EWLL – Seminar 2017

GERMAN REPORT

EUROPA-UNIVERSITÄT VIADRINA FRANKFURT (ODER)

Table of Content

Question 1): General Constitutional Framework

"Right to privacy": Is a right to privacy recognized in your system of law (apart from art. 8 ECHR and art. 7 and 8 of the Charter of Fundamental Rights of the European Union [CFR]), i.e. in the constitution, in statutes, in national case law? If there is no explicit recognition of such a right, how are elements of it protected in your legal system? What has the role of the right to privacy in art. 8 ECHR and art. 7, 8 EU-CFR been in your domestic legislation and case law?

I. A "Right to Privacy" in the German System of Law

The German "Basic Law for the Federal Republic of Germany" ("Grundgesetz", hereinafter the Constitution) does not explicitly state a right to privacy or personality. However, this does not mean, that there is no protection of the privacy of individuals in the German system of law. Although the German constitution does not incorporate an explicit protection of a general right to personality or privacy, it contains various fundamental rights which have a dimension towards privacy – for example the freedom of speech. Furthermore, the German system of law ensures a comprehensive protection level for personality rights in additional acts on a level subordinate to constitutional law.

1. Explicit Constitutional Protection

The German constitution came into force in May 1949 and grants nineteen fundamental rights and six rights, equivalent to a fundamental right. In total, the constitution guarantees in its articles 1 to 19 a catalogue of human, civil, political, economic and social rights, such as the inviolability of human dignity, freedom of assembly or the right to effective judicial protection. In addition, several fundamental rights include (as mentioned) different aspects of the protection of personality rights.

a) Art. 5 (2) German Constitution

At first Art. 5 (2) of the constitution ensures the freedom of expression of opinion in speech, writing and pictures. The freedom of expression is the restrained democratically subjective right of free speech.[1] The German constitution defends the freedom of expression in the individual interests of personal development as well as in the interest

[1] BeckOK/Schemmer, Art. 4 GG, recital 1.

of a democratic process, for which it has constitutive significance.[2] Art. 5 (1) warrants both from the individual and objective perspective the freedom of expression and dissemination of opinion on the one hand. On the other hand, the freedom of information is protected as an element of a process of communication. Objectively protected is the communication process entirely, subjectively the freedom to participate.[3] So the freedom of speech protects privacy insofar, as the process of communication is concerned.

b) Art. 6 (1), (2) German Constitution

Art. 6 of the German constitution contains the protection of marriage, family and childcare. The article assigns a binding role to the state with regard to marriage, family, parents and children. The public authorities have to respect this section as personal area of freedom, but on the other side legislative measures shall grant effective protection for a liberal living.[4] Therefore Art. 6 is not only designed as an individual fundamental right, but also lays down an institutional warranty as well as a fundamental standard for all law.[5]

As a fundamental right Art. 6 protects marriage and family as a closed and against authorities shielded sphere of living and autonomy.[6] As an institutional warranty, it grants the existence and significant structures of marriage and family.[7] Finally, as a fundamental standard for all law, Art. 6 gives family and marriage special protection under the system of government.[8] So the authorities may not infringe the privacy of families and married couples.

c) Art. 10 (1) German Constitution

Furthermore Art. 10 of the constitution ensures the privacy of correspondence, posts and telecommunications. These privacy rights guarantee the free development of personality shielded from public and secure the private exchange of information. Therefore, these rights are an elementary part of the protection of the right to privacy and

[2] Federal Constitutional Court, ruling of 15. 1. 1958 – 1 BvR 400/57.
[3] Federal Constitutional Court, ruling of 16.06.1981 – 1 BvL 89/78.
[4] ErfK/Schmidt, Art. 6 GG, recital 1.
[5] Federal Constitutional Court, ruling of 19. 6. 2012 – 2 BvR 1397/09
[6] Federal Administrative Court, ruling of 29.10.1992 – 2 C 24/90.
[7] Federal Constitutional Court, ruling of 17. 7. 2002 – 1 BvF 1/01, 1 BvF 2/01.
[8] Federal Constitutional Court, ruling of 17. 1. 1957 – 1 BvL 4/54.

human dignity.[9] In concrete Art. 10 (1) protects the confidentiality of individual communications. This includes the protection against state control of mail, recording and exploitation of communication data or storage of recorded data.[10] Overall Art. 10 guarantees a subjective right of defense against governmental action. Nevertheless, Art. 10 of the German constitution does not only affect the relation between citizen and state but also affects the legal relation between citizens. As an objective principle of law, the privacy of correspondence, posts and telecommunications has a radiating effect into civil law.[11]

d) Art. 13 (1) German Constitution

In Art. 13 (1) of the constitution the right of inviolability of the home is written down. This right to housing protects all properties, which are used mainly for residential purposes against unlawful entry, state search and seizure or surveillance. As a place of retreat for personal life is the home amenable to special protection of the legal system. Situations that touch the inviolable area of human freedom must not be accessible to state control. This results into the prohibition on exploitation of personal conversations between persons in a position of trust, e.g. close relatives, attorneys, physicians.

e) Art. 14 (1) German Constitution

Finally, also Art. 14 of the constitution protects guarantees private property which includes a fraction of the right to privacy. As far as personal rights have a measurable asset value, they are protected by Art. 14. The protection includes patent rights, trademark rights or copyrights as intellectual property.[12] The extent of protection stretches to an individual right of property as well as a legal institution of a property guarantee. In the overall structure of all fundamental rights, Art. 14 has the task to constitute a space of freedom in the proprietary area and to enable the autonomous framing of life.

2. A General Right to Privacy in the German Constitution

Although a fundamental protection of individual right is granted by the German constitution, there was a need for a more extensive, encompassing and general protection

[9] Federal Constitutional Court, ruling of 5. 4. 2006 – VIII ZR 384/04)
[10] BeckOK/Baldus, Art. 10 GG, recital 25f.
[11] Federal Labor Court, ruling of 27. 05. 1986 – 1 ABR 48/84.
[12] BeckOK/Axer, Art. 14 GG, recital 50.

of the right to privacy and personality. Therefore, the German Federal Court of Justice recognized a general right of personality in 1954 for the first time,[13] even though such an unwritten rule was rejected previously by the highest Court of the Weimar Republic in the 1920's.[14]

a) Derivation of the general right of personality

The term of a constitutional general right of personality originates from the German civil law, where a variety of special rights to privacy and civil general rights to privacy was developed.[15] These legal fundamentals were transferred into constitutional law and further developed – as mentioned above, the constitution does not include a special fundamental right of privacy. Thereby the general right of personality is based on Art. 2 (1) in conjunction with Art. 1 (1):

Art. 1 (1) of the constitution protects the inviolability of the human dignity and thereby contains the primary constitutional principle. Due to its special importance as a guiding principle for the German constitution, the German Federal Constitutional Court, the highest Court in Germany, rather understands Art. 1 (1) as an interpretation guideline for the general right to privacy and not as a source of law.[16]

Art. 2 (1) of the constitution guarantees the general freedom of action. Consequently, one and the same constitutional text includes two different fundamental rights: the freedom of action and the right to privacy. With its wide scope of protection[17] the freedom of action in Art. 2 (1) actually ensures an active element of personal development. In contrast to this, the right of Art. 2 (1) aims at the preservation of the integrity of the human being as a whole and its free interaction with others. It thus involves a passive protection, as any development of the human being is not possible without privacy.

