the purpose of the employment relationship. At this point, reference can be made again to Article 88 of the TKG. In accordance with Article 88 paragraph 1 old. 1 of the TKG, the content of the communication, i.e., the text of the e-mail is subject to the secrecy of telecommunications. As an exception, Article 88 paragraph 3 sentence 3 p 2 of the BDSG allows the employer, as a service provider, to gain knowledge of the content of telecommunication when another statutory provision provides for this and when, at the same time, reference is made specifically to telecommunication processes. However, Article 32 of the BDSG does not function simply as such derogation, so that this, as the legal basis for preventive measures through the monitoring of e-mails, is eliminated.[444]

2.2.3. Conclusion

No specific Act was found regulating this topic in Hungary or in Germany. From the case law in the area of computer and Internet surveillance in workplaces we conclude that the findings of the courts are rarely examining cases from a personal data protection perspective, most of them are based on arguments from Constitutional law, Civil law, Criminal law, or Labour law. On the other hand no clear limits had been appointed by these on the question regarding to the extent which the employer may monitor computer usage, internet and email communication. The jurisprudence of data protection authorities deals with individual cases –

[442] Däubler, 2010, mgn. 377; Lindemann/Simson, 2001, p. 1953.
[443] Däubler, 2010, mgn. 374.
[444] De Wolf, 2010, p. 1210.

in these they consider all the unique circumstances of monitoring, which may vary on a large scale – therefore this can refer only to the negative borders of applying surveillance technologies, and cannot be treated as a coherent legal background on the rules of monitoring technologies. The summary of the research in these issues is that we have to examine the computer, Internet and electronic correspondence monitoring systems and processes in the given situation case by case to determine the limits of their legitimate use.

2.3. Regulation of social networks

Technological advances, especially in recent years, were also accompanied by the development of so-called social networks, which have now to be seen as an integral part of everyday life and enjoy great popularity.[445] This raises the question of how to resolve the tension arising in this context between, on the one hand, self-realization, freedom of expression and social interaction and, on the other hand, informational self-determination of users and non-involved third parties[446] by taking all interests into consideration.

There is a rather high risk that employees use social networks for private purposes in working hours, and so monitoring usage may be important for the employer, but may also breach the employee's privacy, and also raise data protection and labour law issues.[447] 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. In order to follow the technologically driven social changes form a legal point of view the Article 29 Data Protection Working Party adopted an opinion on social networks in 2009,[448] what can serve as a basis when building a common jurisdiction in the Member States.

2.3.1. On the nature and functioning of social networks

The term social network refers to internet platforms that allow an individual to present himself.[449] In their functioning, there is almost no difference between the individual networks. The user first registers on the platform by creating a profile with a username[450] which is secured by a user ID and password. In this context, it is also the user who decides what and how much information he discloses. Depending on the structure of the social network, this information may be both private and professional in nature.[451] Whilst in professional networks it is primarily information on the employment history and of the activity carried on which

[445] Facebook, the Internet portal founded in 2004, could already claim 500 million members in the following year, heise, 2010.
[446] Cf. Lerch/Krause/Hotho/Roßnagel/Stumme, 2010, p. 454.
[447] Arany Tóth, 2008b, p 170, Hegedűs, 2006b, p. 81.
[448] Opinion 5/2009 on online social networking (WP 163)
[449] Oberwetter, 2011, p. 417.
[450] At least on social networks with a commercial connection this will be in all civil law, as the user specifically intended, a serious, adequate image of itself relevant to commercial practice. In contrast, on private networks we find many fictitious names or nicknames or variations on their own name.
[451] Oberwetter, 2011, p. 417. The most prominent example of a private social network is, without question, Facebook. In Germany networks such as studiVZ, meinVZ or Flickr, in Hungary IWIW enjoy great popularity. In the field of official social networks, XING, LinkedIn und Expeerteer have most registered users.

play a role,[452] in private networks these are supplemented by information such as the relationship status.[453] The disclosure of this data includes, at the same time, the consent of the person concerned.[454] In addition to the simple presenting of one's own person, social networks also allow interaction with other members, either by individual communication (messages, chats, posts), by joining discussion forums or by networking with other users (either directly or indirectly through joining interest groups). The general linking of individual profiles which develops on the basis of multiple interactions ultimately creates the network.[455]

2.3.2. The importance of social networks in the digitized world of work

In the digital world of work social networks are becoming increasingly important. There is now not only an enormous influence on the world of work attributed to the field of social media, but the forecast of the future relevance of social networks is also optimistic.[456] For example, the shift of social network functions into the company is emphasized as the most important future trend in the industry.[457] This development naturally brings along not only advantages, but holds also significant risks for the employee regarding the handling of his personal data.[458] In order to create personal profiles, data is collected from generally accessible sources by means of a so-called 'crawler'.[459] The data to which particular importance is attached are above all those from social networks.[460]

2.3.3. Hungarian regulation

2.3.3.1. 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.

2.3.3.2. Case law of the Data Protection Commissioner

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.[461]

---

[452] With XING these data, for example, are aggregated under the main heading of Business data.
[453] Oberwetter, 2011, p. 417. Generally, however, in both types of social network comprehensive statistics business and private possible.
[454] In accordance with Section 5 of Hungarian New Data Protection Act, and Article 4, paragraph 1, 4a of the BDSG. Ott, 2009, p. 161; Weichert, 2007, p. 189.
[455] Oberwetter, 2011, p. 417.
[456] Cf. with reference to the details of the current SID/FIT Social Media Report 2010/2011, (SID/FIT, 2011).
[457] Re the establishment of Corporate XING cf. the Press Release of Fraunhofer FIT (FIT, 2010).
[458] Re Personal Search Engines cf. Ott, 2009, p. 158 and Weichert, 2007, p. 188. By means of search engines such as Isearch (http://www.isearch.com) or Intelius (http://www.intelius.com), personal or background checks can already today be carried out. Cf. in depth Bissels, 2009a.
[459] Basically these are found on the Internet, for example via a search engine, accessible data, e.g., Bundestag, 2010b, p. 16.
[460] Ott, 2009, p. 158. In the literature it is thought that the consent of the person involved should be so interpreted that search engines, can legitimately 'crawl' and use the data, cf. Ott, 2009, p. 161; and also Weichert, 2007, p. 189.
[461] 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.

2.3.4. German regulation

2.3.4.1. Cases from the jurisdiction

So far there has been no court decision made, which had as subject matter the sanctioning of employees by their employer due to the use of Web 2.0.[462] The same applies to sanctions imposed due to the monitoring of social networks by the employer. However, due to the growing popularity of the portals, a discussion within the judiciary on this subject is regarded as vital.[463]

2.3.4.2. Academic debate[464]

As already mentioned, in accordance with the right to manage, the employer may, in principle, be free to prohibit the use of the internet completely at the workplace. Nevertheless, the principles which are applied here do not, by a long way, correspond with reality. Rather, using the internet for official purposes and also private use are an integral part of business practice.[465] This raises the question of the extent to which the employer may make use of his right to manage regarding online self-presentation by employees. Then again, this depends on whether it concerns a private or a professional network.

2.3.4.2.1. Right to manage regarding self-presentation in private social networks

It is fundamental to emphasize that in principle, the employer may only issue instructions which are related to the activities of the employee.[466] The jurisdiction has already declared that the personal circumstances of an employee may be disclosed only to the extent to which a legitimate, justified and equitable interest of the employer exists in relation to the employment relationship.[467] This leads to two limitations of the right to manage by the employer regarding the appearance of workers in a private social network: first, regarding the employee's private handling of the content of social networks, the employer simply must not give instructions. Secondly, social networks which mainly serve to offer private presentation to the employee are completely closed to the employer.[468]

2.3.4.2.2. Right to manage regarding self-presentation in professional social networks

The picture concerning the legal situation regarding employees in professional social networks is different. It should first be noted that employee data are disclosed not only

[462] Raif/Bordet, 2010, p. 88. The theme has already been dealt with, at least abroad, cf. the notice given to a female employee because of the appearance of her profile on Facebook whilst she was on sick leave; SPIEGEL ONLINE, 2009.
[463] Bissels, 2009b, p. 2197; cf. Raif/Bordet, 2010, and also p. 88 Ege, 2008, p. 72.
[464] Due to the size of the presentation there should be some consideration of the situation during employment and after the employment was terminated. At the application stage cf. the statements in Oberwetter, 2011, p. 417 also Forst, 2010, p. 427 and Bissels/Lützeler/Wisskirchen, 2010, p. 2433 Cf. re the extent of the personal questioning which was carried out in the run up to the job interview the study of the FEDERAL Association of German Management Consultants (BDU) of 2007, BDU, 2007. For the application of § 6a BDSG on E-Recruiting on the Internet, Gola, 2010a, mgn. 417 f.
[465] Oberwetter, 2011, p. 418.
[466] Oberwetter, 2011, p. 418.
[467] BAG, NZA 1986, 739, 739.
[468] Oberwetter, 2011, p. 418.

internally, but basically on a generally accessible platform on the internet.[469] Therefore, the disclosure of this data depends fundamentally upon the consent of the worker concerned.[470] An exception occurs when the data are required to meet work requirements, or it is customary to disclose such.[471] In the public sector, according to the Federal Administrative Court, at least when no safety concerns preclude it, the disclosure of the name, function, and official contact information of those officials who are responsible for external relations shall be considered as permitted by law.[472] Concerning this, some country data protection authorities express themselves rather critically in respect of the fact that, by crossing borders, the data are also available in countries without adequate data protection standards.[473] Ultimately, as a result, it is possible for the employer to arrange only an incomplete profile in official social networks according to the right to give instructions.[474]

2.3.4.2.3. Requirements of the right to manage in terms of content

The employer is entitled to develop the use of the internet, by prohibiting or restricting it. In this respect the principles applicable to communication via e-mail also apply to the legal assessment of social networks. In contrast to simple internet use, within the social networks interactions take place between individual users. Compared to sending purely business e-mails, the monitoring of communications in social networks is, for the employer, disproportionately more difficult.[475] In addition to this factual issue, the question from a legal perspective is whether the view of subjecting official e-mails to the possibility of monitoring by the employer,[476] may be carried over to monitoring exchanges within social networks. It seems highly questionable that messages sent in social networks be classified as corporate e-mails or as business letters (Article 257 of the German Commercial Code.)[477] However, a parallel can be drawn concerning the fact that in both cases the communication takes place in the form of text and constitutes part of business communication, hence giving the company the right to do so. Ultimately, however, there is no complete agreement, as it cannot be clearly established whether, for example, such statements of the employee in discussion forums have been made on behalf of the company or whether they are expressions of the employee's own opinion. It is recommended to differentiate according to the relevance of the topics to the company. According to this, topics irrelevant to the company should rather be assigned to the private sector, whilst those in the corporate sector should be in the form of statements

[469] Oberwetter, 2011, p. 418.
[470] Gola/Wronka, 2010. mgn. 1155, 1166 ff. With reference to the requirement for consent of § 22 KUG re the publication of photographs of employees.
[471] Gola/Wronka, 2010. mgn. 1155
[472] BVerwG, RDV 2009, 30; re information on first (given) names in the email address LAG Schleswig-Holstein, RDV 2008, 212.
[473] Gola/Wronka, 2010. mgn. 1166. Moreover, consent is also needed on significant grounds, since registration on the platforms of official social networks is normally tailor-made for natural persons who submit their own profile, Oberwetter, 2011, p. 419. However, together with these members' it is also possible to produce a business profile - see cf. e.g. Xing, 2011.
[474] Oberwetter, 2011, p. 419.
[475] Oberwetter, 2011, p. 419.
[476] See above, subsection 2.1.3.5.2.
[477] Oberwetter, 2011, p. 419.

concerning its products.[478] However, the company should be involved if the question concerns the correspondence of employees with customers, if performed within the framework of their activities and where project-related factors are the subject matter.[479]

2.3.4.2.4. Dealing with employee data on termination of employment

At the latest with the termination of the employment relationship, the question arises as to who holds the rights to the user's account of the social network and to the corresponding data (such as business contacts and customer relationships).[480] After leaving the company, the employee is obliged to return any and all equipment provided to him.[481] A user account is surrendered by the disclosure of the relevant access data.[482] Concerning this, however, the employee is only required to do so if membership in the social network was funded by the employer or the user account was made available to him otherwise but nevertheless by the employer.[483] Such a claim for surrender is not justified by the mere establishment of a user account in the network with the knowledge and intention of the employer. If the employee is subject to an obligation to return, he has the right to delete personal data before handing over the user account. This applies even if the employer was allowed only purely official use. Since, even through purely business-related dealings with clients, content with private references can be exchanged, the employer cannot assert any economic interests in such. Should the employer gain knowledge of these data, this would mean an unlawful interference in the personal rights of employees.[484] On the contrary, even if the employer does not require the employee to disclose the access data, the employee may be required to make available certain data contained in his account.[485] Thus, such data must be disclosed to the employer which are required to carry on the business of the employee that is, for example, any customer files[486] or customer data[487] created by the employee. In addition, the obligation to surrender also covers the business correspondence relevant in economic terms, either regarding current projects or those documents which are *ipso jure* required by the employer.[488]

2.3.5. Conclusion

So far there has been no cases taken to the courts or to the data protection authorities regarding the use of social networks in the workplace, however the spreading of these sites and the more employee joining and log into them will turn this subject regarded as vital, and start a discussion within the judiciary. Another point worth mentioning is that without the existence of relevant case law in any of the examined countries, German academic sphere is

[478] Oberwetter, 2011, p. 419; which at the same time stresses that it is not a universally valid statement. Insofar as it appears to be a statement relating to a single case although appreciating the total circumstances of the statement indicated.
[479] Oberwetter, 2011, p. 419.
[480] Bissels/Lützeler/Wisskirchen, 2010, p. 2438.
[481] Schaub/Linck, 2009, p. 1584. This follows either from an expressly contractual interpretation or, in case this does not apply, from §§ 861, 862, 677, 985 BGB, Bissels/Lützeler/Wisskirchen, 2010, p. 2438.
[482] Oberwetter, 2011, p. 420.
[483] Oberwetter, 2011, p. 420; likewise Bissels/Lützeler/Wisskirchen, 2010, p. 2438.
[484] Oberwetter, 2011, p. 420.
[485] Bissels/Lützeler/Wisskirchen, 2010, p. 2438.
[486] LAG Hamm, ARSt 1991, 182, 182 f.
[487] Preis, 2011, § 611 BGB mgn. 754; cf. BGH, NJW 1993, 1786 for business representative.
[488] Oberwetter, 2011, p. 420.

on a significantly higher level of debate concerning the use of social networks in workplaces than Hungarian data protection experts.

2.4. Monitoring of telephone calls

The employer may also have an interest in monitoring his employees' telephone calls,[489] especially telemarketing calls, sales follow-up calls, and technical support calls.[490] It is usually necessary for the employer to be able to monitor the use of voice telephony (mobile or fixed), especially in cases where the cost of telephone usage is covered by the employer. On the other hand surveys show that we have extended our expectations of privacy for phone calls in the workplace, employees believe that that no one is secretly listening in to a call.[491]

In addition it has to be stressed that audio surveillance is a broad category that includes sounds within, and also outside of human hearing, although covers computerized technologies used to analyse the content of the communication or stress level of the subject.[492] These allow a much broader range of application:

- Eavesdropping stands for the common voice surveillance of other people's conversation, which is often applied in the context of relationship difficulties or business spying.
- Wiretapping is a rapidly developing technology used mainly by law enforcement agencies to investigate and convict cases related to violent crimes and drug trafficking, usually it refers to a court-authorized covert monitoring of conversations.
- Mobile listening or recording, also known as "wearing a wire" has a questionable legality, as it is sometimes covers the use of hidden microphones and transmitting or recording devices for the purpose of monitoring or saving the information of a communication. In the workplaces they can be applied to safeguard personal rights, employees and potential employees sometimes wear a wire to record incidences of discrimination, sexual harassment or workplace abuse.
- Sound monitoring and listening devices may be installed to monitor safety around industrial equipment and to enquire about employees working in hazardous areas in general, used primarily with laser or electronic listening equipments placed in working areas.[493]

[489] On aspects of Internet telephony (Voice over IP, VoIP), Telephony or video telephony enabled over normal Internet links will not be separately addressed since the questions arising are closely connected with conventional telephony as well as the links with other media, Gola, 2010a, mgn. 281 ff. with reference to TBS, 2006.
[490] Petersen, 2007, p. 966.
[491] Lane, 2003, p. 107.
[492] Petersen, 2007, p. 105.
[493] Petersen, 2007, pp. 115-116.

2.4.1. Hungarian regulation

2.4.1.1. Legislation

There is no specific regulation concerning the use of telephones by the employees, although it is indirectly regulated by the Civil Code; by the Law on Electronic Communications;[494] by the Labour Code; and also in general by the Personal Data Protection Act.

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.[495]

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.[496]

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.[497]

Telephone usage always involves the processing of personal data and so the rules laid down in the Hungarian Personal Data Protection Act shall also be applied to the use of telephones by employees.

2.4.1.2. Case law of the Data Protection Commissioner

The processing of personal data of the employees relating to the use of voice telephony technology is a recurring issue for the Commissioner. The most important recommendations issued recently are taking into consideration the following subject matters:

- Monitoring telephone and internet use of the employees;[498]
- Monitoring the use of telephone in the workplace in respect of personal income tax regulations;[499]
- Recommendation on accessing data on telephone calls made by public servants.[500]

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

- 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 called and received telephone calls and their duration, since data concerning telephone calls are containing not only the personal data of the employee but of the other party to the individual calls.
- The same rule applies to cases when personal income tax-related rules handle in different ways the expenditure on personal and official calls.

[494] Act C of 2003 on Electronic Communications (hereinafter: Act on Electronic Communications)
[495] Civil Code, §§ 75-85.
[496] Law on Electronic Communications, § 156(14)
[497] Labour Code, § 103(1)
[498] DPC, 1767/K/2006
[499] DPC, 1672/K/2006
[500] DPC, 3362/P/2009

- 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.
- 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.

2.4.1.3. Judicial case law

There is no judicial case law in this specific field.

