Chapter 9
PRIVACY AND DATA PROTECTION AT THE WORKPLACE IN GERMANY

Thomas Hoeren, Sonja Eustergerling[1]

9.1 Historical Development of Data Protection in Germany

9.1.1 Introduction

Data protection is a very important issue for the Germans, not only because of the historical experiences.

As a consequence of the occurrences on 11 September 2001 the law enforcement agencies gained more rights. With the 'Terrorismusbekämpfungsgesetz' from 9 January 2002[2] the field of application of the 'Sicherheitsüberprüfungsgesetz'[3] has been adjusted. Employees in companies dealing with energy production or with telecommunications, including their wives or partners can, under specific circumstances, become subject to security controls. Therefore, critics worry about an excess of state control. An effective means to combat terrorism is highly desirable, as long as this would not result in abandoning personal rights, a situation that would be forced by terrorists.

Although the German law covers almost all parts of life, a special law for workplace privacy has not yet been enacted. Adjudication and experts deduce the data protection in the workplace from constitutional rights and general data protection terms.

For a few years the discussion about enacting a special data protection act securing workplace privacy has intensified. The cabinet plans to present a draft act within this legislative period.[4] Even the European Commission shows interest in creating a new framework for workplace privacy in Europe.[5]

---

[1] Both authors are affiliated to the Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung, Westfälische Wilhelms-Universität, Münster, Germany.

[2] Freely translated: 'Combating of Terrorism Act'; BGBl. I No. 3, 11 January 2002.

[3] Freely translated: 'Security Survey Act'; BGBl. I, p. 867, 20 April 1994.

[4] BT-Drs. 14/8456, S. 66, (79); Research report, March 2002; 15. Legislative period: 2003-2008.

[5] Second formal consultation of the social partners in Brussels, 31 February 2002.

S. Nouwt, et al. (Eds), Reasonable Expectations of Privacy?

Because of the very rapid developments in and the utilisation of modern technology in the workplace, there exist more and more areas which can be monitored. In particular, the internet opened a huge field of surveillance possibilities for the employer. People in Germany do not trust the technical safety of new technologies. A survey in 2001 found that 45 per cent of all employees who use a computer at work abstain from surfing the internet at work in order to avoid security problems.[6] The access to personal data has never been as easy as today. Every third person has the impression of being a victim of data abuse.

The transfer of previous case law to theses issues seems to be impossible. Therefore, the number of open questions in the area of data privacy is increasing.[7]

The topic of 'workplace privacy' includes everything which interrelates with employers and employees and at the same time with information.

The protection begins when the employer and the employee first contact each other and ends when the data has been deleted.

In Germany 'data' is defined as all information which relates to a person, including those data which allow any inference with a person's personal attributes or character. A person's curriculum vitae or state of health is in the same way part of this personal data as well as how long a person retains a certain page on the internet.

9.1.2 **The development of data protection**

People have not long been aware of the necessity to have special data protection, but this awareness is steadily increasing.

9.1.2.1 *Formation of the Bundesdatenschutzgesetz (BDSG)*[8]

At the beginning of the 1970s, when data processing began to emerge, the public began to criticise the risks involved in personal data.[9] In 1970 the first Landesdatenschutzgesetz (LDSG)[10] was enacted,[11] in 1977 the BDSG followed. This was the birth of the first written regulations on data privacy.

This progression was a reaction to the technological development. Although the trend was still in its infancy, people already realised that the change would have an extensive influence on living and economic conditions in the developed nations.

Already in 1968 the desire for a social reorientation became evident with the change of political power.

[6] Opaschowski, 'Quo vadis, Datenschutz? Die Angst vor dem Datenklau breitet sich aus', *DuD* 2001, p. 678, (679), with reference to a representive B.A.T. analysis.

[7] Wedde, 'Schutz vor verdeckter Kontrolle im Arbeitsverhältnis', *DuD* 2004, p. 21, (22).

[8] Freely translated: 'Federal Data Protection Act'; BGBl. I 1990, 2954, 2955, amended on 14 January 2003, I 66.

[9] Hoeren, Internetrecht, p. 4.

[10] Freely translated: ' State Data Protection Acts'.

[11] Hessisches Datenschutzgesetz, GVBl. I, p. 625.

During this time, the public tenor against the state, society and industry changed. People gained the impression that the authorities posed a risk to their freedom. At this time the processing only took place in insulated central data processing centres which gave the public the feeling of being subject to state control.

Considering the fact that these regulations enabled extensive interference with the organisation of the economy and administration,[12] it is remarkable that the rapid formation of certain rules thereon based on the strong will of the legislature, although there was never a special reason for this, such as data problems. The legislative body also realised early on that the new computer systems contained a high potential for risks.[13]

The BDSG enacted in 1977 was amended in 1990 as a reaction to the new techniques.

With a delay of a few years the EU directive[14] was transposed into German law by the 'Gesetz zur Änderung des Datenschutzgesetzes und andere Gesetze'.[15] The plan to modernise the whole BDSG in connection with this transformation has not been successful, and is not expected soon as the latest events in the USA and also Spain demonstrate.[16]

Regrettably, also this act still lacks specific regulations concerning workplace privacy, although the density of written regulations in data protection law has reached a very high degree of concentration in Germany.[17]

9.1.2.2 *'Data privacy' as a constitutional civil right – 'Volkszählungsurteil'*

In its 'Volkszählungsurteil'[18] the Bundesverfassungsgericht[19] created and accepted data privacy as a constitutional right. The human rights laid down in the German Constitution, including the right to privacy, serve in the first place as rights against interference by the state, and are, therefore, not applicable between private persons. The Bundesverfassungsgericht stated, however, that constitutional rights are elements of an objective order which, as a basic ruling, have importance for all areas of 'rights' and, therefore, have an impact on private law as well.[20] Constitutional rights are therefore also effective between employers and employees.[21]

[12] Rossnagel-Abel, Handbuch des Datenschutzes, 2.7., Rn 1.

[13] Ibidem; the key issue has been central databases.

[14] Directive 95/46/EG of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[15] Freely translated: 'Act to change the BDSG and (…)'; BGBl. I, 904, which was enacted on 23 May 2001.

[16] Ibidem.

[17] Tinnefeld, 'Die Novellierung des BGDS', *NJW* 2001, p. 3078 (3079).

[18] BVerGE 65, S.1ff.; population census judgment, PN2004-189.

[19] Supreme Federal Constitutional Court.

[20] BVerfGE 7, S. 189, (205), BVerfGE 73, S. 261, (268), Jarass/Pieroth, Jarass, GG, Preliminary note before Art. 1 GG, Rn. 9.

[21] Pieroth/Schlink, Staatsrecht II, Rn. 181.

The constitutional right of data privacy is derived from general personality rights which are explicitly inserted in the constitution. Article 2, para. 1 GG[22] states: 'Everybody has the right of free development of personality (...)'

This has to be understood so that general personality rights with regard to the highest constitutional principle, the human dignity (Article 1 para. 1 GG), guarantee the almost absolute preservation of the most private and intimate sphere.[23]

The reason for the judgment of the Bundesverfassungsgericht was the enforced population census under the 'Volkszählungsgesetz 1993'.[24] Many citizens fought against the population census by handing in a petition to the constitutional court. Because of the collection and storage of personal data they feared being spied upon by the state.

The Bundesverfassungsgericht shared these concerns about the population census and established conditions which need to be met before such data collection can be tolerated.

The court explained; BVerfGE 65, p.1 ff.:

> 'Manual file cards are no longer in use as was previously the case, but rather, with the help of automatic data processing, personal and factual circumstances of a certain person are available in seconds. Single dates can be used to form an image of a person's personality which is not under the control of the people concerned. Therefore, people's behaviour will be influenced by this possibility which exerts mental pressure. Whoever does not know what is known about him/her at a certain time, becomes self-conscious and loses the freedom to plan and to make free decisions.[25] Furthermore, the intimidation caused by informational predominance will not only effect individual development, but will also have an influence on common welfare. Self-determination is an elementary condition of democracy which is based on the possibility that everyone is able to act and to participate freely. Constitutional sovereignty should not undermine its own basic principles'.

Thus, the constitutional court decided that evaluation programmes for statistical purposes can only be used when it is impossible to catalogue certain persons by recording dates.

The general personality right (Article 2 para. 2 in accordance with Article 1 para. 1 GG) grants everyone the authority to decide on the abandonment and use of his/her personal data; everyone has the right of informational self-determination. Since then, every inquiry or application of data has to be explicitly allowed by a specific Act of Parliament,[26] thus with a legal basis or the consent of the affected

[22] Grundgesetz; Constitution.
[23] BVerfGE 54, P. 148 (153).
[24] Freely translated: 'Population Census Act'; BGBl I, S. 369, 25 March 1982.
[25] Tinnefeld /Ehmann, Einführung in das Datenschutzrecht, p. 44.
[26] According to the German constitutional law this relates to all rights which include a legal reservation. Only a few fundamental rights are granted without such a legal reservation. If the right is granted without such a reservation it is only possible to interfere with this right when there is a clash with another constitutional right, by creating a 'practical concordance', but not by means of another legal act. Mückenberger, KJ 1984, S. 9.

person. In a social community it is not possible to abandon the possibility to confine this right in order to protect public welfare.[27]

The population census judgment gave rise to the legislatures of the German Länder enacting their own Landesdatenschutzgesetz.[28]

9.1.3 The legislation within the federal state

In Germany the applicable law is created by establishing general rules for the citizens and the authorities by written laws. The rules do not describe the actual state of affairs in the present time or in the future, they rather tend to lay down obligations and prohibitions for everyone. The norms are general which means that they usually do not appeal to an individual case like a concrete judgment, but in fact to a non-specific number of citizens. Some acts modify constitutional rights, provided that the right comprises a legal reservation.

Germany consists of 16 German Länder, which all have state competence, derived from the federation. This federalism makes an allowance for the diversity in different regional distinctions.

The constitution gives both the federation and the states certain legislative competences. Article 70 para. 1 GG gives basic legislative competence to the German Länder and states that the federation is only competent when this is explicitly stated in the constitution. The federation has many explicit legislative competences, more, in fact, than any Länder.[29]

The federal legislator does not have jurisdiction for data protection in general. Therefore, the federal legislature has to concentrate its activities on enacting regulations concerning those issues within the scope of its legislative power.[30] The federal legislator is competent in questions relating to the secret service, the Military Counter-intelligence Service and passports, for example.

Some matters only belong to the federal competence if it is necessary to establish equal living conditions within the whole country (competing legislation Article 72 GG).