These two articles were used as general legal principles and as an aid for interpretation to support the legal idea of a general right to privacy in the system of fundamental rights in the German constitution. As an "unamend" and abstract liberty right,[18] the

[13] Federal Civil Court, ruling of 25. 5. 1954 - I ZR 211/53.
[14] Court of Justice 12.05.1926 - I 287/25.
[15] Federal Civil Court, ruling of 25. 5. 1954 - I ZR 211/53.
[16] Federal Constitutional Court, ruling of 15. 1. 1970 - 1 BvR 13/68.
[17] BeckOK/Lang, Art. 2 GG, recital 31.
[18] Federal Constitutional Court, ruling of 19.4.2016 – 1 BvR 3309/13.

general right of personality complements the special and "named" fundamental liberty rights.

b) Scope of protection

As a "protection of a status",[19] the general right of personality affects the respect for the right of integrity of personality in particular. Generally speaking, the material area protected by this right aims at the defense of harm of personal privacy, self-determination and fundamental conditions of personal development.[20] As a constitutionally protected value, the human personality stands for an independent decision of a personal and self-determined way of living.[21]

Due to its special legal background and derivation as a further development of the written law, the general right of personality from Art. 2 (1) in conjunction with Art. 1 (1) of the constitution has no precisely definable scope of protection.

The scope of protection is rather a variety of particular personality expressions, which are developed through case law. Therefore, the protection of the general right of personality finds its expression in case-law-related groups.[22] Consequent on this, the scope of protection solely deduces from the decisions of the German Federal Constitutional Court. Thereby the Federal Constitutional Court emphasizes the "openness to development" of the general right of personality.[23]

To outline the contour of the general right to privacy and to keep it manageable, the scope of protection is frequently split into three different spheres: the sphere of social life, the sphere of private live and the sphere of privacy.[24]

[19] Federal Civil Court, ruling of 25. 5. 1954 – I ZR 211/53.
[20] Maunz/Dürig/Di Fabio, Art 2 GG, recital 147.
[21] Ibidem.
[22] BeckOK/Lang, Art. 2 GG, recital 32.
[23] Federal Constitutional Court, ruling of 3. 6. 1980 – 1 BvR 185/77.
[24] Maunz/Dürig/Di Fabio, Art 2 GG, recital 157.

aa) Sphere of privacy

The highest intensity of protection is regarded to the sphere of privacy. Due to its particular proximity to human dignity, privacy is inviolable and withdrawn from governmental authority.[25] State interventions in this protected core area of private life are not justifiable.[26] If a certain fact of living is assigned to the core area of private life or not, depends on its level of personal character.

The sphere of privacy includes firstly those aspect of personality, which are excluded from insights of others or communication with third parties. Secondly, the sphere of privacy extends to sexuality and sex life.[27]

Examples for the sphere of privacy are the protection of personal secrets – like diaries, personal notes[28] or sexual self-determination by gender reassignment.

bb) Sphere of private life

The sphere of private life comprises wider personal life, especially family life. It protects a space, in which the individual is unobserved, left to its own device or to persons of trust, regardless of social expectations and without fear of state imposed sanctions.[29]

In contrast to the sphere of privacy, the sphere of private life shows a significant level of social reference.[30] That is why state interventions are permissible by predominant interests of the broader public and under strict application of the principles of proportionality.[31]

Examples for the sphere of private life are the secrecy of patient's files;[32] the external appearance of a person – like clothing or hair cut[33] or personal observation through the police[34].

---

[25] Federal Constitutional Court, ruling of 30. 1. 1973 – 2 BvH 1/72.
[26] Federal Constitutional Court, ruling of 3. 3. 2004 – 1 BvR 2378/98.
[27] BeckOK/Lang, Art. 2 GG, recital 39.
[28] Federal Constitutional Court, ruling of 14. 09. 1989 – 2 BvR 1062/87.
[29] Federal Constitutional Court, ruling of 26.04.1994 – 1 BvR 1689/88.
[30] Federal Constitutional Court, ruling of 13. 6. 2007 – 1 BvR 1783/05.
[31] Federal Constitutional Court, ruling of 15. 12. 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83.
[32] Federal Constitutional Court, ruling of 8. 3. 1972 – 2 BvR 28/71.
[33] Federal Constitutional Court, ruling of 14. 2. 1978 – 2 BvR 406/77.
[34] Federal Constitutional Court, ruling of 08.11.2012 – 1 BvR 22/12.

cc) Sphere of social life

As the widest sphere, the sphere of social life protects the right to self-presentation and the social claim to be respected by others.[35] The scope of protection extends to a social identity and the participation in public life and grants the freedom of representation of the own person.

This includes:

- the right to one's own picture and words and their disclosure: protection against the use of manipulated images or wrong reproduction of quotes.[36] In addition, the protection against secret recording is included.[37]
- the right of reply to false media coverage[38]
- the protection against self-incrimination[39]
- the protection of good reputation: protection against untrue assertions and disparaging comments or behaviors.[40]

dd) The right to information self-determination

Also, included in the scope of protection of the German general right to personality is the so-called “right to informational self-determination”. This grants the right for everybody to decide autonomously about the exposure and use of personal data.[41] The central importance lies in the limitation of data collection, use and transfer.

ee) The warranty of confidentiality and integrity of information technology systems

From the general right to personality was also the warranty of confidentiality and probity in information technology systems developed. This special right protects individuals against automatically collected data by information technology systems.