2.4.1.4. Academic debate

In the legal literature further summaries of the recommendations of the Commissioner can be found.[501] 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, therefore in employment relationships, the consent of the employee as the basis for personal data processing is always questionable.[502]

2.4.2. German regulation

2.4.2.1. Cases from the jurisdiction

In fundamental decisions of the BAG[503] and the BVerwG[504] concerning outgoing official telephone calls, the employer was basically entitled to the right to collect, store and use telephone data for cost control and cost accounting purposes.[505] Should the employer wish to overhear a phone conversation for later evidence, the consent of the external conversation partner is usually needed.[506] In the special work situation of a call centre, open listening-in is permitted by law for performance assessment purposes only to the extent to which it serves

[501] Cf. Székely/Szabó, 2005 pp. 129-130; Hartai, 2003 p. 48; Hajdú, 2005 pp. 172-173.
[502] Arany Tóth, 2008a pp. 305-306.
[503] DB 1986, 2086; NZA 1987, 515.
[504] NJW 1982, 840; RDV 1990, 24; DuD 1990, 426.
[505] This opinion is backed by the Data Protection Authorities cf. e.g., Supervisory Authority Baden-Württemberg, Ref. to BDSG Nr. 3, Staatsanzeiger (Government Gazette) of 1.7.1978, Nr. 52, S.4 Nr. 8.1. Different opinions of the Jurisdiction and of the Supervisory Review Board reject this in respect of the question whether whole of the number called may be saved, cf. BAG, DRV 1991, 7; Wohlgemuth/Mostert, ArbuR 1986, p. 138.
[506] BVerfG, RDV 2003, 23; 1992, 121; BGH, RDV 2003, 237. the right to wiretapping telephone conversations further BVerfG, NJW 1992, 815; RDV 2008, 18; BAG, NJW 1998, 307 and also Grosjean, 2003, pp. 2650-2651.

the training process and takes place in the most unobtrusive way - hence limited to the probationary period.[507]

2.4.2.2. Academic debate

Regarding the admissibility of the recording and monitoring of telephone calls and telephone communication data, it is mainly the explanations regarding the monitoring of e-mail and Internet use which apply. The assessment of the legitimacy of the surveillance measures depends therefore again on the question as to whether the employer also permits the private use of official landline and mobile phones.[508]

2.4.2.2.1. Permitted private use

A worker does not have the right to use official telephones for private purposes.[509] Should the employer have allowed private use, again, the provisions of the TKG are applied with the result that the employer's monitoring options are possible to a clearly much more limited extent.[510] Phone call data (destination number, time and duration of the call, number of charge units incurred) may be collected and controlled in accordance with Article 96 paragraph 1 of the TKG[511] only if they are needed for billing purposes, see Article 97 of the TKG. This is conceivable if private use is permitted only against payment.[512] However, this is in practice usually not the case.[513] Regarding the volume of collected and used data, the full destination number is unnecessary for cost calculation, since the area code is already sufficient for the determination of the charging zone.[514] If the employee can use a business telephone free of charge, the employer may generally evaluate the communication data only in the case of troubleshooting (Article 100 paragraph 1 of the TKG), or if there is a reasonable suspicion of abuse (Article 100 paragraph 3 of the TKG).[515] However, the employee's performance assessment must not be linked to the collection of communication data.[516] Both listening to and recording the content of telephone conversations are prohibited as interfering with the right of the spoken word.[517] Moreover, private conversations of the employee enjoy protection through telecommunication secrecy as set out in Article 88 of the TKG.[518] Monitoring the content of the conversation is limited to very exceptional cases. What might be conceivable here is, for instance, the existence of reasonable suspicion of a crime against the employee, which has a significant effect on the employment relationship (such as disclosing trade secrets

[507] BAG, RDV 1986, 30. Cf. on the use of silent monitoring and voice recording Jordan/ Bissels/Löw, 2008, p. 2626.
[508] Wellhöner/Byers, 2009, p. 2312.
[509] Mengel, 2004a, p. 1446; Altenburg/v. Reinersdorff/Leister, 2005, p. 135.
[510] Wellhöner/Byers, 2009, p. 2312.
[511] Vietmeyer/Byers, 2010, p. 809.
[512] Wellhöner/Byers, 2009, p. 2312; Heldmann, 2010, p. 1239; Vietmeyer/Byers, 2010, p. 809.
[513] Wellhöner/Byers, 2009, p. 2312.
[514] Mengel, 2004a, p. 1451; Gola, 1999, p. 327; Altenburg/v. Reinersdorff/Leister, 2005, p. 137; Wank, 2011, § 28 BDSG, mgn. 19.
[515] Heldmann, 2010, p. 1239; Vietmeyer/Byers, 2010, p. 809; Mengel, 2004, p. 1451; Oberwetter, 2008, p. 611.
[516] Gola, 1999, p. 327; Oberwetter, 2008, p. 611.
[517] Wellhöner/Byers, 2009, p. 2312; Oberwetter, 2008, p. 611; Mengel, 2004a, p. 1451; Moll, 2009, § 100 TKG mgn. 46.
[518] Oberwetter, 2008, p. 611; Altenburg/v. Reinersdorff/Leister, 2005, p. 135, 137, Gola, 1999, p. 325.

or the sexual harassment of colleagues at work).[519] Regarding the recording and monitoring of telephone calls and communication data in the case of the permitted private use of official mobile phones, there are no differences as to the legal situation regarding the monitoring of landline phones.[520] It should be noted that the employer may call the mobile phone of the employee to ask his/her actual whereabouts.[521]

2.4.2.2.2. Exclusive official use

If only official use of landline and mobile phones is permitted to the employee, the scope of application of the TKG is not broadened and the admissibility of surveillance measures is to be measured against the provisions of the Federal Data Protection Act.[522] Since, however, the employer does not act as telecommunications provider, violations of telecommunications secrecy do not apply. The recording and monitoring of telephone communication data is basically allowable.[523] In the absence of monitoring of the conversation content there is no interference with the right to one's own words,[524] although it does interfere with the employee's right to informational self-determination.[525] However, as part of the assessment process, the legitimate interests of the employer in expense and abuse control are normally given greater weight.[526] Again, the full destination number does not need to be recorded, since the first part of the called number is sufficient for cost control purposes.[527] There can be deviations from this in the case of abuse control, in order to provide evidence of private use.[528] Conversely, telephone communication data must not be recorded for general performance assessment, even if the private use of telephones is prohibited.[529] Regarding the monitoring of the content of official telephone calls, a stricter rule than that apply to the monitoring of e-mail content is used.[530] Listening to and recording telephone calls is to be generally considered as unlawful interference with the right to one's own word.[531] In very exceptional cases justification may possibly arise, if, for instance, there is well-founded suspicion of a criminal offence which has an effect on the employment relationship.[532] Ultimately this derives also from the wording of Article 32 paragraph 1 sentence 2 of the BDSG,[533] which can be used as justification for the detection of a crime committed within the

[519] Altenburg/v. Reinersdorff/Leister, 2005, p. 137; Mengel, 2004a, p. 1451.
[520] Wellhöner/Byers, 2009, p. 2312.
[521] Oberwetter, 2008, p. 612; Gola, 2007, p. 1142.
[522] Altenburg/v. Reinersdorff/Leister, 2005, p. 136; Mengel, 2004a, p. 1447.
[523] Wellhöner/Byers, 2009, p. 2313.
[524] Mengel, 2004, p. 1448; Altenburg/v. Reinersdorff/Leister, 2005, p. 136.
[525] Wellhöner/Byers, 2009, p. 2313.
[526] Oberwetter, 2008, p. 611; Altenburg/v. Reinersdorff/Leister, 2005, p. 136; Mengel, 2004a, 1448; Gola, 1999, pp. 326-327
[527] Gola, 1999, p. 326.
[528] BAG, NJW 1987, 674, 677; Simitis, 2010, § 28 BDGS mgn. 107; Oberwetter, 2008, p. 611; Altenburg/v. Reinersdorff/Leister, 2005, p. 136.
[529] Gola, 1999, p. 327; Oberwetter, 2008, p. 611. On the special features of call centers cf. Gola/Wronka, 2010, mgn. 758 ff.
[530] Wellhöner/Byers, 2009, p. 2313.
[531] Oberwetter, 2008, p. 611; Mengel, 2004a, p. 1451.
[532] Oberwetter, 2008, p. 611; Altenburg/v. Reinersdorff/Leister, 2005, p. 136; Mengel, 2004a, p. 1449; Dann/Gastell, 2008, p. 2948. Also conceivable is eavesdropping in cases of suspicion of the betrayal of commercial secrets cf. Dann/Gastell, 2008, p. 2948; Oberwetter, 2008, p. 611.
[533] Wellhöner/Byers, 2009, p. 2313.

employment relationship.[534] The legal situation regarding open listening to official telephone calls appears differently. This measure may be allowed for training and monitoring purposes.[535] Comprehensive employee monitoring is again unjustified. This argumentation applies also in respect of the business use of mobile devices.[536] Since normally the consent of the caller does not exist, in the case of the use of ISDN technology the storage of his/her call number as well as other data is specified according to Article 28 paragraph 1 sentence 1 No. 2 of the BDSG.[537] If the incoming calls are private in character, this shall not lead to the application of the TKG.[538]

2.4.3. Conclusions

As in both countries many forms of acoustic surveillance are in use for decades, the legal literature had time to discuss various aspects of the practice, and authorities could build up the legal framework around the legality of these technologies. Besides this fact the better equipped workplaces and development in surveillance technologies will raise new legal challenges in this field, and specific legislation may be drawn up for audio surveillance in the future. From the case law of telephony surveillance we conclude that employees usually have only limited rights to use official telephones, but it depends on the policy of the employer in each case. If private calls are limited (or banned) in a workplace employer do not have the right to access the complete call history of the employees or to request service providers to provide data concerning their calls. Another point worth mentioning is that monitoring the content of conversations in the workplace is limited in both countries to very exceptional cases, and the third party, who becomes also the subject of the monitoring, shall always be able to give or refuse his consent for this type of surveillance.

2.5. Video surveillance

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. CCTV cameras are often regarded as Big Brother's electronic eyes, as 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. The costs of installing these systems are falling by degrees, and video captures can be easily fed directly onto the internet, so distant employers can monitor numerous cameras.[539] Thus, the frequent use of CCTV systems generates a great deal of personal data, what can be used to create a personality profile of the employee,[540]

[534] Deutsch/Diller, 2009, p. 1464; von Steinau-Steinrück/Mosch, 2009, p. 451; Wybitul, 2009, p. 1583.
[535] Wellhöner/Byers, 2009, p. 2313. As an example we can consider the induction of new employees in Telephone or Call Centers, Dann/Gastell, 2008, p. 2948; Mengel, 2004a, p. 1449; Gola, 1999, p. 325. In respect of training the consent of the employee concerned is needed, Dann/Gastell, 2008, p. 2948; Oberwetter, 2008, p. 611. Cf. an exceptional permissible secret record Gola/Wronka, 2010, mgn. 785.
[536] Wellhöner/Byers, 2009, p. 2313.
[537] Gola, 2010a, mgn. 202.
[538] Gola, 1999, pp. 324-325; Däubler, 2000, p. 327; Post-Ortmann, 1999, p. 102.
[539] Lane, 2003, p. 118. In some cases employers may use remote video surveillance even in real time or near-real time over the Internet to monitor their employees and contractors who work offsite. Cf. Petersen, 2007, p. 535.
[540] Stanton/Stam, 2006, p. 59.

while on the other hand, surveys indicate that privacy expectations of employees in their workplace are lower than outside working hours.[541]

Monitoring and supervision by the employer may cover the use of all the tools, implements and equipment for the sake of protecting confidential knowledge and information, to monitor safety and to check on employees working around hazardous areas.[542] However, 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. Due to the continuous pressure associated with video surveillance, personal rights are especially at risk in the workplace,[543] therefore giving the subject of various international research projects in the last decade.[544] The national level of camera use regulation in European workplaces is heavily influenced by the general framework of the EU law, yet do not cover all aspects of CCTV surveillance.[545] The legal form and scope of video monitoring regulations differ due to the implementation of EU directives in the Member States, even there is a lack of specific legislation on this issue in some countries.[546] In order to form a common jurisdiction in this field the European Data Protection Supervisor issued a guideline on video surveillance in 2010.[547]

2.5.1. Hungarian regulation

2.5.1.1. Legislation

Under the Hungarian regulation there are no specific rules in the Labour Code on the installation and use of CCTV systems in the workplace,[548] 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 the Data Protection Commissioner.

2.5.1.2. Judicial case law

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. Only one employee has filed a lawsuit against an employer because of the installation and use of a hidden camera in the place of his continuous work. In this case the court has applied only the provisions of the Civil Code, not even mentioning the Data Protection Act, and decided contrary to the jurisdiction of the Data Protection Commissioner, allowing this practice for the employer.[549] Consequently we have no explicit court decision on the conditions of the legitimate use of video surveillance.

[541] Nouwt/de Vries/Loermans, 2005, p. 348. Cf. also Stanton/Stam, 2006, p. 241.
[542] Petersen, 2007, p. 523.
[543] BAG, NZA 1988, 92; NZA 2003, 1193, 1194; NZA 2004, 1278, 1281.
[544] e.g. "Reasonable expectations of privacy and the reality of data protection" research project carried out by TILT, Tilburg Institute for Law, Technology, and Society 2002-2004.
[545] Nouwt/de Vries/Loermans, 2005, pp. 325-326.
[546] Nouwt/de Vries/Loermans, 2005, p. 331.
[547] EDPS Video-surveillance Guidelines, 17 March 2010
[548] Arany Tóth, 2008. p. 277; Szabó/Székely, 2005, pp. 278-279.
[549] Szegedi Ítélőtábla, Pf. II. 20348/2010.

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.[550]

2.5.1.3. Case law of the Data Protection Commissioner

The crucial point of debate on the legitimate use of CCTV systems is the goal of the 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 staffs 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.

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.[551] 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.[552]

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.[553] Consequently the operation of a hidden camera is a serious and extreme infringement of Employee Privacy.[554]

2.5.1.4. 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.[555] 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

[550] 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.
[551] E.g. DPC, 94/A/2002 Cf. the details in Szabó/Székely, 2005, pp. 268-269.
[552] DPC, 461/A/1998
[553] DPC, 475/H/2000
[554] Arany Tóth, 2008, p. 289.
[555] Majtényi, 2006, pp. 347-348.

consideration, as these details can reasonably affect the legitimacy of the surveillance. She highlights that the individualized observation of a given employee, as well as monitoring with the use of hidden cameras are unlawful acts.[556] 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.[557]

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.[558] 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.[559]

2.5.1.5. 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."

2.5.2. German regulation

2.5.2.1. Cases from the jurisdiction

In a number of decisions[560] the Court has indicated that the privacy rights of employees takes general precedence over the security interests of the employer.[561]

2.5.2.2. Academic debate[562]

In respect of methods of video surveillance, a distinction must be made between publicly and privately accessible areas and between overt and covert systems.

---

[556] Arany Tóth, 2008, pp. 287-289.
[557] Arany Tóth, 2008, pp. 294., 311.
[558] Jóri/Hegedűs/Kerekes, 2010, p. 286. Cf. also 35/2002. (VII.19.) AB decision.
[559] Szőke, 2011, p. 204.
[560] BAG, RDV 1988, 137; NZA 1988, 92 RDV 1992, 178; NJW 2003, 3436; NJW 2005, 313; RDV 2005, 216; RDV 2008, 238.
[561] Gola, 2010a, mgn. 65.
[562] For a legal evaluation of Camera-Dummies cf. detail Kirsch, 2011, 317919.

2.5.2.2.1. Video surveillance in publicly accessible areas, Article 6b of the Federal Data Protection Act

After the re-introduction of Article 6b of the BDSG, a legal basis is provided in German law for the surveillance of publicly accessible areas. Article 6b paragraph 1 of the BDSG regulates the question of admissibility of the collection of personal data by means of optical-electronic devices.[563] It is clear from the explanatory memorandum, the objective of the standard is the preservation of informational self-determination by means of an appropriate balance of interests.[564] A regulation should be developed, which on the side of the operator of the installation provides for a restrictive practice, whereby video surveillance is limited to sensitive observation purposes.[565] Due to the fact that even the observation itself is recorded, the relevance of data protection law shall not depend on whether or not the image material is stored in the port.[566] What is normally referred to by the provision set out in Article 6b of the BDSG are public and private places within the meaning of Article 2 of the BDSG within the framework set by the regulation. If video surveillance is conducted on behalf of the employer by a contractor, according to Article 11 of the BDSG, in the case of contract data-processing, the corresponding place shall continue to be so.[567]

Scope of application

The scope of application of Article 6b of the BDSG is limited to publicly accessible rooms. Due to the literal meaning of the term 'room' what is to be understood is a three-dimensional space - i.e., in addition to the floor, the space above this surface is also covered.[568] In addition, it is unclear what requirements a 'publicly accessible space' should meet. On the one hand, opinion is that the room should be defined as a constructionally delimitable enclosed place.[569] Others reject this criterion. The reason given is that an adequate requirement can be derived neither from the wording of Article 6b of the BDSG nor from legal argument.[570] The decisive point is rather whether, according to the wish of the legal owner, the room is dedicated to the public or to public traffic.[571] Therefore, such places fall within the scope of application, whose intended purpose is to be visited or used by an indefinite number of persons or by persons identified only according to general characteristics.[572] Accordingly, public use is only indisputable if a decision to allow public use has been made by the persons entitled to do so.[573] In accordance with the explanatory memorandum, this also includes platforms, the exhibition halls of museums, retail shops[574] or ticket halls.[575] In assessing whether work

[563] Zscherpe, 2010, 6b BDSG mgn. 21.
[564] Bundestag, 2000a, p. 38.
[565] Zscherpe, 2010, § 6b BDSG mgn. 5; Gola/Schomerus, 2010, § 6b BDSG mgn. 1.
[566] Bundestag, 2000a, p. 38.
[567] Zscherpe, 2010, § 6b BDSG mgn. 19.
[568] Zscherpe, 2010, § 6b BDSG mgn. 31.
[569] For prevailing opinion, cf. only Bizer, 2011, § 6b BDSG mgn. 36.
[570] Zscherpe, 2010, § 6b BDSG mgn. 32; Gola/Schumerus, 2010, § 6b BDSG mgn. 8.
[571] Bizer, 2011, § 6b BDSG mgn. 37; Gola/Schumerus, 2010, § 6b BDSG mgn. 12.
[572] BAG, NZA 2004, 1278, 1282; NJOZ 2005, 2708, 2713; Zscherpe, 2010, § 6b BDSG mgn. 32.
[573] Gola/Schumerus, 2010, § 6b BDSG, mgn. 9.
[574] Such as shops or stores, Bayreuther, 2005, p. 1038, who adds banks, filling stations and restaurants as examples.
[575] Bundestag, 2000, p. 38.

places are to be classified as public places, a differentiated approach should be adopted. In the case of these, public accessibility is often missing.[576] Article 6b of the BDSG is therefore only a guide for the admissibility of video surveillance of publicly accessible places, if the employees perform their work in premises open to the public.[577] In individual cases making a distinction between publicly accessible and non-public places may run into difficulties. There were attempts to withdraw the cash desk area of a supermarket from the scope of application of the provision as an enclave within the public sales area not directly accessible by public traffic.[578] However, for technical reasons, it is quite unavoidable that a video camera directed on the cash area not accessible to customers, will also record parts of the publicly accessible area or that customers – e.g. during the payment process when entering the PIN code of their bankcard – will find themselves in range of the camera.[579] Consequently, the cash area cannot be classified as a separate, delimitable place within the publicly accessible area.[580] It remains to be established that Article 6b of the BDSG can be the sole permissive rule for the observation of publicly accessible places; the infringement of the limits between the public and non-public places is however currently not permitted. Thus, cameras must be positioned in a manner in which solely the public place is observed.[581]

Open video surveillance

The question is how open video surveillance of publicly accessible places should be evaluated in legal terms.

Details of admissibility

According to Article 6b paragraph 1 of the BDSG, the observation of publicly accessible places by means of optical electronic devises (video surveillance) is only permitted if it is required only to fulfil the duties of the authorities (Nr. 1), to exercise householder's rights (Nr. 2) or to safeguard specified interests (Nr. 3) and there are no indications that legitimate interests outweigh those affected. When it comes to assessing the admissibility of video surveillance, therefore, a number of steps are to be implemented.