For other matters the federal government is competent to create a framework for rules which can be regulated in greater detail by the Länder (framework legislation Article 75 GG).

If the Länder and the federal government have enacted acts concerning the same matter, the federal law outranks the state law.[31] But at least the states can exercise the federal law according to their own responsibility (Article 30 GG).

[27] BVerfGE 65, p. 1 (45), PN 2004-189.
[28] State data protection acts.
[29] Jarrass/Pieroth, Pieroth, GG-Kom., Art. 70, Rn. 1.
[30] Rossnagel-Tinnefeld, Handbuch des Datenschutzes, 2.6, Rn. 10.
[31] Art. 72 GG highlights the 'strained relationship' which is inherent to a federal state. On the one hand, the federal government shall have legislative competence in the field of concurrent legis-

When the federal government does not have legislative competence, or has not yet made use of it, every state can create its own rules which are only relevant for that particular state.

This allocation of rights led to the fact that both the federal government and the states enacted data protection acts. The LDSG regulates only the protection of personal data within the range of data collection, processing or use by state authority of the Länder. Only in this field do the states have legislative competence. It is also possible to find data protecting norms in different state laws. For example, the Bavarian Erziehungs- und Unterrichtsgesetz[32] rules on the handling of data of school pupils. Bavaria also enacted rules which regulate the registration of statistics in Bavaria.

While the state laws in the field of data protection are directed towards the statistical authorities only and because merely a few rules relate to data privacy in the workplace, no further attention will be paid to them.

The tendency in the area of data protection is towards federal regulations. According to the aspect of a consistent single European market this applies to regulatory law, private law, industrial law and criminal law.

The legislature is bound by EU Community law, which means that it is not allowed to create regulations which conflict with Community Law and it also has to transpose EU Directives into national law.[33]

9.2 The Legal Basis of and Restrictions on Data Protection in the Workplace

As already pointed out, in Germany a special act for workplace privacy does not exist. Because the German legal system is based, next to constitutional basic principles, on written acts and decrees, workplace privacy itself can only be based on such written norms. A presentation of relevant regulations is therefore necessary.

Some acts contain norms which enable judges to constitute rules for workplace privacy. Some rules also have direct relevance to issues of workplace privacy.

9.2.1 Constitutional basic principles

Constitutional rights have effect as far as third parties are concerned, and, therefore, have to be respected by private persons, and, eventually, also within the employer-employee relationship. Thus, the employer has to pay attention to the right of informational self-determination in the course of data processing, for example.

lation if a norm is necessary for the whole country; on the other hand, the single states shall be as independent as possible; see Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, p. 96.

[32] Freely translated: 'Bavarian Educational- and Teaching Act'.

[33] Jarras/Pieroth, Pieroth, GG-Kom., Art. 70, Rn. 1.

9.2.1.1 *Allgemeines Persönlichkeitsrecht – the constitutional right to freely develop one's personality*

Different constitutional rights are deduced from this right.

Privat- und Intimsphäre – The Private sphere and privacy protection
Personal development shall be ensured by guaranteeing that the private sphere, the sphere of domestic freedom and the freedom towards the community will not be monitored by others.[34]

Recht am gesprochenen Wort – The rights according to the spoken word
Already in its 'Tonbandentscheidung' in 1973 the Bundesverfassungsgericht decided that the impartiality of human communication would be disturbed if everyone has to live with the knowledge that every single word one utters, maybe every thoughtless or uncontrolled comment, can be reproduced in a different situation and in a different context with the result that it can be used against the person who originally uttered that comment.[35] Today, case law agrees upon the principle that the rights according to the spoken word guarantee everyone, exclusively, the right to appoint the addressee of his/her spoken words.[36] The spoken word is also protected against secret tape recordings and against a supposition of words which no one actually uttered.[37]

Recht am eigenen Bild – The right according to one's image
The right according to one's image grants everybody the right to be the only person who decides if and how he wants to present himself towards others and to decide how and in how far a third person can assume one's personality.[38]

Recht auf informationelle Selbstbestimmung – Right of informational self-determination; Article 2 para. 2 according to Article 1 para. 1 GG
Emanating from the right of self-determination is the right to be the only person who decides when and within what scope one's personal circumstances of life will be revealed, unless this right is not restricted.[39]

[34] BVerfGE 27, p. 1, (6).

[35] BVerfGE 34, p. 238 (247); Biegel, 'Überwachung von Arbeitnehmern durch technische Einrichtungen', p. 25.

[36] BVerfGE 54, p. 148, (155).

[37] BVerfG 19.12.1991 in: Wedde, 'Schutz vor versteckten Kontrollen im Arbeitsverhältnis', *DuD* 2004, p. 21 (23).

[38] BVerfGE 35, p. 202 (220).

[39] BVerfGE 65, p. 1 (42). If a constitutional right is violated its commensurability always has to observed. That means that the desired purpose is allowed to be pursued. Pieroth/Schlink, Grundrechte, Rn. 279.

9.2.1.2 *Menschenwürde – human dignity*

According to Article 1 para. 1, first sentence GG, human dignity is indefeasible. Although some do not regard human dignity as a fundamental right, the Bundesverfassungsgericht classifies human dignity as such a right.[40]

What has to be summarised under the dignity of man can be negatively circumscribed. However, according to the 'Objektformel', the dignity of man will be violated if a human being is treated like an object.[41]

9.2.1.3 *Fernmeldegeheimnis – secrecy of telecommunications*

Article 10 GG is considered to grant a special constitutional right for data protection.[42] According to this right, a non-inscripted telecommunication is protected. This includes all individual communication by wired or wireless electromagnetic waves. This right will be violated if the content of a communication is listened to or read or if the transmission dates will be noted. The secrecy of telecommunications comprises the content of the telecommunication as well as the question of whether and how this communication has taken place. The purpose is to avoid any abuse of confidence by the transmitter.[43] This right is granted with a legal reservation, and can, therefore, be restricted by law.

9.2.2 **General legal principles**

While constitutional civil rights contain a general defence and claim rights against the state, general laws, including the obligations and prohibitions contained therein, have to be directly obeyed by everyone.

9.2.2.1 *Bundesdatenschutzgesetz (BDSG) – Federal Data Protection Act*

According to Article 1 para. 1 BDSG every single person should be protected from intrusions into their personal rights, especially the right of informational self-determination. In this respect, this basic right has gained a simple legal basis.[44]

The BDSG does not apply to actions which relate exclusively to familial or personal activities. Furthermore, any processing which makes no use of data processing equipment nor automated files is excluded.

Included is every type of data processing as long as it concerns personal data. These are, according to Article 3 para. 1 BDSG, particulars concerning the personal and objective circumstances of an identified or identifiable natural person.

[40] BVerfGE 15, p. 249, (255).
[41] BVerfGE 9, p. 89, (95); 57, p. 250, (275).
[42] OVG Bremen, CR 1994, 700 ff; Rossnagel-Rieß, Handbuch Datenschutz, p. 1025.
[43] Rossnagel-Rieß, Handbuch Datenschutz, 6.4, Rn. 12.
[44] Simitis, BDSG-comm., Art. 1, Rn. 29.

It is furthermore assumed that no public authority will be the collecting authority; otherwise the local state law has to be applied.

The BDSG only concerns absorbing law which means that more special federal regulations override the BDSG according to Article 1 para. 4 sent. 1 BDSG.

According to the BDSG, data may only be collected, stored or processed if there is legal authorisation for this or an effective consent according to Article 4 para. 1 BDSG. Explicitly, the processing of personal data is acceptable for business purposes (Article 28 BDSG), which is also the case for employment contracts.

The condition which enables the collection, storage or processing is that it is justified by the purpose and that contact with the data for this purpose is suitable and required[45] and the recognised interests of the persons concerned are not transgressed. If personal data is collected, according to Article 28 para. 1 sent.2, the purpose for which the data is collected has to be clearly determined in advance. It is prevailingly assumed that the purpose of collecting data in employment relations has to exceed the employment relationship.[46] The law does not give further details concerning this employment relationship; this is why guidelines given by the constitution have to be relied upon to fulfil the aims of the law.[47]

If data is, collected, according to Article 3a BDSG, the principle of data care and data prevention has to be observed. According to this principle, data may only be collected, processed or used if that is absolutely essential. If the collection cannot be avoided, dates need to be made anonymous or used as a pseudonym, insofar as the purpose can be attained in this way.

Article 6b BDSG has been newly introduced in 2001. This article legitimises the video supervision of publicly accessible areas. This includes business premises, train platforms or exhibition rooms in museums, but not factory floors.[48]

Video surveillance can only be licit if this is essential for a public authority to fulfil its tasks, if an injunction to stay away from certain premises cannot be enforced in another way, or if the surveillance serves legitimate interests for specifically stated purposes.

According to this provision, an employer can monitor according to the 2nd and 3rd alternatives, if ideal or economic interests cannot be protected by other means.

According to Article 6 para. 3 BDSG, the further processing and use of the collected data has to be connected to the original purpose. This can result in the collection of video data itself being legitimate while the processing or transfer of that data will be illegitimate because of the lacking purpose connection.[49]

[45] Erfurter-Kommentar, § 160, BDSG, Rn. 2.
[46] Däubler, 'Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht', *NZA* 2001, p. 874, (875).
[47] Däubler, Gläserne Belegschaft, Rn. 69.
[48] BT-Drs. 14/4329, p. 38.
[49] Simitis, BDSG-comm., Art. 6b, Rn. 75.

Fortunately, the targeted transparency obligation in Article 6b para. 2 BDSG states that video surveillance has to be marked by practical measures, so that the persons concerned can prepare themselves accordingly.[50]

A previous control shall prevent the possibility of the creation of human profiles from different video surveillances which would mean a massive intrusion with privacy.

The BDSG also contains regulations which shall ensure that the requirements of the BDSG itself, as well as those of other data protection laws, are complied with.

On the federal level the public authorities of the federal administration shall create an independent third authority under Article 24 BDSG. This 'Bundesbeauftragte für Datenschutz'[51] is established by the federal parliament according to Article 22 BDSG, following a proposal by the federal government. The tasks of this commissioner include ensuring confidential contact with the data of citizens and proposing the enhancement of this protection.

Every two years, the representative has to present a report on his activities enabling the Deutsche Bundestag[52] to obtain an overview concerning data protection. Furthermore, the representative is also obliged to consider different views and opinions on data protection, if this is requested by the Bundestag or the Bundesregierung.[53] Everyone who is worried about a potential infringement of his rights by a public authority using his data can address the representative (Article 21 BDSG).

