PRIVACY IN THE WORKPLACE

NATIONAL REPORT ON GERMANY

AUTHOR

Dipl.-Jur. Falk Hagedorn

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

JUNE, 2011

CONTENT

1. INTRODUCTION AND BACKGROUND

Nowadays, thanks to the rapid development of modern 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. Now, in the light of a variety of so-called data scandals in German companies,[1] public discussion on creating a separate Employee's Data Protection Act – already alive for a number of years – has finally moved (and correctly so) 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. However, to what dangers are employees exposed in the workplace? At what point do controlling, measuring and monitoring by come up against the juridical boundaries? How are we to succeed in developing new technologies such as GPS, GSM or RFID?[2] How can individuals defend themselves? What possibilities are open to the employer? What can be expected in practice and what are the feasible alternatives to current approaches? These and other questions need to be answered against the background of responsible dealing with employee data. Moreover, there is on occasion a low threshold between what is allowed and what is not – between legal and illegal monitoring. The employer treads a narrow path between enforcing his legitimate interests and encroaching on the personal rights of his employees.

1.1. Objective and methodology

The following examples should provide an overview of the essential questions of the current and planned legal situation in the field of the employee's data protection law and serve to make the reader sensitive to the issue of privacy in the workplace. First an inventory of essential background information is shown which contains, beside the constitutional-juridical context, a depiction of the potential conflicts of interest between employer and employee. In this connection carefully chosen monitoring measures are introduced and analysed. To show a more practical aspect, the position of the data protection authorities is shown with particular reference to a more responsible handling of employee's data. Finally the sanctions are shown before a closing statement follows on the legal situation.

[1] Cf. e.g. the overviews of Däubler, 2010, mgn. 2a ff., as well as of Schmidt, 2010, pp. 207-208 and Oberwetter, 2008, p. 609.

[2] GPS = Global Positioning System; GSM = Global System for Mobile Communications; RFID = Radio Frequency Identification.

1.2. 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[3] 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).[4] The law has been the subject of numerous court decisions,[5] and it is and will remain so. Deriving from Art. 2 par. 1 GG, in conjunction with Art. 1 par. 1 GG,[6] the general right to privacy grants a comprehensive right of respect for the individual and for his personal development.[7] The reference point of this protection is the privacy of the basic legal entity, the person, as such.[8] From this there emerges the obligation of the "fundamental 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."[9] The Federal Constitutional Court stresses that the need for such loophole-closing[10] exists in particular "also in view of modern developments and with them to related new dangers for the protection of the human personality".[11] 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.[12] It goes without question that this personal protection must be also be applied in the workplace.

1.3. 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 –

[3] Gola, 2010a, mgn. 45. On the historical development of the personality right protection, cf. Gola/Wronka, 2010, mgn. 1 ff.
[4] Kerstin Orantek, 2008, p. 51.
[5] 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.
[6] Constant jurisdiction of BVerfG, Cf. just: BVerfGE, 35, 202, 219; 72, 155; 82, 236, 269; 90, 263, 270.
[7] BGHZ 13, 334, 338; 26, 349, 354.
[8] BVerfGE 27, 1; Ehmann, 1997, p. 196; Schmidt, 1974, p. 243.
[9] BVerfGE 54, 148, 153; 95, 220, 241; 99, 185, 193; 101, 361, 380.
[10] BVerfGE 106, 28, 39.
[11] BVerfGE 54, 148, 152; 65, 1, 41.
[12] Di Fabio, 2011, Art. 2 GG mgn. 127.

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.[13]

1.3.1. 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[14] but the fundamental right as an objective value-system prevails over the general clauses[15] in the domain of the private economy.[16] 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.

1.3.1.1. The protection of personality rights over the right of informational self-determination[17]

As far as the area of working conditions is concerned[18] 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.[19] 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).[20] 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."[21] He can basically decide himself when and within what framework he is prepared to reveal his personal circumstances. Thus "there are no more

---

[13] 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.

[14] According to Art. 20. Sec. 3 GG the legislative, executive und judicature are bound to the fundamental rights.

[15] As e.g. the general clauses of BDSG and BGB, Thüsing, 2010, mgn. 342.

[16] 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.

[17] 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.]

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

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

[20] 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).

[21] BVerfGE 65, 1, 44.

irrelevant data among the conditions of automatic data processing"[22] 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.[23] 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.[24] Data must be collected directly from the person concerned (the principle of direct collection).[25] Extensive computer-assisted profiling and complete data collection is forbidden, insofar as this allows a complete picture of the individual involved to be created.[26] 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.[27] The core issue of private life is inviolable;[28] 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 notified of relevant matters, to correct data, to block or even delete it.[29] The person involved has also the opportunity to find legal remedies and turn to the data protection authority.[30]

1.3.1.2. The precedence of the personality right protection over the right to ensure the integrity and confidentiality of information technology systems[31]

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.[32] This expands the guarantees derived from constitutional rights and from the rights to informational self-determination.[33] 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.[34] Secret access to the information technology system that an employee uses or can use are, according to this, not allowed.[35] 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.[36] The IT law is subsidiary and comes after, e.g., telecommunication privacy (Art. 10 Paragraph 1 GG) or the right to informational self-

[22] BVerfGE 65, 1, 44.
[23] BVerfGE 65, 1, 45.
[24] Tinnefeld/Petri/Brink, 2010, p. 727.
[25] Cf. to this aspect Gola/Wronka, 2010, mgn. 454 ff.
[26] BVerfG, NJW 2010, p. 839; 1 BvR 370/07 with reference to BVerfGE 65, 1, 42.
[27] BVerfGE 65, 1, 44-45.
[28] BVerfGE 109, 279, 291.
[29] Cf. BVerfGE 65, 1, 46; Tinnefeld/Petri/ Brink, 2010, p. 727.
[30] Cf. BVerfGE 65, 1, 46.
[31] So-called fundamental right to IT, Tinnefeld/Petri/ Brink, 2010, p. 727.
[32] NJW 2008, p. 822.
[33] Tinnefeld/Petri/ Brink, 2010, p. 727.
[34] BVerfG – 1 BvR 370/07, 1 BvR 595/07 (clause 201).
[35] 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, pp. 55 ff.
[36] BVerfG, NJW 2008, p. 824.

determination.[37] 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.[38] The new dangers, which can occur due to technical development and to new life-circumstances, can, in this way, be avoided.[39]

1.3.1.3. 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.[40]

1.3.1.3.1. The right to the spoken word[41]

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.[42] 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 spoken word is also protected.[43] This relates to categories such as secret voice-recordings[44] or listening with the help of monitoring equipment.[45] Concerning the level of protection, there is no congruity with the right to privacy.[46] 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.[47]

1.3.1.3.2. 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.[48] 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.[49]

1.3.1.3.3. 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.[50] 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

[37] BVerfGE 120, 274, 302.
[38] Durner, 2011, Art. 10 GG mgn. 59.
[39] BVerfG, NJW 2008, p. 824 with reference to BVerfGE 54, 148, 153; 65, 1, 41; 118, 168.
[40] 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.
[41] Concerning the right of the spoken word cf. BVerfGE 34, 238, 246 f.; 54, 148, 154.
[42] BVerfGE 54, 148, 153; BGHZ 27, 284, 286; BAGE 80, 366, 376; Dieterich, 2011, Art. 2 GG mgn. 43.
[43] BGHZ 80, 25, 42; BVerfG, NJW 1992, p. 816.
[44] BVerfG 1992, 815, 816; BAG, NJW 1998, 1331, 1332.
[45] Gola, 2010a, mgn. 48.
[46] BVerfGE 106, 28, 41.
[47] Gola, 2010a, mgn. 49. Cf. further BGH, NJW 2003, p. 1728.
[48] Gola, 2010a, mgn. 51.
[49] Cf. further BVerfGE 80, 367.
[50] Gola, 2010a, mgn. 58.

when he would like to present himself to third parties or to the public[51] and, further, who may save, use and transmit the data in the form of a picture.[52] 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).[53]

1.3.1.3.4. 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.[54]

Scope of protection

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.[55] Art. 10 GG is applied independently of the content and method of sending a letter or of sending a message via telecommunication.[56] All forms of transmission of information by means of telecommunication equipment belong to the field.[57] An important connection for the confidentiality of telecommunication is the actual medium of communication used and the dangers of confidentiality which result from the use of the medium.[58] The protection involves the whole process of communication as such – that is, the time from the beginning to the end of the transmission.[59] When the protection actually starts has so far not been discussed either by the jurisdiction nor by the literature,[60] 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".[61] 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[62] operations.

Limitation of the right of information self-determination based on the actual control of data

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

[51] BVerfGE 63, 131 and 142; constant jurisdiction of the BGH, cf. NJW 1996, p. 986 with further references.
[52] Gola, 2010a, mgn. 58.
[53] Seitz, 2011, part 8 mgn. 6.
[54] BVerfGE 85, 386, 398; 100, 313, 366; 115, 166, 183; Gola, 2010a, mgn. 94.
[55] BVerfGE 67, 157, 171; 100, 313, 358.
[56] Gola, 2010a, mgn. 94.
[57] BVerfGE 85, 386, 396; 100, 313, 358.
[58] BVerfGE 124, 43, 54 f.
[59] Gerhards, 2010, p. 192.
[60] De Wolf, 2010, p. 1209.
[61] BVerfGE 115, 166, 184.
[62] BVerfG, NJW 2002, p. 3620; Gola, 2010a, mgn. 95.

person involved.[63] 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.[64] 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.[65]

1.3.2. 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.[66] When examining a breach of personal rights we must also take into consideration the relevant personal rights of the employer.[67] Personal protection is, hence, limited by the valid (company) interests of the employer.[68] Breaches of the personal rights of the employee can, therefore, be justified by accepting the greater validity of the interests of the employer.[69]

This conflict of fundamental rights is to be harmonised in such a way that the conflicting rights can be harmonised most reasonably.[70] 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) should be considered.[71] Even in respect of important interests of the employer (such as issues of legal compliance)[72] the principles of data protection must also be taken into consideration to an appropriate degree.[73] 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.

1.3.2.1. 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

[63] BVerfG, NJW 2006, p. 976.
[64] BVerfG, NJW 2006, p. 978. Gerhards, 2010, p. 193; de Wolf, 2010, p. 1209; Vietmeyer/Byers, 2010, p. 809.
[65] BVerfGE 115, 166, 184; BVerfG, NJW 2008, p. 825.
[66] Tinnefeld/Petri/Brink, 2010, p.728.
[67] Or the related interests of the colleagues of the employee, Moll, 2009, § 32 BDSG mgn. 45.
[68] Tinnefeld/Petri/Brink, 2010, p. 728. Moll, 2009, § 32 BDSG mgn. 45.
[69] BAG – 2 AZR 485/08 remark 36.
[70] Dieterich, 2011, introd. mgn. 71.
[71] Tinnefeld/Petri/Brink, 2010, p.728.
[72] 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.
[73] Cf. to this aspect e.g. Petri, 2010, pp. 305 ff.

ICT in Telecommunications Act or in Telemedia Act.[74] 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.[75] The purpose of this norm is, on the one hand, to provide for those working for the public sector a uniform data protection right.[76] On the other hand it ensures the principle of equal treatment in public and non-public working-relations.[77] 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.[78]

1.3.2.2. 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.[79] 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,[80] unauthorised access to the e-mails of employees in their absence[81] as well as generally doing everything possible to ensure smooth running[82] and avoiding the responsibility for criminal or for civil offences and obligations to provide information to the security authority[83] could play the role.[84] For example, committing an offence in relation to the employer-employee relationship may well lead to a loss of reputation by the employer.[85] 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.

1.3.2.3. 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

[74] Gola/Wronka, 2010, mgn. 31.
[75] 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.
[76] Gola/Schomerus, 2010, § 12 BDSG mgn. 7.
[77] Wedde, 2009, § 12 BDSG mgn. 14.
[78] Cf. Weißnicht, 2003, p. 450; Mengel, 2004b, p. 2015.
[79] Gola/Wronka, 2010, mgn. 833.
[80] 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.
[81] Vietmeyer/Byers, 2010, p. 808.
[82] Cf. Pauly/Osnabrügge, 2009, § 6 mgn. 128.
[83] Gola, 2010a, mgn. 28, 29, 198.
[84] Cf. to this aspect Holzner, 2011, p. 13 which opposes cost-risk analysis and also working time argumentation.
[85] Pauly/Osnabrügge, 2009, § 6 mgn. 127.

employer and of employee, be considered in terms of proportionality.[86] 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).[87] 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."[88] 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.[89]

1.3.2.4. Mutual dependence within the employment relationship

The employer-employment relationship is, in general, a continuing account of mutual indebtedness.[90] The relationship is typically marked by a higher degree of obligation between the parties.[91] 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 agree 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.