Carrying out lawful video surveillance in accordance with § 6b paragraph 1 of the BDSG requires first a permissible observation purpose.[582] In the area of employee data, according to Nr. 1, the purpose is only of minor significance and also the perception of company regulations (Nr.2.) serve only rarely as the legal basis for video surveillance.[583] Thus, the company regulations include the civil rights of the owner (Articles 903 f., 1004 of the BGB), and of the authorized user (Articles 859 ff. of the BGB), which are aimed at expelling the

[576] Meyer, 2009, p. 15; Zscherpe, 2010, § 6b BDSG mgn. 37. Grimm/Schiefer, 2009, p. 331.
[577] Grimm/Schiefer, 2009, p. 331; Däubler, 2001b, p. 874; Wiese, 2004, p. 923; Gola/Klug, 2004, p. 72.
[578] LAG Mecklenburg-Vorpommern – 1 Sa 387/03; Helle, 2004, p. 346.
[579] Grimm/Schiefer, 2009, p. 331.
[580] ArbG Frankfurt, RDV 2006, 314; Wank, 2011, § 6b BDSG mgn. 1; Grimm/Brock/Windeln, 2006, p. 180; Wilke, 2006, p. 33; Grimm/Schiefer, 2009, p. 331. For further debatable cases cf. Zscherpe, 2010, § 6b BDSG mgn. 36. Cf. further Bayreuther, 2005, p. 1039. re the organisation of branches in shopping centres.
[581] Zscherpe, 2010, 6b BDSG mgn. 38; different view earlier BGH, NJW 1995, 1955, 1956.
[582] Zscherpe, 2010, 6b BDSG mgn. 51.
[583] Thüsing, 2010, mgn. 353 f.

troublemaker from a room and also at prohibiting his/her future entry.[584] However, employees must obtain access to the work place in order to be able to perform their job,[585] and so the perception of the legitimate interests for the precisely specified purposes (Nr.3)[586] is the most important purpose of the video surveillance of publicly accessible places.[587]

In a second step the appropriateness and necessity of the measure (Article 6b paragraph.1 last main clause of the BDSG) must be reviewed. According to this, a measure is necessary if it represents the least stringent among the available and equally appropriate means necessary to achieve the desired success. In this context it is necessary to clarify whether and how the purpose of monitoring can be achieved and whether the selected video surveillance is at all objectively suitable for this purpose.[588] It is also necessary to consider whether the objective pursued could have been achieved even with a milder, equally effective [589] means, which however is less restrictive regarding the personal rights of employees.[590]. Due to the scope, video surveillance must therefore be limited functionally and spatially to a necessary minimum extent.[591] Concerning this, it should be considered whether the increased use of security personnel or the use of other security devices (e.g. locks, safety checks) would also serve the purpose and could therefore replace the use of video surveillance.[592] As long as this is the case, video surveillance would be inadmissible due to the lack of necessity. Regarding the implementation of control measures, among others it is to the principle of data avoidance and data economy set out in Article 3a of the BDSG.[593] Mostly video surveillance is among several equally appropriate means the most invasive one.[594] Furthermore, as far as possible, cameras should be installed so that as little personal information is collected, as possible, for example, videos shall only be recorded, if it is really necessary (e.g. during bank- or shop business hours) and in spatial terms only the scope is recorded, which is really necessary for the purpose.[595] If solving of inventory discrepancies is at issue, employees may only be observed by means of video surveillance, if measures of internal audit and revisions of the enterprise's resource planning system taken in advance, and other examinations of work processes have not yield a result.[596] In assessing the question of whether there are other technical alternatives available, it should be considered, whether the stored records are necessary or remote monitoring is also sufficient.[597] This latter was classified by the court

[584] Bizer, 2011, § 6b BDSG mgn. 48; Müller, 2008, p. 456. Should however the employer have a need to monitor (e.g., to keep a somewhat drunken employee off the premises), then as a rule there would be no requirement for the monitoring measures (for this purpose immediately), cf. Thüsing, 2010, mgn. 354.
[585] BAG, NZA 2004, 1278, 1283; NJOZ 2005, 2708, 2714.
[586] The purpose according to Nr. 3 could be only according to Bundestag, 2001, p. 61; only for non-public places.
[587] Thüsing, 2010, mgn. 355.
[588] Zscherpe, 2010, § 6b BDSG, mgn. 51; Bizer, 2011, § 6b BDSG mgn. 56
[589] Wedde, 2009, § 6b BDSG mgn. 39; Bayreuther, 2005, p. 1040.
[590] Zscherpe, 2010, § 6b BDSG mgn. 51.
[591] BAGE 127, 276 mgn. 20; BAG, NZA 2004, 1278, 128; Bergmann/Möhrle/Herb, 2011, § 6b BDSG mgn. 27.
[592] Zscherpe, 2010, § 6b BDSG mgn. 55 in conjunction with mgn. 51.
[593] Zscherpe, 2010, § 6b BDSG mgn. 56; Wedde, 2009, § 6b BDSG mgn. 41.
[594] Thüsing, 2010, mgn. 356.
[595] Zscherpe, 2010, § 6b BDSG mgn. 56
[596] BAG, NZA 2003, 1193, 1195; ArbG Düsseldorf, NZA-RR 2004, 345, 346.
[597] BAGE 127, 276 mgn. 27; BAG, NZA 2004, 1278, 1283.

however as not equally effective as recording, in particular for the investigation of theft.[598] The approach, the considerations of which include the alternative of a human rather than technical observation by supervisors and colleagues,[599] raises practical concerns. It is, therefore, a criticism that equal suitability of the means used tends not to apply, especially if the misconduct to be cleared up is aimed at secrecy.[600] Apart from that, it is doubtful whether in-house spying would affect the personal rights of employees less that open video surveillance.[601]

As a final step, as it follows also from Article 6b paragraph 1 last main clause of the BDSG, that an examination of appropriateness[602] should take place. Here, the employer's interests represented by video surveillance and the monitoring purposes should be weighed against the legitimate interests of the employees involved in the observation.[603] In this regard, conflicts of constitutional rights can often arise, such as the right to informational self-determination and the right to privacy on the one hand, and property and physical integrity (for example in case of impending attacks) on side of the employer.[604] The degree of importance attached to the interests of the observed persons in the course of consideration, depends largely on the intensity of the invasion of the general right to privacy.[605] In particular, spatial, temporal, personnel and technical factors may play a role in the consideration. Important in terms of classification of the severity of the infringement is the place where the surveillance takes place.[606] In any case, observations are inadmissible that violate the privacy of the people observed, such as the surveillance of toilets and changing rooms for theft prevention.[607] In general, observation will not include particularly sensitive issues of privacy, but will rather encroach on the less vulnerable social sphere.[608] It must be noted here that workers in publicly accessible places are in such an environment where they cannot assume that they are always unobserved.[609] Additionally, the temporal component is significant in terms of the extent of the observation pressure generated by the video surveillance system. On the one hand it is decisive whether the surveillance measure is limited to a specified period or is performed

[598] BAGE 127, 276 mgn. 27.
[599] BAG, NZA 2003, 1193, 1195; NZA 2004, 1278, 1283. This could, in the view of the BAG, happen specifically with employees involved in monitoring duties and possibly including exit-control and personal checking, NZA 2004, 1278, 1283. Active parties should, in the framework of their assessment prerogative be prepared to relinquish such measures if stolen goods are "not without further ado recognisable as such", BAGE 127, 276 mgn. 27.
[600] BAG NZA 2003, 1193, 1195; Grimm/Brock/Windeln, 2006, p. 180.
[601] Bayreuther, 2005, p. 1040.
[602] Proportionality in the narrow sense, BVerfG, NJW 2008, 1505, 1515; BAGE 127, 276 mgn. 31.
[603] Grimm/Schiefer, 2009, p. 331. If necessary the fundamental law re third parties must be borne in mind. With a view to video surveillance of postal distribution centres the BAG has incorporated in its weighting of interests the privacy of letters (Art. 10 GG) as well as property rights (Art. 14 GG) of the potential of customers affected by postal theft to be included in consideration, BAG, NZA 2004, 1278, 1283; E 127, 276 mgn. 21, 24.
[604] Zscherpe, 2010, § 6b BDSG mgn. 59.
[605] BAGE 127, 276 mgn. 21; Grimm/Schiefer, 2009, p. 331.
[606] Grimm/Schiefer, 2009, p. 331.
[607] Bundestag, 2001, p. 62; Zscherpe, 2010, § 6b BDSG mgn. 60.
[608] BAG, NZA 2003, 1193, 1195; comprehensively in terms of gradation as developed by the BVerfG within the sphere of personal rights. Wank, 2011, Art. 2 GG mgn. 60 (with further references); Grimm/Schiefer, 2009, p. 331.
[609] BAG, NZA 2003, 1193, 1195.

permanently.[610] On the other hand, it is important to know how many hours per week monitoring takes place and whether the employees have any knowledge of the operating hours of the surveillance system.[611] In quantitative terms, the number of people affected by the monitoring plays a role.[612] Further, it is important whether the persons involved have created an attributable cause for the surveillance (e.g. by violating the law) or whether this was done without giving reasons.[613] It may, however, be taken into account that those affected by the surveillance are thus given the possibility of being relieved of suspicion of a crime or wrongdoing.[614] In technical terms it is a determinant factor of consideration whether the employer uses analogue or digital recording technology.[615] By using digital video recording, it is possible to process the acquired images automatically and also to zoom out and filter individual persons.[616] The invasion of the right to privacy may be accordingly intensive.[617] The use of so-called 'thinking cameras', which are able to evaluate images independently according to predefined patterns, and to trigger alarms when abnormalities happen, is to be evaluated even more critically.[618] There may also be cases where the interests of the person concerned are critically impaired if, for example, he is not identifiable by the observers (primarily because the optical-electronic device works with low resolution).[619] As a result, therefore, general statements regarding the balancing of interests are prohibited.[620]

Targeted surveillance of employees

As a rationale for targeted surveillance of employees the suspected committing of a crime or other misconduct may be considered.[621]

In terms of assessing the admissibility of video surveillance measure the degree of suspicion and the concrete situation is relevant and decisive. According to the Federal Labour Court this is to be determined on the basis of evaluating the overall circumstances by weighing up the intensity of the infringement against the weight of justifiable reasons.[622] The secret video surveillance of an employee[623] is permitted in the event of concrete suspicion of a criminal offence or other serious misconduct committed to the detriment of the employer, less

[610] BAG, NZA 2004, 1278, 1281.
[611] BAG, NZA 2004, 1278, 1284.
[612] BAGE 127, 276 mgn. 39; BAG, NZA 2004, 1278, 1284.
[613] BAGE 127, 276 mgn. 21.
[614] BAG, NZA 2003, 1193, 1195.
[615] Grimm/Schiefer, 2009, p. 332. Video monitoring with the use of digital technology makes use of an automated processing operation, in the sense of § 3 par. 2 s. 1 BDSG, Wedde, 2009, § 6b BDSG mgn. 7; Bergmann/Möhrle/Herb, 2011, § 6b BDSG mgn. 5. For such an operation § 4d Para. 1 BDSG laid down a reporting requirement according to § 4e BDSG. It is imperative that there be a regular pre-check of the video monitoring system in the sense of 4d Para. 5 BDSG, Scheja, 2010, § 4d BDSG mgn. 65.
[616] Grimm/Schiefer, 2009, p. 332
[617] BAG, NZA 2004, 1278, 1284.
[618] Gola/Wronka, 2010, mgn 844; Oberwetter, 2008, p. 610. On smart cameras and automatic behaviour analysis cf. Hornung/Desoi, 2011, p. 153.
[619] Zscherpe, 2010, § 6b BDSG mgn. 65.
[620] Also cf. Grimm/Schiefer, 2009, p. 332.
[621] Grimm/Schiefer, 2009, p. 332.
[622] Constant jurisdiction of the BVerfG (NJW 2008, 1505, 1505 with reference to E 109, 279); BAG, NZA 2004, 1278, 1280 f.; NZA, 2008, 1187, 1190.
[623] In the concrete case it was a question of the monitoring of the cash-till area of a supermarket.

restrictive means to investigate the suspicions have been exhausted, the hidden video surveillance is practically the only remaining means and is otherwise not considered as disproportionate.[624] The initial suspicion needed for open video surveillance must be sufficiently specific in personal, spatial and functional terms. As a measure, it is proposed to assume, but at the same time also to be content that the alleged misconduct can be handled, is likely to be contained and is generally likely to happen.[625] The disproportionate nature of surveillance does not come from the mere fact that suspicion is not only and solely limited to the employee observed. In this regard, there must be proportionality in the sense that the observation is used to limit the suspicion already identified in spatial and functional terms to a concrete person. At the same time, monitoring represents the only means of excluding other employers from the narrow circle of suspects.[626] In the resolutions concerning mail distribution centres, the Federal Labour Court also addressed the question of suspicious circumstances.[627] According to the basic message, it may be established from the decisions that video surveillance can be proportionate at least if carried out independent of a suspected offence of specified individuals and is limited in spatial terms to the area of suspicious action, and, in temporal terms, to the investigation of the incident. Regulations without any spatial, temporal and personal limitations are inadmissible. However, since a far larger group of uninvolved employees will be involved in the surveillance, the privacy rights of many more employees will be encroached on without giving rise to such.[628] In this respect also no video surveillance may take place for the mere monitoring of employees' performance and organisational conduct.[629]

The question of whether the targeted surveillance of employees may be performed even if the threshold of the case of suspect sufficiently concretized in personal, physical and functional terms is not yet reached, remains unanswered by the courts. In the literature, it is proposed to consider such an approach, at least for monitoring the employees' performance and organisational conduct in the absence of suspicion as inadmissible. To be able to safeguard the interest of the employer, the employee's job performance to a specific degree in a quality manner and thus to compare it to the remuneration payable, breach of the employee's privacy rights - intensive due to permanent monitoring pressure - cannot be justified.[630]

There are situations conceivable in which, although there are still no adequate grounds for suspecting an employee of a criminal offence, the need for crime prevention exists because of the particularly high risk of crime being committed in the workplace. In such situations, the employer's interests are less at risk with the result that an abstract-preventive observation can be considered only in exceptional cases.[631] This requires the existence of a special risk situation,[632] i.e. a hazardous situation which goes beyond the general possibility of the risk of

[624] BAG NZA 2003, 1187, 1193.
[625] Bayreuther, 2005, p. 1039.
[626] BAG, NZA 2003, 1193, 1195.
[627] BAG, NZA 2004, 1278; NZA, 2008, 1187, 1190.
[628] BAG, NZA, 2008, 1187, 1191.
[629] Bayreuther, 2005, p. 1039.
[630] Bayreuther, 2005, p. 1039; Grimm/Schiefer, 2009, p. 332.
[631] Bayreuther, 2005, p. 1039.
[632] BAG, NZA 2004, 1278, 1283 f.

crime.[633] This must be explained in detail by the employer,[634] and the explanation must meet stringent requirements. In addition to the likelihood of the occurrence of criminal offences, possible damage can also constitute a serious reason.[635] It is proposed, therefore, that consideration should favour the employer's interest in prevention, this at the expense of the personal rights of employees, if already isolated instances of misbehaviour can cause serious damage.[636]

Video surveillance of non-involved third parties

In companies serving the public the focus of surveillance is mostly not on a targeted employee, although this constitutes a generally desirable by-product.[637] For the operators of optical-electronic devices it will be important primarily to preserve their in-house authority within the property boundaries[638] and to use video surveillance for preventive purposes[639] or as a repressive means for the prosecution of offenders.[640] It has not yet been cleared, whether and to what extent the principles established by case law apply, if employees are also merely monitored. Partly, it is proposed to treat the same set of circumstances as in the case of targeted employee surveillance.[641] This approach, however, crosses factual boundaries, since the, now usual, independent video surveillance is inadmissible in supermarkets, banks, museums, or on railway station platforms once employees come into the recording field of the camera (which, in practice, cannot be avoided,[642] since the range of goods must be checked and filled in supermarkets and the waste containers must be emptied on railway platforms). Another view argues that video surveillance is always to be accepted as inherent in the workplace, if permitted in relation to any third party in accordance with Article 6b of the BDSG.[643] This is perceived as inadequate, because in Article 6b of the BDSG the legitimate interests of all stakeholders are taken into account, hence also those of the observed employees.[644] Nevertheless, it is found that in the case of the surveillance of non-operating third party as the employer's main motive, a preventive purpose could be considered as fundamentally legitimate.[645] At this point, the set of interests differ from that of the targeted surveillance of employees.[646]

Temporal boundaries of increasing surveillance and adaptation pressure

[633] Grimm/Schiefer, 2009, p. 332.
[634] BAG, NZA 2004, 1278, 1283.
[635] Grimm/Schiefer, 2009, p. 333.
[636] Grimm/Schiefer, 2009, p. 333 with reference to the example named by Bayreuther, 2005, p. 1039 mgn. 7 of the monitoring of employees in a diamond polishing establishment and of the relevant note that, in general, security-related areas are not open to the public.
[637] Grimm/Schiefer, 2009, p. 333.
[638] BGH, NJW 1995, 1955, 1957; Gola/Schomerus, 2010, § 6b BDSG mgn. 16 (with further references).
[639] There are preventive objectives especially in avoiding theft, criminal damage or disturbance, BAG NZA 2008, 1187, 1193.
[640] Wedde, 2009, § 6b BDSG mgn. 33.
[641] Roloff, 2009, § 5 mgn. 39.
[642] Grimm/Schiefer, 2009, p. 333.
[643] Gola/Wronka, 2010, mgn 816. Cf. further SG München RDV 1992, 85.
[644] Bayreuther, 2005, p. 1039; Grimm/Schiefer, 2009, p. 333.
[645] Grimm/Brock/Windeln, 2006, p. 180.
[646] Grimm/Schiefer, 2009, p. 333 with reference to the of the BAG (NZA 1187, 1193).

So far the question has remained unclear how long workers must endure the surveillance and adaptation pressure. In the literature, efforts are made to make a distinction in this context between the different operating areas. When monitoring the outside and entrance areas, the mentioned pressure can be classified as rather low, due to the fact that employees rarely do their work there. The situation is different in the publicly accessible and for the employer sensitive indoor areas. Even if the situation is, for the employees, very close to constant surveillance pressure, the interests of the employer are to be classified as more substantial relative to those of the involved employees - at least in the case, when, in the inside areas, video surveillance is the only promising way to take preventive action against crime by customers.[647] This can be assumed, at least for a publicly accessible company, in which the commission of certain crimes[648] represent a typical business risk.[649] This does not require the realisation of the danger. On the contrary, it is unreasonable for the owner of the company to wait for the installation of a video camera until he himself first becomes the victim of such an offence.[650] Regarding the risk of criminal offences committed by customers, the owner of the company considers himself to be exposed to a clearly larger, typically anonymous group of potential offenders than the case would be regarding crime committed by employees. The interests of the employer protected by Article 14 of the GG weighs accordingly heavy in protecting his in-house authority and protection of his property.[651] In contrast, on the employees' side it is a relatively minor breach of privacy, if their surveillance is not the purpose but only an unintended side effect of preventive video surveillance. In most cases, workers are staying only temporarily in the focus of the camera. Also note that, for example, in the case of the surveillance of bank branches, the surveillance serves ultimately also for their own security.[652] Against this background, in order to encroach on the privacy right as little as possible, video equipment may not be used in an inappropriate manner in order to perform the targeted surveillance if employees.[653] For the prevention of store robberies it is sufficient, for example, to direct the camera at the cash desk passage, instead of focusing on watching the conduct of the employees by means of directing it on to the cash register itself.[654] This would again require concrete suspicion.[655]

Secret video surveillance in public places despite Article 6b paragraph 2 of the BDSG?

The Federal Labour Court has considered secret video surveillance in public places in circumstances of a concrete suspicion of a crime or other serious misconduct as permissible. The employer can claim permissibility, to the detriment of the employer, if less restrictive measures had been exhausted and covert video surveillance was thus the only remaining means left for the business and this was not, overall, disproportionate.[656] Due to the fact that,

[647] Grimm/Schiefer, 2009, p. 333.
[648] E.g. shoplifting on retail premises or hold-ups in banks, Bayreuther, 2005, p. 1039.
[649] Wiese, 2004, p. 925
[650] Bayreuther, 2005, p. 1039.
[651] Grimm/Schiefer, 2009, p. 333; similar also BAG, NZA, 1193, 1195.
[652] Grimm/Schiefer, 2009, p. 333 f.
[653] Grimm/Schiefer, 2009, p. 334.
[654] Cf. also BAG, NZA, 1193, 1195.
[655] Grimm/Schiefer, 2009, p. 334.
[656] BAG, NZA 2003, 1193, 1195; left open by LAG Sachsen-Anhalt – 11 Sa 522/07.

in respect of secret video surveillance, prior legal protection is virtually precluded and subsequent legal protection is made difficult, this weighs more heavily on the judiciary than does open surveillance.[657] Whether, despite the introduction of Article 6b of the BDSG and the associated requirements, the fact of observation and the responsible entity can be made recognizable and restrained by appropriate measures (Article 6b paragraph 2 of the BDSG) is arguable. The purpose of the norm is primarily to ensure transparency.[658] The affected party should be able to adjust his behaviour in a manner that he may be observed or to be able to avoid observation.[659] Therefore, recognisability is a prerequisite for the legality of video surveillance in publicly accessible areas.[660] As to which requirements are prescribed concerning recognisability, the question is answered inconsistently. On the one hand, the installation of the camera in such a manner that it is clearly seen when entering the public space should be sufficient. However, on the other hand, hanging a sign - or even indicating whether people are observed or recorded, is required.[661] Although others see no need for detailed information about the nature of the surveillance, they require at least some recognizable reference to the camera, which rules out covert action.[662] As is apparent from the wording,[663] to make the observation identifiable is the obligation of the responsible entity.[664] Accordingly, some argue that covert video surveillance is *per se* and without exception inadmissible and, despite the associated consequence that, for employers this will be the only effective means used in individual cases to clear up criminal offences, if committing such is based on secrecy.[665] Hence, recognising exceptions to the prohibition of secret video surveillance as recourse to general reasons for justification and the grounds for excuse,[666] is argued against.[667] This contradicts a number of representatives who affirm the applicability of general reasons for justification and legal excuse.[668] It is mentioned, in respect of the latter view in particular, that, if the legislature had wished, exceptionally, to exclude the applicability of these interdisciplinary legal principles from the area of data protection law, it would have required an express exclusion of this regulation.[669] If we apply this reasoning, then, in exceptional situations, it is possible to conduct covert video surveillance in public places in spite of Article 6b Paragraph 2 of the BDSG - which can be supported by the legislation of the Federal Labour Court.