In the private sector the compliance with data protection regulations shall be observed by the privates themselves. Since 1977 Article 4f BDSG obliges companies and enterprises to establish an operational Commissioner for Data Protection [Datenschutzbeauftragter], if the company has at least 5 employees working with automated data processing or at least 20 employees, but no automated data processing.

The duty to appoint a commissioner for data protection has in the meantime been extended to the public administration.

> 'The Commissioner for Data Protection is a person who functions under the personal responsibility of enterprises and who monitors the data protection and data securing measures as an instance of internal control. Even before this person was incorporated into the BDSG in 1977 a significant number of enterprises had voluntarily appointed someone in charge of data protection. At this time this person was mainly charged with data security. After a while it transpired that it was necessary and reasonable to create a uniform central authority to be able to assert, co-ordinate and monitor appropriate measures.[54] This development created a person who became the vanguard of data protection by self-monitoring'.

[50] Simitis, BDSG-comm., Art. 69, Rn 66;see also *supra* n. 47, Rn. 307.
[51] Freely translated: 'Federal Commissioner for Data Protection'.
[52] Lower house of the German parliament.
[53] Federal Government.
[54] Schlemann, Recht des betrieblichen Datenschutzbeauftragten, 1996, p. 37.

When the BDSG was revised in 1991 the legislature dispensed with the creation of external control by public authorities.[55] Therefore, qualifications to be able to function as a Commissioner for Data Protection are pretty high. The interested person needs to have expert knowledge and has to be absolutely reliable. The responsibility for the misuse of data remains with the employer, which makes it impossible to pass this responsibility on to the Commissioner. The Commissioner is not under the control of the employer. The person in question may emanate from the company itself although this is not necessarily so. It is important that the work of the Commissioner for Data Protection does not clash with the interests of his/her employment.[56] For example, the leader of the data processing office or the legal department is suitable for the post,[57] because his/her independence is not guaranteed. The employer has the duty to help the Commissioner by supporting his work as much as possible. The tasks of the Commissioner are described in Article 4g BDSG which states (freely translated):

> '(1) The Commissioner for Data Protection will ensure that this law and other regulations on data protection are obeyed. (...). In particular he has
> 1. to monitor the proper use of data processing programs when they are used for processing personal data; for this reason he has to be informed in good time about the intention to use automatic data processing programs for personal data;
> 2. to familiarise the person who processes personal data (...) with the special needs of data protection'.

If the Commissioner for Data Protection doubts that 'his' enterprise does not observe the rules for data protection, he can appeal to the regulatory authority (Article 4g para. 2 BDSG). This public agency is charged with ensuring that the law is obeyed with regard to data protection.

It further controls the self-control of the enterprises. The legislature did not want to dispense with the possibility to control the work of the Commissioners.

If a company or public authority does not adjust the function of the Commissioner for Data Protection, or does not adjust it in the right way, it is possible to impose a fine about 25,000 Euro (Article 43 para. 1 No. 2 BDSG). Because it is costly to adjust the function of the Commissioner many institutions which are bound to adjust this function have not in fact done so. It is assumed that only one third of companies employ a reliable Commissioner.[58]

If any person suffers damage as a result of the unlawful use of data, the agency has to compensate this damage (Articles 7, 8 BDSG). A person can also incur a penalty when it wilfully does not observe the rules (Article 44 BDSG).

[55] Simitis, BDSG-comm., Art. 4f, Rn. 1.
[56] BAG, DB, 1994, p. 1678.
[57] Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, p. 408
[58] Schlemann, Recht der betrieblichen Datenschutzbeauftragten, p. 91.

9.2.2.2 *Landesdatenschutzgesetze (LDSG) – State Data Protection Acts*

After the creation of the BDSG in 1977 every land enacted its own LDSG. The LDSGs govern only data protection concerning the processing of personal data by a state's own public agency, for example, the local authorities. Because the federal government does not have legislative competence for the state public administration, it was not able to enact regulations for those state authorities with the BDSG. The regulations in the LDSG have mostly been adapted by those of the BDSG; the protection standard is even higher.[59]

It is worth noting that every state enacted regulations which commit themselves to appointing a 'State Commissioner for Data Protection' [Landesdatenschutzbeauftragter]. This person has similar duties to the Federal Commissioner for Data Protection. This shows that compliance with the data protection law is, for the welfare of the citizens, important for the state governments as well.

9.2.2.3 *Information- and telecommunications acts*

The fairly new telecommunications acts, the TKG,[60] the TDSV,[61] and the TDDSG[62] aim to develop the precise goals of the BDSG.[63] As these regulations are more precise they complement the rules of the BDSG which is only applicable if the more special laws do not regulate specific questions.

Some laws contain special data protection provisions for providers of a teleservice. According to the prevailing opinion, also the employer is such a provider of teleservices in terms of the TKG, TDSV and TDDSG, provided that the employer allows his employees to use the telecommunication facilities for private purposes. Unfortunately, the employer is not classified as a provider of teleservices (Article 1 No. 1 TDDSG) if he allows the employees to use the telecommunication service exclusively for work purposes, precisely because in this case the employer offers the service for himself only and not to a third person as the law calls for. Otherwise, the discussion about the legitimacy of surveillance by the employer would be obsolete, because such surveillance would only be legal under the guidelines of the telecommunication laws.[64] Employees who do not have permission to use the telephone or internet for private purposes depend on the regulations of the less strong BDSG and constitutional rights.

[59] See *supra* n. 47, Rn. 49.

[60] Telekommunikationsgesetz, BGBl 1996, 1120, last amended by Art. 221, 25 November 2003, I 2304; freely translated: Telecommunications Act.

[61] Telekommunikations-Datenschutzverordnung, BGBl I 2000, 1740, last amended by Art. 2 G, 9 September 2003, I 1590; freely translated: Telecommunications-Data Protection Ordinance.

[62] Gesetz über den Datenschutz bei Telediendsten, BGBl I 1997, 1870, 1871, modified by Arts. 3 and 4 para. 3 G, 14 December. 2001, I 3721; freely translated: Act on Data Protection in Teleservices.

[63] Simitis, BDSG-comm., § 28, Rn 5.

[64] Bizer, 'Die dienstliche Telekommunikation unter dem Schutz des Fernmeldegeheimnisses', *DuD* 2001, p. 618; Wedde, 'Schutz vor verdeckten Kontrollen im Arbeitsverhältnis', *DuD* 2004, p. 21 (22).

Article 85 TKG and Article 1 TDSG state that the providers of telecommunication services are not allowed to acquaint themselves with the content or the circumstances of any communication process.

They are only allowed to explore and record those dates which they absolutely need to perform their business services. The provider is bound to keep all dates which are connected with the communication secret, because the Fernmeldegeheimnis of Article 10 GG [secrecy of telecommunications] has been expanded to cover the relationship between a provider and user under Article 85 TKG.[65]

The provider needs to adjust appropriate protection measures, Article 87 TKG. This not only technical surveillance facilities, but also organisational measures which are able to ensure, that the principles will be respected.[66] If data collection is permitted, Article 4 TDDSG states that the principle of spare data use has to be respected. Personal data need to be used anonymously as long as it is possible to attain the goal of the contract with anonymous data.[67] It is only permitted to collect data when this is necessary to itemise a bill, for example. Dates which are not essential have to be deleted.

9.2.2.4 *Betriebsverfassungsgesetz (BetrVG)*[68] *– Works Council Constitution Act*

The Betriebsverfassungsgesetz shall ensure the independent representation of employees' interests. This aim was first discussed in the Frankfurter Nationalversammlung 1848[69] and culminated with the creation of the BertrVG.[70] The elementary data protection regulations were integrated into the BetrVG without any changes. The main provision is that an enterprise will have a works council (on employees' committee).[71]

> 'According to the BetrVG enterprises which employ more than 5 persons have to elect an employees' council every 4 years. Everybody who works for that enterprise can be elected there of. The employees' council is the agent of all the employees by law.[72] At

[65] Büttgen, 'Ein langer Weg – Telekommunikations-Datenschutzverordnung endlich in Kraft', *RDV* 2001, p. 6, (7).

[66] Beck'scher TKG-comm./Ehmer, Art. 87, Rn.18.

[67] Simitis, BDSG-comm., Art. 28, Rn. 6.

[68] Freely translated: Works Council Constitution Act; BGBl I 1972, modified by the announcement of 25 September 2002, I 2518, further modified by Art. 81 G, 23 December 2003, I 2848.

[69] The Frankfurter Nationalversammlung [German national assembly] was the parliament which was elected by all states which belonged the German federation after the outbreak of the revolution in 1848; The assembly met on 18.5.1848 in Frankfurt am Main, the domicile of the Deutschen Bundestag, in the Paulskirche (church) to discuss the constitution.

[70] Däubler/Kittner/Krebel, BetrVG-comm., Einleitung, Rn 1.

[71] Rossnagel-Wedde, Handbuch Datenschutz, 6.3, Rn. 10.

[72] Erfurter-comm., § 220 BetrVG, Rn 6.

the employer's own expense the employees' council has to be trained as regards rights and duties. The committee has some rights of co-determination towards the employer. If the employer does not comply with these rights, the implementation of a provision without the employees' council's agreement is not effective, for example a dismissal. If the council does not agree, the employer has to resort to the courts to obtain permission to implement such a provision. If the employer does not comply with the rights of co-determination in the area of data protection, it is not permitted to use those date and they have to be deleted, § 35 BDSG'.[73]

According to Article 74 para. 2 BetrVG, the employer is additionally obliged to enhance the free development of employees' personality. Compliance with this duty will be by the council, Article 80 para. 1 no. 1 BetrVG. The employees' council also has to supervise the compliance of the employer with the data protection norms, and the committee further oversees and supports the equal treatment of all employees.

In the field of workplace privacy the most important norm is Article 87 para. 1 no. 6 BetrVG. This article grants the works council the right of co-determination when the employer wants to introduce technical facilities which are intended for monitoring the conduct of employees or their efficiency at work. The council cannot ask for such facilities and is further not able to prohibit them in their entirety,[74] but the least infringing means of surveillance can be claimed.

Worth mentioning is also Article 94 BetrVG. According to this article the works council has a right of co-determination when the employer uses a personal question sheet. This guarantees employees the possibility to influence the questions which job applicants will be asked.

The right of co-determination can be enforced by the works council by applying for an interim injunction. The use of surveillance facilities can then be prohibited by law. The employees also have a right of retention according to their work without losing their wage entitlement.[75] The employees' council can resort to the controlling institution which, as a state authority, is in charge of supervising compliance with the data protection law, Article 38 BDSG. However, the council is first bound by the principle of peaceful settlement to try to settle any dispute amicably with the employer.