---

[35] Maunz/Dürig /Di Fabio, Art 2 GG, recital 166.
[36] ErfK/Schmidt, Art. 2 GG, recital 39.
[37] ibidem.
[38] Federal Constitutional Court, ruling of 08.02.1983 – 1 BvL 20/81.
[39] BeckOK/Lang, Art. 2 GG, recital 39.
[40] Federal Constitutional Court, ruling of 10.10.1995 – 1 BvR 1476/91, 1 BvR 1980/91, 1 BvR 102/92 and 1 BvR 221/92.
[41] Federal Constitutional Court, ruling of 19.4.2016 – 1 BvR 3309/13.

c) Functions of the general right to personality

The different objects of protection from the general right to personality mentioned before, can be affected legally or factually by public authorities. Functioning in the classic sense as rights of defense against governmental repression, the general right of personality protects the individual against interference.

Besides, the function as a right of defense, the right of personality serves as a legislature's duty to protect the personal integrity. Therefore, the right to privacy can be violated if the legislator fails to take action, even though the personal integrity is threatened through social influences.[42] The omission to intervene can in some cases be classified as an impairment.

In addition, the general right to personality affects the civil law and applies as a constitutional value. In the field of civil law, the general right of personality works as an important interpretation aid for undefined legal concepts.[43]

3. Civil Claims to protect Rights to Privacy

Beneath the constitutional system of protection for the rights of personality, the German civil law ensures a number of various claims against legal violation of personal rights.

First § 823 and § 1004 of the German Civil Code guarantee a civil general right to personality, which is protected against interpersonal violations or other impairments. These claims are damage claims or injunctive reliefs. In addition, § 12 of the German Civil Code grants the right to a personal name.

The collection, use and processing of personal data is protected and regulated by special legislation, the Federal Data Protection Act (FDPA).

4. Fundamental rights in employment relationships

As mentioned before, fundamental rights also have an impact to the civil law. This impact does not only spread to an objective value system for the German system of law or an interpretation aid for undefined legal concepts, but also influences contracting

[42] Federal Constitutional Court, ruling of 10. 11. 1998 – 1 BvR 1531–96.
[43] Maunz/Dürig/Di Fabio, Art 2 GG, recital 138.

parties indirectly. Although private parties are not addressees of fundamental right and fundamental rights do not apply directly between the contracting parties, they unfold indirect third-parties-effects.[44]

This effect is derived both from the spill-over-effect of fundamental rights to civil law as interpretation aid and the legislature's duty of protection. Therefore, fundamental rights have to be used as interpretation guidelines for civil general, undefined clauses, e.g. §§ 138, 157, 242, 826 German Civil Code. This is for example the case concerning the principle of "necessity" in the (FDPA), which is addressed below. If an employee is dismissed, the same is the case, as any dismissal is subject to proportionality. When determining what is proportional, fundamental rights have to be taken into account.

a) The right to privacy as protection obligation in civil law

As a fundamental right, the German general right to privacy grants a protection obligation also to the civil law. To meet these requirements the legislator expressly stipulated, "the employer and the works council shall safeguard and promote the untrammelled development of the personality of the employees", § 75 (2) Work Constitution Act (Betriebsverfassungsgesetz, hereinafter WCA).

Furthermore, the right to privacy enters the employment contract relationship from the obligations to mutual consideration, protection and support standardized in § 242 German Civil Code.

b) Examples of protection of personality for employees

In employment contract relationships, the protection of personality of employees has a great significance, but also has to be harmonized with opposite interest of the employers.

First, off-duty behaviour is not subject to employer's restriction. Therefore, employees do not have to conform their personal way of living to the employer's ideas of morality and ethics.[45] Nevertheless, it may be permissible to regulate off-duty behaviours by

[44] Boecken/Düwell/Diller/Hanau, Art. 3 GG, recital 50.
[45] ErfK/Schmidt, Art. 2 GG, recital. 76.

employment contract or collective agreements, if it is necessary to ensure the corporate credibility.[46]

As well as the personal way of living, the external appearance belongs to the personal right of employees. Therefore, personal styling of hair or clothes is not a matter of the employer. As an exception, the external appearance may be prescribed, if it is required for safety reasons. In addition, the employer may prescribe work clothes, if the process of balancing legal and other interests results in the need for work clothes.

As a last example, the right to personality requests comprehensive protection against defamation. Generally speaking, the general right to personality protects employees against behaviours, which compromises the claim of social validity. Degrading treatments are permanent and groundless video surveillance, body search without a special reason, as well as every form of sexual harassment.[47] The employer also has to take measures in case of workplace bullying or permanent harassment by supervisors.

5. The Role of Art. 8 ECHR and Art. 7, 8 EU-CFR in the German Case Law

In the recent jurisprudence, both the Federal Constitutional Court and the Supreme Court use Art. 8 ECHR as well as the German right to personality conjointly as source of law for a right to privacy. From an overview of the legal scope of Art. 8 ECHR as well as Art 2 (1) in conjunction with Art. 1 (1) of the German constitution, the courts develop a general legal concept for the protection of privacy rights.

For example, the Supreme Court adjudicated in a case of violation of the right to privacy by spam mails.[48] It affirmed an illegal intrusion in the general right of personality and based the judgment both on Art. 8 ECHR and Art 2 (1) in conjunction with Art. 1 (1) of the German constitution.

[46] Ibidem.
[47] ErfK/Schmidt, Art. 2 GG, recital. 76.
[48] Federal Civil Court, ruling of 15.12.2015 – VI ZR 134/15.

Question 2): Legal Workplace Surveillance

In what cases and in which form is surveillance of employees at work legal and in which cases/forms is it prohibited? Please consider: (secret) video and audio taping, monitoring of computer and email activities, GPS tracking, personal searches etc. What are the relevant sources of law?

I. Legal Framework

An employment contract is the agreement between the employer and the employee that commits both of them to carry out certain rights and obligations. The employer has the right to monitor the employee's duties under the employment contract.

In work reality, there is a growing tendency of using technical devices to monitor the workplace. In face of omnipresence of surveillance mechanisms, the employer has a powerful instrument, which could be used for intimidation causing highly psychological pressure.[49] Consequently, the work performance could diminish, the rate of illness could increase and worst of all the monitoring pressure could cause a worker's alienation from its work. The German legislator, therefore, tries to reduce the misusing of workplace monitoring. According to the constitutional law, especially the general right of personality (article 2 (1) in conjunction with article 1 (2) German constitution), three elements shall be taken in into account: (1) the right of self-determination, (2) the right of self-probation and (3) the right of self-expression. Those three elements unfold third-party effects on all fields of law beneath constitutional law. In a context of workplace monitoring the legislator created obstacles for an unobstructed surveillance of employees codified in the Federal Data Protection Act [Bundesdatenschutzgesetz], hereinafter, FDPA.