---

[657] *BVerfG*, NJW 2008, 1505, 1507 f.; BAG, NZA 2008, 1187, 1190.
[658] Bundestag, 2000a, p. 38.
[659] Zscherpe, 2010, § 6b BDSG mgn. 66.
[660] AG Frankfurt – 7 Ca 3342/05 mgn. 53; Bayreuther, NZA 2005, 1038, 1040, Roloff, 2009, § 5 mgn. 38; Maschmann, 2002, p. 17; dubious is: Gola/Schomerus , 2010, § 6b BDSG mgn. 28.
[661] For opinions cf. Gola/Schomerus, 2010, § 6b BDSG mgn. 25 f.; Bizer, 2011, § 6b BDSG mgn. 68, 70.
[662] Bizer, 2011, § 6b BDSG mgn. 67; Grimm/Schiefer, 2009, p. 334.
[663] „Sind“ (translated: „are“), cf. § 6b par. 2 BDSG.
[664] Zscherpe, 2010, § 6b BDSG mgn. 66; Grimm/Schiefer, 2009, p. 334.
[665] Bayreuther, 2005, p. 1040.
[666] Self-defence (§§ 227 BGB, § 32 StGB) and also emergence (§ 34 StGB) can be considered as justification, Grimm/Schiefer, 2009, p. 334.
[667] Bayreuther, 2005, p. 1040f.
[668] ArbG Freiburg – 4 Ca 128/04; Grosjean, 2003, p. 2651; Grimm/Brock/Windeln, 2006, p. 181. In details cf. Grimm/Schiefer, 2009, pp. 334-335.
[669] Grosjean, 2003, p. 2651; Grimm/Brock/Windeln, 2006, p. 181, Grimm/Schiefer, 2009, p. 334.

Legality of further use, Article 6b Paragraph 3-5 of the BDSG

From the admissibility of observation under Article 6b paragraph 1 of the BDSG, the legitimacy of the processing or use of personal data obtained under paragraph 3 does not automatically follow. This requires separate examination.[670] According to Article 6b paragraph 3 clause 1 of the BDSG, the processing or use of data collected under paragraph 1 shall be allowed if it is necessary to achieve the objective pursued and there are no indications that the legitimate interests of those affected are damaged. As a result, for each processing step of data produced by video surveillance, an independent balancing of interests must take place.[671] If the data are no longer required to achieve the purpose or the legitimate interests of those affected are in conflict with further storage, they must be immediately deleted (Article 6b paragraph 5 of the BDSG),[672] i.e. usually within one to two working days. The most effective way to meet the automatic deletion requirement is through periodic deletion, or through self-overwriting of past recordings. Again, the principle of data avoidance and data economy (Article 3a of the BDSG) in this context is crucial.[673] If the data collected by video surveillance are assigned to a particular person, the duty to notify shall exist regarding the processing or use, in accordance with Articles 19a and 33 of the BDSG, see Article 6b paragraph 4 of the BDSG. Specifying a purpose to be determined, on a case-by-case basis, and as mentioned in Article 6b paragraph 3 clause 1 of the BDSG, has particular importance.[674] The admissibility of any further processing of the images must strictly follow the precise purpose of the observation to be determined according to Article 6b paragraph 1 of the BDSG.[675] The processing or use of the data for other purposes is possible only under the conditions set out in Article 6b paragraph 3 clause 3 of the BDSG, i.e., to the extent necessary to prevent threats to the state and public security and to prosecute crimes.

2.5.2.2.2. Video surveillance of publicly inaccessible areas

It is also unclear to what degree video surveillance is aimed at non-public areas.[676] Non-public places include all spaces which may be entered only by a certain group of people.[677]

Justification by consent

Again starting from the point of preventive prohibition and subject to permission as stipulated in Article 4 paragraph 1 of the BDSG, the admissibility of the video surveillance of publicly inaccessible areas may arise from the consent given by workers, as long as this possibility is allowed in the employment relationship.[678]

---

[670] Bundestag, 2001, p. 62; Schaffland/Wiltfang, 2010, § 6b BDSG mgn. 5; Bizer, 2011 § 6b BDSG mgn. 75; Zscherpe, 2010, § 6b BDSG mgn. 76
[671] Bizer, 2011, 6b BDSG mgn. 75.
[672] Consequently, without culpable hesitation, cf. § 121 par. 1 s.1 BGB, Thüsing, 2010, mgn. 359.
[673] Bundestag, 2001, p. 63.
[674] Zscherpe, 2010, § 6b BDSG mgn. 77.
[675] Grimm/Schiefer, 2009, p. 335.
[676] Grimm/Schiefer, 2009, p. 335. Measures designed simply to trick the employees are however forbidden (§ 226 BGB), Thüsing, 2010, mgn. 361.
[677] Bizer, 2011, § 6b BDSG mgn. 43.
[678] See also above - section 1.3.2.4.1.

No analogous application of Article 6b of the BDSG

The use of Article 6b of the BDSG could be considered as other legislation in accordance with Article 4 paragraph 1 of the BDSG analogously for video surveillance in publicly inaccessible work places. The prerequisite for an analogy is the existence of an unintended regulatory gap, and also comparative interests.[679] However, there are currently no unintended regulatory gaps,[680] and so the legislator deliberately restricted the scope of application of Article 6b of the BDSG regarding publicly accessible areas, and the need for special regulations was emphasised as part of a separate Employee Data Protection Act.[681] Comparable interests are also lacking. In contrast to publicly accessible places, this does not involve a group of mostly anonymous people recorded by the camera for only a very short time, but the employees observed are well-known to the employer in non-publicly accessible workplaces.[682] Since the employees spend a longer period of time at their respective workplaces, and due to their contractual obligations, they usually have no possibility to avoid observation and are exposed to much longer monitoring and greater pressure to conform.[683] The fact that, in individual cases, the intensity of invasion can be larger in publicly accessible than in publicly inaccessible places,[684] is not in contradiction to the fact that, when drafting Article 6b of the BDSG, the legislator focused on rather less intensive encroachment.[685]

Breach of Articles §§ 28, 32 of the BDSG

To the extent that Article 6b of the BDSG is inapplicable – as in the case of video surveillance in publicly inaccessible places - the admissibility of video surveillance measures are determined depending on the objectives pursued by the surveillance measures according to Articles 28 and 32 of the BDSG.[686]

Open surveillance

Although for repressive purposes, Article 32 paragraph 1 clause 2 of the Federal BDSG is applied for open video surveillance of publicly inaccessible areas, it must not be generally used for the conviction of the perpetrator.[687] Other cases are to be measured against Article 32 paragraph 1 clause 1 of the BDSG and in accordance with the government reasoning also against Article 28 paragraph 1 No. 2 of the BDSG.[688] Just as in the case of Article 6b of the BDSG, the measure must not only be appropriate and necessary, but it must also be fair, which again depends on the individual case and requires the consideration of legal interests.[689]

---

[679] Cf. the extraordinary vote of Judge Haas, BVerfGE 115, 51, 74: 'An analogy can be conceived with the appearance of some loophole unforeseen by the legislator where, on grounds of concrete circumstances this can be positively determined."
[680] BAG NZA 2004, 1278, 1282; Maties, 2008, p. 2221.
[681] Bundestag, 2000a, p. 38.
[682] Grimm/Schiefer, 2009, p. 336.
[683] BAG, NZA 2004, 1278, 1282.
[684] Bayreuther, 2005, p. 1041.
[685] Grimm/Schiefer, 2009, p. 336.
[686] Thüsing, 2010, mgn. 347 f.
[687] Thüsing, 2010, mgn. 360.
[688] Thüsing, 2010, mgn. 361, which leads further (mgn. 348) whether § 28 par. 1 s. 1 no. 2 BDSG can further be applicable.
[689] Thüsing, 2010, mgn. 362.

According to government reasoning, the data protection principles developed by the Federal Labour Court are to be taken as the basis of such consideration,[690] and here again, in particular, account should be taken of the principle of proportionality.[691] Under narrow circumstances, the balancing of interests can fail at the expense of the employees,[692] if, in the case of employee surveillance in publicly inaccessible places, it is a by-product of other surveillance purposes,[693] and the measure also serves to protect the employees working there, or the employer has a legally justified security interest.[694]

Covert surveillance

Concerning publicly inaccessible places, there raises the problem of whether or not Article 6b Paragraph 2 of the BDSG reveals a blocking effect.[695] According to government reasoning, a special statutory regulation is needed for covert surveillance.[696] Regarding the balancing of interests, it should again be noted that the self-protection possibilities of employees are restricted in the case of covert surveillance.[697] Due to the high intensity of invasion, the latter may be considered only as a last resort. Further, in the area of privacy (for example, in showers, changing rooms or toilets) video surveillance must not take place.[698]

2.5.3. Conclusion on the use of CCTV systems

Although the countries surveyed have relatively different legal regimes, a common ground is that in employment relations they follow the regulation of the European Union, despite not having a single sector-specific legislation on camera surveillance. From the case law in the area of camera surveillance we conclude that it plays a major role in regulating workplaces. In Hungary data controllers generally follows the recommendations of the Data Protection Commissioner, what is based on the general rules of data protection and have already formed a vast body of case law. The academic debate is also based on the case law of the Data Protection Commissioner. Contrary, there are only a small number of legal cases brought before the courts, and do not have a significant role in the legal practice. The German regulation and academic debate is more detailed, and judicial decisions also play an important role for determining the legal background of installing and using camera surveillance in the workplace. In this point we have to conclude that there can be no general, universal description concluded on the legitimate practice of video surveillance, as each CCTV system, and also their goals, way of use may differ. We have to take into consideration all the aspects of the given case, and implementation of guidelines, standards for monitoring and examination of the special circumstances in individual cases are more important than searching for an overall, joint best practice, a case-by-case approach has to be applied.

---

[690] Bundestag, 2009a, p. 35.
[691] BAGE 127, 276 mgn. 17. Cf. re proportionality – a detailed survey in Thüsing, 2010, mgn. 362 ff.
[692] BAG, NZA 2004, 1278, 1283.
[693] Grimm/Schiefer, 2009, p. 337.
[694] LAG Mannheim, RDV 2000, 27, 27 f.; LAG Köln, BB 1997, 475, 476. A need for monitoring machines or production plant can, for example, be found in nuclear energy or chemical plants, Roloff, 2009, § 5 mgn. 29.
[695] Thüsing, 2010, mgn. 368.
[696] Bundestag, 2000a, p. 38.
[697] See also above - section 2.4.2.1.4.
[698] BAG, NZA 2003, 1193, 1195; Thüsing, 2010, mgn. 175.

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

The monitoring of employees outside actual company premises is also possible.[699] To extend the physical scope of monitoring, all that is needed is to use one of the various technical aids which are available, such as GPS or GSM.[700] GPS technology can be used for tracking the movement of employees, providing accurate positioning between 4 and 15 meters.[701] If the employer makes equipment available to the employee, he can continuously detect the location of the employee and monitor his activity.[702]

The most common data protection problems are related to the use of GPS devices tied to vehicle movements driven by employees, but also the tracking of individuals connected to their work is being implemented to a greater extent.[703] It has to be stressed that mobile phones and smart devices of the employees equipped with GPS and with the related applications have raised personal data protection issues recently.[704]

2.6.1. GPS location

GPS is a global navigation tracking system which can be used to determine the location of an employee, becoming an affordable off-site monitoring option for even small companies. Due to the drop in their price GPS systems are widely applied in order to reduce fuel costs for company vehicles, to increase employee efficiency by saving time through real time routing, and increasing productivity by increasing billable hours.[705] GPS tracking is also possible via mobile devices.[706] For this a GPS receiver must either be installed in the terminal itself or the device itself should be able to connect to an external GPS receiver. Using the software installed on the device the GPS position can be requested at specific intervals and transmitted through the cellular network, where the mobile phone acts as a GPS transmitter.[707] It is also relevant, that on most of the mobile devices and phones, also in vehicles it is possible to turn off the GPS function.[708]

2.6.2. GSM location

In addition to GPS in connection with mobile devices, GSM positioning is also a possible measure for monitoring employees. When using this technique, the positioning of the mobile device is carried out through using the cellular structure of the cellular network to determine the location. Specifically, first of all, the respective radio cell is detected in which the device is located, since a specific ID is assigned to each cell. Depending on the density of radio cells,

---

[699] For example when field representatives or courier drivers shall be controlled, cf. Däubler, 2005, p. 770.
[700] Global System for Mobile Communications, Mozek/Zendt, 2011, part 23 mgn. 9.
[701] WP185, p. 5.
[702] Meyer, 2009, p. 18.
[703] Petersen, 2007, p. 337. There is also concern about privacy invasion when some employer use tracking systems to monitor employees even in private places or off the job.
[704] In order to follow the technologically driven social changes form a legal point of view the Article 29 Data Protection Working Party adopted an opinion on Geolocation services on smart mobile devices (WP185).
[705] National Workrights Institute, 2003, p. 6.
[706] Gola, 2007, p. 1143.
[707] Meyer, 2009, p. 19.
[708] National Workrights Institute, 2003, pp. 15-17.

the location can be determined with an accuracy of up to 100 meters.[709] Although, with the aid of complementary measures such as calculations concerning running-time, more accurate positional determinations can be made, GSM positioning in terms of accuracy ultimately remains significantly behind that of GPS.[710] The use of technology is, by contrast, quite simple. Hence, to implement the measure only a mobile phone is needed, this is unlocked for determining its position and operated within the GSM network. The activation itself takes place mostly not through the mobile phone operators, but through external third parties. Depending on the method of the service, the simple sending of a one-time SMS is enough, the affected person being informed by SMS from any location - or is asked for his consent.[711]

WiFi access points can be seen also as a source of geolocation information,[712] however their relevance is still low in employment relationships nowadays.

2.6.3. Hungarian regulation

2.6.3.1. Legislation

There is no specifically GPS or GSM surveillance 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.

2.6.3.2. 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;[713]
- Determining a geographical position with the help of SIM-card cell information in respect of employees;[714]
- Recommendation on the use of a position determination system in employees' mobile 'phones;[715]
- Recommendation on monitoring the location of employees on the basis of mobile telephone cell information;[716]
- Recommendation on the use of a GPS-based position-tracking system in employees' vehicles;[717]

[709] Meyer, 2009, p. 19.
[710] Wittern, 2006, § 98 TKG mgn. 4.
[711] Meyer, 2009, p. 19.
[712] Cf. in details WP185, pp. 5-6.
[713] DPC, 559/A/2006 and 1664/A/2006
[714] DPC, 920/K/2006
[715] DPC, 663/P/2009
[716] DPC, 1092/P/2009
[717] DPC, 415/K/2009

- Recommendation on a GPS system installed in the mobile 'phones of employees;[718]
- Recommendation on the GPS system introduced by a multi-national company;[719]
- Personal data protection conditions relating to personnel-tracking systems.[720]

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.[721] 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.

2.6.3.3. Judicial case law

There is no judicial case law in this specific field.

2.6.3.4. Academic papers, scientific opinions

In the legal literature further summaries of the recommendations of the Commissioner can be found.[722]

2.6.4. German regulation

2.6.4.1. Cases from the jurisdiction

Since location systems have not been the object of law court decisions in relation to employee data protection, it is suggested that the pronouncements of the judiciary on the subject of video monitoring should be referred to.[723]

2.6.4.2. Academic debate

Often, by using GPS for tracking company cars and mobile phones, operational profiles of employees are created.[724]

2.6.4.2.1. GPS tracking of company vehicles[725]

[718] DPC, 636/K/2009
[719] DPC, 857/K/2009
[720] DPC, 922/2/2010
[721] This section of the Labour Code states that the employee shall appear at the place and time specified and spent in the working hours performing work.
[722] Székely/Szabó, 2004, p. 130. Jóri/Hegedűs/Kerekes, 2010, pp. 289-290.
[723] Raif, 2010, p. 359; Meyer, 2009, p. 19; Gola/Schomerus, 2010, § 32 BDSG mgn. 19.
[724] Vogt, 2009, p. 4212; Meyer, 2009, p. 18; Raif, 2010, p. 359.

If the employer is interested only in monitoring the working hours of workers, this can normally be achieved by analysing the data from the digital tachograph of the company vehicle.[726] If, additionally, however, a status report is to be produced in order to monitor the use of the company vehicle, a GPS transmitter is usually installed in or on the vehicle. Technically, GPS stations permit the position of all objects or people to be tracked and determined although it is mainly used in tracking vehicles.[727] As far as the function is concerned, the sender's own position is first determined via data-matching with GPS satellites.[728] After this, the location data are stored for a specific time, compressed and transmitted.[729] This is done by setting up a wireless connection to a predefined receiver. For evaluating and processing data, special software is used which permits the visualisation of the route being driven on a map. If the systems allow the assignment of positional data to a specific person, their use should be measured against BDSG § 6c. Such direct individual reference is always needed if the issue is not only the general determining of a vehicle's position, but when an employee is assigned as the only driver of a particular company car. Similar to RFID systems, one medium processes and transmits data independently, and the employee is unable to trace when and how much of their personal data is being handled.[730] Accordingly, the employer must again meet the information requirements of § 6c BDSG.[731] Further, the collection and storage of data requires the consent of the employee or a firm legal basis. In the absence of specific statutory regulations for location systems, recourse must be had to the general data protection rules.[732] This means that §§ 28, 32 BDSG again are at the centre of the admissibility test of data protection laws. In this respect it is highly relevant to the above evaluation criteria. In the literature there is a parallel to be drawn to jurisprudence developed in connection with video surveillance, and monitoring is required to be carried out in a legitimate way with the knowledge of the employee; also required is an adequate assessment of employers and employees' interests.[733] It should be taken into account at this point that tracking a person's movements by GPS has not previously been classified by the courts as the most intensive intrusion into the general right to privacy.[734] At least in relation to video surveillance or to the recording of telephone conversations, which open up wide-ranging monitoring control options, there is a lower intensity of intervention in the GPS positioning. Since in this case the given location of the employee is only approximate, then this allows, at most, indirect conclusions concerning the behaviour of an employee.[735] Again, however, we should try to avoid sweeping assumptions; an assessment should be made on a

[725] Since GPS transmitters are mainly used for locating vehicles (Meyer, 2009, p. 18.), the following details are limited to this field.
[726] Gola, 2007, p. 1142.
[727] Meyer, 2009, p. 18. Re the different (due to their smaller size) potential uses of the GPS transmitters see further Gola, 2007, p. 1143.
[728] Roloff, 2009, § 5 mgn. 72. Compared to navigational systems, the main difference is that in this case position data is neither recorded, nor distributed.
[729] BVerfGE 112, 304, 308; Roloff, 2009, § 5 mgn. 72. With appropriate technical arrangements data transmission can take place even in real time, Meyer, 2009, p. 18.
[730] Meyer, 2009, p. 19.
[731] Schmitz/Eckhardt, 2007, p. 173 fn. 22.
[732] Raif, 2010, p. 359; Gola/Schomerus, 2010, § 6c BDSG mgn. 5.
[733] Raif, 2010, p. 359.
[734] Roloff, 2009, § 5 mgn. 81.
[735] Cf. the details in BVerfGE 112, 304, 308, 317.

case-by-case basis depending on the legal situation. In this way the time of checking and the particular circumstances can be evaluated. As basic permissible interests of the employer, in addition to the random monitoring of the behaviour of colleagues, increased 'out-of- office' efficiency[736] and the costs of a company's cars are also to be considered.[737]

Tracking by GPS whilst on duty

If tracking is carried out only during working hours where the legitimate interests of the employer are concerned, ongoing suspicion means that independent monitoring of employees may be considered.[738] The reason for this is that private journeys using the company car should, in principle, not be undertaken. If, however, private use of the vehicle is allowed, the tracking system should be disabled during this period. The priority of the employee's interest in not being monitored in his private sphere is to be maintained over the employer's interest in monitoring the vehicle which he owns.[739] Tracking should not extend to the leisure time of the employee.[740]

Covert use of GPS tracking

§ 6c BDSG does not accept the use of covert GPS tracking.[741] According to § 4 paragraph 3 BDSG and § 98 paragraph 1 TKG,[742] due to the supposed informing of employees by the employer, there is the strong view that the covert use of GPS tracking for obtaining residence data should not be allowed.[743] Others consider, more liberally, covert tracking at least in cases where a particular employee is suspected of having committed a crime or serious misconduct and where there are no other alternatives for investigating the suspicion.[744] At this point, as a consequence, a parallel to secret video surveillance could be drawn. Should we allow this, GPS monitoring must be a *maiore ad minus* admissible due to the relatively low intensity of intervention.[745]

2.6.4.2.2. Privacy in telecommunication

The provisions related to telecommunications data protection require service providers to obtain prior permission for location operations.[746] The use of location data is regulated in § 98 TKG [747] and, according to the clarification appended to the government draft, the progressive development of telecommunications should be taken into account, which allows the site-