9.2.2.5 *Fiduciary duty of the employer deriving from Article 611 BGB*

The fiduciary duty is an accessory obligation resulting from the contract of employment, therefore as a duty deriving from Article 611 BGB and from the principle of

[73] Gola/Klug, 'Die Entwicklung des Datenschutzes in den Jahren 2002/2003', *NJW* 2003, p. 2420, (2424).

[74] Bijok/Class, 'Arbeitsrechtliche und datenschutzrechtliche Aspekte des Internet-Einsatzes', *RDV* 2001, p. 52, (55).

[75] See *supra* n. 47, Rn. 822.

utmost good faith laid down in Article 242 BGB. The employer is therefore bound to preserve the freedom of action and the personal integrity of the employees. In the case of any infringement the employee may seek damages or an injunction.

9.2.2.6 *Criminal issues*

According to Article 201 StGB[76] a person who records a non-public spoken word on a sound storage medium or eavesdrops on this with a listening device will incur a penalty. The permitted facilities which telephones have and which make it possible to listen in are not considered to be such listening devices in the sense of the law.[77]

A person who obtains access to data which are not meant for him or have been specifically protected against unauthorised access will be prosecuted, Article 202a StGB. An employee working at a post office or with a telecommunications provider may be penalised when he discloses facts which are subject to a restriction under the 'Fernmeldegeheimnis'.

9.3 Agreements

In principle the employee can agree to his rights being restricted. Nowadays, special agreements are usually made in employment contracts, in works council agreements or in collective agreements which legitimise interference with employees' rights by the employer.

9.3.1 **Employer/works council agreement; collective labour agreements**

Works councils, as a result of their right to co-determination, are in a position to enter into agreements about issues relating to the enterprise. Therefore, those agreements are 'other regulations' in terms of Article 4 BDSG. These regulations can digress from the regulations of the BDSG. The same is true for questions relating to the enterprise which are arranged in collective agreements. A collective labour agreement is, according to Article 1 para. 1 TVG,[78] a contract between one or more employers or employers' associations and a labour union, to regulate the rights and duties of the parties.[79]

[76] Strafgesetzbuch, RGBl 1871, 127, amended by the announcement of 13 November 1998, I 3322; last amended by Art. 1 G, 27 December 2003, I 3007.

[77] BGHSt 39, S. 335, (343); *NJW* 1994, p. 596 ff.

[78] Tarifvertragsgesetz, WiGBl 1949, 55, amended by the announcement of 25 September1969, I 1323; amended by Art. 175 V, 25 November 2003, I 2304; Freely translated: Collective Labour Agreement Act.

[79] Däubler, Arbeitsrecht, Rn 82ff.

The competences of the works councils are restricted by the already mentioned duty to protect the personal rights of the employees. They are, for example, not competent to agree on complete surveillance of employees' effectiveness. The works council is rather charged with positively influencing the working conditions and working towards free personal development.[80] It further has to comply with the principle of adequate measures (commensurability), otherwise the agreements have no legal effect.[81]

Also the parties to the collective arrangement are bound by the general law, the constitutional law and the basic principles of employment law.

9.3.2 **Consent**

The possibility of waiving one's constitutional rights connected to data privacy is accepted.[82] Therefore, the employee can agree to restrictions of his constitutional right of personal freedom. If the waiving of these rights goes beyond the sense of fairness according to applicable moral concepts (Article 138 BGB) or violates human dignity, it will be improper. In principle, the consent does not have to meet formal requirements. However, the consent is only effective if it was given on an unsolicited basis, without any pressure or force.[83] The consenting person has to be fully informed about the consequences of its action and, therefore, the dimension of the planned measures has to be exactly defined by the employer.[84]

Difficulties arise with regard to the question of how to deal with unsolicited agreements with job applicants. As the number of unemployed persons is continually increasing (there are currently more than four million unemployed in Germany), the applicant is under great pressure, and is, therefore, not able to decide freely. In order to get the job the applicant may accept any restrictions of his rights.[85] Some voices in the literature are of the opinion that consent which has been given upon the conclusion of an employment contract will only be effective if the person had the possibility to choose freely.[86] Other experts hold that the employee generally lacks the independence to decide freely, thus the applicant is never able to consent to restrictions of his personal rights.[87]

[80] Wedde, 'Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht', *DuD* 2004, p. 169 (173).

[81] BAG vom 7 November 1989, AP No. 46 zu Art. 77 BetrVG 1972.

[82] Beckmann, 'Probleme des Grundrechtsverzichts', *JZ* 1988, p. 57 (58).

[83] BVerfG of 18 August 1981; *NJW* 1982, p. 375, II 1. Here the BVerfG decided that the suspected person was not able to agree to a lie detector test because that consent was given under pressure; a denial might have given the impression that the person had something to hide, PN 2004-191.

[84] Münchner-comm. ArbR-Blohmeyer, Art. 53, Rn.34.

[85] Wedde, 'Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht', *DuD* 2004, p. 169 (171).

[86] See *supra* n. 47, Rn. 152; Wedde, 'Die wirksam Einwilligung um Arbeitnehmerdatenschutzrecht', *DuD* 2004, p. 169 (172).

[87] Data Protection Commissioner for Hamburg, Hamburger DSB, 18 TB, p. 197.

Also the federal legislator has recognised this problem and, therefore, has standardised the requirement of effective consent in data processing, data storage and data analysis. Article4a BDSG states:

> 'Consent is only effective when it is based upon a free decision of the person in question. That person has to be informed about the purpose of the data processing and usage, and, further, if required according to the circumstances of the individual.
> The consent needs to be in written form, unless special circumstances (…)'.

Even if the job applicant has given consent in written form, its effectiveness is doubtful. Others are of the opinion that it is impossible to remove from the applicant the possibility to agree, as this in itself relates to the right of informational self-determination.

Workplace privacy has reached a pretty high standard, although it lacks a specific law concerning this issue. Indeed, the employer needs to rely on prevailing case law. The consequences resulting from the application of the presented acts, regulations and basic principles will be depicted in what follows.

9.4 Data Privacy at the Application Stage

At the application stage a confidential relationship between the applicant and the employer will emerge from the 'preliminary agreement stage' (culpa in contrahendo). This can already constitute additional obligations and damage claims. Since the new formation of the BDSG this is applicable to those preliminary agreement stages as well. Already at the application stage the employer has to respect the regulations of the BDSG. According to the BDSG, the storage or use of data is prohibited unless it is necessary for the purpose of the contract. As this earmarking for a specific purpose is not defined, the constitutional rights and the accepted guidelines provided by case law can eventually help in the interpretation of these requirements.[88]

9.4.1 **Questions which are allowed to be asked**

In contract negotiations dealing with potential employment the object of the agreement is a person in contrast to acts of sale. The interest of information concentrates on personal things. Not only because of the high pressure of competition, the job applicant may feel that he/she is being forced to answer questions which, according to objective standards, interfere with his/her personal sphere. A limitless right to ask questions would also lead to a further selection according to the 'perfect employee'. The Bundesarbeitsgericht (BAG) [Federal Labour Court] realised this problem and tried to protect the employees. The Court found that the fundamental rule

[88] See *supra* n. 47, Rn. 183.

was that employers are only allowed to ask questions whose answers are likely to produce facts about the applicant which are essential to the employer and he has a qualified and legitimate interest in asking such questions.[89] The reason for this has been the possible impact on the personal rights of the job applicant. Employers can only have a legitimate interest in facts which can have an influence on the employer/employee relationship or might influence the efficiency of the company.

According to this principle questions which refer to the applicant's living conditions, public activities, family background, free time activities or friends cannot be included. Prohibited are also questions about certain illnesses which are of no interest to the work in question.[90]

The question about an HIV infection is only allowed if by doing work there is a danger of passing it on to others (care work, working with food).[91] The prevailing opinion and case law state that questions relating to AIDS are permitted, because there is no possibility of a cure and the permanent total disability is measurable.[92] Questions concerning a police record are allowed if they are relevant to the kind of work in question.[93] Questions which might give rise to a suspicion of discrimination, for example questions about religious confession, party affiliation, or the membership of certain organisations (labour union), are not allowed because the freedom of association is guaranteed in Article 9 para. 3 GG.

The case law on asking about pregnancy at a job interview has been the subject of development. Ten years ago, the BAG held that this question was permissible. Under European pressure the BAG had to abandon this legal practice.[94]

> 'In 1961 the BAG decided that the employer has an extensive economic interest in asking this question because of the financial burden resulting from maternity protection.[95] Although Article 611a BGB had been enacted which established a prohibition on sex-specific discrimination, the BAG did not deviate from this decision.
> Article 611a BGB was enacted because an EU Directive forced the legislature to do so. At the request of a Dutch court in 1990 an interlocutory decision was delivered by the European Court of Justice according to directive 76/207/EWG on which Article 611a BGB is also based. The European Court of Justice decided that the rejection of a pregnant applicant only because of the financial burden emanating from the pregnancy would be illegal direct discrimination. In this context it is also of no interest if, in general, only women would apply for the job'.[96]

[89] BAG, *NZA* 1986, p. 739.
[90] BAG, *NZA* 2001, p. 1241.
[91] Keller, 'Die ärztliche Untersuchung des Arbeitnehmers im Rahmen des Arbeitsverhältnisses', *NZA* 1988, p. 561 (563).
[92] Heilmann, 'Aids am Arbeitsplatz', *BB* 1989, p. 1413 (1414).
[93] BAG, AP, Art. 2 to Art. 123 BGB in: Wolfgang /Däubler, GB, Rn. 217; BAG, NZA 1999, p. 975.
[94] BAG judgment from 15 October 1992, 2 AZR-27/92, DB 1993, p. 435.
[95] BAG 11, p. 270 (273) in: *NJW* 1962, p. 74 (75).
[96] EuGH, Urteil 8 November 1990 –RsC- 177/88 in: *NJW* 1991, p. 628.