Any collection of personal data concerning individual employees by the employer within an employment relation is subject to the limits set by the Federal Data Protection Act. This law is not only binding for public authorities, but also for private entities as soon as they process or use data by means of data processing systems or collect data for such system. Data collection or the use of data is only permitted with the consent of the concerned person (= the "owner" of data) or if one of the provisions of the FDPA

[49] Richardi/Kortstock, p. 383.

or another law (for example the Telecommunications Act) specifically allows it (§ 4 FDPA). Consent has to be declared in written form (§ 4a FDPA).

Details concerning the collection, process and use of personal data are stipulated in § 32 FDPA. Workplace surveillance in any form is a collection of personal data. § 32 FDPA stipulates that data may – without the consent of the employee – only be collected, if a necessity requires the employer to do so. This is the case if the employer is obliged by law to collect data (for example for tax or social security calculations) or if the execution of the working contract makes the collection necessary. If such a necessity exists or not is a case-to-case question. The interests of both parties of the working contract have to be taken into consideration.

The § 4 of FDPA provides that the employer must inform the employee about all monitoring activities, especially how the recorded data is processed and used, and those activities must be confirmed by the employee in question. The mentioned consent must be declared freely by the employee.

In conclusion, the basic principles in German law for monitoring are, that every surveillance activity without necessity or consent is regularly illegal.

II. Visual Monitoring

There are special legal regulations in German law concerning the kind of monitoring equipment. In particular, the use of TV surveillance systems and photography needs a precise legal evaluation. The law distinguishes between public and non-publicly accessible areas. Openly visible TV surveillance systems located in a publicly accessible area need to be made discernible by appropriate means, § 6b (2) FDPA. Monitoring in publicly accessible areas is only allowed in so far it is necessary for the employer to exercise the right of domiciliary or to pursue rightful interests for precisely defined purposes, § 6b (1) Number 1 and 2 FDPA. Strictly forbidden is the monitoring inside bathrooms or locker rooms.[50] It is for example legal, to install video equipment in supermarkets to prevent theft by customers. Therewith any hidden surveillance of public areas is in principle prohibited.[51]

[50] Dann/Gastell, p. 2948.
[51] Federal Labor Court, ruling of 27.03.2003 – 2 AZR 51/02.

§ 6b FDPA is furthermore not applicable for non-publicly accessible areas. In German law, there is no specific regulation dealing with monitoring in non-publicly areas. This lack of regulation is filled by the judiciary arguing that the group of persons in restricted areas are more manageable than in public areas, therefore it would not be reasonable to justify a broader surveillance.[52]

Hidden TV recordings may be legal if there is a heavy suspicion or any other activity detrimental to the interest of the employer. Insofar the general rule for data collection in a working relation, § 32 FDPA is applicable. It specifically acknowledges suspected felonies as a reason for data collection. The utilization of hidden monitoring equipment can be justified in those cases as long as the employer complied the principles of proportionality and if no other gentler measure had been chosen. In case of doubt one has to ask if the call for police forces to investigate a suspected felony.

Nevertheless, in companies with works councils the employees have the right to interfere in the questions of implementing surveillances measure, § 87 (1) No. 6 Works Constitution Act [Betriebsverfassungsgesetz]. This law binds the employer and in case of infringement the works council can stop unlawful surveillances with ordering provisional measures. The role of the works council will be addressed below, see question No. 3.

The infringement of the above-mentioned regulations constitutes a criminal offense of § 201a German Criminal Code [Strafgesetzbuch] (Violation of intimate privacy by taking photographs) and shall be punished with a fine or up to two years' imprisonment.

III. Acoustic Controls

Eavesdropping on telephones and reading fax or SMS is only allowed by judicial order, otherwise it constitutes a criminal offence against § 201 German Criminal Code (Violation of the privacy of the spoken word). In this context, not only the privacy of the employee may be violated, but also the rights of the person on the other end of the line. The German courts said that any form of eavesdropping is to be seen as an attack of privacy.[53] Exceptionally, the eavesdropping is allowed when telephone conversations are an essential part of business practice. For example, in businesses like call-

[52] Federal Labor Court, ruling of 07.10.1987 – 5 AZR 116/86.
[53] Federal Constitutional Court, ruling of 31.01.1973 – 2 BvR 454/71.

center services eavesdropping can be necessary for quality control. The listing can be legal in these cases as long as the interference is – according to content, form and circumstances – required and the least restrictive measure at the same time.

On the other hand, the surrounding circumstances of telephone calls, e.g. time spent for a call, telephone numbers and telephone costs, can be monitored. But here the above-mentioned limit of necessity applies. Surrounding data may only be collected, if this is necessary, which is for example the case for quality control, for billing reasons, or to maintain the orderly function of the company's telecommunication system itself. At this point the employer's right may take precedence over the employee's right of personality.[54] Professions with duty of confidentiality are excluded from this regulation. According to § 203 German Criminal Code (violation of private secrets) it constitutes a criminal offence if conclusion could be drawn to the interlocutors.

Private telephone calls at work are subjects to § 88 (1) Telecommunications Act [Telekommunikationsgesetz]. Thus, every private call falls under confidentiality of communication. The violation of this policy is a criminal offence punishable by §§ 201, 206 German Criminal Code.

IV. Email, Inter- and Intranet and Data Reconciliation

The same regulations are applied on the surveillance of electronic means of communication as for the acoustic controls. According to the Federal Labor Court the use of email communication shows more similarities with a telephone conversation than with a formal letter, because of its fast and immediate exchange of information.[55] This shall not apply if the email communication serves as commercial letter in terms of § 257 Commercial Code [Handelsgesetzbuch] in conjunction with § 126b German Civil Code [Bürgerliches Gesetzbuch]. The addressee and recipient have to assume that in working process such emails will be read by several third parties. As long as the email has no commercial nature it can be expected that emailing is a fast and furtive form of communication like a telephone call.

Basically, the employer is at most allowed to monitor the surrounding circumstances of an email communication. Concurrently, the employer has a significant economic

[54] Federal Labor Court, ruling of 27.05.1986 – 1 ABR 48/84.
[55] Wolf/Mulert, p. 443.

interest in knowing officially exchanged emails in order to possibly plan ahead. Therefore, the employer may demand such emails. In the event that private email-accounts are set up on the employer' server, any form of immediate and mediate surveillance is strictly prohibited. In summary, according to § 32 (1) FDPA employers can access any email communication as long as the email has a pure commercial nature and is not flagged as private in any way.