[736] Cf. only Raif, 2010, p. 359, who regards the conduct of employees working off-site but who do not travel directly to their clients as being in serious breach of their contractual agreement.
[737] Vogt, 2009, p. 4212, with the note that, in contrast, the continuous monitoring of employees will be deemed inadmissible (likewise Gola/Wronka, 2010, mgn. 908, which speaks explicitly against continuous monitoring).
[738] Roloff, 2009, § 5 mgn. 83, likewise Meyer, 2009, p. 19.
[739] Meyer, 2009, p. 19. Vogt, 2009, p. 4212.
[740] Vogt, 2009, p. 4212
[741] Meyer, 2009, p. 19.
[742] § 98 TKG deals with handling (see the extended interpretation of the concept of processing Munz, 2010, BDSG, § 98 TKG mgn. 4.) location data. According to § 3 Nr. 19 TKG what should be understood here are data that are collected or used in a telecommunications network and the location of the terminal end user is provided to the public by a telecommunications service.
[743] Vogt, 2009, p. 4212.
[744] Steinkühler/Raif, 2009, p. 216.
[745] Meyer, 2009, p. 19 with reference to Roloff, 2009, § 5 mgn. 87.
[746] Gola, 2007, p. 1143.
[747] Concerning the necessity of acquiescence in line with § 98 TKG Jandt, 2007, p. 74.

related use of telecommunications services (Location Based Services, LBS).[748] In this regard, dealing with location data depends on the consent of the participant[749] as a contractor or service provider.[750] In accordance with § 3 No. 20 TKG, any natural or legal person who has signed a contract with a provider of telecommunications services for the provision of such services counts as a participant. If the subscriber and the user of the mobile device is not the same person, § 98 paragraph 1 sentence 2 TKG prescribes informing the user about prior consent.[751] As a consequence, it is legally permissible that the employer leaves the transfer mobile device unlocked for location determination without informing the employee about the possibility of permanent localisation.[752] Insofar as the requirements of § 98 TKG are available, it indicates no permission for the employer to be able to carry out a localisation check at any time.[753] Rather, going further (and, therefore, far beyond the area of telecommunications data protection) it is questionable whether or not an impermissible intrusion takes place into the personal rights of the employee, if he or she is left with an unlocked mobile device.[754] In the planned balancing of interests, several factors play a role. Comparing the localisation of the mobile phones with that of a company car with permitted private use as mentioned above, with the first measure, the employee has, in theory, a chance to avoid localisation, if he or she switches off the device.[755] By contrast, impermissible invasion in the personal rights of the employee might occur if there is a commitment for the employee to carry the device with him outside regular working hours to be accessible. Unless there is a legitimate interest of the employer, the employee will have to tolerate at least – parallel to the GPS tracking of company cars – location checks during the period of service. As a minimum requirement, an employee will then be able to require the employer to establish criteria for the implementation of site rules and to be kept informed.[756] Regardless of the scope of § 98 TKG, this follows from § 6c BDSG, which is also applicable to the SIM card of a mobile device.[757]

2.6.5. Conclusion

While the introduction of GPS technology into the workplace has yet to be addressed by the courts, the Hungarian Data Protection Commissioner has dealt with numerous cases relevant to the topic, and the academic debate in German has already started on the legality of determining the employees' location. It is clear from their opinions that in both countries there are many positive and legitimate uses for GPS equipment. Employees must be aware of the possible invasion of privacy that comes with the technology, especially in cases when they are allowed to use official vehicles and devices in off-working hours, and for private routes. It is

[748] Munz, 2010, 98 TKG mgn. 1. referring to Bundestag, 2004, p. 89.
[749] The participant is according to § 3 Nr. 20 TKG each natural or legal person, who has concluded a contract with a supplier from a telecommunications service for the provision of such a service.
[750] Meyer, 2009, p. 20.
[751] Wittern, 2006, § 98 TKG mgn. 7.
[752] Meyer, 2009, p. 20; Gola/Wronka, 2010, mgn. 897.
[753] Gola, 2007, p. 1143.
[754] Meyer, 2009, p. 20.
[755] Gola/Wronka, 2010, mgn. 905; Meyer, 2009, p. 20.
[756] Meyer, 2009, p. 20.
[757] Von Westerholt/Döring, 2004, p. 714; Gola/Schomerus, 2010, § 6c BDSG mgn. 2a.

highly recommended for employers to make it possible, and inform workers about the possibility, to switch of these devices out of their working periods, and use other processes and regulation to prevent the overuse of company-owned properties.

2.7. Regulation of transponder-based and biometric identification systems

A common method of preventing the entry of unauthorised third parties to the working area as well as to the more sensitive areas of corporate premises is the use of entry monitoring systems. With such a system, employees and others can have access only to certain areas.[758] In this chapter several types of identification systems connected to workplaces are examined, however one of the most regularly used technology, Radio-frequency identification system (RFID) has to be the subject of a separate chapter due to its wide range of applicability.

2.7.1. Description of commonly used systems

2.7.1.1. Transponder-based systems

One way to control access is with the help of transponders.[759] To restrict entry to an area, the transponder must be placed in a transponder field, so that any data which is left there (e.g., the ID-number of an employee) can be sent. If the owner of the transponder accepts him as legitimate, he will be admitted. In this way the system can be set up so that the transponder will allow access only to particular areas or at certain times - that is, in terms of space and time. Smart cards are widely used as transponders, as these are putting information and processing power on credit card–size devices.[760] As the employee will normally have his own personal transponder (e.g. access card or key) and must carry this with him at all times, it will – depending on the number of transponder fields and the intensity of the monitoring – enable to log an individual's entry and exit patterns and sometimes also their movements. Further, various smart cards have been in use for physical access control, as these more complex transponder systems offer a central, computer-based control, which facilitates the systematic recording of the use of the transponder, hence a relatively accurate employee location system, resulting in the generation of movement profiles.[761] By this, with the use of suitable software, for example conclusions can be drawn about the whereabouts of an employee or his contacts with other employees.[762]

2.7.1.2. The use of biometric systems

Access or entry control can also be carried out by means of the comparison of biometric data.[763] Biometrics involves techniques used to identify individuals based on a particular trait

[758] Meyer, 2009, p. 16.
[759] The concept 'Transponder' is formed from the words 'transmitter' and 'responder together, Däubler, 2010, p. 184 fn. 141. Applied using chip card or coin, cf. Roloff, 2009, § 5 mgn. 53.
[760] Stanton/Stam, 2006, p. 60.
[761] Petersen, 2007, pp. 899-900.
[762] Meyer, 2009, p.16.
[763] Biometric data was defined by the Article 29 Working Party in Opinion 4/2007 (WP136) as "biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those

or physical characteristic unique to that individual.[764] 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;
- Collectability: the characteristic can be measured quantitatively.[765]

As biometric features, physiological or passive (e.g., fingerprints, face, iris or vein-recognition) or active (e.g., voice recognition, signature, password) can serve.[766] By using biometric techniques, the identification of individuals is made possible - solely on the basis of their personal, individual physical features.[767] 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. 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.[768]

The use of such access control systems will certainly be opposed, since the biometric information concerning the employee will be stored in a central databank. On the other hand, it should be accepted that biometric data comprises sensitive information. To avoid any possibility of data misuse, the treatment and handling of such data must be appropriately careful and discreet.[769] If transponder systems and biometric authentication are linked, the

features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability."

[764] In details cf. WP80.

[765] McGuire, 2000, p. 444.

[766] Gola/Wronka, 2010, mgn. 874; Bartmann/Wimmer, 2007, p. 199.

[767] Raif, 2010, p. 359.

[768] Betzel, 2005, p. 520.

[769] Cf. detailed legal analysis on biometric profiling in Kindt, 2010, pp. 139-144.

merit of the former, due to the lower level of intrusion into personal rights when employees are monitored, must be acknowledged.[770]

2.7.2. Hungarian regulation

2.7.2.1. 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 in the Labour Code or in the Data Protection Act on collecting and processing biometric data in the field of work, however basic principles of data protection are interpreted by the Data Protection Commissioner in the light of transponder based or biometric surveillance systems.[771]

2.7.2.2. 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 or distributing social relief, which is not relevant in the scope of our project.

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.[772] In connection to biometric entry systems in workplaces the Commissioner highlighted, that these can be applied legally only if they process data essential for and directly connected to a justifiable goal, and no other surveillance methods (e.g. entry camera surveillance, or recording the time of passing through the access control system) are applied simultaneously.[773] In case of installing entry surveillance systems employers should choose devices which process no, or less sensitive or personal data, preferably smart cards or access keys (if it is also possible) rather than biometric systems.[774] In similar cases 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.[775]

2.7.2.3. Judicial case law

There is no relevant judicial case law.

2.7.2.4. Academic papers, scientific opinions

No significant academic essays on this matter.

---

[770] Meyer, 2009, p. 17; Roloff, in: Besgen/Prinz, § 5 mgn. 66; Petersen, 2007, p. 900.
[771] DPC, 166/K/2007
[772] DPC, 1454/K/2010
[773] DPC, 290/A/2005
[774] DPC, 1744/P/2007; cf. also 89/K/2007
[775] DPC, 926/H/2010

2.7.3. German regulation

2.7.3.1. Cases from the jurisdiction

There are only a limited number of judicial decisions referring to entry control systems to date.[776] It is, however, proposed to draw on jurisdiction dealing with surveillance or monitoring by video.[777]

2.7.3.2. Academic debate

Biometric data can, on an individual case basis, and depending on the specific utilisation[778] be classified as a special form of personal data in the sense of § 3 Abs. 9 BDSG. Whilst this is not the case if what is involved is a simple check of the right of the employee to enter there would, perhaps, be conclusions to be drawn in respect of the health of an employee with the aid of biometric data which might be judged to have been obtained other than legally.[779]

Data protection admissibility is evaluated according to whether the handling of data is covered by the consent of the person concerned or by legally permitted conditions. By the use of personalised transponders, personal data is taken and processed so that the legal evaluation of the use of such a system accords with the BDSG.[780] However, if when using the system it occurs that one employee attached to a group of people authorised to enter the centre stands in the midst of them and is the only person not recorded, then the utility value of the BDSG in relation to personnel cannot be accepted.[781] In the scope of the BDSG the evaluation of the legitimacy of the measures again accords to the requirements of the law pertaining to encroachment of §§ 28, 32 BDSG and subject to the rationale of the specific test criteria. It is conceivable that priority will be given to recording the time of passing through the access control system, if what is needed is the related data for examining working hours and remuneration issues.[782] Also the reliability of the employee in terms of his location within the business premises in cases where, from the standpoint of the employer there are special reasons for using an extensive entry control system, e.g., due to particular security requirements or because of some special characteristics of the business.[783] Amongst these will be businesses which handle especially hazardous materials or where corporate know-how is particularly valuable.[784] In the absence of a suitable security need, at least no biometric technology needs to be installed.[785] It should also be noted that biometric processes assume that the employee knows of their use. The covert recording of biometric data is in conflict with the employer having knowledge of the properties of the system as per § 1 AGG,[786] for

[776] Z.B. BAG, RDV 2004, 122 (Co-determination with Biometric Entry Control Systems).
[777] Gola, 2010a, mgn. 82.
[778] Cf. as an example of this Gola/Schomerus, 2010, § 3 BDSG mgn. 56.
[779] Meyer, 2009, p. 17, with the assertion that § 6a BDSG is not applicable.
[780] Meyer, 2009, p. 17.
[781] Roloff, 2009, § 5 mgn. 55. To be considered here is, for example, the use of Transponders without individual ID, Meyer, 2009, p. 17.
[782] Zöll, 2010, § 32 BDSG mgn. 22; Gola/Wronka, 2010, mgn. 885.
[783] Meyer, 2009, p. 17.
[784] Roloff, 2009, § 5 mgn. 68.
[785] Roloff, 2009, § 5 mgn. 71.
[786] Raif, 2010, p. 359.

example in respect of the basic health or background of his employee.[787] Storing such features and other sensitive data as per § 3 Abs. 9 BDSG is normally conditional on the consent of the employee.[788] However, storage of the data cannot be justified by agreement between management and works committee, since the legitimacy of the processing of sensitive data can, according to § 28 Abs. 6 BDSG, only come with the consent of the individual concerned or with the submission of an exemption application according to § 28 Abs. 6, 7 or 9 BDSG.[789]

2.7.4. Conclusion

On one hand country reports clearly show that in both countries entry control systems are applied in workplaces due to particular security requirements, or for examining working hours and remuneration issues. On the other hand no specific legislation can be found on this topic, therefore basic principles can be drawn only from exceptional cases of data protection authorities (in Germany also from court jurisdiction), which are the basis for academic debate. The relevant jurisdiction confirmed that in general the lower level of intrusion into personal rights when employees are monitored, must be acknowledged, but each case of installing biometric access control system has to be examined separately to decide if they can be operated legally.

2.8. 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. RFID systems, in comparison with the previously examined access control systems make possible one essentially more accurate monitoring of employees, in which, by means of radio tags, information can be retrieved about the location, movement, or audio signals associated with their use.[790] The technology has improved extensively since the 1990s, the cost of RFID devices have dropped, and real-time tracking are now available, giving the possibility of individual object tracking, that could be used legally for logistics operations such as warehousing and delivery.[791] Due to their small size, these tags can be used in workplaces as an in-house pass or for other purposes,[792] and can, in extreme cases even be fixed to the clothing.[793] With the aid of RFID technology,

[787] Gola/Wronka, 2010, mgn. 875; Steinkühler/Raif, 2009, p. 217.
[788] Raif, 2010, p. 359. Representing a more strict view (Oberwetter, 2008, p. 612, cf. further Gola/Wronka, 2010, mgn. 875) even opt for the general inadmissibility of authentication in respect of sensitive data, within the meaning of § 3 par. 9 BDSG respectively characteristics within the meaning of § 1 AGG is inadmissible in general.
[789] Raif, 2010, p. 359.
[790] Cf. on the function of RFID, von Westerholt/Döring, 2004, p. 710; Gola/Wronka, 2010, mgn. 870. In general on the basics of RFID technology, on the setting up of a system of transponder (tag), reader and RFID-middleware as well as on the differentiation between active and passive tags cf. John, 2011, 3rd section part 300 mgn. 1 ff.
[791] Petersen, 2007, p. 328. A highly controversial area of RFID application involves the insertion of devices under the skin of pets or even people, cf. Stanton/Stam, 2006, p.60.
[792] Gola/Schomerus, 2010, § 6c BDSG mgn. 2a; von Westerholt/Döring, 2004, p. 711. Employers may even try to enforce wearing RFID tags off-working hours cf. Petersen, 2007, p. 337.
[793] Däubler, 2010, mgn. 324a.

personal data can be handled if information with the identification data of a person (photo, name, address, and recurring ID number) can be loaded on an RFID tag.[794]

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 within two digits in terms of metres without the knowledge of the individual, it is possible to gather sensitive data about an individual without his consent.

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.[795]

The European Commission and its Article 29 Working Party follow the changes in this field and issued several documents to ensure that the RFID industry and the relevant stakeholders develop a framework for privacy and data protection impact assessment. Firstly released a recommendation on the principles of guarantees of privacy in the field of radio frequency identification in 2009,[796] and then improved it to an Opinion of the Working Party in 2011.[797] These prescribe 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.

2.8.1. Hungarian regulation

2.8.1.1. Legislation

In Hungary there are only two legal documents in relation 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.

2.8.1.2. 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.

2.8.1.3. Judicial case law

There is no relevant judicial case law.

[794] WP105, p. 29; Buchner, 2010, § 3 BDSG mgn. 18.
[795] Gola, 2010a, mgn. 78; with reference to technological aspects by Hansen/Wiese, 2004, p. 109. John, 2011, 3rd section part 300 mgn. 9 defines a range, in long-range systems of up to 30m when using active Tags.
[796] WP180, p. 3.
[797] Cf. WP180.

2.8.1.4. Academic papers, scientific opinions

There is no relevant academic papers.

2.8.2. German regulation

2.8.2.1. Cases from the jurisdiction

Decisions referring to entry control systems are, to date, on a small scale,[798] and RFID systems have not yet been the subject of judicial decisions. It is, however, proposed to draw on jurisdiction dealing with surveillance or monitoring by video.[799]

2.8.2.2. Academic debate

By the use of personalized RFID tags, personal data is taken and processed so that the legal evaluation of the use of such a system accords with the BDSG.[800] From the perspective of legal data protection the use of RFID systems should be treated more circumspectly in contrast to the situation with the transponders and biometric surveillance technologies mentioned earlier.[801] The use of tags by the employee is often not sufficiently transparent. If, perhaps, RFID readers can be installed to cover the area of the business premises, an accurate and unbroken movement profile of the workers will be produced without the need for any action by the personnel. Due to the increased danger of the misuse of RFID systems, there must, in comparison with other technologies, be a higher level of protection available for use than with other technologies.[802] At least in respect of active RFID tags[803] there should apply § 6c BDSG[804] which governs the mobile storage and handling of personal data[805] (§ 3 Abs. 10 BDSG).

Basically, all media fall within this category, which are equipped with a single processor-chip.[806] Also, if somewhat differently, this would apply, if as with a normal entry control system, essentially unchangeable information such as an ID number is involved.[807] From the user § 6c BDSG requires a variety of explanatory information such as the duty of the individual concerned to reveal his identity, or, because of the mode of operation of the technology also his rights in respect of the giving of information, insofar as knowledge of this had not already been required. Alongside this there exists, depending on the particular case, with each concrete use of the RFID technology, an additional requirement to inform,

[798] Z.B. BAG, RDV 2004, 122 (Co-determination with Biometric Entry Control Systems).
[799] Gola, 2010a, mgn. 82.
[800] Meyer, 2009, p. 17.
[801] Cf. also Schmitz/Eckhardt, 2007, p. 172 on the different possibilities of use and related thoughts.
[802] Meyer, 2009, p. 18.
[803] Active RFID Tags are able, due to their own energy source (battery or solar cell) to transmit information as soon as a reader-unit receives an activating impulse. John 2011, 3rd section part 300 mgn. 3.
[804] Von Westerholt/Döring, 2004, p. 714; more differentiation Schmitz/Eckhardt, 2007, p. 173.
[805] As follows from § 3 Para. 10 BDSG, with mobile storage and processing media, it is a question of data carriers issued to the employee on which personal data, in addition to being stored, can be processed either at the point of origin or automatically elsewhere, and where the person concerned can influence this processing only by use of the medium.
[806] Gola/Schomerus, 2010, § 3 BDSG mgn. 58; Gola, 2010b, § 6b BDSG mgn. 2.
[807] Zscherpe, in: Taeger/Gabel, BDSG, § 6c mgn. 52; Meyer, 2009, p. 18.

according to § 6c Abs. 3 BDSG, which is not defined more precisely.[808] It is, however, recommended that there should be some signal marking the recording of data – perhaps an acoustic tone.[809] The use of RFID technology is part of the information to be provided to employees, in that perhaps this also must be given as information insofar as the analysis by the particular electronic reading process creates a movement profile.[810] For the rest, the same general approach should apply as for the already mentioned entry control systems.[811] What concerns the surveillance of the whereabouts of an employee with technological help (as, perhaps, with RFID) for the purpose of performance monitoring, will generally be inadmissible. Something else can emerge in special cases such as, for instance, setting up special checkpoints on the regular rounds of the security personnel.[812]

2.8.3. Conclusion

The use of RFID systems in the workplace means an up-to date technological threat to our privacy, therefore EU bodies have taken it as a hot issue and conducted various researches in the last few years. However, in Hungary and Germany there were only a few cases in connection to RFID and workplace privacy. Hence, academic debate focuses on this issue as a theoretical problem, what needs to be analysed more in details in the future. Till then the suggestions of the data protection authorities and general rules of personal data play a significant role.

[808] Gola, 2010b, § 6c BDSG mgn. 3.
[809] Meyer, 2009, p. 18.
[810] Meyer, 2009, p. 18; who stresses that there can be a need of creating motion profiles by all means, like for security personnel, for example.
[811] Schmitz/Eckhardt, 2007, p. 175.
[812] Wank, 2010, § 6c BDSG mgn. 19; Gola/Wronka, 2010, mgn. 885.

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

3.1. Hungarian regulation

3.1.1. Sanctions according to Data Protection Law

3.1.1.1. 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.[813]

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.[814]

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

3.1.1.2.1. 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

[813] DPA § 17, new DPA § 22
[814] DPA § 18, new DPA § 23

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.[815]

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.[816]

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.[817] 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.[818] The Data Protection Commissioner did not have the right to impose a fine if illegal data processing is detected.

3.1.1.2.2. 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 after three years at the end of 2011, 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.[819]

The new Authority is empowered with all the powers that the Commissioner has, except for the right to turn to the Constitutional Court. The "ombudsman-like" powers are summarized in the '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;

[815] DPA §§ 24, 27(1)
[816] DPA § 25(3)
[817] DPA § 25(2), (4)-(5)
[818] Majtényi, 2006, p. 138
[819] According to the current news, the European Commission is now analyzing the situation and considers starting an infringement action. http://www.globallawwatch.com/2011/12/analysis-hungarys-new-data-protection-act-raises-concerns-prompts-call-for-european-commission-infringement-action/ [18.01.2012]

- the Authority may prepare a report (which is open to the public) if it does not initiate an administrative or court procedure;
- 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'.[820]

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.[821]

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.[822]

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.