According to the case law it is permissible to ask a job applicant if he is an invalid.[97] The 'invalid law' assigns many different duties on the employer which tends to place a high burden on employers. Controversially discussed in the literature is whether this legal practice has to be abandoned in accordance with the EU Directive on equal treatment in employment (2000/78/EG).[98]

If an improper question is asked, the job applicant does not have to disclose the truth. The employee does not have to fear any negative consequences because of this lie. The employer is not allowed to dismiss a person who has not disclosed the truth when faced with an improper question.[99]

9.4.2 Medical and psychological examinations

The number of medical check-ups for new employees is growing rapidly in Germany. The grey area between necessary check-ups and those which are only designed to disclose health risks is estimated to be high by the parliamentary Enquiry which was set up by the German Bundestag.[100]

The legitimacy and the extent of those check-ups are not regulated by law. Some laws,[101] collective agreements and some rules for accident prevention by the Employers' Liability Insurance Association state that medical examinations need to be carried out before the recruitment of personnel. Thus those rules do not protect the employer concerning the medical examination of job applicants, they only protect employees. Such a right for the employer does not emanate from the preliminary agreement stage either. The preliminary agreement stage only compels the parties to reveal those facts and circumstances which are able to frustrate the employment contract.[102]

If a person's state of health does not allow him to fulfil the job, the person in question has to reveal this fact. If only a small possibility exists that an illness, which would make the person unable to do the corresponding work, might break out in the next few years, the employee does not have to reveal this fact. The employer rather has the possibility to compensate for this risk when setting the wages. In almost the same manner a previous examination cannot ensure that the employee

[97] BAG, *NZA* 2001, p. 315; BAG, *NZA* 1999, p. 584; BAG, *NJW* 1994, p. 1369.
[98] On this see Messingschlager, 'Sind Sie schwerbehindert? Das Ende einer (un)beliebten Frage', *NZA* 2003, p. 301 ff., against see Schaub, 'Ist die Frage der Schwerbehinderung zulässig?', *NZA* p. 299ff.
[99] Schatzschneider, 'Die Frage nach der Schwangerschaft und gemeinschaftsrechtliches Diskriminierungsverbot', *NJW* 1993, p. 1115.
[100] 'Gentechnische Diagnostik und Arbeitsmedizin' der Expertenanhörung der Enquete-Kommission „Recht und Ethik der modernen Medizin' des Deutschen Bundestages, Themengruppe 3 (Gentechnische Daten), 4 December 2000, p. 5.
[101] Compare: Art. 18 para. 1 Bundesseuchengesetz, freely translated: 'Federal Epidemic Protection Act'; Art. 10 para. 1 No.1, Druckluftverordnung, freely translated: 'Air Pressure Decree'; Art. 67 para. 1 Strahlenschutzverordnung, freely translated: 'Radiation Protection Act'.
[102] Notz, 'Zulässigkeit und Grenzen ärztlicher Untersuchungen von Arbeitnehmern', p. 36.

will not have an accident. In any event the medical examination of future employees will mostly take place with the prior consent of the applicant. It has already been mentioned, however, that such consent is questionable.

Anyway, lawyers agree on the opinion that the employer's right to inquire is confined to the same extent as the right to question the applicant as to facts which are important for the respective work. It is at least prohibited to search for specific illnesses. The physician has respect professional secrecy as well and is not allowed to furnish a third person with the results of medical diagnosis. He is only authorised to provide a general assessment regarding the suitability of the applicant for the respective job.[103]

The same principles also apply to psychological testing. Due to the strong influence on the personal sphere, only personal attributes which are relevant for the job are allowed to be tested and the medical practitioner is only allowed to provide a general assessment.

A DNA analysis is deemed to be a special case. Scientist differentiate between genetic sequencing which has the purpose of mapping the entire human genome and DNA analyses which have the purpose of disclosing single characteristics. Genetic sequencing is not considered to be very important[104] in practice and it is not considered that it will become so in the future.[105] People speculate, though, that the interest in DNA analyses will increase substantially as soon as examinations become cheaper.[106]

Basically regulations on the legitimacy of DNA analyses during the application procedure do not exist. Only a few exceptions are regulated. Some preventive medical check-ups are mentioned by Employers' Liability Insurance Associations and biomonitoring is referred to in the Gefahrstoffverordnung.[107] If a person has to work with benzene (G 8) a chromosome analysis is recommended and when a person carries out 'driving activities' (G 25) a 'colour sense test' is recommended.[108]

Unfortunately, after the new draft the current version of the BDSG also does not contain any legal regulations concerning the legitimacy of DNA analyses when selecting applicants stage.

According to the prevailing opinion, Gene-analyses are prohibited.[109] In this context the Bundesverfassungsgericht[110] decided that everyone has the 'right to know one's own ancestry'. It is possible derive from this precedence, that the ge-

[103] Erfurter Kommentar/Preis, Art. 230, Art. 611, Rn. 367; Keller, 'Die ärztliche Untersuchung des Arbeitnehmers im Rahmen des Arbeitsverhältnisses', *NZA* 1988, p. 561 (563).
[104] Ross, 'Gentechnik –Chancen und Risiken', *AuR* 2001, p. 121 (123).
[105] See *supra* n. 100.
[106] See *supra* n. 104.
[107] Freely translated: Dangerous Substance Decree.
[108] See *supra* n. 100, p. 6,7.
[109] Ross, 'Gentechnik- Chancen und Risiken', *AuR* 2001, S. 121; Weichert, 'Der Schutz genetischer Informationen', *DuD* 2002, p. 133 (144).
[110] BVerfGE 54, p. 148, (153); BVerfGE 80, p. 367 (373).

netic fundament is one of the basic elements of personal rights.[111] Therefore it is part of the private sphere, which is absolutely meriting protection. The danger to become a 'transparent x-rayed observation object' by being catalogued is too high. Besides, by such examinations the possibility of an efficiency-oriented selection is created.

According to the literature the fact that, due to certain examinations, the outbreak of a particular disease might be prevented has not gone unappreciated. A great importance for genetic examinations can be found in the clarification of genetic reactions to specific substances that are important for the respective employment. But even such preventive methods are criticised. Genetic examinations give rise to the danger that some employees would simply disappear from the market.[112] The job should match the employee and not the employee the job. Therefore employers have the duty to improve working conditions and not to improve the employees by medical selection. Furthermore, it cannot be ensured that other 'job-neutral' illnesses are not revealed against the wishes of the employee.

According to the literature a DNA check of new employees is prohibited, but as prohibiting laws do not exist and the courts have not yet been able to take a firm stand, the employer who asks for a medical examination does not have to be afraid of any consequences. If he wants to get the job, the applicant will usually not have the possibility to refuse an examination. The Parliamentary Enquiry therefore argued that such check-ups at the application stage lack a preventive character and need to be prohibited by law. The employer has an information interest provided by his constitutionally granted commercial freedom of action (Article 12 para. 1 GG). But this interest does not overweigh the more sensitive rights of the applicant. The federal prosecutor for data protection [Bundesbeauftragter für Datenschutz] therefore advocates penal provisions.[113] Some even advance the opinion that the state legislature has the duty provide protective laws as a result of the 'gene self-determination right'.[114]

9.4.3 Data collection with respect to third persons

The BAG states that employers are allowed to help other employers to protect their interests under the aspect of social partnership.[115] Information about former employees might therefore be disclosed to the respective employer even against the will of the respective employee.

This right to disclose information only goes as far as the right to question the applicant. The protection of the employee by the restricted right to ask shall not be undermined by the right to disclose information to another employer.

[111] Ross, annotation to VGH Baden-Würtemberg Urteil vom 28 November 2000 – PL 15 S 2838/99 in: *AuR* 2001, p. 469, (472).
[112] Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, p. 26.
[113] 19th Activity Report 2001-2002.
[114] Ross, annotation to VHG Baden-Würtemberg judgment from 28 November 2000, *AuR* 2001, p. 469 (472).
[115] BAG judgment from 25 October 1957, AP BGB, Art. 630 No. 1.

9.5 Data Protection in the Course of Employment

The occasional surveillance of working behaviour by senior staff or colleagues is an unavoidable restriction of the personal sphere, resulting from the work process. The employer definitely has the right to control employees with respect to their duties and to the agreements emanating from the employment contract.

It is assumed that the employee has agreed to such obvious restrictions by concluding the employment contract. But this consent does not include secret or complete surveillance.

If the employer monitors the workforce the legality of the surveillance is controlled by the applicable laws. If, in special cases, a law does not exist, or has to be interpreted, the courts will take constitutional rights into account.

The employer is not allowed to present illegally obtained information before the court.

9.5.1 Surveillance of telecommunications

As already mentioned, the legality of telecommunication surveillance has to be seen in accordance with special laws, presuming that the employer has allowed his employees to use telecommunication facilities for private purposes. According to Article 85 TKG, employees are protected in that the employer is not allowed to make information available about the content or the circumstances of any communication (telephone or internet). It is only allowed to collect data which are necessary to provide the service, e.g., the amount of phone units used, but not the dialled phone numbers.

According to the use of the internet and e-mail, an employer is allowed to collect certain data, e.g., sending and receiving times, the size of sent files, as long as those data are necessary for the service to be provided, e.g., for accounting purposes. Otherwise he is not allowed to collect any content or access data. By recording phone calls or installing surveillance facilities the employer will usually not receive any information which he needs to provide the telecommunication service. Therefore those monitoring systems are generally illegal.

Exceptionally, greater surveillance is allowed if there is a strong suspicion that the telecommunication facilities are being abused. If the employee acts against his obligations emanating from the employment contract or if he commits infringements of copyright or 'software piracy', or if he has gained access to hardcore pornography (for example, pornography involving children), or if he is suspected of having betrayed the company or giving away business secrets, the employer is allowed to collect data which go beyond the secrecy of telecommunications under Article 85 TKG.[116]

[116] Weißnicht, 'Die Nutzung des Internet am Arbeitsplatz', *MMR* 2003, p. 448 (450).

If private use is prohibited or the telecommunication acts do not regulate a private question, the data collection needs to comply with § 28 Abs. 1 BDSG, which allows data collection for a sufficient purpose if the interests of the employees do not prevail. If the interests of the employer and the personal rights of the worker conflict, the courts will try to solve this problem by balancing the interests under the principle of commensurability. In any case, complete surveillance is justified to solve offences which have been committed, the betrayal of trade secrets or, for example, sexual harassment by e-mail.[117] Surveillance for other reasons has to be judged according to that particular case.

Telephone surveillance

The employer's interest in monitoring employees' phone calls is increasing because of the added use of Call-Centres and similar institutions. From 1995 to 2000 telephone monitoring trebled in Germany.[118] Anyhow at least 10 per cent of phone calls in this field are monitored as employers consider this to be their right of quality assurance.[119] Often the employees and employers will enter into agreements on the right to monitor phone calls whereby the effectiveness of the employee's consent is questionable. But when there is no agreement employers still attempt to control phone calls. If the TKG is applicable, of course such, actions are illegal.

If private use is not permitted, the telephone tapping needs to be in line with the BDSG and the employees' constitutional rights. Concerning the illegality of phone tapping, the courts' decisions vary. The labour courts as well as the constitutional court share the opinion that the legality of phone monitoring has to meet the provisions of the constitutional right according to one's spoken word.[120] It is undisputed that this private right is even applicable to official or business calls.[121]

While the protection accepted by the constitutional court is very comprehensive, the BGH, which is the highest court in civil matters, has decided that not every case of phone monitoring breaches the caller's personal rights.