1.3.2.4.1. The consent of the employer and the criterion of voluntariness

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[92] 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.[93] The possibility that parity in a contact may be disturbed and, hence, the negotiating balance between the two[94] could mean that a situation involving compulsion might arise to the disadvantage of the employee.[95] Therefore one of the main features of consent in work-practice is the criterion of voluntariness.[96] 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

[86] 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).
[87] BAG, NJW 1986, 2724, 2726; Pauly/Osnabrügge, 2009, § 6 mgn. 43.
[88] BAG, NJW 1986, 2724, 2726.
[89] BVerfG NJW 2002, 3619, 3624 by reference to E 34, 238, 248; 367, 373 ff.
[90] Müller-Glöge, 2009, § 611 BGB mgn. 16.
[91] Kramer, 2007, book 2 introd. mgn. 97.
[92] 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.
[93] 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.
[94] Gola/Schomerus, 2010, § 4a BDSG mgn.6 f.
[95] 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;
[96] Cf. to this Wedde, 2009, § 28 BDSG mgn. 24; Richardi/Kortstock, 2005, p. 384; Maties, 2008, p. 2220.

the possibility of consent in general[97] with, among other reasons, the explanation that illegal intrusions in the person rights of the employee cannot be legitimised by consent,[98] as the employee would lack the necessary independence.[99] In this way there could be the permanent danger that consent was the result of the abuse f the employer's position of power.[100] 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.[101] The situation would be different if there were a works council and if outline conditions had been negotiated with them.[102] Others are of the opinion that a general and unlimited refusal of voluntary consent would not be possible,[103] 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.[104] Very often, however, the individual has practically no right of choice concerning the erasure of his data[105] This is only true in the context that practising his profession ultimately serves shaping and maintaining his livelihood.[106] 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.[107] 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.[108]

1.3.2.4.2. The employer's possibilities in case of misuse of data by employees

Employers may 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.[109] 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.[110] 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

---

[97] E.g. Simitis, 1999, p. 628; Simitis, 2001, p. 431; Meyer, 2008, p. 372; Meyer, 2009, p.16; Trittin/Fischer, 2009, p. 344.
[98] Kunst, 2003, p. 77.
[99] Schrader, 2002, p. 197; similar Meyer, 2009, p. 17.
[100] Däubler, 2005, p. 770; Gola/Schomerus, 2010, § 4a BDSG mgn. 7.
[101] Meyer, 2009, p. 17.
[102] 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.
[103] Taeger, 2010, § 4a mgn. 60; Hilber, 2005, p. 147; Hold, 2006, p. 252; Schuster, 2009, pp. 135-136; Müller, 2008, p. 36.
[104] Grimm/Schiefer, 2009, p. 337.
[105] Wohlgemuth, 1988, mgn. 12; Gola, 2010a, mgn. 324.
[106] 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.
[107] Maties, 2008, p. 2221.
[108] Forst, 2010, p. 1044.
[109] Regarding the prevention of economic crime by business enterprises cf. Langrock/Samson, 2007, p. 1684.
[110] Gastell, 2008, p. 2945.

which he takes action against the employee for example according to § 17 UWG (Unfair Competition Act).

1.4. Overview of the relevant legal sources

The employee's data protection law takes from a number of different legal sources, including both European and National sources.

1.4.1. European law dimension[111]

1.4.1.1. Charter of Fundamental Rights of the European Union

With the entry into force of the Treaty of Lisbon[112] the Charter of Fundamental Rights of the European Union[113] acquired a binding legal force.[114] 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,[115] was extended by a written catalogue of fundamental human rights through Article 6 Paragraph 1 Sub-par. 1 of TEU.[116] The Charter of Fundamental Rights of the EU deals explicitly with the protection of personal data in Article 8.

1.4.1.1. EU data protection directives

A superordinate meaning shall behove in this context the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and of the free movement of such data of 24th October 1995.[117] It is to a great part the basis of the current German Federal Data Protection Act (BDSG), and it can accordingly serve as a mean of interpretation aid in case of doubt.[118] In the field of data protection regarding electronic communication services the Directive 2002/58/EG of 31st July 2002 is applicable.[119]

1.4.2. Legal sources of national data protection law

In addition to the constitutional principles[120] a number of various legal sources have gained increasing significance in terms of privacy at the workplace.[121]

---

[111] Cf. furthermore to the aspects of international law Däubler, 2010, mgn. 64 ff.
[112] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007
[113] 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.
[114] Calliess, 2011, § 6 EUV mgn. 1.
[115] Cf. Art. 6 par. 3 TEU. Calliess, 2011, § 6 EUV mgn. 1.
[116] Cf. Art. 6 par. 1 TEU.
[117] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
[118] Däubler, 2010, mgn.61. To further questions cf. Klug, 2001, p. 266.
[119] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
[120] Cf. as above, Sub-sections 1.2 and 1.3.
[121] 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.

1.4.2.1. 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.[122] According to the subsidiarity 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.[123] 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[124] 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.[125]

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

Frequently there are no field-specific regulations, thus the processing[126] of employees' data should be assessed against the provisions of the Federal Data Protection Act.

1.4.2.2.1. § 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,[127] § 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.[128]

1.4.2.2.2. 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

---

[122] 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, 9-10, 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.

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

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

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

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

[127] 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).

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

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.[129] 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.[130] Pursuant to § 32 par. 1. s. 1. of the Federal Data Protection Act the admissibility of the processing of employee 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.[131] In contrast to the wording, besides the purposes precisely defined in the law[132] all other purposes of the employment relationship should be permitted.[133] Having regard to the wording of § 32 par. 1 s. 1 of the BDSG, the requirements of data processing must meet the necessity criterion.[134] According to the will of the legislature[135] the characteristic of necessity is understood to the largest extent in a sense that a proportionality check must be performed.[136] 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.[137]

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

In relation to the basic offence § 32 par. 1 s. 2 BDSG [138] imposes stricter requirements, in case the admissibility of data processing is considered for disclosure of criminal offences.[139] 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.[140] 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.[141] Having regard to the final half-sentence of the norm, within the scope of weighing up of interests, in particular the

[129] Zöll, 2010, § 32 BDSG mgn. 13.
[130] Bundestag, 2009a, p. 27; cf. § 3 par. 11 BDSG.
[131] 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.
[132] That is, establishing, implementing and terminating the employment relationship
[133] Zöll, 2010, § 32 BDSG mgn. 17, Thüsing, 2009, pp. 865, 867.
[134] Cf. to this criterion the critique mentioned by Thüsing, 2009, p. 867.
[135] 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).
[136] Schmidt, 2009a, pp. 198-199.
[137] Zöll, 2010, § 32 BDSG mgn. 17.
[138] 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.
[139] 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.
[140] Deutsch/Diller, 2009, p. 1462.
[141] Bundestag, 2009a, p. 36; Schmidt, 2009a, pp. 193., 195. regarding the problematic features of the regulation.

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.[142] 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).[143] Regarding the weighting of conflicting interests it is recommended, as far as possible to recourse[144] to the jurisprudence of the Federal Constitutional Court.[145] 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.[146] 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.[147] The secrecy of an action leads thereby to increase of its intensity.[148]

1.4.2.2.4. § 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.[149] According to the explanatory memorandum, in this respect the principles of data protection in employment relationship are dealt with.[150] 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.[151]

1.4.2.2.5. Competition with Article 28 of Federal Data Protection Act[152]

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.[153] In this respect, some suggested, to recourse mainly to the principles developed for Article 28 of the Federal Data Protection Act.[154] According to the explanatory memorandum for employment purposes

[142] Bundestag, 2009a, p. 36.
[143] Zöll, 2010, § 32 BDSG mgn. 46.
[144] BVerfGE 115, 320.
[145] 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.
[146] BVerfGE 115, 320, 347 by reference to E 100, 313, 376; 107, 299, 318 ff.; 109, 279, 353.
[147] BVerfGE 115, 320, 347 by reference to E 100, 313, 376; 109, 279, 353.
[148] BVerfGE 115, 320, 353 by reference to E 107, 299, 321; NJW 2006, 976, 981.
[149] Cf. re the extension of the scope of the BDSG also § 8 Para. 1 BewachV.
[150] Bundestag, 2009a, p. 37 with reference to BAGE 54, 365; 119, 238.
[151] Wank, 2010, § 32 BDSG mgn. 2.
[152] 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.
[153] Bundestag, 2009a, p. 35.
[154] Wellhöner/Byers, 2009, p. 2311. Critical: Thüsing, 2010, mgn. 58 ff.

Article 32 of the Federal Data Protection Act substantiates[155] and rules out Article 28 para 1 sentence 1 No. 1 of the Federal Data Protection Act[156] and thus represents a special rule (lex specialis).[157] Similarly, § 28 par. 1 s. 2 BDSG shall also be ruled out.[158] Furthermore, in addition to Article 32 also Article 28 paragraph 3 sentence 1 No. 1 and Article 28 paragraph 1 sentence 1 No. 2 shall be applicable.[159] However, in individual cases here are many questions open, so that there is no legal clarity.[160]

1.4.2.3. 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.[161] 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".[162] Following the frequently expressed desire for a comprehensive codification of a separate employee data protection law[163] the federal government has decided[164] on the 25th October 2010 to "draft a law regulating the employment data protection".[165] Concerning the opinion of the Federal Council of 11th May 2010,[166] the federal government adopted position then again on 15th December 2010.[167] Recently, in the 25th February 2011 the Bundestag discussed the bill of the federal government in the first reading.[168] 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[169] as well as of the Alliance 90/The Greens,[170] whom was also granted a hearing on the 23th May 2011.

---

[155] In contradiction: Thüsing, 2009, p. 867.
[156] Bundestag, 2009a, p. 34.
[157] Zöll, 2010, § 32 BDSG mgn. 5.
[158] 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.
[159] 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.
[160] Thüsing, 2009, pp. 865., 869.
[161] 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.
[162] Thüsing, 2010, mgn. 77.
[163] 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.
[164] Bundestag, 2010a.
[165] In its approach the Federal Ministry of the Interior (BMI) has already published several drafts (cf. Bundesministerium des Innern, 2010.) which met the critics.
[166] Bundesrat, 2010.
[167] Bundestag, 2010b.
[168] Re the opinions of a speaker in the Bundestag cf. Wybitul, 2011, 315091.
[169] Bundestag, 2009b.
[170] Bundestag, 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.[171] 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
- 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

1.4.3. The concept of self-regulation

Self-regulation[172] may serve as the means of the safeguards of data protection interests.[173] Thus Article 27 of the European Data Protection Directive[174] 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.[175] The objective of § 38a of the BDSG is, among others, to standardize the internal codes of conduct in order to promote and implement data protection regulations.[176] The code of conduct is examined by the supervisory authorities (principle of self-regulation).[177] 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.[178] Although the establishment of a code of conduct would create on the one hand legal certainty and industry-specific data flows,[179] and on the other

[171] Here is the implementation of the agreement of the Government Coalition Parties cf. CDU/CSU/FDP, 2009, p. 106.
[172] Self-regulation is argued by Franzen 2010, pp. 260-261.
[173] Weichert/Kilian, 2011, part 13 ch. 5.1 mgn. 46.
[174] Directive 95/46/EC
[175] Weichert/Kilian, 2010, part 13 ch. 5.1 mgn. 48.
[176] Bundestag, 2000a, p. 30.
[177] Roßnagel, 2003, ch. 3.6, mgn. 47 f., 68 ff.
[178] Weichert/Kilian, 2010, part 13 ch. 5.1 mgn. 49.
[179] State parliament Schleswig-Holstein, 2009, p. 89.

hand, the transparency of the type of data treatment would increase for those concerned,[180] 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.[181][182] 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.[183] 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".[184] 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.[185] 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.

[180] Kinast, 2010, § 38a BDSG mgn. 3..
[181] Federal Association for Information Technology, Telecommunications and New Media.
[182] 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.
[183] Cf. de Mazière, 2010.
[184] Friedrich, 2011.
[185] 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).

2. ADMISSIBILITY OF SELECTED MONITORING MEASURES DE LEGE LATA

With regard to individual supervision measures, the matter must also and in particular be investigated according to the corresponding legal status.

2.1. The supervision of personal computers and notebooks

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.