3.1.2. Sanctions based on the Labour Code

Firstly, 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,[823] 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.[824]

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

[820] 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.
[821] New DPA § 60(4)
[822] New DPA § 61(1)
[823] Kiss, 2005, p. 285.
[824] Cf. Arany Tóth, 2004a

party.[825] The regulation of the Labour Code conforms to the regulation of the DPA, as both of the Acts contain the same special liability rule.

3.1.3. Other sanctions

3.1.3.1. Sanctions based on the Civil Code

Since data protection, the right to one's 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;[826]

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

3.1.3.2. Sanctions based on the Criminal Code

In case of some really serious breach of privacy, irrespectively of happens 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.[827]

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

[825] New Labour Code § 166
[826] Civil Code § 84
[827] Criminal Code § 177/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.[828]

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.[829]

3.2. German regulation

Similar to the Hungarian regulation examined before the violation of laws by employers and employees can also lead to sanctions of data protection, labour law and to further sanctions in Germany.

3.2.1. Sanctions in the field of data protection

Apart from a wide range of sanctions in specific data protection regulations (see some examples of the criminal and civil penalty provisions of §§ 148, 149 TKG) the Federal Data Protection Act states for example, that infringements against the data protection law are punishable with fines as misdemeanours. The catalogue in § 43 BDSG offers a number of ways to sanction non-compliance of legal requirements. Thus, according to § 43 paragraph 3 sentence 1 BDSG violations of notification and information requirements (see § 43 paragraph 1 No. 8 and No. 8a BDSG) can be fined with up to 50,000 €, an infringement in cases of paragraph 2 can be punished with a fine of up to 300,000 €.[830] On § 44 BDSG certain acts are even criminalized.[831] The obligations of the BDSG meet the responsible entity (§§ 1, paragraph 2, 2 BDSG) this means the head of the department or the management.[832] Besides the rights mentioned in § 6 paragraph 1 BDSG, in some cases, the parties also have an opportunity to assert their cancellation rights or claims for damages for unauthorized or incorrect collection, processing or use of their personal data in accordance with § 7 BDSG.[833] The violation of a notification does not disclose this possibility. For public-legal sector employers, for example, a strict liability may arise from § 8 BDSG.[834]

---

[828] Criminal Code § 178

[829] Criminal Code § 178/A

[830] See also: § 43 par. 3 p. 2 and 3 BDSG: The fine shall exceed the economic advantage gained by the perpetrator from the offence. Should the amounts mentioned in clause 1 not be sufficient for this, then these can be exceeded.

[831] Often, however, special rules will become relevant, see: Gola/Wronka, 2010, mgn. 1296.

[832] Gola/Wronka, 2010, mgn. 1292.

[833] § 7 BDSG is the basis for a claim for liability arising from suspected negligence, Däubler, 2010, mgn. 574.

[834] Gola/Wronka, 2010, mgn. 338, 1370. See also: mgn. 1371 ff. concerning liability in case of government activity under Art. 34 of the constitutional law, in conjunction with § 839 of the Civil Code as well as in the fiscal area on the basis of possible contractual or delictual liability pursuant to §§ 31, 89 and § 831 of the Civil Code as well as § 839 of the Civil Code.

3.2.2. Sanctions in the field of Labour Law

Regarding the process, there is a chance of suspension of banning the use of legal consequence of an improper act, based on unauthorized employee monitoring.[835] Illegally obtained evidence in civil proceedings is generally not unusable, only when according to protective purpose a prohibition of use is announced in the gathering of evidence an injured norm.[836] This is especially the case if through obtaining the evidence constitutionally protected basic positions have been violated,[837] furthermore if the employer has violated privacy rights of the employees.[838] In this context it is important to note that employer and the works council meet a duty of care in accordance with § 75 paragraph 2 sentence 1 BetrVG,[839] which prescribes protection and promotion of the free development of personality of the workers engaged. But employees also have to reckon with the consequences for breach of duty. Unauthorized use of, for example, operational information and communication technologies threaten them with warning letters, with ordinary or in some cases with instant dismissal[840] as well as pay cuts.[841] Sometimes they may get liable for causing damage unlawfully.[842] Regarding pecuniary consequences it is important to note that there are privileges in employment liability which, depending on the degree of indebtedness and the extent of damage may limit or even exclude the liability.[843] This applies only to damages that have occurred in connection with the operations of the employee, but not for damage due to unauthorized private use.[844]

3.2.3. Other sanctions

The sanctions of German law are by no means confined only to the work- and data protection area. Especially when illegal surveillance activities are in question, the employer runs the risk of being punished under the provisions of the StGB. The protection of information in the broadest sense, can predominantly be realized through § 202a StGB (Spying data), § 202b StGB (Interception of data), § 202c StGB (Preparing the spying and interception of data), §

---

[835] Thüsing, 2010, mgn. 564.

[836] BVerfGE 117, 202, 214. See regarding the evidential consequences of efficacy theory, the distinction between evidence collection and utilisation, and the dispute as to when an utilisation prohibition may in particular be adopted, Thüsing, 2010, mgn. 564 ff.

[837] BGH, NJW 2005, 497, 498 ff.

[838] Consistent practice of the Courts since the decisions of the Federal Court in civil matters BGHZ 27, 284, 286; see regarding this BVerfG, NJW 2002, 3619, 3624; NZA 1992, 307, 308; BAGE 105, 356, 358. See the relevant dispute on the topic Kratz/Gubbels, 2009, p. 655. See further Lunk, 2009, p. 459 ff. The protection of personal rights of employees belongs to the protection and collateral obligations of the employer within the meaning of. § 241 Abs. 2 BGB, BAG, NZA 1988, 53, 53; Preis, 2011, mgn. 615, 620. Regarding the obligation to have regard for the welfare (especially with regard to § 75 paragraph 2 sentence 1BetrVG) as well as, in general, concerning the persons addressed by the data protection obligations, see: Gola/Wronka, 2010, mgn. 1292 ff.

[839] Gola/Wronka, 2010, mgn. 1292.

[840] See also Gola, 2010a, mgn. 364 ff.; Trappehl/Schmidl, 2009, p. 987 ff; and Gola/Wronka, 2010, mgn. 1383 ff.

[841] Gola, 2010a, mgn. 361.

[842] See also Gola/Wronka, 2010, mgn. 1343 ff.

[843] Fundamentally BAG, DB 1993, 939.

[844] Gola, 2010a, mgn. 384, which also agrees on giving credit to possible contributory negligence by the employer within the meaning of § 254 BGB.

203 (Violation of private secrets), § 263a (Computer fraud), § 268 StGB (Falsification of technical records), § 269 StGB (Falsification of evidentiary data), § 270 (Deception in data processing in legal relations) § 274 StGB (Suppression of evidentiary data), § 303a StGB (Changing data) und § 303b StGB (Computer sabotage).[845]

In case the employer accesses contacts illegally or controls telephone calls improperly, he may be liable to prosecution for violation of telecommunications secrecy (§ 88 TKG) to § 206 StGB.[846] Apart from the feature as a telecommunication provider, criminality according to § 201 StGB (Violation of the confidentiality of the word) is added.[847] What is more the violation of the law on the written word entails also a criminal offense under § 202 of the Penal Code (violation of the secrecy of correspondence.). The sending of messages through electronic ways has not been mentioned yet. This means that the closed character of the document is missing.[848] Here, again, § 206 StGB[849] appears, which also includes the protection of e-mail traffic.[850] On part of the employee a fraud may be committed (§ 263 StGB) if due to unauthorized private use costs can be feigned as officially necessary.[851] Furthermore, it is possible to penalize the violation of specific duties of confidentiality, e.g. of § 17 UWG (betrayal of business and trade secrets) or § 67 BBG (secrecy).[852] In addition, in the retrieval and dissemination of content from the Internet there can also appear a violation of criminal or copyright (see the offenses of §§ 106 ff. UrhG)[853] provisions.[854] Since the present data protection liability standards of §§ 7, 8 BDSG there are no final regulations represented,[855] a possible recourse to the general civil claims remains.[856] Illegal surveillance measures can entail e.g. sensitive compensation claims.[857]

3.3. Conclusion

The concept of informational self-determination and the current legal framework of the protection of personal data was started to be implemented into the Hungarian national law only in the end of the 1980s, close to the fall of the communist regime.[858] After all, nowadays in Hungary, just like in Germany – where privacy rights have been developed for decades, at

[845] Trappehl/Schmidl, 2009, pp. 985, 990; Schmidl, 2010, pp. 476, 479; Gola/Wronka, 2010, mgn. 1341.
[846] Gola, 2010a, mgn. 103 ff.
[847] Concerning the inadmissibility of secret phone-tapping, see BVerfG, NJW 2002, 3619 and BGH, RDV 2003, 237. Regarding the criminal use of phone-tapping techniques see: Gola, 2010a, mgn. 244 ff.
[848] Gola, 2010a, mgn. 51
[849] Violation of postal or telecommunications secrecy.
[850] Gola, 2010a, mgn. 52 and also the details Gola, 2010a, mgn. 103 ff. Regarding the scope of telecommunications secrecy see further Durner, 2011, Art. 10 GG mgn. 67.
[851] Gola, 2010a, mgn. 378.
[852] Gola/Wronka, 2010, mgn. 1296.
[853] The employer then can assert his claim for relief and removal, see Trappehl/Schmidl, 2009, pp. 985, 990.
[854] E.g. § 86 StGB (Dissemination of propaganda of unconstitutional organisations), § 184 StGB (Dissemination of pornography writings) or § 184b StGB (Dissemination, acquisition and possession of child pornography writings) can be violated, Gola, 2010a, mgn. 197 fn. 26 ff.
[855] Bundestag, 2000b, p. 2.
[856] Gabel, 2010, § 7 BDS mgn. 23, § 8 BDSG mgn. 2. See the main legal bases for claims Gabel, 2010,§ 7 BDSG mgn. 24 ff. as well as Grimm/Schiefer, 2009, pp. 343-344. and Thüsing, 2010, mgn. 503 ff.
[857] See for instance the recent verdict that an employer should pay compensation of €7,000 for unauthorised video surveillance, LAG Hessen, 2011, 346.
[858] Szabó/Székely, 2005, p. 249.

least in West Germany – the current regulation contains various legal procedures and sanctions in case of unlawful processing of personal data. Despite of the lack of sector-specific and secondary norms regulating the monitoring, especially the technical surveillance of workers, there is a complex system of legal protection available for employees. There are many applicable laws like Acts on data protection, Civil law, Labour law, or Criminal law; and ways to get remedies, such as turning to court or to supervisory bodies calling for investigation of individual cases, or the level of privacy protection in their workplace. There are reasonable expectations for privacy in the workplace in both of the countries, the court rulings and data protection authorities interpret the general rules of data protection – even though some of the decisions are quite unpredictable[859] – and offer a high degree of legal protection to the workers.

To conclude the question of supervision regimes we have to highlight, that there are various forums and proceedings available for employees to choose from in case of privacy breach occurs. Contrary, as it was clear from the low number of cases and recommendations could be found connected to the issues examined, subjects of unlawful monitoring are in the absence of knowledge about their rights and possibilities, and their informed consent as the legal basis of data processing may be questioned.

[859] Szabó/Székely, 2005, pp. 255-256.

4. LITERATURE AND REFERENCES

4.1. Books, essays and articles

Albrecht, Florian – Maisch, Michael Marc (2010): Bluttests und Verhaltensanalysen bei Bewerbern, Datenschutz-Berater, pp. 11-18. [Downloaded from http://beck-online.beck.de]

Altenburg, Stephan – von Reinersdorff, Wolfgang – Leister, Thomas (2005): Betriebsverfassungsrechtliche Aspekte der Telekommunikation am Arbeitsplatz, Multimedia und Recht, pp. 135-138. [Downloaded from http://beck-online.beck.de]

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.

Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2009): Orientierungshilfe „Protokollierung“, http://www.bfdi.bund.de/SharedDocs/Publikationen/Orientierungshilfen/OHProtokollierung.pdf?__blob=publicationFile. [01.04.2011]

Art. 29 Data Protection Working Party and Working Party on Police and Justice, The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 02356/09/EN, 2009. (WP168), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf [18.01.2012]

Art. 29 Data Protection Working Party, Opinion 1/2001 on Employee Evaluation Data, 5008/01/EN/Final, (WP42), 2001. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp42en.pdf [18.01.2012]

Art. 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, 2001. (WP48) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf [18.01.2012]

Art. 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11750/02/EN/Final, 2004. (WP89) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf [18.01.2012]

Art. 29. Data Protection Working Party Opinion 4/2007 on the concept of personal data, 01248/07/EN, 2007. (WP136) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf [18.01.2012]

Art. 29 Data Protection Working Party, Opinion 5/2010 on the Industry Proposal for Privacy and Data Protection Impact Assessment Framework for RFID Applications, 00066/10/EN, 2010. (WP175) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf [18.01.2012]

Art. 29. Data Protection Working Party Opinion 13/2011 on Geolocation services on smart mobile devices, 81/11/EN, 2011. (WP185)
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf [18.01.2012]

Art. 29. Data Protection Working Party Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 00327/11/EN, 2011. (WP180)
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf [18.01.2012]

Art. 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, 5401/01/EN/Final, 2002. (WP 55)
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf [18.01.2012]

Art. 29. Data Protection Working Party Working document on biometrics, 12168/02/EN, 2003. (WP80) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf [18.01.2012]

Art. 29. Data Protection Working Party Working document on data protection issues related to RFID technology, 10107/05/EN, 2005. (WP105)
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf [18.01.2012]

Aufsichtsbehörde Baden-Württemberg (1978), Hinweis zum BDSG Nr. 3, Staatsanzeiger vom 1.7.1978, Nr. 52.

Backes, Volker – Eul, Harald – Guthmann, Markus – Martwich, Robert – Schmidt, Mirko (2004): Entscheidungshilfe für die Übermittlung personenbezogener Daten in Drittländer, Recht der Datenverarbeitung, pp.156-163.

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

Bartmann, Dieter – Wimmer, Martin (2007): Kein Problem mehr mit vergessenen Passwörtern: Webbasiertes Password Reset mit dem psychometrischen Merkmal Tippverhalten, Datenschutz und Datensicherheit, pp. 199-202.

Bausback, Winfried (2006): Fesseln für die wehrhafte Demokratie?, Neue Juristische Wochenschrift, pp.1922-1924. [Downloaded from http://beck-online.beck.de]

Bayreuther, Frank (2005): Videoüberwachung am Arbeitsplatz, Neue Zeitschrift für Arbeitsrecht, pp. 1038-1044. [Downloaded from http://beck-online.beck.de]

Beckschulze, Martin (2003): Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz – Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen, Der Betrieb, pp. 2777-2786. [Downloaded from http://www.juris.de]

Beckschulze, Martin (2009): Internet- und E-Mail-Einsatz am Arbeitsplatz, Der Betrieb, pp. 2097-2103. [Downloaded from http://www.juris.de]

Beckschulze, Martin – Henkel, Wolfram (2001): Der Einfluß des Internets auf das Arbeitsrecht, Der Betrieb, pp. 1491-1506. [Downloaded from http://www.juris.de]

Beckschulze, Martin – Natzel, Ivo (2010): Das neue Beschäftigtendatenschutzgesetz, Betriebs-Berater, pp. 2368-2375. [Downloaded from http://www.juris.de]

Behling, Thorsten B. (2010): Compliance versus Fernmeldegeheimnis, Betriebs-Berater, pp. 892-896. [Downloaded from http://www.juris.de]

Beisenherz, Gerhard – Tinnefeld, Marie-Theres (2010): Sozialdatenschutz – eine Frage des Beschäftigtendatenschutzes?, Datenschutz und Datensicherheit, pp. 221-224.

Bergmann, Lutz – Möhrle, Roland – Herb, Armin (2011): Datenschutzrecht, Boorberg, Stuttgart, Munich, Hanover.

Besgen, Nicolai – Prinz, Thomas (2009): § 1 Dienstliche Nutzung von Internet, Intranet und E-Mail, in: Besgen, Nicolai – Prinz, Thomas (eds): Handbuch Internet: Arbeitsrecht: Rechtssicherheit bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn.

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.

Bierekoven, Christiane (2010): Korruptionsbekämpfung vs. Datenschutz nach der BDSG-Novelle, COMPUTER UND RECHT, pp. 203-208.

Bissels, Alexander (2009a): Background Checks bei der Begründung des Arbeitsverhältnisses – Was darf der Arbeitgeber?, juris AnwaltZertifikatOnline Arbeitsrecht remark 2 [Downloaded from http://www.juris.de]

Bissels, Alexander (2009b): Standpunkt Twitter & Co.: Neue Herausforderungen an das Arbeitsrecht, Betriebs-Berater, p. 2197. [Downloaded from http://www.juris.de]

Bissels, Alexander – Lützeler, Martin – Wisskirchen, Gerlind (2010): Facebook, Twitter & Co.: Das Web 2.0 als arbeitsrechtliches Problem, Betriebs-Berater, pp. 2433-2439. [Downloaded from http://www.juris.de]

Bizer, Johann (2011), in: Simitis, Spiros (ed): Bundesdatenschutzgesetz, Nomos, Baden-Baden.

Bloesinger, Hubert (2007): Grundlagen und Grenzen privater Internetnutzung am Arbeitsplatz, Betriebs-Berater, pp. 2177-2184. [Downloaded from http://www.juris.de]

Bonn, Heinz Paul (2011): BITKOM press release of 06 April 2011, http://www.bitkom.org/files/documents/RFID_PIA_06_04_2011.pdf [06.04.2011]

Braun, Frank – Spiegl, Katarina (2008): E-Mail und Internet am Arbeitsplatz – Was ist erlaubt? Was ist verboten?, Arbeitsrecht im Betrieb, pp. 393-397.

Brink, Stefan – Schmidt, Stephan (2010): Die rechtliche (Un-)Zulässigkeit von Mitarbeiterscreenings – Vom schmalen Pfad der Legalität, MultiMedia und Recht, pp. 592-596. [Downloaded from http://beck-online.beck.de]

Buchner, Benedikt (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

Büllesbach, Alfred (2003), in: Roßnagel, Alexander (ed): Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, Beck, Munich.

Bundesministerium des Innern (2010): Hintergrundpapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes: Kabinettbeschluss vom 25.08.2010, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/pressepapier_beschaeftigtendatenschutz.pdf;jsessionid=875DDC94DFC4D74B5F2EF98355FF1A07.1_cid165?__blob=publicationFile [1.4.2011]

Burton, William C. (2006): Burton's Legal Thesarus, McGraw-Hill Professional, New York.

Busse, Julia (2009): § 10 Datenschutz, in: Besgen, Nicolai – Prinz, Thomas (eds): Handbuch Internet: Arbeitsrecht: Rechtssicherheit bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn.

Callies, Christian (2011), in: Calliess, Christian – Ruffert, Matthias (eds): EUV, AEUV: Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Beck, Munich.

Caspar, Johannes (2011): Interview with Dipl.-Jur. Falk Hagedorn (18 May 2011), http://pawproject.eu/en/sites/default/files/page/interview_caspar_de.pdf [20.09.2011]

CDU – CSU – FDP (2009): Wachstum. Bildung. Zusammenhalt, Koalitionsvertrag zwischen CDU, CSU und FDP, http://www.cdu.de/doc/pdfc/091026-koalitionsvertrag-cducsu-fdp.pdf [01.04.2011]

Dammann, Ulrich (2011), in: Simitis, Spiros (ed): Bundesdatenschutzgesetz, Nomos, Baden-Baden.

Dann, Matthias – Gastell, Roland Gastell (2008): Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, Neue Juristische Wochenschrift, pp. 2945-2949. [Downloaded from http://beck-online.beck.de]

Däubler, Wolfgang (2000): Nutzung des Internet durch Arbeitnehmer, Kommunikation und Recht, pp. 323-327.

Däubler, Wolfgang (2001a): Grundrechte-Charta und kollektives Arbeitsrecht, Arbeit und Recht, pp. 380-384.

Däubler, Wolfgang (2001b): Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht, Neue Zeitschrift für Arbeitsrecht, pp. 874-881. [Downloaded from http://www.juris.de]

Däubler, Wolfgang (2004): Internet und Arbeitsrecht, Bund-Verlag, Frankfurt, M.