Case BGH, judgment of 17 February 1992 – *NJW* 1992, p. 1397 ff:[122]

'The BGH decided that a witness, who had listened to a phone call made by the parties, could be heard before the court. In this phone call the question was discussed

[117] Bijok/Class, 'Arbeitsrechtliche und datenschutzrechtliche Aspekte des Internet-Einsatzes', *RDV* 2001, p. 52 (54).

[118] Opaschowski, 'Quo vadis, Datenschutz? Die Angst vor dem Datenklau breitet sich aus', *DuD* 2001, p. 678 (680), with reference to a B.A.T. survey.

[119] See *supra* n. 7.

[120] Cases: BVerfG, AP No. 24 regarding § 611 BGB; BAG 29.10.1997 – 6 AZR 508/96 in: *DB* 1998, p. 371.

[121] BVerfG resolution from 19 December 1991 – 1 BvR 382/85 in: *NJW* 1992, p. 815.

[122] PN 2004-192.

whether one party had agreed to an abrogation of a lease contract for a flat. The witness had listened to the call using the speaker of the phone system without telling anybody. Because the parties only talked about business, the BGH said that the caller's personal right had not been violated by the witness. Nowadays, in the age of modern telecommunications, everybody needs to be aware that people use such facilities in order to listen to phone calls. Only if the secret listening in of the witness had been malicious would she not have been able to be heard before the court'.

Case BAG, judgment of 29 October 1997 – *NZA* 1998, p. 307 ff:[123]

'In this similar case the parties argued about the amount of wages which the claimant (C) had earned for her work as a prompter in a theatre. When C spoke to her employer about the employment and the wages on the phone her husband listened to the call via the speaker. C said in court that the assistant had promised her on the phone that she was entitled to a wage of 3500 German Marks per month.
Her husband, who had listened to that phone call, was not allowed to be heard before the court. The BAG stated that evidence given by the claimant's husband was not admissible, because the secret listening in had violated the employer's constitutional personal rights'.

Whoever listens in on an official call cannot base a dismissal on the information that was received that way.

Case BVerfG, 19 December 1991 – *NJW* 1992 p. 815 ff:[124]

'Since1983 the appellant had been employed as an editor-in-chief by the respondent, the publisher of the newspaper D. The employer had the possibility to 'cut' into calls; he was able to interrupt the call or to listen to it secretly. When the appellant called the journalist R in Vienna, the employer listened to the call. Some comments made by the appellant had offended the employer. Because of those comments the employer dismissed the appellant. The Local Labour Court decided at first instance that the employer did not have the right to dismiss the appellant. The court stated that such evidence was inadmissible.
On appeal, the state labour court allowed R to be heard as a witness and dismissed the action. The state court argued that the employer had not received the information unlawfully. The call was not confidential, but rather a business call. Business calls are regularly intended for the employer to know about. The appellant also knew that the employer had the possibility to 'cut' into calls. The employer did not violate the personal right of the appellant by listening secretly. The offending content of the call was considered to be sufficient for the dismissal.
The claimant lodged an appeal to the Bundesverfassungsgericht. The Bundesverfassungsgericht reversed the judgement of the lower instance court. It stated that the appellant's personal rights and the right according to one's word had been violated.

[123] PN 2004-193.
[124] PN 2004-194.

Therefore it was prohibited to hear the witness R. The right according to the spoken word protects people against secret taping and the speaker against the supposition of words he did not utter. Knowledge about the possibility of the employer to listen to calls does not change the fact that the employer would have needed the explicit consent of the employee to be able to do so. The use of an official work phone does not imply such consent'.[125]

The BAG accepts phone monitoring if the employer has a legitimate interest.

Resolution of 30 September 1995 – 1 ABR 4/95 – *NZA* 1996, p. 218 ff:[126]

'The BAG decided that secretly listening in to the calls of a trainee is justifiable during the first three months of training, because of the legitimate interest of the employer to train new workers.
This interference with the personal right of the trainee is acceptable because the employer can only instruct his trainee workforce by giving them advice on 'phone behaviour'. The intervention intensity was very low because the monitoring only took place during the first three months and because the calls were only business calls'.[127]

The BGH also stated that in cases where none of the callers know about the recording[128] or in cases where comments are secretly recorded on tape, those results cannot be used to provide evidence in court because of the violation of the personal rights of those persons. Furthermore, it can be assumed that the decision of the BAG is appropriate to questions of workplace privacy because it has a closer factual relationship.

E-mail and Internet in the workplace

Because there has not yet been a decision by the German supreme court on the surveillance of internet activities, the rules on telephone monitoring, in cases where private use is not permitted, can in some cases be transposed to cases where e-mails are read by the employer or when other internet activities are monitored.[129] In many cases, however, the position is not clear.

The employer has the right to view outgoing e-mail, as well as the right to look at ordinary business mail. The employer also has a legitimate interest in taking samples of incoming e-mails. A minority in the literature, however, advocate a general prohibition of controlling the content of e-mails because this violates the personal sphere of the employee. Any control would only be justified, if there is a

[125] Compare: Kopke, 'Heimliches Mithörenlassen eines Telefongesprächs', NZA 1999, p. 917 (918).
[126] PN 2004-195.
[127] BAG resolution from 30 August 1995 – 1 ABR 4/95 in: *NZA* 1996, p. 218 (221).
[128] See *supra* n. 7, p. 21 (26).
[129] Rossnagel-Büllesbach, Part 6.1, Rn. 81ff.

suspicion of criminal activities or the betrayal of business or company secrets.[130] Others think that the surveillance of e-mails is allowed as long as the works council has agreed.

More or less the majority in the literature accept the right of the employer to check which internet sites the employee has visited during working hours, as long it is only a random test. Because it is possible to draw conclusions about individual interests and personal characteristics from which internet sites a person has visited (e.g. <www.one-night-stand.com>), any surveillance and logging must be constant.[131] Others think that the interest of the employer in knowing whether the employees adhere to the prohibition on using the internet for private purposes is more important than the employees' privacy, so that the logging of web sites, the date, the time and specifications relating to the employees is also allowed on a constant basis.[132] In this context, there is also disagreement as to whether an employer is allowed to check data files which the worker has downloaded on to the computer. Some are of the opinion that a preponderant interest of the employer would not justify such a deep intrusion into the rights of the employee. To discover whether a downloaded file is of an official or private character, it is usually enough to know the address (e.g. <www.wether.com>).[133]

Automatically controlling of the content is strictly forbidden. The systematic monitoring of incoming and outgoing e-mails, screenshots or the analysis of content by searching for specific terms to provide efficiency and to control behaviour is illegal because it constitutes serious interferences with the personal rights of the employees.[134]

When special spying programs are used, the protection of the employee is difficult. So-called Key-Loggers save everything on the Personal Computer. The system-administrator of an enterprise might control everything. The administrator is able to view any e-mail or he can check usage times. Of course the administrator is not allowed to divulge the acquired information to the employer. Access authorisations need to ensure that only authorised persons can have access to personal data.

9.5.2 Video surveillance

The amount of video surveillance is increasing in all areas because of the rapid technical developments. In 2001 the total number of surveillance systems in the non-public sector was estimated to be 400,000.[135] In 2001 about 1500 cameras

[130] Weißnicht, 'Die Nutzung des Internet am Arbeitsplatz', *MMR* 2003, p. 448 (451).
[131] See *supra* n. 47, Rn. 359.
[132] See *supra* n. 130.
[133] Däubler, Internet und Arbeitsrecht, p. 120.
[134] See *supra* n. 47, Rn. 351.
[135] Simits-Bizer, BDSG-comm., Art. 6b, Rn 2; DSGK, Reimer: 59. Konferenz der DSB des Bundes und der Länder , Entschließung vom 14./15 March 2000, Grenzen der Videoüberwachung, *DuD* 2000, p. 302 (304).

were used by the federal government in 55 federal localities.[136] Video surveillance of public areas is mainly tolerated by citizens, but acceptance has decreased within the last few years.[137] In 1998 the fear of crime outweighed the fear of becoming a totally transparent person and therefore 83 per cent of the population accepted video surveillance in public areas. In 2001, however, only 75 per cent accepted video surveillance.[138] After all, almost 50 per cent of families with children and 50 per cent of retired persons consider the video supervision of inner-city areas by which individual persons can be identified to be reasonable.[139] Therefore, the danger of wide-scale supervision of the public is again being raised.

By enacting Article 6b BDSG in May 2001, the widely practised video surveillance was supposed to be given a legal basis.[140] Video surveillance has to fulfil certain requirements to ensure the protection of the individual's constitutional rights.

Before the introduction of Article 6b BDSG, video surveillance was only allowed by law to avert a danger. Special federal laws concerning the Bundesgrenzschutz [Federal Border Guards], the Bundeskriminalamt [Federal Bureau of Crime Investigation], the Customs Investigation Department, the Secret Service, the right of assembly and criminal law contain further regulations which allow video surveillance or similar surveillance without the knowledge of the affected persons.[141] The BDSG is a subsidiary of those regulations.

Furthermore, the BDSG is not applicable if video surveillance takes place only for private reasons. Such video surveillance is, according to the case law, only acceptable for property protection.[142]

The meaning of optical control devices is quite considerable in practice.[143] Through the introduction of Article 6b BDSG video surveillance was also legalised for employers, as long as it concerns a public area. This relates especially to video cameras in salesrooms if they are needed to ensure domestic authority or to protect property.

Concerning non-public areas, case law states that permanent video surveillance is an infringement of the constitutional right according to one's picture, because the

[136] BT-Drs. 14/7905, 18 December 2001.
[137] Opaschowski, 'Quo vadis, Datenschutz? Die Angst vor dem Debakel breitet sich aus', *DuD* 2001, p. 680.
[138] Ibidem.
[139] Ibidem.
[140] BT-Drs. 14/4329, p. 38.
[141] Compare: Art. 28 para. 2 No. 2a) Bundesgrenzschutzgesetz (BGSG), freely translated: Federal Frontier Portection Act; further: Art. 23 para. 2 No. 2a) Bundeskriminalamtsgesetz (BKAG) freely translated: Federal Bureau of Criminal Investigation Act, Art. 19, 29 Zollfahndungsdienstgesetz (ZFdG von 2002) freely translated: Customs Investigation Department Act , Art. 100c Strafgesetzbuch (StGB), Artt. 12, 19a Versammlungsgesetz (VersG) freely translated: Law Regulating Public Meetings.
[142] BGH judgment from 25 April 1995 – VIZR 272/94 (KG) in: *NJW* 1995, p. 1955 (1957).
[143] Biegel, Überwachung von Arbeitnehmern durch technische Einrichtungen, p. 55.

affected person's behaviour and mood can be observed.[144] Case law assumes that with 'Big Brother' methods a person's free behaviour and privacy are restricted, which also affects the elementary basis of democracy.[145] Actually, a violation of human dignity is assumed if video surveillance takes place in order to increase working speed or if toilets are monitored to prevent people reading newspapers in secret.[146] In such cases, surveillance is always illegal.