2.1.1. The employer's right to manage and/or issue instructions as a starting point in using personal computers and notebooks

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.[186] 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.[187] The common result of this is that the duty of the employee is to use the equipped workplace for official purposes.[188] 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.[189] 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.[190] In addition, the general principle of equal treatment set out in Art. 3 Sec. 1 of the basic constitutional law[191] requires the employer to equip all comparable work places with computers.[192] 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.[193] 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.[194] By this the

[186] Pauly/Osnabrügge, 2009, § 6 mgn. 120.
[187] Cf. also § 106 GewO.
[188] 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.
[189] Pauly/Osnabrügge, 2009, § 6 mgn. 120.
[190] BAG, NZA 1993, 89, 91.
[191] Cf. Küttner/Kania, 2011, Gleichbehandlung, mgn. 9 ff.
[192] Pauly/Osnabrügge, 2009, § 6 mgn. 120.
[193] BAG, NZA 1984, 201, 202.
[194] Pauly/Osnabrügge, 2009, § 6 mgn. 121.

employer can assert different claims concerning the return, as he deems appropriate.[195] As the owner of the means of operation,[196] 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.[197] Thereby the employee may basically neither claim permission for private use,[198] nor may the internet be used for private purposes in the absence of the employer's permission (no matter whether *expressis verbis* or implied).[199] In emergencies or in urgent cases,[200] private use is exceptionally permitted, irrespective of the type of communication means used.[201] Generally, on the other hand, such use is forbidden which violates the law or is obviously contrary to business interests.[202]

2.1.2. Cases from the jurisdiction[203]

The jurisdiction has already dealt on several occasions with the use of computers and the corresponding control over them.[204] 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.[205]

2.1.3. Academic debate

The private use of e-mail and internet is often neither specifically forbidden nor explicitly permitted by the employer.[206] 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.

---

[195] Cf. for details Pauly/Osnabrügge, 2009, § 6 mgn. 11 ff.
[196] BAG, NZA 2006, 98.
[197] Beckschulze, 2003, pp. 2777, 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.
[198] Bloesinger, 2007, p. 2177; Mengel, 2004a, pp. 1445, 1446 (with further references); Vietmeyer/Byers, 2010, p. 808; Beckschulze/Natzel, 2010, pp. 2368, 2373; Mengel, 2004b, pp. 2014-2015; Weißnicht, 2003 p. 448.
[199] Rath/Karner, 2007, pp. 446, 449. Re definitive granting of permission cf. Gola, 2010a, mgn. 185.
[200] Hanau/Hoeren, 2003, p. 20.
[201] Holzner, 2011, p. 12; cf. further BAG, NZA 1986, 643 (telephone use) and also, Ernst, 2002 pp. 585, 588 (Organisation of communication via e-mail or VoIP).
[202] 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.
[203] Cf. in general to the most relevant Supreme Court decisions Gola/Wronka, 2010, p. 575 ff.
[204] 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).
[205] Gola, 2010a, mgn. 206.
[206] Rath/Karner, 2007, pp. 446, 448.

2.1.3.1. 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.[207] 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.[208] This view, however, misjudges the fact that, due to lost working hours, the employer suffers considerable damage from his employees.[209] 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.[210] In this respect private use is principally to be excluded without explicit authorisation or toleration by the employer.[211]

2.1.3.2. 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.[212] Furthermore, the set up of a private e-mail address through the employer is to be considered as implied authorisation of private use.[213] The mere provision of internet access, however, is to be considered differently.[214] 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.[215]

2.1.3.3. 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

---

[207] LAG Köln, NZA 2006, 106; ArbG Wesel NJW 2001, 2490; ArbG Frankfurt a.M., NZA 2002, 1093.
[208] AG Köln, NZA 2006, 106; ArbG Frankfurt a.M., NZA 2002, 1093; LAG Rheinland-Pfalz , NZA-RR 2005, 303.
[209] 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.
[210] Kratz/Gubbels, 2009, pp. 652, 652; also as a result: Gola, 2010a, mgn. 181.
[211] Cf. BAGE 115, 195 and also Beckschulze, 2003, p. 2377; Ernst, 2002, pp. 585, 586; Dickmann, 2003, p. 1009; Kramer, 2004, pp. 458, 461; Mengel, 2005, pp. 752, 753.
[212] Nägele/Meyer, 2004, pp. 312, 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. 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, pp. 592, 593.
[213] Erler, 2003, p. 18; as well Kratz/Gubbels, 2009, p. 652.
[214] Mengel, 2004a, pp. 1445, 1446; also Mengel, 2004b, pp. 2014, 2015; Ernst, 2002, pp. 585, 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).
[215] Gola, 2010a, mgn. 185.

employee could sufficiently rely.[216] This is rejected by the view whereby,[217] 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.[218] 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.[219] This view, however, misjudges the qualitative difference between simple omission and toleration.[220] 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[221] without complaint.[222] 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.[223] Consequently, the contractual primary and ancillary obligations of the employee comprise the standard to be used to determine where one stands.[224] 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 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,[225] 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.[226] 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.[227] Likewise, within the scope of their contractual ancillary obligations, employees must respect the operational and financial interest of the employer.[228] In addition, the employer subsequently cannot merely specify the limits of the permission for use,[229] but he can also prevent the development of operational practice in advance, by specifying adequate

[216] Kratz/Gubbels, 2009, p. 652.
[217] Cf. Beckschulze, 2009, p. 2097; Koch, 2008, p. 911; Waltermann, 2007, pp. 529, 531.
[218] Bissels/Lützeler/Wisskirchen, 2010, p. 2433. with reference to BAG, NJW 2006, 540; LAG Hamm, BeckRS 2010, 67373; Beckschulze, 2009, p. 2097.
[219] Bissels/Lützeler/Wisskirchen, 2010, p. 2433.
[220] In this direction argue also Kratz/Gubbels, 2009, p. 652. as does Gola, 2010a, mgn. 186.
[221] The time limits are laid down differently in the academic debate (Beckschulze/Henkel, 2001, pp. 1491, 1492 and also Ernst, 2002, pp. 585, 586; Däubler, 2004, mgn. 180 a half year in Kramer, 2004, p. 457 as opposed to a year.)
[222] Gola, 2010a, mgn. 186.
[223] BAG, NZA 2006, 107, 108.
[224] Kratz/Gubbels, 2009, pp. 652, 653. Likewise Gola, 2010a, mgn. 193. regarding the legal responsibilities for safeguarding the IT security of the business see Trappehl/Schmidl, 2009, pp. 985, 987.
[225] ArbG Wesel, NJW 2001, 2490, 2492; Mattl, 2008, p. 49; Kliemt, 2001, pp. 532, 534; Ernst, 2002, pp. 585, 586; Mengel, 2004b, pp. 2014, 2015; Kramer, 2004, pp. 457, 460.
[226] Kratz/Gubbels, 2009, pp. 652, 653.
[227] Kratz/Gubbels, 2009, pp. 652, 653 with reference to Ernst, 2002, pp. 585, 586 (The practice of trust-based working time) and Däubler, 2004, mgn. 170.
[228] Cf. the examples given by Kratz/Gubbels, 2009, pp. 652, 653 on the damage to the resources and other legal assets of the employer (with further references).
[229] Gola, 2010a, mgn. 188.

regulations in the bylaws and service agreements[230] for reasons of legal certainty[231] - and by enforcing and monitoring compliance with the prohibition of private use by means of monitoring [232]and also by formally sanctioning the offences.[233]

2.1.3.4. Restriction and withdrawal of permission

Restrictions of the permission for private use can be imposed in terms of time, place and content.[234] 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.[235] 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.[236]

2.1.3.5. 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.[237]

2.1.3.5.1. Limits of purely official and private internet communication[238] 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 distinction must be made.[239] Use, basically, always has an official character if it is designed to promote the work.[240] 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.[241] Further, the social exchange at work can be assigned, even through e-mail traffic, to the sphere of official use.[242] In fact, the

[230] Vietmeyer/Byers, 2010, pp. 807, 808.
[231] LAG Rheinland-Pfalz, NZA-RR 2005, 303, 306.; Rath/Karner, 2007, pp. 446, 449.
[232] Rath/Karner, 2007, pp. 446, 449.
[233] Gola, 2010a, mgn. 188.
[234] For details cf. Dickmann, 2003, p. 1009.
[235] Gola, 2010a, mgn. 189.
[236] BAG, RDV 2010, 68.
[237] Full controlling is already prohibited for reasons of proportionality, Gola, 2010a, mgn. 291.
[238] If apart from purely official use, private use is permitted, we speak of so-called mixed use, Rath/Karner, 2007, pp. 446, 450.
[239] Rath/Karner, 2007, pp. 446, 449; Rasmussen-Bonne/Raif, 2011, 80; Hoppe, 2010, p. 388; Vietmeyer/Byers, 2010, p. 807.
[240] Ernst, 2002, pp. 585, 588.
[241] Rath/Karner, 2007, pp. 446, 449. Cf. further in respect of telephone conversations BAG, NJW 1987, 674, 678.
[242] Ernst, 2002, pp. 585, 588.

employer cannot prevent this totally.[243] All other forms of external communication are to be assigned to the private sphere.[244]

2.1.3.5.2. 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[245] is to be judged according to the contractual purpose of Article 32 sec. 1 of the Federal Data Protection Act[246] by taking into consideration the employee's right to informational self-determination.[247] External data (e.g. sender and receiver of the e-mails,[248] time of sending) can serve as connection data in relation to the e-mail traffic.[249] Concerning internet use, the time of accessing a site,[250] the duration of the internet use and the protocols of accessed websites,[251] as well as any expenses incurred[252] (for instance for reasons of the control of abuse and cost control),[253] or the prevention and removal of interference with the EDP[254] 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.[255] The monitoring of e-mail in terms 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.[256] Hence, by permitting purely official use, the employer may, in general, only store the employees' data[257] 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

[243] Rath/Karner, 2007, pp. 446, 449.
[244] Däubler, 2000, pp. 323, 324.
[245] Traffic data are data which are generated, collected, processed or used by the provision of a Telecommunication services, § 3 Nr. 30 TKG.
[246] 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.
[247] Rath/Karner, 2010, pp. 469, 470, with reference to Mengel, 2004b, pp. 2014, 2015; Ernst, 2002, pp. 585, 588; Lindemann/Simon, 2001, pp. 1950, 1951.
[248] Gola, 2010a, mgn. 288. Cf. Also loc.cit., 2010, mgn. 289 (with further references) re the issue of the storage of details of addressees.
[249] Vehslage, 2001, p. 145, 148; Däubler, 2010, mgn. 351, 354; Naujock, 2002, pp. 592, 593; constrictive Ernst, 2002, pp. 585, 590.
[250] Gola, 2010a, mgn. 288.
[251] Vietmeyer/Byers, 2010, pp. 807, 808.
[252] Gola, 2010a, mgn. 288.
[253] Raffner/Hellich, 1997, pp. 862, 867.
[254] Hoppe/Braun, 2010, pp. 80, 81; Kramer, 2010, p. 164.
[255] 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, cf. only Gola, 1999, pp. 322, 326; Weißnicht, 2003, p. 451; Lindemann/Simon, 2001, p. 1952; Mengel, 2004b, p. 2017, Rath/Karner, 2007, p. 450.
[256] Gola, 1999, pp. 322, 326; Rath/Karner, 2007, pp. 446, 450.
[257] Rasmussen-Bonne/Raif, 2011, p. 80.

conduct (e.g., Internet addresses, time of access to a website) of the employees.[258] In addition to this, by means of detailed log files[259] the employee's data traffic can be analysed.[260] 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.[261]

2.1.3.5.3. 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).[262] 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[263] and Article 2 Sec. 1 No. 1 of the Telemedia Act, the employer is to be considered as service provider.[264] 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.[265] Partly it is believed that, by making a written general declaration, employees release the employer from respecting the telecommunication secrets and could, therefore, have control over authorised private use.[266] 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.[267]

---

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

[259] 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.

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

[261] 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).

[262] Rath/Karner, 2010, pp. 469, 470.

[263] 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.).

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

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

[266] Hartmann/Pröpper, 2009, p. 1300. Critically: Kramer, 2010, p. 164.

[267] Kramer, 2010, p. 164.

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,[268] the employer has the obligation to protect telecommunication secrets.[269] 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.[270] 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[271] even *de lege ferenda* nothing alters the fact that the employer is classified as telecommunication supplier.[272] 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.[273] 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.[274] 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 telecommunications and personal data. In addition to technical and organizational measures, this also includes monitoring measures taken regarding the maintenance of the stipulated principles.[275] Specifically, unauthorized persons must not obtain knowledge of connection of

[268] Thüsing, 2010, mgn. 295.
[269] Thüsing, 2010, mgn. 221.
[270] Weißnicht, 2008, p. 164; Rath/Karner, 2010, pp. 469, 470.
[271] 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.
[272] Vietmeyer/Byers, 2010, p. 807.
[273] De Wolf, 2010, pp. 1206, 1209. Cf. also BVerfGE 124, 43, 54 with reference to E 120, 274, 341.
[274] De Wolf, 2010, pp. 1206, 1209.
[275] Däubler, 2010, mgn. 370 with reference to the antecessor regulation of § 109 TKG mentioned by Ehmer, 2006, § 87 TKG mgn. 18.