Concerning intranet-based computer systems, German law is more rigorous. If network-based computer systems were used for creating working and behavior profiles of employees, the whole personality of the employee and the work quality would be registered and categorized.[56] The lawmaker forestalled a complete surveillance.[57] Hence the using of the intranet in order to collect data concerning data content or working speed is illegal. Rather, the employer must be confined to quality controls on a random basis.[58] Employees with free working hours must not be monitored in any way.[59] If the employer wants to prevent any private use of the Internet, filtering software and entrance barriers can be installed.[60]

Generally impermissible is the use of technical devices in purpose of motion profiling. The principle of German law is to forestall the "glass human being", otherwise it would cause an absolute lack of freedom. The monitoring with tracking software, e.g. RFID, GPS, is only legal, when the monitoring is absolutely necessary under the working contract, it must be transparent, the employee has to express his/her explicit consent and monitoring will not cause any disadvantage for employee.[61]

In summary, in German law there is basically a prohibition of any form of surveillance behind the back of an employee. Exceptionally, the employer could use such surveillance if the employee shows a suspicious behavior. In those cases, the employer always has to respect the principle of proportionality and shall use the least stringent means. In case of doubt the employer shall inform investigatory authorities. The infringement constitutes a criminal offence.

---

[56] Zum Mikrozensus BVerfG v. 16.6.1969, 1 BvL 19/63, BVerfGE 27, 1, 6.
[57] Fitting, § 87 BetrVG, recitals 232 ff, 252 f.
[58] Burkhard et al., § 611 BGB, Rn. 530.
[59] Ibidem.
[60] Däubler, ArbR, recital 477.
[61] Labor Court Kaiserslautern, ruling of 27.08.2009 – 1 BVGa 5/08.

Question 3): Collection and Use of Health Data

Data protection relating to health: In which cases (if at all) may the employer ask employees (or applicants) to reveal information relating to his/her health or submit to medical tests? What are the relevant sources of law?

I. Collection of Health Data

In the German data protection law, health data are ranked among the "special types of personal data" according to § 3 (9) FDPA. Health data includes biometric data like fingerprints or retina patterns as well as data concerning illnesses. Their collection, processing and use is regulated by § 28 (6) FDPA. Hereafter particularly strict standards apply to employers, higher as the above mentioned general standard of § 32 FDPA.

Health data collection is – without the consent of the employee – only permitted if "this is necessary in order to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in excluding such collection, processing or use" (§ 28 (6) No. 3 FDPA). Beneath the general necessity principle, health data collection requires an assessment of the interests of employee and employer and can only be collected in direct connection with a legal dispute. Health data may according to § 28 (6) FDPA also be collected when the life of the employee or third persons is at stake.

II. Health Data in Job-Application Processes

With regard to pre-contractual data collection, § 28 (6) FDPA also applies to job interviews.[62] Vague and general questions recording to the overall health of the applicant are prohibited.[63] Only if concrete indications allow the conclusion to doubt the medical fitness to fulfil prospective workplace requirements, the right to ask a corresponding question may be accepted.[64] The employer cannot be forced to employ a person which is with some probability unable to fulfil the prospective position. But in a second step it has to be assessed if the applicant's interest of privacy overweighs the employer's

[62] Thüsing/Lambrich, p. 1152.
[63] ErfK/Preis § 611BGB, recital 282.
[64] Federal Labor Court, ruling of 12.08.1999 – 2 AZR 55/99.

interest in the disclosure of health data.[65] Such protectable interests of the employee may be confidential diseases, which may cause stigmatization (e.g. HIV, alcoholism).

The Federal Labor Court derives from these restrictions the following limitation of the right to question:[66]

- Does an illness or an impairment of health exist, which limits the suitability for the intended position in a permanent or periodical way?

- Do contagious diseases exist, which do not have an effect to the efficiency, but might endanger further associates?

- Can it be expected, that at time of starting the new position an inability to work is present, e.g. by a planned surgery?

Questions about disabilities are fundamentally unlawful, § 8 (1) General Equal Treatment Act (GETA). In exceptional cases, the employer may ask about disabilities, if the absence of these is necessary as a substantially and crucially professional requirement.[67]

A distinction must be made between the permissibility of the right to question in relation to personal health data and the permissibility of medical examinations.

An examination shall be permitted only, if it does not pose a considerable impact to mental and body well-being.[68] Therefore, medical examination must be required to ensure essential and decisive professional requirements.[69]

Similar to the right to question regarding to personal health data in the pre-contractual phase, the right to question also is limited during the employment. If an employee is absent due to illness, the employer has a claim to get immediate notification of the duration of absence, § 5 (1) Continued Remuneration Law. However, he has no claim to get the medical diagnosis or the medical reason for the absence.[70]

As well as pre-employment, medical check-ups are (as stated above) legally limited, routine check-ups during the employment are generally unlawful. As an exception, the

[65] Boecken/Düwell/Diller/Hanau/Brink, § 32 BDSG, recital 62.
[66] Federal Labor Court, ruling of 07.06.1984 – 2 AZR 270/83.
[67] Federal Labor Court, ruling of 17.12.2009 – 8 AZR 670/08.
[68] Bayreuther, p. 682.
[69] Boecken/Düwell/Diller/Hanau/Brink, § 32 BDSG, recital 66.
[70] Boecken/Düwell/Diller/Hanau/Brink, § 32 BDSG, recital 97.

employer can request a medical examination if concrete indications show a physical or psychological relation to the workplace requirements.[71]

III. Health Data Collection through "Wearables"

A special data protection issue is the "wearable". These are mini computers or a part of a technical device, which is carried on the body. Sensors track and record personal health data and storage them for personal analysis of health and fitness.

From a data-protection point of view, wearables may cause a loss of control of privacy and personal data. This also may cause issues in the business environment.

To begin with, there is the possibility that the employer could arrange the usage of wearables.[72] In that case it is necessary to respect the WCA, Works Constitution Act [Betriebsverfassungsgesetz] in addition to the Federal Data Protection Act (FDPA) and there has to be a mandatory consultation with the collective representation bodies. This process derives from the usage of wearables because it is inevitably related with the processing and recording of individual-related data.

Second, employees could use wearables voluntarily for reasons, which are linked to their health care. It is also in this case necessary to respect the WCA and the FDPA. Besides this, it is essential that the employees sign a declaration of consent to verify that they have decided voluntarily to participate at a company health care program.[73]

The third and last group of possibilities contains cases in which the employees bring their own devices (wearables) into the company and use them for private interests only. Because of this purpose of usage, the FDPA is not applicable, neither is the WCA.