A general prohibition of video supervision in the workplace is partially stipulated.[147] A complete prohibition would however interfere with the constitutional rights of the employer.

Usually, the employee will not consent to supervision in non public areas; therefore the interests of both parties, the employer and the employee, have to be considered in order to determine whether the supervision is lawful. A mere desire to control the work of employees cannot justify video surveillance, because then the right pertaining to one's own picture would practically be nullified.[148]

In cases where, for example, a machine's efficiency can only be ensured by video surveillance, the employer's interest is predominant because he wants to accomplish something that exceeds the employment relationship. In those cases it is important that employees are recorded as little as possible.[149] In any case, the employee has to have the possibility of leaving the supervised area.[150] Surveillance may only take place secretly if crimes cannot be prevented by other means.[151] This also applies to cameras that can be activated at any time.[152]

If the employer videotapes without justification, the employee can claim damages. A state labour court has decided that an employer had to pay 1300 German Marks to an employee. The employer had videotaped part of the working area of that employee (but not his office) for two months.[153]

Case BAG judgment of 27 March 2003 – *DuD* 2003, p. 705 ff:[154]

> 'The matter in dispute was the effectiveness of a behaviour-related dismissal. The complainant (K) had worked for the defendant (B) since 1994 in a food and beverage market. Sine 1997 stocktaking differences had occurred from time to time. In March 2000 B installed a hidden video camera directly above the cashier's desk and a few months later one above the corridor of the market without having consulted the works' council. K was then dismissed without notice and with permission of the works' council due to the suspicion of false accounting. With her lawsuit K appealed against her dismissal. She denied having falsified the accounts. She contested that it was prohibited to use videos from the surveillance systems in the proceedings as it was disproportional and therefore illegal and violated her personal rights. Furthermore, the works' council would not have accepted the installation of the equipment.
> B pointed out that the stocktaking differences could only arise from unlawful conduct at the cashier's desk. The installation of visible cameras would not have had the same effect because not only future crimes should be prevented, but former ones should also be solved.
>
> K's action was dismissed. The video recordings were accepted as proof. In the BAG's opinion the video evidence had been legitimately obtained. The video surveillance was justifiable because the differences in the stocktaking had given rise to strong suspicions.
> Also the effected supervision did not take place in a haphazard manner and was not therefore inadequate and did not serve to generally control behaviour. The absence of the works' council's acceptance was irrelevant. Although the council's right of co-determination under § 87 No. 6 BetrVG was violated this infringement did not mean that the use of the evidence was prohibited. A prohibition on using the evidence would only arise if the works' council had not agreed to the use of the recording and the dismissal on which it was based, but here the council had agreed to the dismissal'.

[144] See *supra* n. 143, p. 25.; LAG Hamm 24 July 2001, NZA-RR 2002, p. 464; LAG Niedersachsen 19 December 2001 – 6 Sa 1376/01.
[145] See *supra* n. 47, Rn. 297.
[146] See *supra* n. 143, p. 57
[147] Däubler, Das Arbeitsrecht, 2, Rn. 471ff..
[148] See *supra* n. 47, Rn. 311.
[149] See *supra* n. 143, p. 58.
[150] Däubler, 'Erheben von Arbeitnehmerdaten', *CR* 1994, p. 101 (108).
[151] Cases: BAG, AP, No. 15 about Art. 611 BGB, Bl. 309; BAG 27.3.2003, *DuD* 2003, 705ff; LAG Köln, *BB* 1997, p. 476; LAG Baden-Würtemberg, *BB*, 1999, p. 1439; further: Däubler, 'Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht', *NZA* 2001, p. 874 (878).
[152] BGA, *NZA* 1988, p. 92.
[153] ArbG Frankfurt in: *RDV* 2001, p. 288 ff.
[154] PN 2004-196.

When this case was decided, video surveillance in public areas had not yet been standardised according to Article 6 b BDSG. Because the person who tapes needs to inform the person he is taping about the data processing (Article 6b para. 2), this case is still interesting. Thus the rules have to be transposed to situations of video surveillance in non-public areas and to situations in which the preconditions of Article 6b BDSG have not been met, as in this case.

Case BAG judgment of 7 October 1987 – 5 *AZR* 116/86:[155]

> 'In this case the parties argued about the right to introduce an electronic surveillance system that works with hidden video cameras.
> The complainant was an employee of the defendant and he worked as a salesman in the department store of the Army and Air Force Exchange Service Europe, a store for American members of the armed forces in Munich.
> When the respondent, the employer, planned to install hidden video cameras in the showroom in order to monitor activities in that area, the complainant filed a complaint. The BAG upheld the complaint and held that by the permanent possibility of supervision a serious infringement of the personal rights of the complainant had taken place.

[155] PN 2004-197.

Personal rights protect against permanent surveillance by secret photographic control and the 'surveillance pressure' created thereby. The court accepted that personal rights can be restricted when other interests also need to be protected, but the mere allegation that there had been losses by thefts would not be enough for the interest of the employer to take precedence. The defendant should have explicitly mentioned that thefts could only be prevented by installing hidden cameras'.

This judgment is also older than the introduction of Article 6b BDSG. It is questionable whether this case would be decided in the same way today, because the mention of losses could be sufficient to fulfil the needs of Article 6b para.1 BDSG.

9.5.3 Genome analyses

In employment relationships an increasing amount of preventive medical checkups are being carried out. Being afraid of losing their jobs, few employees refuse them, although they are usually voluntary.

The main alliance of the Employers' Liability Insurance Associations, for example, recommends a basic program (BAPRO). Through the recommended extensive medical examinations the general state of health, individual lifestyles and hereditary diseases are determined by using questionnaires. These phenotypical examinations were classified as dangerous by the Parliamentary Enquiry which considered the danger of being 'x-rayed' involuntarily. By evaluating the questioned data, conclusions regarding genetic diseases can be drawn. According to the Enquiry, examinations within the employment relationship should be prohibited in the same way as examinations at the application stage, because the employee cannot sufficiently protect himself. Exceptions should only be made in special cases. This is considered to be important because the knowledge of one's own state of health can have serious physical and psychological implications. According to the right of self-determination, human beings also have the right not to know.[156]

The VGH Baden Württemberg [Higher Administrative Court of Justice for the land of Baden Württemberg] decided that secret DNA analyses are not allowed within the employment contract.

Case VGH Baden-Würtemberg judical decree of 28 November 2000 – PL 15 S 2838/99 – *AuR* 2001, p. 449 ff:[157]

'In a savings bank an anonymous letter had been circulated which defamed a department director. Due to a well-founded suspicion the employee P was invited to a party where he was given cake, coffee and wine. The saliva he left on the pastry fork, the coffee cup and the wine glass became the subject of a DNA analysis as well as the glued joining in of the anonymous letter. According to the test result, all the saliva samples belonged to the same person. The board of directors of the savings bank then wanted to dismiss P. The works' council did not agree to this.

The board of directors took action at the appropriate court to have the works councils' acceptance substituted by the court's decision.

The VGH decided that the test result could not be used as the ground for an extraordinary dismissal.

The utilisation of bodily cells to determine DNA identification patterns was a violation of the right of informational self-determination (Article 2 para. 1 according to Article 1 para. 1 GG). A transgression of the employees' rights is justified if the employer has an overwhelming interest and if this is the only possible way to find the offender. The writing of defamatory letters is not sufficiently important to suppress the right of informational self-determination'.

[156] See *supra* n. 47, p. 27.

[157] PN 2004-198.

9.5.4 Employer/works' council agreements; the right of co-determination

The normative justification for listening into phone calls is derived from many works council agreements. An increasing amount of these agreements contain regulations concerning the admissibility of viewing e-mails and the legitimacy of data-logging and an analysis of internet surfing.[158]

Case law considers works' committee agreements to be acceptable if they concern the logging of data like the number, date, time and target of phone calls,[159] and also agreements which allow door controls in companies with a high theft risk.[160] A works' committee agreement which allows the employer to use a two-way mirror will be considered illegal because it is a violation of human dignity.[161]

The right of co-determination in Article 87 para. 1 no. 6 BetrVG (Introduction of technical control devices) has been accordingly strengthened by case law because the courts have found it to be applicable to any possible control devices. For example, the right of co-determination exists when the fingerprints of employees are collected for a bio-metrical access control system,[162] or if an employer wants his bus drivers to wear a name badge on their uniform.[163] Furthermore, employees have to be informed about the use of control devices.[164]

[158] Naujock, 'Internet-Richtlinien: Nutzung am Arbeitsplatz; Ein Plädoyer für eine klare Regelung', *DuD* 2002, 592.

[159] BAG, 27 May 1986, AP No. 16 for Art. 87 BetrVG 1975.

[160] BAG, 26 May 1988, AP No. 14 for Art. 87 BetrVG 1972.

[161] Wedde, 'Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht', *DuD* 2004, p. 169 (174).

[162] ArbG Frankfurt a. M., resolution from 18 February 2002 – 15 BVGa 32/02, *RDV* 2002, p. 248 ff.

[163] BAG, *NZA* 2002, p. 1299.

[164] Bijok/Class, 'Arbeitsrechtliche und datenschutzrechtliche Aspekte des Internet-Einsatzes', *RDV* 2001, p. 52 (54).

9.6 Special Rules for the Civil Service

In former times public servants and officials who basically could not rely on constitutional rights in the course of their employment were less protected than 'private' employees.

For example, the restriction of the right to ask certain questions to applicants did not apply.[165] This legal practice was changed by the BDSG. Article 12 para. 4 BDSG makes public servants and officials subject to rules on data collection in the private sector. It is not necessary that personal data are processed in an automated way or in a non-automated way or are used or collected for this purpose. That means that the BDSG is also applicable if the personal file is neither retained by data processing nor if it is filed electronically. Since 1992 special provisions referring to the legitimacy of collecting data can be found in the Bundesbeamtengesetz[166] (Article 9 para. 4) and in the Beamtenrechtsrahmengesetz[167] (Article 56 para. 4). According to this, data collection is only admissible if it is necessary for the creation, the processing, the ending or the termination of a service.