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.[276]

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.[277] 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.[278] 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).[279] Here, Article 11 sec. 3 of the Telemedia Act restricts the scope of application of telemedia, which consist mainly[280] of the transmission of signals over the telecommunication networks and are, therefore, also subject to the TKG.[281] Offering the private use of corporate e-mail and other internet applications to employees is also usually considered as telemedia.[282] 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.[283] 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.[284] 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.[285] 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 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.[286] Furthermore, the checking of free services is

[276] Däubler, 2010, mgn. 370 f.
[277] Däubler, 2010, mgn. 342.
[278] 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.).
[279] Gola, 2010a, mgn. 166.
[280] 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.
[281] Gola, 2010a, mgn. 166.
[282] Moos, in: Taeger/Gabel, BDSG, § 12 TMG mgn. 32; Heidrich, CR 2009, 168, 173; Gola, 2010a, mgn. 167.
[283] Gola, 2010a, mgn. 167.
[284] Däubler, 2010, mgn. 378.
[285] Däubler, 2010, mgn. 373.
[286] Däubler, 2010, mgn. 377.

forbidden.[287] 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.[288] 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.[289]

2.2. Monitoring 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.[290] This raises the question of how to resolve the tension arising in this context between, on the one hand, self-realization, freedom of

[287] Däubler, 2010, mgn. 377; Lindemann/Simson, 2001, pp. 1950, 1953.
[288] Däubler, 2010, mgn. 374.
[289] De Wolf, 2010, pp. 1206, 1210.
[290] Facebook, the Internet portal founded in 2004, could already claim 500 million members in the following year, heise, 2010.

expression and social interaction and, on the other hand, informational self-determination of users and non-involved third parties[291] by taking all interests into consideration.

2.2.1. On the nature and functioning of social networks

The term social network refers to internet platforms that allow an individual to present himself.[292] 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[293] 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.[294] Whilst in professional networks it is primarily information on the employment history and of the activity carried on which play a role,[295] in private networks these are supplemented by information such as the relationship status.[296] The disclosure of this data includes, at the same time, the data protection consent of the person concerned in accordance with Articles 4, paragraph 1, 4a of the BDSG.[297] 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.[298]

2.2.2. 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.[299] For example, the shift of social network functions into the company is emphasized as the most important future trend in the industry.[300] This development naturally brings along not only advantages, but holds also significant risks for the employee regarding the handling of his personal data.[301] In order to create personal profiles, data is collected from generally

---

[291] Cf. Lerch/Krause/Hotho/Roßnagel/Stumme, 2010, p. 454.
[292] Oberwetter, 2011, p. 417.
[293] 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.
[294] Oberwetter, 2011, p. 417. The most prominent example of a private social network is, without question, Facebook. In Germany networks such as Twitter, studiVZ, meinVZ or Flickr enjoy great popularity. In the field of official social networks, XING, LinkedIn und Expeerteer have most registered users.
[295] With XING these data, for example, are aggregated under the main heading of Business data.
[296] Oberwetter, 2011, p. 417. Generally, however, in both types of social network comprehensive statistics business and private possible.
[297] Ott, 2009, pp. 158, 161; Weichert, 2007, pp. 188, 189.
[298] Oberwetter, 2011, p. 417.
[299] Cf. with reference to the details of the current SID/FIT Social Media Report 2010/2011, (SID/FIT, 2011).
[300] Re the establishment of Corporate XING cf. the Press Release of Fraunhofer FIT (FIT, 2010).
[301] 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.

accessible sources by means of a so-called 'crawler'.[302] The data to which particular importance is attached are above all those from social networks.[303]

2.2.3. 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.[304] 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.[305]

2.2.4. Academic debate[306]

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.[307] 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.

2.2.4.1. 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.[308] 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.[309] 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.

---

[302] Basically these are found on the Internet, for example via a search engine, accessible data, e.g., Bundestag, 2010b, p. 16.

[303] Ott, 2009, p. 158. In the literature it is thought that the agreement of the person involved should be so interpreted that search engines, can legitimately 'crawl' and use the data, cf. Ott, 2009, pp. 158, 161 and also Weichert, 2007, pp. 188, 189.

[304] 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.

[305] Bissels, 2009b, p. 2197; cf. Raif/Bordet, 2010, and also p. 88 Ege, 2008, p. 72.

[306] 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.

[307] Oberwetter, 2011, pp. 417, 418.

[308] Oberwetter, 2011, pp. 417, 418.

[309] BAG, NZA 1986, 739, 739.

Secondly, social networks which mainly serve to offer private presentation to the employee are completely closed to the employer.[310]

2.2.4.2. 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 internally, but basically on a generally accessible platform on the internet.[311] Therefore, the disclosure of this data depends fundamentally upon the consent of the worker concerned.[312] An exception occurs when the data are required to meet work requirements, or it is customary to disclose such.[313] 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.[314] 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.[315] 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.[316]

2.2.4.3. 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.[317] 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.[318] 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,[319] 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.)[320] However, a

---

[310] Oberwetter, 2011, pp. 417, 418.
[311] Oberwetter, 2011, pp. 417, 418.
[312] Gola/Wronka, 2010. mgn. 1155, 1166 ff. With reference to the requirement for consent of § 22 KUG re the publication of photographs of employees.
[313] Gola/Wronka, 2010. mgn. 1155
[314] BVerwG, RDV 2009, 30; re information on first (given) names in the E-Mail address LAG Schleswig-Holstein, RDV 2008, 212.
[315] 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, pp. 417, 419. However, together with these members' it is also possible to produce a business profile - see cf. e.g. Xing, 2011.
[316] Oberwetter, 2011, pp. 417, 419.
[317] See above, subsection 2.2.1.
[318] Oberwetter, 2011, pp. 417, 419.
[319] See above, subsection 2.1.3.5.2.
[320] Oberwetter, 2011, pp. 417, 419.

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 concerning its products.[321] 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.[322]

2.2.4.4. 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).[323] After leaving the company, the employee is obliged to return any and all equipment provided to him.[324] A user account is surrendered by the disclosure of the relevant access data.[325] 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.[326] 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.[327] 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.[328] 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[329] or customer data[330] created by the employee. In addition, the obligation to surrender

[321] Oberwetter, 2011, pp. 417, 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.
[322] Oberwetter, 2011, pp. 417, 419.
[323] Bissels/Lützeler/Wisskirchen, 2010, p. 2438.
[324] 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.
[325] Oberwetter, 2011, pp. 417, 420.
[326] Oberwetter, 2011, pp. 417, 420; likewise Bissels/Lützeler/Wisskirchen, 2010, pp. 2433, 2438.
[327] Oberwetter, 2011, pp. 417, 420.
[328] Bissels/Lützeler/Wisskirchen, 2010, pp. 2433, 2438.
[329] LAG Hamm, ARSt 1991, 182, 182 f.
[330] Preis, 2011, § 611 BGB mgn. 754; cf. BGH, NJW 1993, 1786 for business representative.

also covers the business correspondence relevant in economic terms, either regarding current projects or those documents which are *ipso jure* required by the employer.[331]

2.3. Monitoring of correspondence and telephone calls

It is debatable whether, and to what extent, the employer is allowed to monitor the correspondence and telephone calls of his employees.

2.3.1. Monitoring of correspondence

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.[332]

2.3.1.1. Legal basis of the protection of the written word

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.[333]

2.3.1.2. 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.[334]

2.3.1.3. 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.[335] Unlike business post, which may

[331] Oberwetter, 2011, pp. 417, 420.
[332] Protection of written correspondence is – apart from the constitutional law dimension – secured in particular by § 202 StGB.
[333] 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.
[334] 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.
[335] Sassenberg/Bamberg, 2006, pp. 228-229; Gola/Wronka, 2010, mgn. 17.

be accessed by the employer,[336] written messages that are apparently destined for the employee personally must be delivered sealed.[337]

2.3.2. Monitoring of telephone calls[338]

The employer may also have an interest in monitoring his employees' telephone calls.

2.3.2.1. Cases from the jurisdiction

In fundamental decisions of the BAG[339] and the BVerwG[340] 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.[341] Should the employer wish to overhear a phone conversation for later evidence, the consent of the external conversation partner is usually needed.[342] 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 the training process and takes place in the most unobtrusive way - hence limited to the probationary period.[343]

2.3.2.2. 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.[344]

2.3.2.2.1. Permitted private use

A worker does not have the right to use official telephones for private purposes.[345] 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

[336] Pröpper/Römermann, 2008, p. 514; Wolf/Mulert, 2008, p. 443. (with further references).
[337] Gola/Wronka, 2010, mgn. 17.
[338] On aspects of Internet telephony (Voice over IP, VoIP), Telephony or videotelephony 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.
[339] DB 1986, 2086; NZA 1987, 515.
[340] NJW 1982, 840; RDV 1990, 24; DuD 1990, 426.
[341] 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.
[342] 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.
[343] BAG, RDV 1986, 30. Cf. on the use of silent monitoring and voice recording Jordan/ Bissels/Löw, 2008, p. 2626.
[344] Wellhöner/Byers, 2009, pp. 2310, 2312.
[345] Mengel, 2004a, p. 1446; Altenburg/v. Reinersdorff/Leister, 2005, pp. 133, 135.

extent.[346] 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[347] 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.[348] However, this is in practice usually not the case.[349] 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.[350] 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).[351] However, the employee's performance assessment must not be linked to the collection of communication data.[352] Both listening to and recording the content of telephone conversations are prohibited as interfering with the right of the spoken word.[353] Moreover, private conversations of the employee enjoy protection through telecommunication secrecy as set out in Article 88 of the TKG.[354] 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 or the sexual harassment of colleagues at work).[355] 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.[356] It should be noted that the employer may call the mobile phone of the employee to ask his/her actual whereabouts.[357]

2.3.2.2.2. 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.[358] 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

[346] Wellhöner/Byers, 2009, pp. 2310, 2312.
[347] Vietmeyer/Byers, 2010, pp. 807, 809.
[348] Wellhöner/Byers, 2009, pp. 2310, 2312; Heldmann, 2010, pp. 1235, 1239; Vietmeyer/Byers, 2010, pp. 807, 809.
[349] Wellhöner/Byers, 2009, pp. 2310, 2312.
[350] Mengel, 2004a, pp. 1445, 1451; Gola, 1999, pp. 322, 327; Altenburg/v. Reinersdorff/Leister, 2005, pp. 135, 137; Wank, 2011, § 28 BDSG, mgn. 19.
[351] Heldmann, 2010, pp. 1235, 1239; Vietmeyer/Byers, 2010, pp. 807, 809; Mengel, 2004, pp. 1445, 1451; Oberwetter, 2008, pp. 609, 611.
[352] Gola, 1999, p. 327; Oberwetter, 2008, pp. 609, 611.
[353] Wellhöner/Byers, 2009, pp. 2310, 2312; Oberwetter, 2008, pp. 609, 611; Mengel, 2004a, p. 1451; Moll, 2009, § 100 TKG mgn. 46.
[354] Oberwetter, 2008, pp. 609, 611; Altenburg/v. Reinersdorff/Leister, 2005, p. 135, 137, Gola, 1999, pp. 322, 325.
[355] Altenburg/v. Reinersdorff/Leister, 2005, pp. 135, 137; Mengel, 2004a, pp. 1445, 1451.
[356] Wellhöner/Byers, 2009, pp. 2310, 2312.
[357] Oberwetter, 2008, p. 612; Gola, 2007, p. 1142.
[358] Altenburg/v. Reinersdorff/Leister, 2005, p. 136; Mengel, 2004a, p. 1447.

basically allowable.[359] In the absence of monitoring of the conversation content there is no interference with the right to one's own words,[360] although it does interfere with the employee's right to informational self-determination.[361] However, as part of the assessment process, the legitimate interests of the employer in expense and abuse control are normally given greater weight.[362] 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.[363] There can be deviations from this in the case of abuse control, in order to provide evidence of private use.[364] Conversely, telephone communication data must not be recorded for general performance assessment, even if the private use of telephones is prohibited.[365] 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.[366] Listening to and recording telephone calls is to be generally considered as unlawful interference with the right to one's own word.[367] 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.[368] Ultimately this derives also from the wording of Article 32 paragraph 1 sentence 2 of the BDSG,[369] which can be used as justification for the detection of a crime committed within the employment relationship.[370] The legal situation regarding open listening to official telephone calls appears differently. This measure may be allowed for training and monitoring purposes.[371] Comprehensive employee monitoring is again unjustified. This argumentation applies also in respect of the business use of mobile devices.[372] 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.[373] If the incoming calls are private in character, this shall not lead to the application of the TKG.[374]