In any other as the latter case, it is important to cooperate with the collective representation bodies to find some agreement to ensure the personal rights of third parties. The employer must come to an agreement with the works council before he is allowed to implement a new device in his enterprise. This calls attention in particularly with regard to the possibility that employees could use wearables secretly and infringe the individual rights of their colleagues.

---

[71] Ibidem.
[72] Kopp/Sokoll, p. 1352.
[73] Kopp/Sokoll, p.1357.

Question 4): The Role of Collective Representation Bodies

What is the role of collective representation bodies in regard of secret or open surveillance measures? Is the works council's prior approval necessary?

In general, the collective representation bodies have different tasks and functions, especially in the areas where they have participation or co-operation rights. The most important collective representation body in Germany is the works council. Works councils can be formed by the employees through general election. All relevant provisions regarding the works council, its election and its rights can be found in the Works Constitution Act (WCA) [Betriebsverfassungsgesetz – BetrVG].

I. Control Function of the Works Council

One of their main function is to control the management within a company.[74] The works council controls the compliance of the employer with all employee-protecting laws. Therefore, the works councils have to ensure, according to § 80 (1) No. 1 WCA, within the scope of general tasks, that current laws, which are in favor of the employees are applied. Among these laws is the FDPA (mentioned above: Federal Data Protection Act). Correspondingly – because otherwise a control is practically impossible – the works council has a right to be informed by the employer concerning all relevant measures in place to ensure compliance with the data protection legislation.

The works council is also entitled to care for the protection and promotion of the personal rights of employees according to § 75 (2) WCA. Among these personal rights is the right of privacy. If the employer grossly violates data protection laws as the FDPA, the works council may file an injunctive relief at the Labor Court.

II. Codetermination Rights of the Works Council

Some of the most important tools of employee participation are regulated by § 87 (1) WCA. Within the scope of these constrainable rules the employer cannot set working

[74] Forgo/Helfrich/Schneider/Schoof, Kap. 14, recitals 44ff; Schaub/Koch/Linck, ArbeitsR-HdB, Kap. XI, recitals 47f.

conditions unilaterally. It is necessary to know that works agreements are contracts between the employer and the works council, that apply to all employees in the business operation, whether they are trade union members or not. A works agreement shall be executed and displayed by the employer (§ 77 (1), (2) WCA). They are mandatory and directly applicable (§ 77 (4) WCA). Works agreements grant rights – like law or collective agreements – directly for employees, which cannot be waived, except with the agreement of the works council, § 77 (4) WCA. If no agreement between works council and employer is reached, it is possible for the works council to replace unilateral arrangements by the employer through arbitration agreements.[75] As long as no consensus between works council and employer is found, any unilateral regulation by the employer is void, even in the legal relation between employer and employee. But the Federal Labor Court awarded an injunctive relief to the works council, if the employer grossly undermines the works council's codetermination rights (basis for the claim: §§ 1004 (1) BGB, 823 (1) German Civil Code).

The subjects of works agreements are set in § 87 (1) WCA. In the field of surveillance measures at the workplace is for instance § 87 (1) No. 6 WCA relevant. It helps to protect the general personal rights of the employees against interventions from anonymous technical control equipment.[76] This is valid for such equipment, which is suitable to monitor the behavior or performance of the employees. The term "technical control equipment" means any instrument whether it is optical, mechanical, acoustic or electronic.[77] This includes any form of audio and video surveillance, but also time recording devices and tachographs. It is irrelevant whether or not the employer actually processes the data generated by these devices. Both, the Federal Labor Court as well as the predominant opinion of scholars are extending the term "surveillance". They consider that the term involves two dimensions in this context. The codetermination right does not only apply when data is collected electronically by one of the mentioned technical devices. It also applies if someone is working with data collected otherwise e.g. entering non-technically collected data into a computer system. So, this rule is applicable, if an instrument of technical control equipment meets just one of these criteria.[78]

[75] ErfK/Kania, § 87 BetrVG, recital 1.
[76] ErfK/Kania, § 87 BetrVG, recital 48.
[77] Federal Labor Court, ruling of 08.11.1994 – 1 ABR 20/94; DKK/ Klebe, § 87 BetrVG, recital 137; Fitting, § 87 BetrVG, recital 225.
[78] Federal Labor Court, ruling of 10.12.2013 – 1 ABR 43/12.

The employer must come to an agreement with the works council before he is allowed to implement a new device in his enterprise.

Other codetermination rights also have a data-protective dimension. For example, the employer has to explain his long-term staff planning to the works council, which involves the disclosure of personal data. He also needs the consent of the works council if he wants to make the employees fill out questionnaires (§ 94 (1) WCA). And the works council must agree with general guidelines the employer sets up for the choice of new employees, for relocations, for dismissals and regrouping employees.

In the end, it should be clear that the collective representation bodies have an important role (as control authority), especially in the context of surveillance at the workplace. Their rights according to the WCA have to be respected by the employer. If they are not, all one-sided decisions by the employer that affects employees are invalid.[79] Therefore, it is necessary to get the consent from the collective representation bodies.

Question 5): The Role of Independent Authorities

Do executive and/or independents authorities occupied with data protection (=authorities which uphold the laws protecting personal data) exist and what is their role in this context? Can such authorities impose sanctions for non-compliance with data protection legislation? Is it a (criminal) offense to collect or process data in violation of the applicable protective provisions?

Three entities guarantee the data protection for companies: firstly, the data protection officer, secondly collective representation bodies and thirdly the data protection supervisory authority. All of them have the same goal to ensure the data protection laws but each of them has their own perspective on this.

The data protection officer provides the fulfillment of the data protection laws under the interests of the company. Compared to this, the collective representation bodies care about the employees' interests. Thirdly, the data protection supervisory authority carries out its tasks in public interest. It is for this reason that there is a charged relationship between these three actors.[80]

[79] ErfK/Kania, § 87 BetrVG, recital 136.
[80] Kort, p. 1345.

I. The Role of the Company Data Protection Officer and his Sanction Mechanism

According to § 4f and § 4g FDPA (Federal Data Protection Act) it is necessary to have a data protection officer for private companies if they process personal data in an automated way. The same applies if they process data in any other way, when at least 20 persons are permanently employed for that purpose. The task of the data protection officer is to make sure that the enterprise complies with all applicable data protection laws. He works without reference or directives from the CEO or the data protection supervisory authority, but in the private company interest. It is for this reason that the data protection officer is not allowed to give information about possible or real violations of data protection rules to the data protection supervisory authority. He has no own executive power.[81] So if the relevant rules are not observed, the company data protection officer may in principle only report this to the management, but has no power to take further action.