Däubler, Wolfgang (2005): Arbeitsrecht und Informationstechnologien – Vom Umgang eines traditionellen Rechtsgebiets mit neuen Herausforderungen, COMPUTER UND RECHT, pp. 767-772.

Däubler, Wolfgang (2010): Gläserne Belegschaften?: Das Handbuch zum Arbeitnehmerdatenschutz, Bund-Verlag, Frankfurt, M.

De Maizière, Thomas (2010): Bundesministerium des Innern, 14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft http://www.bmi.bund.de/cae/servlet/contentblob/1099988/publicationFile/88667/thesen_netzpolitik.pdf [26.05.2011]

Deutsch, Markus – Diller, Martin (2009): Die geplante Neuregelung des Arbeitnehmerdatenschutzes in § 32 BDSG, Der Betrieb, pp. 1462-1465.

De Wolf, Abraham (2010): Kollidierende Pflichten: Zwischen Schutz von E-Mails und "Compliance" im Unternehmen, Neue Zeitschrift für Arbeitsrecht, pp. 1206-1210. [Downloaded from http://beck-online.beck.de]

Dickmann, Roman (2003): Inhaltliche Ausgestaltung von Regelungen zur privaten Internetnutzung im Betrieb, Neue Zeitschrift für Arbeitsrecht, pp. 1009-1013. [Downloaded from http://beck-online.beck.de]

Di Fabio, Udo (2009), in: Maunz, Theodor – Dürig, Günter (eds): Grundgesetz, Beck, Munich.

Dieterich, Thomas (2011), in: Dieterich, Thomas – Hanau, Peter – Schaub, Günter: Erfurter Kommentar zum Arbeitsrecht, Beck, Munich.

Durner, Wolfgang (2011), in: Maunz, Theodor – Dürig, Günter (eds): Grundgesetz, Beck,

Munich.

Düsseldorfer Kreis (2011): Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 8. April 2011 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08042011lDatenschutzKodex.pdf;jsessionid=E00DA804E1E079427B96060617D5C96F.1_cid136?__blob=publicationFile [08.04.2011]

Ege, Andreas (2008): Arbeitsrecht und Web 2.0 – Online-Tagebücher, Corporate Blogging, Wikis, Arbeit und Arbeitsrecht, pp. 72-74.
Ehmann, Horst (1997): Zur Struktur des Allgemeinen Persönlichkeitsrechts, Juristische Schulung, pp. 193-203. [Downloaded from http://beck-online.beck.de]

Ehmer, Jörg (2006), in: Geppert, Martin – Piepenbrock, Hermann-Josef – Schütz, Raimund – Fabian Schuster (eds): Beck'scher TKG-Kommentar, Beck, Munich.

Erler, Andreas (2003): Die private Nutzung neuer Medien am Arbeitsplatz, Utz, Munich.

Ernst, Stefan (2002): Der Arbeitgeber, die E-Mail und das Internet, Neue Zeitschrift für Arbeitsrecht, pp. 585-591. [Downloaded from http://beck-online.beck.de]

European Commission, Communication from the Commission - First stage consultation of social partners on the possible direction of a community action on the protection of workers' personal data, 2002. http://ec.europa.eu/social/BlobServlet?docId=2503&langId=en [18.01.2012]

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 [18.01.2012.]

Evers, Hans-Ulrich (1965): Verletzung des Postgeheimnisses (Art 10 GG) und Beweisverwertungsverbot im Strafprozeß – Zugleich Besprechung des Beschlusses des LG Stuttgart vom 1964-09-29 IV QS 117/64, JuristenZeitung, pp. 661-666. [Downloaded from http://beck-online.beck.de]

Fleck, Ulrike (2003): Brauchen wir ein Arbeitnehmerdatenschutzgesetz?, Betriebs-Berater, pp. 306-310.

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

Forst, Gerrit (2010): Der Regierungsentwurf zur Regelung des Beschäftigtendatenschutzes, Neue Zeitschrift für Arbeitsrecht, pp. 1043-1048. [Downloaded from http://beck-online.beck.de]

Franzen, Martin (2010): Arbeitnehmerdatenschutz – rechtspolitische Perspektiven, Recht der Arbeit, pp. 257-263.

Fraunhofer-Institut für Angewandte Informationstechnik FIT (2010): Pressemeldung vom 24. November 2010, http://www.fit.fraunhofer.de/presse/10-11-24_de.html [01.04.2011]

Friedrich, Hans-Peter (2011), Gastkommentar in der Financial Times Deutschland vom 26.05.2011, http://www.ftd.de/it-medien/medien-internet/:gastkommentar-des-innenministers-das-internet-braucht-nicht-immer-gleich-gesetze/60056634.html [26.05.2011]

Gabel, Detlev (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

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

Gastell, Dann (2008): Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, Neue juristische Wochenschrift, pp. 2945-2949. [Downloaded from http://beck-online.beck.de]

Gerhards, Julia (2010): (Grund-)Recht auf Verschlüsselung?, Nomos, Baden-Baden.

Gola, Peter (1999): Neuer Tele-Datenschutz für Arbeitnehmer? – Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MultiMedia und Recht, pp. 322-330. [Downloaded from http://beck-online.beck.de]

Gola, Peter (2002): Die Einwilligung als Legitimation für die Verarbeitung von Arbeitnehmerdaten, Recht der Datenverarbeitung, pp. 109-116.

Gola, Peter (2007): Datenschutz bei der Kontrolle „mobiler" Arbeitnehmer – Zulässigkeit und Transparenz, Neue Zeitschrift für Arbeitsrecht, pp.1139-1144. [Downloaded from http://beck-online.beck.de]

Gola, Peter (2010a): Datenschutz und Multimedia am Arbeitsplatz: Rechtsfragen und Handlungshilfen für die betriebliche Praxis, Datakontext, Heidelberg.

Gola, Peter (2010b), in: Hümmerich, Klaus – Boecken, Winfried – Düwell, Franz Josef (eds): AnwaltKommentar Arbeitsrecht, Deutscher Anwaltverlag, Bonn.

Gola, Peter – Klug, Christoph (2004): Videoüberwachung gemäß § 6b BDSG – Anmerkungen zu einer verunglückten Gesetzeslage, Recht der Datenverarbeitung, pp. 65-74.

Gola, Peter – Schomerus, Rudolf (2010): Bundesdatenschutzgesetz: Kommentar, Beck, Munich.

Gola, Peter – Wronka, Georg (2010): Handbuch zum Arbeitnehmerdatenschutz: Rechtsfragen unter Berücksichitgung der BDSG-Novellen, Datakontext, Heidelberg.

Grentzenberg, Verena – Schreibauer, Markus – Schuppert, Stefan (2009): Die Datenschutznovelle (Teil II) – Ein Überblick zum "Gesetz zur Änderung datenschutzrechtlicher Vorschriften", Kommunikation und Recht, pp. 535-543.

Grimm, Detlef – Brock, Martin – Windeln, Norbert (2006): Video-Überwachung am Arbeitsplatz, Der Arbeits-Rechts-Berater, pp. 179-182.

Grimm, Detlef – Schiefer, Jennifer (2009): Videoüberwachung am Arbeitsplatz, Recht der Arbeit, pp. 329-344.

Grobys, Marcel (2003): Wir brauchen ein Arbeitnehmerdatenschutzgesetz!, Betriebs-Berater, pp. 682-683. [Downloaded from http://www.juris.de]

Grosjean, Sascha R. (2003): Überwachung von Arbeitnehmern – Befugnisse des Arbeitgebers und mögliche Beweisverwertungsverbote, Der Betrieb, pp. 2650-2654.

Groß, Thomas (2011), in: Friauf, Karl Heinrich – Höfling, Wolfgang (eds): Berliner Kommentar zum Grundgesetz, Erich Schmidt Verlag, Berlin.

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

Hanau, Peter – Hoeren, Thomas (2003): Private Internetnutzung durch Arbeitnehmer: Die arbeits- und betriebsverfassungsrechtlichen Probleme, Beck, Munich.

Hansen, Marit – Wiese, Markus (2004): RFID – Radio Frequency Identification, Datenschutz und Datensicherheit, p. 109.

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

Hartmann, Daniel – Pröpper, Martin (2009): Internet und E-Mail am Arbeitsplatz – Mustervereinbarung für den dienstlichen und privaten Zugang, Betriebs-Berater 2009, pp. 1300-1302. [Downloaded from http://www.juris.de]

Heckmann, Dirk (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

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.

Heidrich, Joerg (2009): Rechtliche Fragen bei der Verwendung von DNS-Blacklisting zur Spam-Filterung, COMPUTER UND RECHT, pp. 168-173.

Heise online (2010): Newsticker vom 21.07.2010, http://www.heise.de/newsticker/meldung/Facebook-meldet-500-Millionen-Mitglieder-1043251.html [21.07.2010]

Heldmann, Sebastian (2010): Betrugs- und Korruptionsbekämpfung zur Herstellung von Compliance – Arbeits- und datenschutzrechtliche Sicht, Der Betrieb, pp. 1235-1239.

Helle, Jürgen (2004): Die heimliche Videoüberwachung – zivilrechtlich betrachtet, JuristenZeitung, pp. 340-347.

Hesse, Konrad (1985): Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, Müller, Heidelberg.

Hilber, Marc D. (2005): Die datenschutzrechtliche Zulässigkeit intranet-basierter Datenbanken internationaler Konzerne, Recht der Datenverarbeitung, pp. 143-152.

Hillgruber, Christian (2007): Der Staat des Grundgesetzes – nur bedingt abwehrbereit? Plädoyer für eine wehrhafte Verfassungsinterpretation, JuristenZeitung, pp. 209-218.

Hoeren, Thomas – Sieber, Ulrich (2010): Handbuch Multimedia-Recht, Beck, Munich.

Hold, Dieter (2006): Arbeitnehmer-Datenschutz – Ein Überblick, Recht der Datenverarbeitung, pp. 249-259.

Holzner, Stefan (2011): Neues zur Regelung der Nutzung von E-Mail und Internet am Arbeitsplatz?, Zeitschrift für Rechtspolitik, pp. 12-15.

Hoppe, Christian (2010): Arbeitnehmerhaftung und ihre Auswirkungen auf die Nutzung betrieblicher Kommunikationsmittel, Arbeitsrecht Aktuell, p. 388. [Downloaded from http://beck-online.beck.de]

Hoppe, René – Braun, Frank (2010): Arbeitnehmer-E-Mails: Vertrauen ist gut – Kontrolle ist schlecht – Auswirkungen der neuesten Rechtsprechung des BVerfG auf das Arbeitsverhältnis, MultiMedia und Recht, pp. 80-84.

Hornung, Gerrit – Desoi, Monika (2011): "Smart Cameras" und automatische Verhaltensanalyse – Verfassungs- und datenschutzrechtliche Probleme der nächsten Generation der Videoüberwachung, Kommunikation und Recht, pp. 153-158.

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].

Jandt, Silke (2007): Datenschutz bei Location Based Services – Voraussetzungen und Grenzen der rechtmäßigen Verwendung von Positionsdaten, MultiMedia und Recht, pp. 74-78. [Downloaded from http://beck-online.beck.de]

Jenau, Jens (2010): Private Nutzung von Internet und Firmen-E-Mail-Adresse am Arbeitsplatz, Arbeitsrecht im Betrieb, pp. 88-92.

John, Dana (2011), in: Kilian, Wolfgang – Heussen, Benno (eds): Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis, Beck, Munich.

Jordan, Christopher – Bissels, Alexander – Löw, Christine (2008): Arbeitnehmerkontrolle im Call-Center durch Silent Monitoring und Voice Recording, Betriebs-Berater, pp. 2626-2631.

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

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

Kamp, Meike – Körffer, Barbara (2010): Auswirkungen des § 32 BDSG auf die Aufgabenerfüllung und die strafrechtliche Verantwortung des Compliance Officers, Recht der Datenverarbeitung, pp. 72-76.

Kania, Thomas (2011): Gleichbehandlung, in: Küttner, Wolfdieter – Roller, Jürgen (eds): Personalbuch 2011: Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, Beck, Munich.

Kempf, Dieter (2011): Statement „Datenschutz im Internet“ vom 08.02.2011, http://www.bitkom.org/files/documents/BITKOM_Statement_Datenschutz_Prof_Kempf_08_02_2011.pdf [01.04.2011]

Kinast, Karsten (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

Kindt, Els (2010): Need for Legal Analysis of Biometric Profiling in: Hildebrandt, Mireille – Gutwirth, Serge (eds): Profiling the European Citizen: cross-disciplinary perspectives. Springer, Dordrecht. pp. 139-144.

Kirsch, Markus (2011): Die datenschutzrechtliche Beurteilung von Kamera-Attrappen im Betrieb; MultiMedia und Recht-Aktuell, 317919. [Downloaded from http://beck-online.beck.de]

Kiss, György (2005): Munkajog, Osiris

Kliemt, Michael (2011): Vertrauen ist gut, Kontrolle ist besser? Internet- und E-Mail-Nutzung von Mitarbeitern, Arbeit und Arbeitsrecht, pp. 532-538.

Klug, Christoph (2001): Beispiele richtlinienkonformer Auslegung des BDSG, Recht der Datenverarbeitung, pp. 266-274.

Koch, Frank A. (2008): Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel, Neue Zeitschrift für Arbeitsrecht, pp. 911-916. [Downloaded from http://beck-online.beck.de]

Kort, Michael (2011): Lückenhafte Reform des Beschäftigtendatenschutzes – Offene Fragen und mögliche Antworten in Bezug auf die geplanten §§ 32 ff. BDSG, MultiMedia und Recht, pp. 294-299.

Kramer, Ernst A. (2007), in: Säcker, Franz Jürgen – Rixecker, Roland (eds): Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB: Band 2: Schuldrecht Allgemeiner Teil: §§ 241-432, Beck, Munich.

Kramer, Philipp (2010): Dix in Hamburg: „§ 32 BDSG ist Baustellenschild“, Datenschutz-Berater, pp. 14-16.

Kramer, Stefan (2004): Internetnutzung als Kündigungsgrund, Neue Zeitschrift für Arbeitsrecht, pp. 458-467. [Downloaded from http://beck-online.beck.de]

Kramer, Stefan (2010): Gestaltung betrieblicher Regelungen zur IT-Nutzung, Arbeitsrecht Aktuell, p. 164. [Downloaded from http://beck-online.beck.de]

Kratz, Felix – Gubbels, Achim (2009): Beweisverwertungsverbote bei privater Internetnutzung am Arbeitsplatz, Neue Zeitschrift für Arbeitsrecht, pp. 652-656.

Kunst, Heiko (2003): Individualarbeitsrechtliche Informationsrechte des Arbeitnehmers, 2003 Individualarbeitsrechtliche Informationsrechte des Arbeitnehmers: Ein Beitrag zur Informationsordnung im Arbeitsverhältnis, Lang, Frankfurt, M.

Lane, Frederick S. (2003): The Naked Employee. How Technology Is Compromising Workplace Privacy. AMACOM, New York

Langrock, Marc – Samson, Erich (2007): Bekämpfung von Wirtschaftskriminalität im und durch Unternehmen, Der Betrieb, pp. 1684-1689.

Lauterbach, Ernst (2002): Latein-Deutsch: Zitaten-Lexikon, Lit Verlag, Berlin, Münster, Wien, Zürich, London.

Lembke, Mark (2010), in: Henssler, Martin – Willemsen, Josef – Kalb, Heinz-Jürgen (eds): Arbeitsrecht Kommentar, Verlag Dr. Otto Schmidt, Cologne.

Lerch, Hana – Krause, Beate – Hotho, Andreas – Roßnagel, Alexander – Stumme, Gerd (2010): Social Bookmarking-Systeme – die unerkannten Datensammler – Ungewollte personenbezogene Datenverabeitung?, MultiMedia und Recht, pp. 454-458. [Downloaded from http://beck-online.beck.de]

Leopold, Nils – Meints, Martin (2010): Profiling in Employment Situations (Fraud) in: Hildebrandt, Mireille – Gutwirth, Serge (eds): Profiling the European Citizen: cross-disciplinary perspectives. Springer, Dordrecht. pp. 217-226.

Lindemann, Achim – Simon, Oliver (2001): Betriebsvereinbarungen zur E-Mail, Internet- und Intranet-Nutzung, Betriebs-Berater, pp. 1950-1956. [Downloaded from http://www.juris.de]

Löwisch, Manfred (2009): Fernmeldegeheimnis und Datenschutz bei der Mitarbeiterkontrolle, Der Betrieb, pp. 2782-2786.

Lunk, Stefan (2009): Prozessuale Verwertungsverbote im Arbeitsrecht, Neue Zeitschrift für Arbeitsrecht, pp. 457-464. [Downloaded from http://beck-online.beck.de]

Mähner, Nicolas (2010): Neuregelung des § 32 BDSG zur Nutzung personenbezogener Mitarbeiterdaten – Am Beispiel der Deutschen Bahn AG, MultiMedia und Recht, pp. 379-382. [Downloaded from http://beck-online.beck.de]

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

Marxen, Horst (1958): Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG): Unter besonderer Berücksichtigung der gesetzlich zulässigen Ausnahmen, without obligation, Kiel.

Maschmann, Frank (2002): Zuverlässigkeitstest durch Verführung illoyaler Mitarbeiter?, Neue Zeitschrift für Arbeitsrecht, pp. 13-22. [Downloaded from http://beck-online.beck.de]

Maties, Martin (2008): Arbeitnehmerüberwachung mittels Kamera?, Neue Juristische Wochenschrift, pp. 2219-2225. [Downloaded from http://beck-online.beck.de]

Mattl, Tina (2008): Die Kontrolle der Internet- und E-Mail Nutzung am Arbeitsplatz, Verlag Dr. Kovaĉ, Hamburg.

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.

Mengel, Anja (2004a): Kontrolle der Telefonkommunikation am Arbeitsplatz, Betriebs-Berater, pp. 1445-1453. [Downloaded from http://www.juris.de]

Mengel, Anja (2004b): Kontrolle der E-Mail- und Internetkommunikation am Arbeitsplatz, Betriebs-Berater, pp. 2014-2021. [Downloaded from http://www.juris.de]

Mengel, Anja (2005): Alte arbeitsrechtliche Realitäten im Umgang mit der neuen virtuellen Welt, Neue Zeitschrift für Arbeitsrecht, pp. 752-754. [Downloaded from http://beck-online.beck.de]

Meyer, Sebastian (2008): Ortung eigener Mitarbeiter zu Kontrollzwecken, in: Taeger, Jürgen – Wiebe, Andreas (eds): Von AdWords bis Social Networks: Neue Entwicklungen im Informationsrecht: Tagungsband Herbstakademie 2008, Edewecht, Oldenburg.

Meyer, Sebastian (2009): Mitarbeiterüberwachung: Kontrolle durch Ortung von Arbeitnehmern, Kommunikation und Recht, pp. 14-20.

Moll, Wilhelm (2009): Münchener Anwaltshandbuch Arbeitsrecht, Beck, Munich.

Mozek, Martin – Zendt, Marcus (2011), in: Hoeren, Thomas – Sieber, Ulrich (eds): Handbuch multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, Beck, Munich.

Müller-Glöge, Rudi (2009), in: Säcker, Franz Jürgen – Rixecker, Roland (eds): Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB: Band 4: Schuldrecht Besonderer Teil II §§ 611-704 EFZG, TzBfG, KSchG, Beck, Munich.

Munz, Martin (2010), in Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

Müller, Arnold (2008): Die Zulässigkeit der Videoüberwachung am Arbeitsplatz: In der Privatwirtschaft aus arbeitsrechtlicher Sicht, Nomos, Munich.

Moos, Flemming (2010), in Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

Nägele, Stefan – Meyer, Lars (2004): Internet und E-Mail am Arbeitsplatz: Rechtliche Rahmenbedingungen der Nutzung und Kontrolle sowie der Reaktion auf Missbrauch, Kommunikation und Recht, pp. 312-316.

National Workrights Institute (2003): On Your Tracks: GPS Tracking in the Workplace, http://epic.org/privacy/workplace/gps-traking.pdf [18.01.2012]

Naujock, Anja (2002): Internet-Richtlinien – Nutzung am Arbeitsplatz – Ein Plädoyer für eine

klare Regelung, Datenschutz und Datensicherheit, pp. 592-596.

Nouwt/de Vries/Loermans (2005): Analysis of the country reports, in: Nouwt, Sjaak – De Vries, Brend R. – Prins, Corien (eds): Reasonable Expectations of Privacy? Eleven country reports on camera surveillance and workplace privacy, Cambridge University Press, Cambridge. pp. 323-357.