---

[359] Wellhöner/Byers, 2009, pp. 2310, 2313.
[360] Mengel, 2004, pp. 1445, 1448; Altenburg/v. Reinersdorff/Leister, 2005, pp. 135, 136.
[361] Wellhöner/Byers, 2009, pp. 2310, 2313.
[362] Oberwetter, 2008, p. 611; Altenburg/v. Reinersdorff/Leister, 2005, p. 136; Mengel, 2004a, 1448; Gola, 1999, pp. 326-327
[363] Gola, 1999, pp. 322, 326.
[364] BAG, NJW 1987, 674, 677; Simitis, 2010, § 28 BDGS mgn. 107; Oberwetter, 2008, p. 611; Altenburg/v. Reinersdorff/Leister, 2005, p. 136.
[365] Gola, 1999, p. 327; Oberwetter, 2008, p. 611. On the special features of call centers cf. Gola/Wronka, 2010, mgn. 758 ff.
[366] Wellhöner/Byers, 2009, pp. 2310, 2313.
[367] Oberwetter, 2008, p. 611; Mengel, 2004a, p. 1451.
[368] 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.
[369] Wellhöner/Byers, 2009, pp. 2310, 2313.
[370] Deutsch/Diller, 2009, p. 1464; von Steinau-Steinrück/Mosch, 2009, p. 451; Wybitul, 2009, p. 1583.
[371] Wellhöner/Byers, 2009, pp. 2310, 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 agreement 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.
[372] Wellhöner/Byers, 2009, pp. 2310, 2313.
[373] Gola, 2010a, mgn. 202.
[374] Gola, 1999, pp. 324-325; Däubler, 2000, p. 327; Post-Ortmann, 1999, p. 102.

2.4. Video surveillance

In cases where employees are monitored by video, this shall also be considered as an encroachment on their general personal rights. Due to the continuous pressure associated with video surveillance, these rights are especially at risk in the workplace.[375]

2.4.1. Cases from the jurisdiction

In a number of decisions[376] the Court has indicated that the privacy rights of employees takes general precedence over the security interests of the employer.[377]

2.4.2. Academic debate[378]

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

2.4.2.1. 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.[379] 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.[380] 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.[381] 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.[382] 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.[383]

2.4.2.1.1. 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

[375] BAG, NZA 1988, 92; NZA 2003, 1193, 1194; NZA 2004, 1278, 1281.
[376] BAG, RDV 1988, 137; NZA 1988, 92 RDV 1992, 178; NJW 2003, 3436; NJW 2005, 313; RDV 2005, 216; RDV 2008, 238.
[377] Gola, 2010a, mgn. 65.
[378] For a legal evaluation of Camera-Dummies cf. detail Kirsch, 2011, 317919.
[379] Zscherpe, 2010, 6b BDSG mgn. 21.
[380] Bundestag, 2000a, p. 38.
[381] Zscherpe, 2010, § 6b BDSG mgn. 5; Gola/Schomerus, 2010, § 6b BDSG mgn. 1.
[382] Bundestag, 2000a, p. 38.
[383] Zscherpe, 2010, § 6b BDSG mgn. 19.

space - i.e., in addition to the floor, the space above this surface is also covered.[384] 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.[385] 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.[386] 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.[387] 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.[388] Accordingly, public use is only indisputable if a decision to allow public use has been made by the persons entitled to do so.[389] In accordance with the explanatory memorandum, this also includes platforms, the exhibition halls of museums, retail shops[390] or ticket halls.[391] In assessing whether work places are to be classified as public places, a differentiated approach should be adopted. In the case of these, public accessibility is often missing.[392] 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.[393] 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.[394] 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.[395] Consequently, the cash area cannot be classified as a separate, delimitable place within the publicly accessible area.[396] 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.[397]

2.4.2.1.2. Open video surveillance

[384] Zscherpe, 2010, § 6b BDSG mgn. 31.
[385] For prevailing opinion, cf. only Bizer, 2011, § 6b BDSG mgn. 36.
[386] Zscherpe, 2010, § 6b BDSG mgn. 32; Gola/Schumerus, 2010, § 6b BDSG mgn. 8.
[387] Bizer, 2011, § 6b BDSG mgn. 37; Gola/Schumerus, 2010, § 6b BDSG mgn. 12.
[388] BAG, NZA 2004, 1278, 1282; NJOZ 2005, 2708, 2713; Zscherpe, 2010, § 6b BDSG mgn. 32.
[389] Gola/Schumerus, 2010, § 6b BDSG, mgn. 9.
[390] Such as shops or stores, Bayreuther, 2005, p. 1038, who adds banks, filling stations and restaurants as examples.
[391] Bundestag, 2000, p. 38.
[392] Meyer, 2009, p. 15; Zscherpe, 2010, § 6b BDSG mgn. 37. Grimm/Schiefer, 2009, p. 331.
[393] Grimm/Schiefer, 2009, p. 331; Däubler, 2001b, p. 874; Wiese, 2004, p. 923; Gola/Klug, 2004, p. 72.
[394] LAG Mecklenburg-Vorpommern – 1 Sa 387/03; Helle, 2004, p. 346.
[395] Grimm/Schiefer, 2009, p. 331.
[396] 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.
[397] Zscherpe, 2010, 6b BDSG mgn. 38; different view earlier BGH, NJW 1995, 1955, 1956.

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.

Legitimate observation purposes, Article 6b par. 1 no. 1, 2 and 3 of the BDSG

Carrying out lawful video surveillance in accordance with § 6b paragraph 1 of the BDSG requires first a permissible observation purpose.[398] 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.[399] 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 troublemaker from a room and also at prohibiting his/her future entry.[400] However, employees must obtain access to the work place in order to be able to perform their job,[401] and so the perception of the legitimate interests for the precisely specified purposes (Nr.3)[402] is the most important purpose of the video surveillance of publicly accessible places.[403]

Appropriateness and necessity, Article 6b paragraph 1 last main clause of the BDSG

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.[404] It is also necessary to consider whether the objective pursued could have been achieved even with a milder, equally effective [405] means, which however is less restrictive regarding the personal rights of employees.[406]. Due to the scope, video surveillance must therefore be limited functionally and spatially to a necessary

[398] Zscherpe, 2010, 6b BDSG mgn. 51.
[399] Thüsing, 2010, mgn. 353 f.
[400] 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.
[401] BAG, NZA 2004, 1278, 1283; NJOZ 2005, 2708, 2714.
[402] The purpose according to Nr. 3 could be only according to Bundestag, 2001, p. 61; only for non-public places.
[403] Thüsing, 2010, mgn. 355.
[404] Zscherpe, 2010, § 6b BDSG, mgn. 51; Bizer, 2011, § 6b BDSG mgn. 56
[405] Wedde, 2009, § 6b BDSG mgn. 39; Bayreuther, 2005, p. 1040.
[406] Zscherpe, 2010, § 6b BDSG mgn. 51.

minimum extent.[407] 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.[408] 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.[409] Mostly video surveillance is among several equally appropriate means the most invasive one.[410] 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.[411] 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.[412] 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.[413] This latter was classified by the court however as not equally effective as recording, in particular for the investigation of theft.[414] The approach, the considerations of which include the alternative of a human rather than technical observation by supervisors and colleagues,[415] 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.[416] Apart from that, it is doubtful whether in-house spying would affect the personal rights of employees less that open video surveillance.[417]

Appropriateness,[418] Article 6b paragraph 1 last main clause of the BDSG

As a final step, as it follows also from Article 6b paragraph 1 last main clause of the BDSG, that an examination of appropriateness should take place. Here, the employer's interests represented by video surveillance and the monitoring purposes should be weighed against the

[407] BAGE 127, 276 mgn. 20; BAG, NZA 2004, 1278, 128; Bergmann/Möhrle/Herb, 2011, § 6b BDSG mgn. 27.
[408] Zscherpe, 2010, § 6b BDSG mgn. 55 in conjunction with mgn. 51.
[409] Zscherpe, 2010, § 6b BDSG mgn. 56; Wedde, 2009, § 6b BDSG mgn. 41.
[410] Thüsing, 2010, mgn. 356.
[411] Zscherpe, 2010, § 6b BDSG mgn. 56
[412] BAG, NZA 2003, 1193, 1195; ArbG Düsseldorf, NZA-RR 2004, 345, 346.
[413] BAGE 127, 276 mgn. 27; BAG, NZA 2004, 1278, 1283.
[414] BAGE 127, 276 mgn. 27.
[415] 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.
[416] BAG NZA 2003, 1193, 1195; Grimm/Brock/Windeln, 2006, pp. 179, 180.
[417] Bayreuther, 2005, pp. 1038, 1040.
[418] Proportionality in the narrow sense, BVerfG, NJW 2008, 1505, 1515; BAGE 127, 276 mgn. 31.

legitimate interests of the employees involved in the observation.[419] 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.[420] 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.[421] 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.[422] 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.[423] In general, observation will not include particularly sensitive issues of privacy, but will rather encroach on the less vulnerable social sphere.[424] 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.[425] 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 permanently.[426] 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.[427] In quantitative terms, the number of people affected by the monitoring plays a role.[428] 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.[429] 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.[430] In technical terms it is a determinant factor of consideration whether the employer uses analogue or digital recording technology.[431] By using digital video recording, it is possible to process the acquired images automatically and also to zoom out and filter

[419] Grimm/Schiefer, 2009, pp. 329, 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.
[420] Zscherpe, 2010, § 6b BDSG mgn. 59.
[421] BAGE 127, 276 mgn. 21; Grimm/Schiefer, 2009, p. 331.
[422] Grimm/Schiefer, 2009, p. 331.
[423] Bundestag, 2001, p. 62; Zscherpe, 2010, § 6b BDSG mgn. 60.
[424] 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, pp. 329, 331.
[425] BAG, NZA 2003, 1193, 1195.
[426] BAG, NZA 2004, 1278, 1281.
[427] BAG, NZA 2004, 1278, 1284.
[428] BAGE 127, 276 mgn. 39; BAG, NZA 2004, 1278, 1284.
[429] BAGE 127, 276 mgn. 21.
[430] BAG, NZA 2003, 1193, 1195.
[431] 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.

individual persons.[432] The invasion of the right to privacy may be accordingly intensive.[433] 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.[434] 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).[435] As a result, therefore, general statements regarding the balancing of interests are prohibited.[436]

Targeted surveillance of employees

As a rationale for targeted surveillance of employees the suspected committing of a crime or other misconduct may be considered.[437]

Open video surveillance in concrete case of suspicion

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.[438] The secret video surveillance of an employee[439] is permitted in the event of concrete suspicion of a criminal offence or other serious misconduct committed to the detriment of the employer, less 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.[440] 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.[441] 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.[442] In the resolutions concerning mail distribution centres, the Federal Labour Court also addressed the question of suspicious

[432] Grimm/Schiefer, 2009, p. 332
[433] BAG, NZA 2004, 1278, 1284.
[434] Gola/Wronka, 2010, mgn 844; Oberwetter, 2008, p. 610. On smart cameras and automatic behaviour analysis cf. Hornung/Desoi, 2011, p. 153.
[435] Zscherpe, 2010, § 6b BDSG mgn. 65.
[436] Also cf. Grimm/Schiefer, 2009, p. 332.
[437] Grimm/Schiefer, 2009, pp. 329, 332.
[438] 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.
[439] In the concrete case it was a question of the monitoring of the cash-till area of a supermarket.
[440] BAG NZA 2003, 1187, 1193.
[441] Bayreuther, 2005, pp. 1038, 1039.
[442] BAG, NZA 2003, 1193, 1195.

circumstances.[443] 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.[444] In this respect also no video surveillance may take place for the mere monitoring of employees' performance and organisational conduct.[445]

Targeted video surveillance below the threshold of a specific case of suspicion

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.[446]

Video surveillance in particular risk situations

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.[447] This requires the existence of a special risk situation,[448] i.e. a hazardous situation which goes beyond the general possibility of the risk of crime.[449] This must be explained in detail by the employer,[450] 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.[451] It is proposed, therefore, that consideration should favour the employer's interest in prevention, this at the expense of the

[443] BAG, NZA 2004, 1278; NZA, 2008, 1187, 1190.
[444] BAG, NZA, 2008, 1187, 1191.
[445] Bayreuther, 2005, pp. 1038, 1039.
[446] Bayreuther, 2005, pp. 1038, 1039; Grimm/Schiefer, 2009, pp. 329, 332.
[447] Bayreuther, 2005, pp. 1038, 1039.
[448] BAG, NZA 2004, 1278, 1283 f.
[449] Grimm/Schiefer, 2009, pp. 329, 332.
[450] BAG, NZA 2004, 1278, 1283.
[451] Grimm/Schiefer, 2009, pp. 329, 333.

personal rights of employees, if already isolated instances of misbehaviour can cause serious damage.[452]

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.[453] For the operators of optical-electronic devices it will be important primarily to preserve their in-house authority within the property boundaries[454] and to use video surveillance for preventive purposes[455] or as a repressive means for the prosecution of offenders.[456] 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.[457] 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,[458] 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.[459] 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.[460] 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.[461] At this point, the set of interests differ from that of the targeted surveillance of employees.[462]

Temporal boundaries of increasing surveillance and adaptation pressure

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

[452] Grimm/Schiefer, 2009, pp. 329, 333 with reference to the example named by Bayreuther, 2005, pp. 1038, 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.
[453] Grimm/Schiefer, 2009, pp. 329, 333.
[454] BGH, NJW 1995, 1955, 1957; Gola/Schomerus, 2010, § 6b BDSG mgn. 16 (with further references).
[455] There are preventive objectives especially in avoiding theft, criminal damage or disturbance, BAG NZA 2008, 1187, 1193.
[456] Wedde, 2009, § 6b BDSG mgn. 33.
[457] Roloff, 2009, § 5 mgn. 39.
[458] Grimm/Schiefer, 2009, pp. 329, 333.
[459] Gola/Wronka, 2010, mgn 816. Cf. further SG München RDV 1992, 85.
[460] Bayreuther, 2005, pp. 1038, 1039; Grimm/Schiefer, 2009, pp. 329, 333.
[461] Grimm/Brock/Windeln, 2006, pp. 179, 180.
[462] Grimm/Schiefer, 2009, pp. 329, 333 with reference to the of the BAG (NZA 1187, 1193).