9.7 Data Protection after the Termination of the Employment

According to Article 35 para.2 BDSG data has to be deleted if it is no longer needed for its original purpose. There is therefore a duty to delete data after the termination of employment. This duty emanates from the fiduciary duty of the employer who has to protect employees from any violation of their personal rights.[168]

It must be pointed out that data processing after the termination of employment does not suddenly stop. Mostly the employment relationship also includes a storage duty for some data. Such a duty derives from the employees' right to ask for a reference or from retirement arrangements, or from trade law or tax law regulations. Despite this storage duty the data has to be secure and not accessible.

9.8 Conclusion

With the general acceptance of the constitutional right of informational self-determination data protection has been acknowledged as a constitutional right. This also affects workplace privacy. The protection established by the case law has been widened and strengthened since the beginning. Also many norms ensure workplace privacy. A special employee data protection law is claimed, but also without one

[165] BVerfGE 16, p. 340 (341); see *supra* n. 47, Rn. 243.
[166] Freely translated: Federal Civil Servants Act.
[167] Freely translated: Civil Servants Rights Framework Act.
[168] Erfurter-Comm., Wank, 160, § 35, Rn. 7.

there is a well defined protection, as long as the regulations and case law are observed by the employers.

The amendment of the telecommunication laws and the BDSG marks the legislator's interest in profound data protection, also concerning the workplace. The legislature wanted to make sure that with the rise of the internet and surveillance control systems the use of data protection does not become lost. Indeed, some regulations have decreased protection, as it is quite easy to monitor public places permanently by using the new Article 6b BDSG. And, even when the telecommunication acts are applicable, it is possible to store connection data, which was not allowed under the TDSV from 1996; according to Article 7 para. 2nd sentence TDSV 2000 the service provider may log stock data (names, date of birth, etc.) and also connection data (the length of the connection, the dialled number, etc.). The storage period has also been extended from 80 days to six months. But, it has to be said that these changes are not intended to decrease data protection in the workplace; the regulations are derived from general laws and can therefore only be transferred to situations concerning the workplace under certain preconditions.

Workplace privacy is definitely insufficient in the field of genome analysis, especially during the application stage. Especially the developments in the field of medicine mean that there is a danger that employees are reduced to mere objects by the transfer of sensitive data.

Questions regarding internet usage still have to be decided by case law, so this area is still uncertain. As many relevant questions are not regulated *expressis verbis*, the employee has to trust the point of view of the courts. The judge is basically independent and does not have to obey precedents.

The argument in the literature concerning the supervision of e-mails and internet connections shows that the application of case law is not without problems. Some regulations are confusing or are not sufficiently specific.

Therefore, many voices in the literature and also employees are interested in laying down data protection in the workplace in concrete terms. Ver.di, for example, a large labour union created by the fusion of 5 single unions, has mounted a campaign to promote the creation of an employee data protection act, to ensure better protection for workplace privacy. Ver.di also wants a right for employees to use the internet for private purposes. At the same time they would like to see a prohibition on the employer monitoring private communications.

For employers it is also important to have a clear idea of the legitimate use of data. Nevertheless, it should not be forgotten that Germany is already regarded as being over-regulated in comparison with its European neighbours. To keep this from getting worse and to keep Germany competitive the creation of new regulations has to be done with extreme care.

Concerning the efforts to create a special law concerning data protection in the workplace European efforts have to be kept in mind. The EU Commission has suggested a new social plan concerning data protection in the workplace to its European partners; the second hearing has already taken place.

Underlying this initiative is the fact that the member states treat the personal data of employees in quite different ways, which restrains the domestic market.

The consultation has dealt with the consent of employees and the question of whether this is sufficient for the distribution of sensitive personal data. Regarding their special sensitivity it was discussed whether it would be wise to create a uniform framework for the trade in medical data, as well as a regulation on drug and genome tests. It was also proposed to establish a clear stance concerning the supervision of internet correspondence and activity.[169] From the German point of view regulations on these aspects are certainly desirable.

[169] EU-Commission, Brussels, 31 October 2002.

Annex:
BIBLIOGRAPHY

A. Books

DÄUBLER, 'Gläserne Belegschaft? Datenschutz in Betrieb und Dienststelle', 4th edn., Frankfurt am Main, 2002 – [*Crew out of glass? Data privacy in enterprises and administrative offices*]

– 'Internet und Arbeitsrecht', 2001 – [*Internet and labour law*]

– 'Arbeitsrecht', 5th edn., 2004, Frankfurt am Main – [*Labour law*]

HOEREN, 'Internetrechtrecht', Februar 2004 – [*Internet law*]

PIEROTH/SCHLINK, 'Grundrechte, Staatsrecht II', 19th edn., Heidelberg, 2003 – [*Constitutional rights, constitutional law II*]

ROSSNAGEL, 'Handbuch des Datenschutzes', München, 2003 – [*Handbook of data protection*]

TINNEFELD/EHMANN, 'Einführung in das Datenschutzrecht', 3rd edn., München 1998 – [*Introduction into data protection law*]

B. Commentaries

BECK'SCHER TKG, KOMMENTAR – Telekommunikationsgesetz, München, 1997 – [*Commentary telecommuncation law*]

DÄUBLER/KITTNER/KREBEL, Betriebsverfassungsgesetz mit Wahlordnung – Kommentar für die Praxis, 6th edn., Frankfurt am Main, 2002 – [*Commentary for the Works Council Constitution Act*]

ERFURTER KOMMENTAR ZUM ARBEITSRECHT, 4th edn., München, 2004 – [*Erfurter Commentary for labour law*]

JARASS/PIEROTH, Grundgesetz für die Bundesrepublik Deutschland, 6th edn., München, 2002 – [*Constitution for the Federal Republic of Germany*]

MÜNCHNER HANDBUCH ARBEITSRECHT, Handkommentar, Band 1, Individualarbeitsrecht I, 2. Auflage, München, 2000 – [*Munich handbook-labour law – hand commentary*]

SPIROS/SIMITS, Kommentar zum Bundesdatenschutzgesetz, 5th edn., Baden-Baden, 2003 – [*Commentary – federal data protection act*]

C. Articles

BECKMANN, 'Probleme des Grundrechtsverzichts', *JZ* 1988 P. 57ff – [*Problems of relinquishment of constitutional rights*]

BIJOK/CLASS, 'Arbeitsrechtliche und datenschutzrechtliche Aspekte des Internet-Einsatzes (insbesondere E-mail)', *RDV* 2001, p. 52 ff. – [*Aspects of the internet use in the area of labour law and data protection law (in particular e-mail)*]

BIZER, 'Die dienstliche Telekommunikation unter dem Schutz des Fernmeldegeheimnisses', *DuD* 2001, p. 618 ff. – [*Official telecommunication under protection of the secrecy of telecommunication*]

BÜTTGERN, 'Ein langer Weg – Telekommunikations-Datenschutzverordnung endlich in Kraft', *RDV* 2001, p. 6 ff. – [*Telecommunication-data protection decree finally became operativ*]

DÄUBLER, 'Erheben von Arbeitsnehmerdaten', *CR* 1994, p. 101 ff.– [*Collection of employees data*]

– 'Das Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht', *NZA* 2001, p. 874 ff. – [*The ferderal data protction act and its influence on labour law*]

GOLA/KLUGE, 'Die Entwicklung des Datenschutzes in den Jahren 2002/2003', *NJW* 2003, p. 2420 ff. – [*The development of data protection in 2002/2003*]

HEILMANN, 'Aids und (Arbeit)srecht', *BB* 1989, p. 1413 ff. – [*Aids and (work) law*]

KELLER, 'Die ärztliche Untersuchung des Arbeitnehmers im Rahmen des Arbeitsverhältnisses', *NZA* 1988, p. 561 ff. – [*The medical examination of the empolyee in line with the employment contract*]

KOPKE, 'Heimliches Mithörenlassen eines Telefongesprächs', *NZA* 1999, p. 917 ff. – [*To let someone listen in a phone call secretly*]

MESSINGSCHLÄGER, 'Sind Sie schwerbehindert? Das Ende einer (un)beliebten Frage', *NZA* 2003, p. 301 ff. – [*Are you severely disabled? The end of an (un)popular question*]

NAUJOCK, 'Internet-Richtlinien: Nutzung am Arbeitsplatz; Ein Plädoyer für eine klare Regelung', *DuD* 2002, p. 592 ff. – [*Internet directives: Use at workstation; A parol for a clear regulation*]

OBASCHOWSKI, 'Quo vadis, Datenschutz? Die Angst vor dem Datenklau breitet sich aus', *DuD* 2001, p. 678 ff. – [*Quo vadis, data protection? The fear of data robbery spreads*]

ROSS, 'Gentechnik – Chancen und Risiken', *AuR* 2001, p. 121 ff. – [*Genetic engineering – Chances and risks*]

SCHAUB, 'Ist die Frage der Schwerbehinderung zulässig?', *NZA*, p. 299 ff. – [*Is the question about a severe disability allowed?*]

SCHATZSCHNEIDER, 'Die Frage nach der Schwangerschaft und gemeinschaftsrechtliches Diskriminierungsverbot', *NJW* 1993, p. 1115 ff. – [*The question about pregnancy and EU community law*]

TINNEFELD, 'Die Novellierung des BDSG', *NJW* 2001, p. 3078 ff – [*The amandment of the BDSG*]

WEDDE, 'Schutz vor verdeckter Kontrolle im Arbeitsverhältnis', *DuD* 2004, p. 21 ff.– [*Protection against secret surveillance in the employer/employee relationship*]

– 'Die wirksame Einwilligung im Arbeitnehmerdatenschutzrecht', *DuD* 2004, p. 169 ff. – [*The efficient consent according to employee data protection right*]

WEICHERT, 'Der Schutz der genetischen Information', *DuD* 2002, p. 133 ff. – [*The protection of genetic information*]

WEISSNICHT, 'Die Nutzung des Internet am Arbeitsplatz', *MMR* 2003, p. 448 ff.– [*The use of the internet at the workstation*]

D. Dissertations

Andreas BIEGEL, 'Überwachung von Arbeitnehmern durch technische Einrichtungen', Marburg, 2000 – [*Surveillance of employees by technical equipment*]

Andreas NOTZ, 'Zulässigkeit und Grenzen ärztlicher Untersuchungen von Arbeitnehmern', Frankfurt am Main, 1991 – [*Legitimacy and restrictions of medical examinations of employees*]

Berndt SCHLEMANN, 'Recht des betrieblichen Datenschutzbeauftragten', Solingen, 1996 – [*The right of the Commissioner for data protection in enterprises*]