II. The Role of the Data Protection Supervisory Authority and its Sanction Mechanism

Data protection supervisory authorities are based on the federal level as well as on the state level. The role of the data protection supervisory authority is appealed in § 38 FDPA. The data protection supervisory authority controls that all data protection laws are observed. It also gives guidelines for compliance with these rules to data protection officers on company level. The data protection supervisory authority is entitled to demand information from everybody processing personal data and is also entitled to enter private (non-residential) property during business hours in order to check that any data is only collected and processed according to the relevant provisions of the FDPA. It may forbid any given form of collection or process of data if the right of privacy is grossly violated. In such cases, it may inform the business supervision.

According to § 38 FDPA the public data protection authority is on the other hand not a legal supervisor of the company data protection officer.[82] In the case of lack of knowledge or reliability of the data protection officer it is possible in accordance to § 4f

[81] Kort, p. 1345 f.
[82] Kort, p.1348.

(3) and § 38 (5) FDPA to demand a dismissal from the company. Furthermore, the authority is able to impose penalties, which are according to §§ 43, 44 FDPA financial penalties between 50.000 € and 300.000 € or an imprisonment for two years against the acting manager of the company. A fine can be imposed if the company violates the data protection rules set by the FDPA intentional or at least due to negligence. Imprisonment is only possible if personal data is sold illegally.

III. The Role of the Representation Bodies and their Sanction Mechanism

The role of the representation bodies in context of employee data protection is regulated in § 80 I No. 1 WCA. Furthermore, their right to promote the employees' personal development is put down in § 75 II WCA. According to this regulation it is not only the task of the employer to protect and encourage the development of the free personality of the employees but also of the representation bodies. For the details please see above, question 4. It is for this reason, that beside the data protection officer, the representation bodies ensure the fulfilment of data protection regulation.

We have also elaborated on the works council's codetermination rights out of §§ 87, 92, 94 and 95 WCA.

In view of the Federal Labor Court[83] and out of § 99 (2) No. 1 WCA it is possible for the representation bodies to refuse the approval in the context of displacement or hiring an employee as data protection officer, if this person does not meet the requirements according to § 4f (2) FDPA.[84] But this is only valid for an internal solution of the data protection officer.

IV. Is it possible for the employer to collect and process data against the data protection regulation?

The Supreme Labor Court has decided, that a violation against a participation right or a works agreement is not enough for the inadmissibility of evidence (see below, question 6). It is rather crucial whether using this evidence through the court could violate

[83] Federal Labor Court, ruling of 22.03.1994 – 1 ABR 51/93.
[84] Fitting, § 99 BetrVG, recital 203.

fundamental rights of the opposing party.[85] Compared to this, legally gained evidence is always usable, unless it was forgotten to respect the fundamental rights of the opposing party during legal evaluation of the evidence.[86]

In the end it should be clear, that the data protection officer acts on behalf of the company's interest and besides this the representation bodies ensure the fulfilment of data protection regulation. Furthermore, it is crucial to mention, that a violation against the data protection regulation by the employer is not automatically connected with the inadmissibility of evidence for a trial.

Question 6): Illegally Obtained Material as Evidence in Court

The dispute before a labor court is a civil-law procedure. There is a special code of procedure for labor courts [Arbeitsgerichtsgesetz], but it follows the same principles and widely refers to the general Code of Civil Procedure. German civil courts do not have the right to investigate circumstances by themselves; instead they evaluate allegations and corresponding evidence provided by the parties.[87] In this process the court has to respect law of procedure. These rules do in principle not exclude illicitly acquired material from lawsuit.[88] Dismissals due to suspicion (for example: for theft or fraud) often prove a problem in regard to law of evidence.

In those cases, the employer frequently lists evidence obtained through illegal surveillance measures in court. Generally, neither the Code of Labor Procedure nor the Code of Civil Procedure provide any written limitation on illicitly acquired evidences.[89]

However, the court may consider evidence acquired by illegal data collection (for example: illegal video surveillance) inadmissible due to a violation of the employee's right of privacy.[90] To determine if this is the case, the court weighs the implications of the surveillance measure in light of the employee's fundamental right of privacy on the one

[85] Grau/Dzida, p. 1203.
[86] Ibidem, p. 1204.
[87] ErfK/Koch, § 46 ArbGG, recital 5; Zöller/Greger, introduction to § 128 ZPO, recital 10.
[88] Federal Labor Court, ruling of 16.12.2010 – 2 AZR 485/08; Kratz/Gubbels, p. 655 f; Joussen, p. 42; Frings/Wahlers, p. 3132; Herrmann/Soiné, p. 2927 f; regarding criminal procedure: Federal Constitutional Court, ruling of 07.12.2011 – 2 BvR 2500/09.
[89] Federal Labor Court, ruling of 21.11.2013 – 2 AZR 797/11.
[90] Federal Labor Court, ruling of 21.11.2013 – 2 AZR 797/11.

hand and the employer's right of due process and access to justice – Art. 103 (1) of the constitution on the other.[91] The information procurement has to be justified. This is assumed if the illegal surveillance measure is the last remaining mean to determine an illegal or unfriendly action of a suspicious employee. For the employer, there has to exist a self-defense situation.[92] The evidence is inadmissible, if the employer could have obtained it in a less invasive way.

This is most likely illustrated in that case: The employee worked in a Cash & Carry market and was suspected for repeatedly stealing items from the store. Subsequently his locker was opened by a member of the direction board in the presence of a member of the works council while the employee was on his shift. The locker was filled with items of the employer, price tags and anti-theft buttons removed. Thereupon the employee was fired. The employee sued against the dismissal and won the case. The Federal Labor Court stated that opening the locker in absence of the employee was not the least stringent means.[93] Instead the employer should have opened the locker in the presence of the employee.[94]

Practically that means, those evidences, often TV-surveillance material, shall be inspected visually corresponding the allegation against the employee it is supposed to prove. Doing so – considering that the employer has to commit that he used unlawful measures, § 138 Code of Civil Procedure (obligation to tell the truth) – the court may decide upon the admissibility.

In summary, the use of illicitly evidence is not generally impossible. When considering its admissibility, the courts take into account the constitutional right of privacy of the employee. Illicitly obtained material is only admissible if the surveillance measure is seen as ultimate ratio. If there was no other possibility to prove reasonable allegations and the employer is in a self-defense-like situation, the illegal acquired evidence can be used in court.