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.[463] This can be assumed, at least for a publicly accessible company, in which the commission of certain crimes[464] represent a typical business risk.[465] 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.[466] 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.[467] 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.[468] 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.[469] 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.[470] This would again require concrete suspicion.[471]

2.4.2.1.3. 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.[472] Due to the fact that, 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.[473] Whether, despite the introduction of Article 6b of the BDSG and

[463] Grimm/Schiefer, 2009, pp. 329, 333.
[464] E.g. shoplifting on retail premises or hold-ups in banks, Bayreuther, 2005, pp. 1038, 1039.
[465] Wiese, 2004, pp. 915, 925
[466] Bayreuther, 2005, pp. 1038, 1039.
[467] Grimm/Schiefer, 2009, pp. 329, 333; similar also BAG, NZA, 1193, 1195.
[468] Grimm/Schiefer, 2009, pp. 329, 333 f.
[469] Grimm/Schiefer, 2009, pp. 329, 334.
[470] Cf. also BAG, NZA, 1193, 1195.
[471] Grimm/Schiefer, 2009, pp. 329, 334.
[472] BAG, NZA 2003, 1193, 1195; left open by LAG Sachsen-Anhalt – 11 Sa 522/07.
[473] BVerfG, NJW 2008, 1505, 1507 f.; BAG, NZA 2008, 1187, 1190.

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.[474] 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.[475] Therefore, recognisability is a prerequisite for the legality of video surveillance in publicly accessible areas.[476] 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.[477] 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.[478] As is apparent from the wording,[479] to make the observation identifiable is the obligation of the responsible entity.[480] 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.[481] Hence, recognising exceptions to the prohibition of secret video surveillance as recourse to general reasons for justification and the grounds for excuse,[482] is argued against.[483] This contradicts a number of representatives who affirm the applicability of general reasons for justification and legal excuse.[484] 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.[485] 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.

2.4.2.1.4. 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

[474] Bundestag, 2000a, p. 38.
[475] Zscherpe, 2010, § 6b BDSG mgn. 66.
[476] AG Frankfurt – 7 Ca 3342/05 mgn. 53; Bayreuther, NZA 2005, 1038, 1040, Roloff, 2009, § 5 mgn. 38; Maschmann, 2002, pp. 13, 17; dubious is: Gola/Schomerus , 2010, § 6b BDSG mgn. 28.
[477] For opinions cf. Gola/Schomerus, 2010, § 6b BDSG mgn. 25 f.; Bizer, 2011, § 6b BDSG mgn. 68, 70.
[478] Bizer, 2011, § 6b BDSG mgn. 67; Grimm/Schiefer, 2009, pp. 329, 334.
[479] „Sind“ (translated: „are“), cf. § 6b par. 2 BDSG.
[480] Zscherpe, 2010, § 6b BDSG mgn. 66; Grimm/Schiefer, 2009, p. 334.
[481] Bayreuther, 2005, pp. 1038, 1040.
[482] Self-defence (§§ 227 BGB, § 32 StGB) and also emergence (§ 34 StGB) can be considered as justification, Grimm/Schiefer, 2009, pp. 329, 334.
[483] Bayreuther, 2005, pp. 1038, 1040f.
[484] 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.
[485] Grosjean, 2003, p. 2651; Grimm/Brock/Windeln, 2006, p. 181, Grimm/Schiefer, 2009, p. 334.

automatically follow. This requires separate examination.[486] 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.[487] 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),[488] 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.[489] 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.[490] 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.[491] 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.

2.4.2.2. Video surveillance of publicly inaccessible areas

It is also unclear to what degree video surveillance is aimed at non-public areas.[492] Non-public places include all spaces which may be entered only by a certain group of people.[493]

2.4.2.2.1. 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.[494]

2.4.2.2.2. 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

[486] Bundestag, 2001, p. 62; Schaffland/Wiltfang, 2010, § 6b BDSG mgn. 5; Bizer, 2011 § 6b BDSG mgn. 75; Zscherpe, 2010, § 6b BDSG mgn. 76
[487] Bizer, 2011, 6b BDSG mgn. 75.
[488] Consequently, without culpable hesitation, cf. § 121 par. 1 s.1 BGB, Thüsing, 2010, mgn. 359.
[489] Bundestag, 2001, p. 63.
[490] Zscherpe, 2010, § 6b BDSG mgn. 77.
[491] Grimm/Schiefer, 2009, pp. 329, 335.
[492] Grimm/Schiefer, 2009, pp. 329, 335. Measures designed simply to trick the employees are however forbidden (§ 226 BGB), Thüsing, 2010, mgn. 361.
[493] Bizer, 2011, § 6b BDSG mgn. 43.
[494] See also above - section 1.3.2.4.1.

inaccessible work places. The prerequisite for an analogy is the existence of an unintended regulatory gap, and also comparative interests.[495] However, there are currently no unintended regulatory gaps,[496] 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.[497] 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.[498] 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.[499] The fact that, in individual cases, the intensity of invasion can be larger in publicly accessible than in publicly inaccessible places,[500] is not in contradiction to the fact that, when drafting Article 6b of the BDSG, the legislator focused on rather less intensive encroachment.[501]

2.4.2.2.3. 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.[502]

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.[503] 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.[504] 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.[505] According to government reasoning, the data protection principles developed by the Federal Labour Court are to be taken as the basis of such consideration,[506] and here again, in

[495] 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."
[496] BAG NZA 2004, 1278, 1282; Maties, 2008, p. 2221.
[497] Bundestag, 2000a, p. 38.
[498] Grimm/Schiefer, 2009, pp. 329, 336.
[499] BAG, NZA 2004, 1278, 1282.
[500] Bayreuther, 2005, pp. 1038, 1041.
[501] Grimm/Schiefer, 2009, pp. 329, 336.
[502] Thüsing, 2010, mgn. 347 f.
[503] Thüsing, 2010, mgn. 360.
[504] Thüsing, 2010, mgn. 361, which leads further (mgn. 348) whether § 28 par. 1 s. 1 no. 2 BDSG can further be applicable.
[505] Thüsing, 2010, mgn. 362.
[506] Bundestag, 2009a, p. 35.

particular, account should be taken of the principle of proportionality.[507] Under narrow circumstances, the balancing of interests can fail at the expense of the employees,[508] if, in the case of employee surveillance in publicly inaccessible places, it is a by-product of other surveillance purposes,[509] and the measure also serves to protect the employees working there, or the employer has a legally justified security interest.[510]

Covert surveillance

Concerning publicly inaccessible places, there arises the problem of whether or not Article 6b Paragraph 2 of the BDSG reveals a blocking effect.[511] According to government reasoning, a special statutory regulation is needed for covert surveillance.[512] 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.[513] 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.[514]

2.5. Employee surveillance by entry monitoring systems[515]

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.[516]

2.5.1. Description of commonly used systems

We should examine the technical differences among several types of system in regular use.

2.5.1.1. Transponder-based systems

One way to control access is with the help of transponders.[517] 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. Further, more complex transponder systems offer a central, computer-based control,

[507] BAGE 127, 276 mgn. 17. Cf. re proportionality – a detailed survey in Thüsing, 2010, mgn. 362 ff.
[508] BAG, NZA 2004, 1278, 1283.
[509] Grimm/Schiefer, 2009, pp. 329, 337.
[510] 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.
[511] Thüsing, 2010, mgn. 368.
[512] Bundestag, 2000a, p. 38.
[513] See also above - section 2.4.2.1.4.
[514] BAG, NZA 2003, 1193, 1195; Thüsing, 2010, mgn. 175.
[515] Video surveillance can also be used for monitoring entry. For reasons of scale and in the sense of easier supervision this theme is treated separately, cf. Section 2.4. From this position there follows a discussion of transponder systems, biometric systems and RFID technology.
[516] Meyer, 2009, pp. 14, 16.
[517] 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.

which facilitates the systematic recording of the use of the transponder and hence the generation of movement profiles. As the employee will normally have his own personal transponder 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 a relatively accurate employee location system. 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.[518]

2.5.1.2. The use of biometric systems

Access or entry control can also be carried out by means of the comparison of biometric data. As biometric features, physiological or passive (e.g., fingerprints, face, iris or vein-recognition) or active (e.g., voice recognition, signature, password) can serve.[519] By using biometric techniques, the identification of individuals is made possible - solely on the basis of their personal, individual physical features.[520] 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.[521] Biometric data can, on an individual case basis, and depending on the specific utilisation[522] 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.[523] However, it should at least 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. If transponder systems and biometric authentication are linked, the merit of the former, due to the lower level of intrusion into personal rights when employees are monitored, must be acknowledged.[524]

2.5.1.3. Use of RFID technology[525]

RFID systems, in comparison with the previously mention measures, make possible one essentially more accurate monitoring of employees, in which, by means of Radio Tags (Radio Frequency Identification, RFID) tags, information stored on a micro-chip can be retrieved without contact.[526] Due to their small size, these tags can be used as an in-house pass or for other purposes,[527] and can, in extreme cases even be fixed to the clothing.[528] With the aid of

---

[518] Meyer, 2009, pp. 14, 16.
[519] Gola/Wronka, 2010, mgn. 874; Bartmann/Wimmer, 2007, p. 199.
[520] Raif, 2010, p. 359.
[521] Meyer, 2009, pp. 14, 17.
[522] Cf. as an example of this Gola/Schomerus, 2010, § 3 BDSG mgn. 56.
[523] Meyer, 2009, pp. 14, 17, with the assertion that § 6a BDSG is not applicable.
[524] Meyer, 2009, pp. 14, 17; as well Roloff, in: Besgen/Prinz, § 5 mgn. 66.
[525] Mainly, in this connection, we also speak of so-called 'Ubiquitous computing' (allgegenwärtige Datenverarbeitung), cf. Buchner, 2010, § 3 BDSG mgn. 18.
[526] 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.
[527] Gola/Schomerus, 2010, § 6c BDSG mgn. 2a; von Westerholt/Döring, 2004, p. 711.
[528] Däubler, 2010, mgn. 324a.