Oberwetter, Christian (2008): Arbeitnehmerrechte bei Lidl, Aldi & Co., Neue Zeitschrift für Arbeitsrecht, pp. 609-613. [Downloaded from http://beck-online.beck.de]

Oberwetter, Christian (2011): Soziale Netzwerke im Fadenkreuz des Arbeitsrechts, Neue Juristische Wochenschrift, pp. 417-421. [Downloaded from http://beck-online.beck.de]

Oehler, Dietrich (1954): Postgeheimnis, in: Neumann, Franz L. – Nipperdey, Hans Carl – Scheuner, Ulrich (eds): Die Grundrechte: Handbuch der Theorie und Praxis der Grundrechte: Band 2, Duncker & Humblot, Berlin.

Orantek, Kerstin (2008): Datenschutz im Informationszeitalter: Herausforderungen durch technische, politische und gesellschaftliche Entwicklungen, GUC-Verlag, Lößnitz.

Ott, Stephan (2009): Stephan Das Internet vergisst nicht – Rechtsschutz für Suchobjekte?, MultiMedia und Recht, pp. 158-163. [Downloaded from http://beck-online.beck.de]

Pagenkopf, Martin (2009), in: Sachs, Michael (ed): Grundgesetz, Kommentar, Beck, Munich.

Pauly, Stephan – Osnabrügge, Stephan (2009): § 6 Überlassung und Nutzung von Arbeitsmitteln, in: Besgen, Nicolai – Prinz, Thomas (eds): Handbuch Internet: Arbeitsrecht: Rechtssicherheit bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn.

Petersen, Julie K. (2007): Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications: Spy Devices, Privacy, History and Applications. Auerbach Publications, Boca Raton, FL.

Petri, Thomas (2009): Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, in: Kartmann, Norbert – Ronellenfitsch, Michael (eds): Vorgaben des Bundesverfassungsgerichts für eine zeitgemäße Datenschutzkultur in Deutschland: 17. Wiesbadener Forum Datenschutz, Der Hessische Datenschutzbeauftragte, Der Präsident des Hessischen Landtags, Wiesbaden.

Petri, Thomas (2010): Compliance und Datenschutz, in: Schweighofer, Erich – Geist, Anton – Staufer, Ines (eds): Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik: Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010, OCG books, Wien.

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.

Post-Ortmann, Karin (1999): Der Arbeitgeber als Anbieter von Telekommunikations- und Telediensten, Recht der Datenverarbeitung, pp. 102-109.

Preis, Ulrich (2011), in: Dieterich, Thomas – Hanau, Peter – Schaub, Günter: Erfurter Kommentar zum Arbeitsrecht, Beck, Munich.

Pröpper, Martin – Römermann, Martin (2008): Nutzung von Internet und E-Mail am

Arbeitsplatz (Mustervereinbarung), MultiMedia und Recht, pp. 514-518. [Downloaded from http://beck-online.beck.de]

Raffner, Andrea – Hellich, Peter (1997): Unter welchen Voraussetzungen ist die Überwachung von Arbeitnehmer-E-Mails zulässig?, Neue Zeitschrift für Arbeitsrecht, pp. 862-868. [Downloaded from http://beck-online.beck.de]

Raif, Alexander (2010): Beschäftigtendatenschutz: Wird alles neu bei der Arbeitnehmerkontrolle?, Arbeitsrecht Aktuell, p. 359. [Downloaded from http://beck-online.beck.de]

Raif, Alexander – Bordet, Katharina (2010): Twitter, Facebook & Co. – Arbeitrechtliche Fragen im Web 2.0, Arbeit und Arbeitsrecht, pp. 88-90.

Rasmussen-Bonne, Hans-Eric – Raif, Alexander (2011): Neues beim Beschäftigtendatenschutz – Worauf sich Unternehmen einstellen müssen, Gesellschafts- und Wirtschaftsrecht, p. 80. [Downloaded from http://beck-online.beck.de]

Rath, Michael – Karner, Sophia (2007): Private Internetnutzung am Arbeitsplatz – rechtliche Zulässigkeit und Kontrollmöglichkeiten des Arbeitgebers, Kommunikation und Recht, pp. 446-452.

Rath, Michael – Karner, Sophia (2010): Internetnutzung und Datenschutz am Arbeitsplatz, Kommunikation und Recht, pp. 469-475.

Richardi, Reinhard – Kortstock, Ulf (2005): BAG: Videoüberwachung am Arbeitsplatz – allgemeines Persönlichkeitsrecht – Grundsatz der Verhältnismäßigkeit – Besprechung des Beschlusses BAG v. 29. 6. 2004 - 1 ABR 21/03, Recht der Arbeit, pp. 381-384.

Richardi, Reinhard (2010): Betriebsverfassungsgesetz: BetrVG mit Wahlordnung, Beck, Munich.

Roloff, Sebastian (2009): § 5 Überwachungseinrichtungen, in: Besgen, Nicolai – Prinz, Thomas (eds): Handbuch Internet: Arbeitsrecht: Rechtssicherheit bei Nutzung, Überwachung und Datenschutz, Deutscher Anwaltsverlag, Bonn.

Roßnagel, Alexander (2003): Handbuch Datenschutzrecht: Die neuen Grundlagen für Wirtschaft und Verwaltung, Beck, Munich.

Salvenmoser, Steffen – Hauschka, Christoph E. (2010): Korruption, Datenschutz und Compliance, Neue Juristische Wochenschrift, pp. 331-335. [Downloaded from http://beck-online.beck.de]

Sassenberg, Thomas – Bamberg, Niclas (2006): Betriebsvereinbarung contra BDSG?, Datenschutz und Datensicherheit, pp. 226-229.

Schaar, Peter (2008): Dokumentation der Festveranstaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus Anlass des 25. Jahrestages der Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts am 15. Dezember 2008 im Bürgersaal des Karlsruher Rathauses, http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/Dokumentation25JahreVolkszaehlungsurteil.pdf?__blob=publicationFile [01.04.2011]

Schaar, Peter (2011), Gespräch mit der Projektgruppe Datenschutz der Enquete-Kommission "Internet und digitale Gesellschaft" http://www.bundestag.de/dokumente/textarchiv/2011/33500340_kw08_pa_schaar/index.html [01.04.2011]

Schmidt, Bernd (2009a): Arbeitnehmerdatenschutz gemäß § 32 BDSG – Eine Neuregelung

(fast) ohne Veränderung der Rechtslage, Recht der Datenverarbeitung, pp. 193-200.

Schmidt, Bernd (2009b): Vertrauen ist gut, Compliance ist besser, Betriebs-Berater, pp. 1295-1299. [Downloaded from http://www.juris.de]

Schmidt, Bernd (2010): Beschäftigtendatenschutz in § 32 BDSG – Perspektiven einer vorläufigen Regelung, Datenschutz und Datensicherheit, pp. 207-209.

Schmidt, Walter (1974): Die bedrohte Entscheidungsfreiheit, JuristenZeitung, pp. 241-250. [Downloaded from http://beck-online.beck.de]

Schmitt-Rolfes, Günther (2008): Kontrolle von Internet- und E-Mail-Nutzung am Arbeitsplatz, Arbeit und Arbeitsrecht, p. 391.

Schaffland, Hans-Jürgen – Wiltfang, Noeme (2010): Bundesdatenschutzgesetz (BDSG): Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Erich Schmidt Verlag, Berlin.

Schaub, Günter – Linck, Rüdiger (2009), in: Schaub, Günther: ArbeitsR-Handbuch: Systematische Darstellung und Nachschlagewerk für die Praxis, Beck, Munich.

Scheja, Gregor (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

Schmidl, Michael (2010): Aspekte des Rechts der IT-Sicherheit, Neue Juristische Wochenschrift, pp. 476-481. [Downloaded from http://beck-online.beck.de]

Schmidt, Bernd (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

Schmitz, Peter – Eckhardt, Jens (2007): Einsatz von RFID nach dem BDSG, COMPUTER UND RECHT, pp. 171-177.

Schrader, Hans-Hermann (2002): 18. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten – zugleich Tätigkeitsbericht der Aufsichtsbehörde für den nicht öffentlichen Bereich 2000/2001.

Schuster, Friederike (2009): Die Internetnutzung als Kündigungsgrund, Verlag Dr. Kovaĉ, Hamburg.

Seitz, Walter (2011), in: Hoeren, Thomas – Sieber, Ulrich (eds): Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, Beck, Munich.

SID – FID (2011): SID/FIT Social Media Report 2010/2011
http://www.softwareinitiative.de/studien/SID-FITSocialMediaReport20102011.pdf
[01.04.2011]

Simitis, Spiros (1981): Schutz von Arbeitnehmerdaten, Regelungsdefizite, Lösungsvorschläge, Gutachten erstattet im Auftrag des Bundesministers für Arbeit und Sozialordnung, Bundesminister für Arbeit u. Sozialordnung, Referat Presse- u. Öffentlichkeitsarbeit, Bonn.

Simitis, Spiros (1989): Zur Mitbestimmung bei der Verarbeitung von Arbeitnehmerdaten – Eine Zwischenbilanz, Recht der Datenverarbeitung, pp. 49-60.

Simitis, Spiros (1999): Zur Internationalisierung des Arbeitnehmerdatenschutzes – Die verhaltensregeln der Internationalen Arbeitsorganisation, in: Hanau, Peter – Heither, Friedrich – Kühling, Jürgen (eds): Richterliches Arbeitsrecht: Festschrift für Thomas Dieterich zum 65. Geburtstag, Beck, Munich.

Simitis, Spiros (2001): Arbeitnehmerdatenschutzgesetz – Realistische Erwartung oder Lippenbekenntnis?, Arbeit und Recht, pp. 429-433.

Simitis, Spiros (2003): Zu den erwarteten Auswirkungen auf das deutsche Recht, Recht der Datenverarbeitung, pp. 43-49.

Simitis, Spiros (2010): Bundesdatenschutzgesetz, Nomos, Munich.

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

SPIEGEL ONLINE (2009), http://www.spiegel.de/netzwelt/web/0,1518,621185,00.html [01.04.2011]

Stanton, Jeffrey M. – Stam, Kathryn R. (2006): The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets - Without Compromising Employee Privacy or Trust. Information Today, Inc. Medford, NJ.

Steffen, Till – Weichert, Thilo (2009): Gehört der private Datenschutz ins BGB?, Zeitschrift für Rechtspolitik, p. 95.

Steinkühler, Bernhard – Raif, Alexander (2009): Big brother am Arbeitsplatz: Arbeitnehmerüberwachung auf neustem technischem Stand, Arbeit und Arbeitsrecht, pp. 213-217.

Stück, Volker (2010): LAG Rheinland-Pfalz: Nutzungsverbot für privates Handy während Arbeitszeit, Arbeitsrecht Aktuell, p. 432.

Szabó, Máté D. – Székely, Iván (2005): Privacy and data protection at the workplace in Hungary. in: Nouwt, Sjaak – De Vries, Brend R. – Prins, Corien (eds): Reasonable Expectations of Privacy? Eleven country reports on camera surveillance and workplace privacy, Cambridge University Press, Cambridge. pp. 249-278.

Székely, Iván – Szabó, Máté Dániel (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.

TBS (2006): Technologieberatungsstelle beim DGB NRW e.V.: VoIP – Telefonieren übers Internet – Handlungshilfen für die betriebliche Interessenvertretung, http://www.tbs-nrw.de/cweb/cgi-bin-noauth/cache/VAL_BLOB/789/789/290/UmschlTBSBroschVoIP.pdf [01.04.2011]

Thon, Horst (2006): Datenschutz im Arbeitsverhältnis, in: Bauer, Jobst-Hubertus – Beckmann, Paul Werner – Lunk, Stefan – Meier, Hans-Georg – Schütte, Reinhard (eds): 25 Jahre Arbeitsgemeinschaft Arbeitsrecht im DAV, Deutscher Anwalt-Verlag, Bonn.

Thüsing, Gregor (2009): Datenschutz im Arbeitsverhältnis – Kritische Gedanken zum neuen § 32 BDSG, Neue Zeitschrift für Arbeitsrecht, pp. 865-870. [Downloaded from http://beck-online.beck.de]

Thüsing, Gregor (2010): Arbeitnehmerdatenschutz und Compliance: Effektive Compliance im Spannungsfeld von reformiertem BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, Beck, Munich.

Tinnefeld, Marie-Theres – Petri, Thomas – Brink, Stefan (2010): Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz – Eine erste Analyse und Bewertung, MultiMedia und Recht, pp. 727-735. [Downloaded from http://beck-online.beck.de]

Trappehl, Bernhards – Schmidl, Michael (2009): Arbeitsrechtliche Konsequenzen von IT-Sicherheitsverstößen, Neue Zeitschrift für Arbeitsrecht, pp. 985-990.

Trittin, Wolfgang – Fischer, Esther D. (2009): Datenschutz und Mitbestimmung – Konzernweite Personaldatenverarbeitung und die Zuständigkeit der Arbeitnehmervertretung, Neue Zeitschrift für Arbeitsrecht, pp. 343-346. [Downloaded from http://beck-online.beck.de]

Uecker, Andre (2003): Private Internet- und E-Mail-Nutzung am Arbeitsplatz – Entwurf einer Betriebsvereinbarung, Der IT-Rechts-Berater, pp.158-162.

UNI-Europa's submission to the European Commission in relation to the use of RFID's in the workplace, http://www.uniglobalunion.org/__C1257537004AB759.nsf/0/8F8F0A97716B4A86C1257543003C3928?Open&Highlight=2,rfid [18.01.2012]

Various experts (2011), public hearing of experts on the issue of the government's legislative draft from 23 May 2011, Fachdienst Arbeitsrecht, 318249.

Vehslage, Thorsten (2001): Privates Surfen am Arbeitsplatz, Anwaltsblatt, pp. 145-149.

Vietmeyer, Katja – Byers, Philipp (2010): Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis – Geplante BDSG-Novelle lässt Anwendbarkeit des TKG im Arbeitsverhältnis unangetastet, MultiMedia und Recht, pp. 807-810. [Downloaded from http://beck-online.beck.de]

Vogel, Florian – Glas, Vera (2009): Datenschutzrechtliche Probleme unternehmensinterner Ermittlungen, Der Betrieb, pp. 1747-1754.

Vogt, Volker (2009): Compliance und Investigations – Zehn Fragen aus Sicht der arbeitsrechtlichen Praxis, Neue juristische Online Zeitschrift, pp. 4206-4220. [Downloaded from http://beck-online.beck.de]

Von Steinau-Steinrück, Robert – Mosch, Ulrich (2009): Datenschutz für Arbeitnehmer – Bestandsaufnahme und Ausblick, Neue Juristische Wochenschrift-Spezial, pp. 450-451. [Downloaded from http://beck-online.beck.de]

Von Westerholt, Gräfin Margot – Döring, Wolfgang (2004): Datenschutzrechtliche Aspekte der Radio Frequency Identification – Ein virtueller Rundgang durch den Supermarkt der Zukunft, COMPUTER UND RECHT, pp. 710-716.

Waltermann, Raimund (2007): Anspruch auf private Internetnutzung durch betriebliche Übung?, Neue Zeitschrift für Arbeitsrecht, pp. 529-533. [Downloaded from http://beck-online.beck.de]

Wank, Rolf (2011), in: Dieterich, Thomas – Hanau, Peter – Schaub, Günter (eds): Erfurter Kommentar zum Arbeitsrecht, Beck, Munich.

Wedde, Peter (2009), in: Däubler, Wolfgang – Klebe, Thomas – Wedde, Peter – Weichert (eds): Bundesdatenschutzgesetz: Kompaktkommentar zum BDSG, Bund-Verlag, Frankfurt, M.

Weichert, Thilo (2007): Datenschutz bei Suchmaschinen, MEDIEN und RECHT International, pp. 188-194. [Downloaded from http://www.juris.de]

Weichert, Thilo – Kilian, Wolfgang (2011), in: Kilian, Wolfgang – Heussen, Benno (eds):

Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis, Beck, Munich.

Weißnicht, Elmar (2003): Die Nutzung des Internet am Arbeitsplatz, MultiMedia und Recht, pp. 448-453. [Downloaded from http://beck-online.beck.de]

Weißnicht, Elmar (2008): IT-Risikomanagement und Online-Überwachung von Arbeitnehmern im Konzern, in: Krimphove, Dieter (ed): Reihe: Europäisches Wirtschaftsrecht, EUL Verlag, Lohmar.

Wellhöner, Astrid – Byers, Philipp (2009): Datenschutz im Betrieb – Alltägliche Herausforderungen für den Arbeitgeber?, Betriebs-Berater, pp. 2310-2316. [Downloaded from http://www.juris.de]

Wiese, Günther (2004): Videoüberwachung von Arbeitnehmern durch den Arbeitgeber und Persönlichkeitsschutz, in: Wandt, Manfred – Reiff, Peter – Looschelders, Dirk – Bayer, Walter (eds): Kontinuität und Wandel des Versicherungsrechts: Festschrift für Prof. Dr. Egon Lorenz zum 70. Geburtstag, Verlag Versicherungswirtschaft, Karlsruhe.

Wilke, Matthias (2006): Videoüberwachung - Dürfen Arbeitgeber ihre Angestellten mit Videoanlagen beobachten?, Arbeitsrecht im Betrieb, pp. 31-37.

Wittern, Felix – Schuster, Fabian (2006), in: Geppert, Martin – Piepenbrock, Hermann-Josef – Schütz, Raimund – Fabian Schuster (eds): Beck'scher TKG-Kommentar, Beck, Munich.

Wohlgemuth, Hans H. (1988): Datenschutz für Arbeitnehmer, Luchterhand, Neuwied.

Wohlgemuth, Hans H. – Mostert, Michael (1986): Rechtsfragen der betrieblichen Telefondatenverarbeitung, Arbeit und Recht, pp. 138-146.

Wolf, Thomas – Mulert, Gerrit (2008): Die Zulässigkeit der Überwachung von E-Mail-Korrespondenz am Arbeitsplatz, Betriebs-Berater, pp. 442-447. [Downloaded from http://www.juris.de]

Worzalla, Michael (2008), in: Hess, Harald – Schlochauer,Ursula – Worzalla, Michael – Glock, Dirk – Nicolai, Andrea (eds): BetrVG – Kommentar zum Betriebsverfassungsgesetz, Luchterhand, Cologne.

Wybitul, Tim (2009): Das neue Beschäftigtendatenschutzgesetz: Verschärfte Regeln für Compliance und interne Ermittlungen – Vertrauen ist gut, Kontrolle verboten?, Betriebs-Berater, pp. 1582-1585.

Wybitul, Tim (2011): Bundestag: Streit um den neuen Beschäftigtendatenschutz, MultiMedia Aktuell, 315091.

XING (2011), XING AG Unternehmensprofil,
https://companyprofile.xing.com/de_index.html [01.04.2011]

Zöll, Oliver (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

Zöllner, Wolfgang (1983): Daten- und Informationsschutz im Arbeitsverhältnis, Carl Heymanns Verlag, Cologne.

Zscherpe, Kerstin A. (2010), in: Taeger, Jürgen – Gabel, Detlev (eds): Kommentar zum BDSG und den Datenschutzvorschriften des TKG und TMG, Verlag Recht und Wirtschaft, Frankfurt, M.

4.2. Bundestag printed matters

(2000a): 14/4329 [13.10.2000]

(2000b): 14/4458 [31.10.2000]

(2001): 14/5793 [4.4.2001]

(2004): 15/2316 [9.1.2004]

(2009a): 16/13657 [1.7.2009]

(2009b): 17/69 [25.11.2009]

(2010a): 535/10 [5.11.2010].

(2010b): 17/4230 [15.12.2010]

(2011): 17/4853 [22.2.2011]

4.3. Bundesrat printed matter

535/10 (B) [5.11.2010]

State parliament Schleswig-Holstein (2009), printed matter 16/2439 [3.3.2009]

4.4. Cases of the Hungarian 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]

4.5. Court cases

4.5.1. 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.

4.5.2. 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.;

4.5.3. The main decisions of German High Courts quoted as follows

- court, journal, starting page, page of interest [e.g. BVerfG, NJW (= Neue Juristische Wochenschrift), 822, 824] or
- court, decision, starting page, page of interest [e.g. BAGE 80, 366, 376] respectively
- court, file no. [e.g. in case of not being published, e.g. ArbG Düsseldorf – 4 Ca 3437/01].

The most important decisions can be retrieved from:

http://www.bundesverfassungsgericht.de/entscheidungen.html

http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/list.py?Gericht= bag&Art =en and

http://www.servat.unibe.ch [e.g. decisions of the Federal Constitutional Court (BVerfG) or the Federal Supreme Court (BGH)]

4.6. Other documents

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

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.]