RFID technology, 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.[529] The reading range with an RFID installation is within two digits in terms of metres.[530]

2.5.2. Cases from the jurisdiction

Decisions referring to entry control systems are, to date, on a small scale,[531] 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.[532]

2.5.3. Academic debate

As already stated, data protection admissibility is evaluated according to whether the handling of data is covered by the agreement of the person concerned[533] 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.[534] 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.[535] 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.[536] 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.[537] Amongst these will be businesses which handle especially hazardous materials or where corporate know-how is particularly valuable.[538] In the absence of a suitable security need, at least no biometric technology needs to be installed.[539] 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,[540] for example in respect of the basic health or background of his employee.[541] Storing

[529] Art. 29 Data Protection Working Party, 2005, p. 29; Buchner, 2010, § 3 BDSG mgn. 18.
[530] 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.
[531] Z.B. BAG, RDV 2004, 122 (Co-determination with Biometric Entry Control Systems).
[532] Gola, 2010a, mgn. 82.
[533] As far as the possibility is permitted, see Section 1.3.2.4.1.
[534] Meyer, 2009, pp. 14, 17.
[535] Roloff, 2009, § 5 mgn. 55. To be considered here is, for example, the use of Transponders without individual ID, Meyer, 2009, pp. 14, 17.
[536] Zöll, 2010, § 32 BDSG mgn. 22; Gola/Wronka, 2010, mgn. 885.
[537] Meyer, 2009, pp. 14, 17.
[538] Roloff, 2009, § 5 mgn. 68.
[539] Roloff, 2009, § 5 mgn. 71.
[540] Raif, 2010, p. 359.
[541] Gola/Wronka, 2010, mgn. 875; Steinkühler/Raif, 2009, pp. 213, 217.

such features and other sensitive data as per § 3 Abs. 9 BDSG is normally conditional on the agreement of the employee.[542] 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 agreement of the individual concerned or with the submission of an exemption application according to § 28 Abs. 6, 7 or 9 BDSG.[543] From the perspective of legal data protection the use of RFID systems should be treated more circumspectly.[544] In contrast to the situation with the technology mentioned earlier, 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.[545] At least in respect of active RFID tags[546] there should apply § 6c BDSG[547] which governs the mobile storage and handling of personal data[548] (§ 3 Abs. 10 BDSG).

Basically, all media fall within this category, which are equipped with a single processor-chip.[549] 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.[550] 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, according to § 6c Abs. 3 BDSG, which is not defined more precisely.[551] It is, however, recommended that there should be some signal marking the recording of data – perhaps an acoustic tone.[552] 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

[542] Raif, 2010, p. 359. Representing a more strict view (Oberwetter, 2008, pp. 609, 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.
[543] Raif, 2010, p. 359.
[544] Cf. also Schmitz/Eckhardt, 2007, p. 172 on the different possibilities of use and related thoughts.
[545] Meyer, 2009, pp. 14, 18.
[546] 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.
[547] Von Westerholt/Döring, 2004, p. 714; more differentiation Schmitz/Eckhardt, 2007, p. 173.
[548] 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.
[549] Gola/Schomerus, 2010, § 3 BDSG mgn. 58; Gola, 2010b, § 6b BDSG mgn. 2.
[550] Zscherpe, in: Taeger/Gabel, BDSG, § 6c mgn. 52; Meyer, 2009, pp. 14, 18.
[551] Gola, 2010b, § 6c BDSG mgn. 3.
[552] Meyer, 2009, pp. 14, 18.

the particular electronic reading process creates a movement profile.[553] For the rest, the same general approach should apply as for the already mentioned entry control systems.[554] 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.[555]

2.6. Monitoring of employees outside company premises

The monitoring of employees outside actual company premises is also possible.[556] 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.[557] If the employer makes equipment available to the employee, he can continuously detect the location of the employee and monitor his activity.[558]

2.6.1. Cases from the jurisprudence

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.[559]

2.6.2. Academic debate

Often, by using GPS for tracking company cars and mobile phones, operational profiles of employees are created.[560]

2.6.2.1. GPS tracking of company vehicles[561]

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.[562] 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.[563] As far as the function is concerned, the sender's own position is first determined via data-matching with GPS

[553] Meyer, 2009, pp. 14, 18, who stresses that there can be a need of creating motion profiles by all means, like for security personnel, for example.
[554] Schmitz/Eckhardt, 2007, p. 175.
[555] Wank, 2010, § 6c BDSG mgn. 19; Gola/Wronka, 2010, mgn. 885.
[556] For example when field representatives or courier drivers shall be controlled, cf. Däubler, 2005, p. 770.
[557] Global System for Mobile Communications, Mozek/Zendt, 2011, part 23 mgn. 9.
[558] Meyer, 2009, pp. 14, 18.
[559] Raif, 2010, p. 359; Meyer, 2009, pp. 14, 19.; Gola/Schomerus, 2010, § 32 BDSG mgn. 19.
[560] Vogt, 2009, p. 4212; Meyer, 2009, pp. 14, 18; Raif, 2010, p. 359.
[561] Since GPS transmitters are mainly used for locating vehicles (Meyer, 2009, pp. 14, 18), the following details are limited to this field.
[562] Gola, 2007, p. 1142.
[563] Meyer, 2009, pp. 14, 18. Re the different (due to their smaller size) potential uses of the GPS transmitters see further Gola, 2007, p. 1143.

satellites.[564] After this, the location data are stored for a specific time, compressed and transmitted.[565] 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.[566] Accordingly, the employer must again meet the information requirements of § 6c BDSG.[567] 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.[568] 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,[569] 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.[570] 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.[571] 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.[572] Again, however, we should try to avoid sweeping assumptions; an assessment should be made on a 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[573] and the costs of a company's cars are also to be considered.[574]

2.6.2.1.1. Tracking by GPS whilst on duty

[564] Roloff, 2009, § 5 mgn. 72. Compared to navigational systems, the main difference is that in this case position data is neither recorded, nor distributed, Meyer, 2009, pp. 14, 18.
[565] BVerfGE 112, 304, 308; Roloff, 2009, § 5 mgn. 72. With appropriate technical arrangements data transmission can take place even in real time, Meyer, 2009, pp. 14, 18.
[566] Meyer, 2009, pp. 14, 19.
[567] Schmitz/Eckhardt, 2007, p. 173 fn. 22.
[568] Raif, 2010, p. 359; Gola/Schomerus, 2010, § 6c BDSG mgn. 5.
[569] Concerning the admissibility of video surveillance in detail see: 2.4.
[570] Raif, 2010, p. 359.
[571] Roloff, 2009, § 5 mgn. 81.
[572] Cf. the details in BVerfGE 112, 304, 308, 317.
[573] 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.
[574] 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).

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.[575] 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.[576] Tracking should not extend to the leisure time of the employee.[577]

2.6.2.1.2. Covert use of GPS tracking

§ 6c BDSG does not accept the use of covert GPS tracking.[578] According to § 4 paragraph 3 BDSG and § 98 paragraph 1 TKG,[579] 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.[580] 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.[581] 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.[582]

2.6.2.2. Location by mobile phones

Another measure for employee monitoring is location by mobile phones.

2.6.2.2.1. GPS location

GPS tracking is also possible via mobile devices.[583] 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.[584] Regarding the admissibility of such location methods, the above comments apply.

2.6.2.2.2. 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

---

[575] Roloff, 2009, § 5 mgn. 83, likewise Meyer, 2009, pp. 14, 19.
[576] Meyer, 2009, pp. 14, 19. Vogt, 2009, p. 4212.
[577] Vogt, 2009, p. 4212
[578] Meyer, 2009, pp. 14, 19.
[579] § 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.
[580] Vogt, 2009, p. 4212.
[581] Steinkühler/Raif, 2009, pp. 213, 216.
[582] Meyer, 2009, pp. 14, 19 with reference to Roloff, 2009, § 5 mgn. 87.
[583] Gola, 2007, p. 1143.
[584] Meyer, 2009, pp. 14, 19.

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, the location can be determined with an accuracy of up to 100 meters.[585] 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.[586] 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.[587]

2.6.2.2.3. Privacy in telecommunication

The provisions related to telecommunications data protection require service providers to obtain prior permission for location operations.[588] The use of location data is regulated in § 98 TKG [589] and, according to the clarification appended to the government draft, the progressive development of telecommunications should be taken into account, which allows the site-related use of telecommunications services (Location Based Services, LBS).[590] In this regard, dealing with location data depends on the consent of the participant[591] as a contractor or service provider.[592] 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.[593] 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.[594] 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.[595] 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.[596] In the planned balancing of interests, several factors play a role.

[585] Meyer, 2009, pp. 14, 19.
[586] Wittern, 2006, § 98 TKG mgn. 4.
[587] Meyer, 2009, pp. 14, 19.
[588] Gola, 2007, p. 1143.
[589] Concerning the necessity of acquiescence in line with § 98 TKG Jandt, 2007, p. 74.
[590] Munz, 2010, 98 TKG mgn. 1 referring to Bundestag, 2004, p. 89.
[591] 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.
[592] Meyer, 2009, pp. 14, 20.
[593] Wittern, 2006, § 98 TKG mgn. 7.
[594] Meyer, 2009, pp. 14, 20; Gola/Wronka, 2010, mgn. 897.
[595] Gola, 2007, p. 1143.
[596] Meyer, 2009, pp. 14, 20.

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.[597] 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.[598] Regardless of the scope of § 98 TKG, this follows from § 6c BDSG, which is also applicable to the SIM card of a mobile device.[599]

2.7. Special features of employee screening

During a so-called employee screening process, data already available to the employer or assembled especially for this purpose go under a test grid to help, by means of a points system, specific conclusions to be formulated.[600] In Germany, this form of screening is now widely used when, in respect of the protection of personal rights at work, battling corruption is a priority.[601]

2.7.1. Forms of employee screening

Employee screening occurs unless an arrangement through legislation (§ 4 Paragraph 2 BDSG) is submitted, using one of two formats: firstly, if the prevention of corruption and other compliance violations is an issue, and, secondly, if it is a matter of prosecuting criminal offences and other compliance problems.[602] Preventive screenings are characterised primarily by the fact that on the employer's side there is no evidence for the existence of specific violations of law, but legal compliance should be checked and implemented preventively. By contrast, the employer knows, in the case of investigative screening, about compliance violations and he attempts to draw conclusions about the origin of the violation by various means.[603]

2.7.2. Cases from the jurisprudence

There is still little jurisprudence in the area of employee screening to be referred to.[604] Again, therefore, case law in connection with video surveillance should be used.[605]

---

[597] Gola/Wronka, 2010, mgn. 905; Meyer, 2009, pp. 14, 20.
[598] Meyer, 2009, pp. 14, 20.
[599] Von Westerholt/Döring, 2004, p. 714; Gola/Schomerus, 2010, § 6c BDSG mgn. 2a.
[600] Brink/Schmidt, 2010, p. 592.
[601] Re further screening measures such as cross-checks with terror lists or pre-checking in respect of official applications or social advantage procedures cf. as an example Brink/Schmidt, 2010, pp. 595-596.
[602] Brink/Schmidt, 2010, p. 592; Gola/Wronka, 2010, mgn. 857.
[603] Brink/Schmidt, 2010, p. 592.
[604] Cf. e.g., the report of the BVerfG on a public prosecutors data collection in respect of a new credit card institute, RDV 2009, 113.
[605] Gola/Wronka, 2010, mgn. 856; Mähner, 2010, pp. 379, 381.

2.7.3. Academic debate

For assessing the admissibility of employee screening, according to the current legal situation, both §§ 28, 32 BDSG should be considered as factors relevant to permission.[606] Regarding the question of consent, the voluntary nature of employee screening is especially important from two points of view. Not only is it very doubtful whether an employee really does feel no compulsion to participate in mass screening, but the possible consequences must also be borne in mind which may arise if someone does not participate in one single proceeding which should be undergone consistently by everyone involved.[607] In respect of testing the admissibility of measures in respect of staff screening, the distinction between preventive and investigative measures (referred to previously) should be maintained.

2.7.3.1. Preventive screening measures, § 32 paragraph 1 sentence 1 BDSG

First, § 32 paragraph 1 sentence BDSG should be seen to be relevant, although this may fail – generally in relation to the necessity requirement. An employment relationship is feasible even without a screening process and so the measure is not absolutely necessary.[608] The mere, interest of the employer, even though understandable, in the preventive fight against corruption does not justify (in the case of § 31 paragraph 1 sentence 1 BDSG) the employer's access to the personal data of workers. Even if the question concerned educating employees about potential compliance violations within the company, it requires no reference to past offences, possibly even with the attribution of those responsible.[609] Otherwise the same applies to the treatment of breach of contract on the part of employees, and the fact that it is the employer alone who initiates such an educational process, does not entail any other legal evaluation.[610] Finally § 32 paragraph 1 sentence 1 BDSG is basically excluded as a legitimate basis for the preventive screening of employees.[611]

2.7.3.2. Investigative screening measures, § 32 paragraph 1 S. 2 BDSG

As is clear from the literature, the handling of employee data used for exposing criminal offences must comply with demanding requirements. An attempt at justification by claiming "clarification measures" under § 32 paragraph 1 sentence 2 BDSG, would come into consideration only if there were some serious suspicion of a crime being committed.[612] A mere suggestion that some member of a group of employees might have committed a criminal offence is not sufficient to justify investigative screening measures.[613] Finally, the scope of § 32 paragraph 1 sentence 2 BDSG is, for these reasons, tightly circumscribed.

---

[606] A vindication of Consensual Agreement according to Brink/Schmidt, 2010, p. 593 is however separate. Alternative viewpoint is Vogt, 2009, p. 4214, which recognises a business agreement as legally authorised.
[607] Brink/Schmidt, 2010, pp. 592, 593.
[608] Thüsing, 2009, pp. 865, 867.
[609] Brink/Schmidt, 2010, pp. 592-594.
[610] As well as Thüsing, 2009, pp. 865, 868 f.
[611] As a result ditto Mähner, 2010, pp. 379, 381.
[612] Brink/Schmidt, 2010, pp. 592, 594; likewise Rasmussen-Bonne/Raif, 2011, p. 80.
[613] Mähner, 2010, pp. 379, 381.

2.7.3.3. § 28 paragraph 1 S. 1 Nr. 2 BDSG

Unless, besides the application of § 32 BDSG, recourse to § 28 paragraph 1 No. 2 BDSG is permitted, justification for this permission would be taken into consideration only in exceptional cases.[614] This is conceivable, for example, when the admissibility of the screening is not directed in accordance with § 32 BDSG, or perhaps if the relation of the employees to the employer are to be qualified as with any third party.[615]

2.8. The participation rights of interest groups

If an employer wishes to introduce measures to monitor his employees, this requires the regular involvement of interest groups of employees (company or staff councils).[616] In this respect § 32 paragraph 3 BDSG prescribes that the participation rights of interest groups remain unaffected.[617] This means that, in collective measures, and, hence, in all consistently performed surveillance activities, there is a limit to the scope of what the employer can arrange.[618] Participation requirements should not only be taken into consideration for the formal collection of personal data (§ 94 BetrVG, §§ 75 paragraph 3 Nr. 8, 76 Abs. 2 Nr. 1 BPersVG) and data protection issues relevant to the operational rules and behaviour (§ 81 paragraph 1 BetrVG 1, § 75 paragraph 3 15 BPersVG). This is particularly the case in respect of the automatic data processing of personal data realised with the use of technical surveillance equipment (§ 87 paragraph 1 Nr. 6 BetrVG, § 75 paragraph 3 Nr. 17 BPersVG).[619] According to the theory so far prevailing[620] of the efficacy requirement developed by the BAG,[621] the participation of interest groups is necessary for the effectiveness of a measure. In individual contract terms it follows that, for violations of participation rights, adverse changes for employees or the practice of arrangement rights are ineffective and, therefore, not to be considered.[622] It should also be noted in this context that the right to participate does not extend to the question of permission for private use *per se*.[623]

---

[614] Bierekoven, 2010, p. 205 referring to Bundestag, 2009a, p. 35.
[615] Schmidt, 2010, p. 209; Brink/Schmidt, 2010, p. 594, which confronts, for example, transmitting data re business transactions of the employee to the employer as an arbitrary third party.
[616] Zöll, 2010, § 32 BDSG mgn. 48.
[617] The government reasoning names, for example, § 87 Para. 1 Nr. 6 BetrVG and § 75 Para. 3 Nr. 17 BPersVG, Bundestag, 2009a, p. 37.
[618] Thüsing, 2010, mgn. 531 ff.
[619] Gola/Schomerus, 2010, § 32 BDSG mgn. 43.
[620] Cf. regarding the alternative viewpoint Richardi, 2010, § 87 BetrVG mgn. 104 ff; Worzalla, 2008, § 87 BetrVG mgn. 83 ff.
[621] BAG, NZA 1992, 749, 759; NZA 2004, 331, 333.
[622] BAG, NZA-RR, 469, 471; Thüsing, 2010, mgn. 564.
[623] LAG Hamm, NZA-RR 2007, 20, 21 f.; Ernst, 2002, p. 586; Lindemann/Simon, 2001, p. 1954.

3. EMPLOYEE DATA PROTECTION FROM THE PERSPECTIVE OF DATA PROTECTION AUTHORITIES - AND FURTHER INFORMATION

3.1. The position of the HmbBfDI (Hamburg Commission for Data Protection and the Freedom of Information) concerning personal rights in working life[624]

Regarding the question of personal rights protection of workers, the act of the legislature is in principal greeted by supervisory authorities; but criticisms have also been levelled against the proposed legislature and the need for regulation and improvement in the area of employee privacy have been announced as well. The creation of Clause § 32 BDSG as a general clause for the handling of employee data might, by this, not only be an inadequate, politically motivated and symbolic piece of legislation designed to take the pressure off ongoing discussion. Rather more, it gives birth to considerable problems in practice, specifically in respect of the inadequately clarified competitive relationship with § 28 BDSG. The resulting large degree of legal uncertainty needs to be countered by the creation of a clear legal framework which does not overlook practical considerations. In this it is not only the significance of capital and paid work which are to be taken into account but it should also be recognized that the company is subject to a great variety of new factors and will tend to economize with the use of data. In addition, the issue of relationship between the law and technology will appear. When it comes to the question of where the use of technology on legal-ethical grounds is pushed to its limits, one could easily get in a very difficult assessment process on the political ground. A resolution of this conflict cannot be reached by regulated self-control. Such a model might be interesting in areas in which data protection can be used as a measure of competitive improvement, by following the personal interest of management in optimizing specific processes. It makes little sense where different interests decide or where legal interventions are to be set. From the side of the legislator one should only conditionally comply with the need for a fair consideration of the conflicting positions, as, perhaps with the decision to oppose secret video-monitoring consistently. However, allowing continuous open video-monitoring would also give way to criticism. Such measures should not lead to a situation where, ultimately, every handshake of an employee is digitalized and retrievable. Regarding the possibilities of introducing new and combining existing technologies, as well as reproducing the procedures at any time in operational areas, informational self-determination faces great danger. Naturally, there will be cases in which employers have a legitimate interest in introducing some more modern technology, perhaps improving the security of their property. This, however, should be carried out in a humane way and it should not lead to a total monitoring of the workplace. Together with the basic avoidance of accessing stored data and the basic ban on secret measures, a maximum level of transparency should also be ensured. However, it is not only from a legal perspective that

[624] The explanations are based on an interview with the Hamburg Commissioner for Data Protection and Freedom of Information, Prof. Dr. Johannes Caspar. The full text is available as a separate document.

personal data should be handled carefully. Since the dangers in the digitalized world of work, which start with the selection of candidates, spread over the whole field of legal relationships in the labour law, proper behaviour is required on both the employer's and the employees' side. While on the employees' side a self-reflected and foresighted attitude towards the possible consequences of dealing with personal data is noticeable quite early, i.e. during school days, employers should also display a certain degree of liberality. This implies at last that people who possibly tattooed, even stigmatized themselves digitally, are not to be excluded from the pool of applicants due to the careless handling of data. As a result it remains to be noted that the supervisory goal must be to establish knowledge and set clear guidelines. Besides the necessary reorganizing and restructuring due to the expected rising amount of input at the data protection authorities, for them one thing is clear: modern data protection demands a great deal of personal responsibility also in the future.

3.2. Further information of BfDI

On the homepage of the Federal Commission for Data Protection and Freedom of Information[625] diverse information is available. The organization deals among others with aspects which may gain importance in connection with the protection of personal rights of employees. Otherwise you get here e.g. to important data protection bodies, to the Data Protection Forum, the State Data Protection Representative, the Supervisory Authorities for the Non-public Sector, the Data Protection Officer of the Radio, to the Virtual Data Protection Office, as well as several other interesting sites that provide information in the federal area, in European and in international context.[626]

[625] Available on http://www.bfdi.bund.de

[626] The mentioned data protection bodies are e.g. National Data Protection Conference, Düsseldorf district, European Data Protection and International Data Protection Conference. In addition, there are a variety of other sites [such as from interest groups like the Association of Digital Economy (BVDW) or the Federal Association for Information Technology, Telecommunications and New Media (BITKOM)] that address the issue of employee privacy. Regarding the immensity of the available data on the topic there is no chance of further discussion here.

4. SANCTIONS IN CASE OF VIOLATIONS OF DATA PROTECTION

The violation of laws by employers and employees can lead to sanctions of data protection, labour law and to further sanctions.

4.1. 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 €.[627] On § 44 BDSG certain acts are even criminalized.[628] The obligations of the BDSG meet the responsible entity (§§ 1, paragraph 2, 2 BDSG) this means the head of the department or the management.[629] 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.[630] 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.[631]

4.2. 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.[632] 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.[633] This is especially the case if through obtaining the evidence constitutionally protected basic positions have been violated,[634] furthermore if the employer has violated

[627] 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.
[628] Often, however, special rules will become relevant, see: Gola/Wronka, 2010, mgn. 1296.
[629] Gola/Wronka, 2010, mgn. 1292.
[630] § 7 BDSG is the basis for a claim for liability arising from suspected negligence, Däubler, 2010, mgn. 574.
[631] 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.
[632] Thüsing, 2010, mgn. 564.
[633] 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.
[634] BGH, NJW 2005, 497, 498 ff.

privacy rights of the employees.[635] 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,[636] 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[637] as well as pay cuts.[638] Sometimes they may get liable for causing damage unlawfully.[639] 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.[640] 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.[641]

4.3. 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), § 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).[642]

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.[643] Apart from the feature as a telecommunication provider, criminality according to §

[635] 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, pp. 652, 655. See further Lunk, 2009, pp. 457, 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.

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

[637] See also Gola, 2010a, mgn. 364 ff.; Trappehl/Schmidl, 2009, pp. 985, 987 ff; and Gola/Wronka, 2010, mgn. 1383 ff.

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

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

[640] Fundamentally BAG, DB 1993, 939.

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

[642] Trappehl/Schmidl, 2009, pp. 985, 990; Schmidl, 2010, pp. 476, 479; Gola/Wronka, 2010, mgn. 1341.

[643] Gola, 2010a, mgn. 103 ff.

201 StGB (Violation of the confidentiality of the word) is added.[644] 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.[645] Here, again, § 206 StGB[646] appears, which also includes the protection of e-mail traffic.[647] 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.[648] 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).[649] 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)[650] provisions.[651] Since the present data protection liability standards of §§ 7, 8 BDSG there are no final regulations represented,[652] a possible recourse to the general civil claims remains.[653] Illegal surveillance measures can entail e.g. sensitive compensation claims.[654]

[644] 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.
[645] Gola, 2010a, mgn. 51
[646] Violation of postal or telecommunications secrecy.
[647] 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.
[648] Gola, 2010a, mgn. 378.
[649] Gola/Wronka, 2010, mgn. 1296.
[650] The employer then can assert his claim for relief and removal, see Trappehl/Schmidl, 2009, pp. 985, 990.
[651] 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.
[652] Bundestag, 2000b, p. 2.
[653] 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.
[654] See for instance the recent verdict that an employer should pay compensation of €7,000 for unauthorised video surveillance, LAG Hessen, 2011, 346.

5. SUMMARY

As pointed out above, the field of protection of personal rights of employees is undergoing a change recently. The regulation de lege lata proves to be inadequate, also and especially it is opposed to the new requirements of the digitalized world of work. Though there are certain approaches the intention of which would be desirable, especially with regard to the jurisprudence developed by the BAG concerning the assessment process. However at the current state of affairs it is not possible to talk about having sufficient resources to realize an employee data protection which represents a just solution for both employers and employees. The open mindedness of legislature towards criticism is still in question, as far as the willingness,[655] the capability of the elimination of the weaknesses of the current outline is concerned, as well as creating a balanced and with regard to practice, a sensible regulation, which one can call sufficiently just towards the requirements of legal certainty and clarity. Until then, the parties will equally advise one thing: „Abundans cautela non nocet!"[656]

[655] See for instance Tinnefeld/Petri/Brink, 2010, p. 727; Wybitul, 2011, 313091 or also expert criticism of Wybitul, 2011, 318249.

[656] Too much caution does not hurt (translated from Latin, by Lauterbach, Latin - German: Quotation Encyclopaedia, p 135)

6. LITERATURE AND REFERENCES

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]

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 (2005), RFID, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_de.pdf. [18.04.2011]

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.

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.

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]

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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

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

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]

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]

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.

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.

Naujock, Anja (2002): Internet-Richtlinien – Nutzung am Arbeitsplatz – Ein Plädoyer für eine klare Regelung, Datenschutz und Datensicherheit, pp. 592-596.

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.

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.

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.

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

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.

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.

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.

Comments on printed matter and court decisions in the realm of the protection of privacy in the workplace generated a variety of further significant printed material:

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]

Bundesrat, printed matter:

- 535/10 (B) [5.11.2010]

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

In addition there are many relevant court decisions in respect of questions concerning Employee Data Protection. The main decisions of 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

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