[91] Federal Constitutional Court, ruling of 09.10.2002 – 1 BvR 805/98; Federal Labor Court, ruling of 21.06.2012 – 2 AZR 153/11 and ruling of 20.06.2013 – 2 AZR 546/12.
[92] Federal Labor Court, ruling of 21.11.2013 – 2 AZR 797/11 and ruling of 20.06.2013 – 2 AZR 546/12.
[93] Federal Labor Court, ruling of 20.06.2013 – 2 AZR 546/12.
[94] Ibidem.

Question 7): Protection of whistleblowers against dismissal

I. Definition of whistleblowing

The term derives from the literal meaning in English „to blow a whistle “, but in the broadest sense it means to reveal actual or alleged wrongdoings in companies (this includes illegal actions, cases of corruption, violations and breaches of tax law, social security law, working conditions acts and environmental protection legislation) by critical comments or lodging a complaint of one of the employees of the company. In many Anglo-American countries whistleblowing policies have become part of the compliance-culture, whereas in Germany there are no generally binding regulations hence every case has to be analyzed separately. There are only a few sparse provisions that affect the German civil servants' rights. Some political parties started legislative initiatives to codify the rights and obligations of whistleblowers, but so far none of them were successful.

To be able to understand how whistleblowers can be protected in Germany, it is important to know that the German judiciary differentiates between internal and external whistleblowing. That is why both phrases have to be defined.

1. Definition of internal whistleblowing

Using a chain of communication within the enterprise established to report wrongdoings by colleagues or superiorst is not considered as whistleblowing at all. If the informant does not use the generally established lines of communication or reporting channels within the company, which is usually reporting wrongdoings to colleagues, supervisors, the management, works council or others, then this is the so-called “internal whistleblowing”.[95]

[95] Kania, in: Röller, Whistleblowing recital 9.

2. Definition of external whistleblowing

If the informant contacts external authorities such as a law enforcement agency, a supervisory authority, or the media, then this is the so-called “external whistleblowing”.[96]

II. Legal consequences of internal whistleblowing

First of all, it has (again) to be pointed out that there is no protection law or general binding regulations for whistleblowers in Germany. So, a dismissal is a strong possibility in whistleblowing-cases. In Germany, there are different kinds of dismissals concerning the notice period, a dismissal according to the legal notice period is called ordinary termination, one that ends the contract and working relation immediately is called extraordinary termination. Furthermore, the German legislator differentiates in the Act against Unfair Dismissals (Kündigungsschutzgesetz) between the grounds for dismissal:

- behavioral dismissal
- dismissal on personal grounds
- compulsory redundancy.

A dismissal is only possible if one of these reasons is present in a given case – at least within the realm of application of the Act against Unfair Dismissals. When whistleblowers are dismissed, it is (pretty much) always because of their behavior, whether the legal notice period is kept or not depends on the factual circumstances. The crucial question is the following: Does whistleblowing represent a misbehavior which is sufficiently severe to justify a dismissal? Furthermore, the employee should in principle be given a chance to change her/his behavior hence the employer has to warn her/him before she/he can dismiss the employee. In some very severe cases when it would be unbearable for the employer to work any longer with the person because of a very bad breach of trust or violation against some legal regulation, the employee can be dismissed immediately.

[96] Kania, in: Röller, Whistleblowing recital 2.

Again: As no statuary law concerning whistleblowing exists in Germany, the following "rules" are a compilation of the case law given by the courts.

When it comes to internal whistleblowing, different cases can be distinguished: A sufficiently severe misbehavior (to justify an immediate dismissal) is acknowledged for example: If a whistleblower claims knowingly or grossly negligent untrue or false facts about the employer or colleagues and if this either disturbs the industrial peace, has severe negative impacts on the work atmosphere or the performance. Such a violation can be a reason for dismissal, in cases when a prior warning about it was unsuccessful.[97]

If the whistleblower files a true wrongdoing and reports it to someone within the company, she/he cannot be dismissed for it unless one of the severe consequences (disturbance of industrial peace etc.) occurs – in general, and in any case if a specially established reporting channel is used.[98]

III. Legal consequences for external whistleblowing

In cases of external whistleblowing (the public exposure of wrongdoing in the company) a conflict arises between the interests of the employer and of the public. The employer wants the protection of his good reputation, his business interests concerning the secrecy of internal processes and data. Also, external whistleblowing violates the contractual duty of loyalty of the employee. In contrast, a legitimate interest of an adjustment of the wrongdoing and a public interest in being informed about the wrongdoings when it comes to significant impediments exists. Again: the relevant question is: Does whistleblowing represent a misbehavior which is sufficiently severe to justify a dismissal? That is why all interests involved have to be balanced.

Whistleblowers are not always protected; hence the publication of internal information can represent a ground for dismissal according to § 626 (1) German civil code because of the breach of the contractual duty of loyalty. The decision whether it is a sufficient reason for dismissal or not depends on the exact case. Thereby many aspects have

[97] Federal Labor Court, ruling of 17.03.1988 – 2 AZR 576/87 and State Labor Court of Sachs, ruling of 21.01.2011 – 3 Sa 181/10.
[98] Kania, in: Röller, Whistleblowing, recital 6.

to be taken into account e.g. the former behavior of both parties, the reason for whistleblowing and so on.[99] Generally speaking: the more severe the reported wrongdoing was the less a dismissal is justified.

1. Protection of Whistleblowers in cases of external whistleblowing

In former times, external whistleblowing was always seen as a sufficient reason for dismissal.[100] Nowadays the judiciary has changed into a more liberal way of judging cases. Again: the question is if the whistleblowing constitutes a breach of the contractual duty of loyalty to the employer which is so severe that it is unbearable for the employer to continue the working relation.

This depends on the circumstances of any given case, especially on the behavior of both parties prior to the whistleblowing, the motivation of the employee to do so, and the extent of the reported misconduct of the employer.

There are some things that have to be taken into account. Every employee has the duty of consideration according to § 241 (2) German Civil Code. This includes that the employee is only allowed to file a public complaint against his employer when a legitimate interest exists; when the complaint is neither a disproportionate nor hasty reaction to new information and when the negative publicity of launching of a criminal judicial procedure does not carelessly endanger the existence of the company.[101] Before going public, the employee should try to inform other members of the company of the wrongdoing within the company and file an internal complaint first. There are cases in which this procedure is not possible and external whistleblowing represents the only option. In the following some examples for unreasonable internal whistleblowing are given.

Internal whistleblowing is neither possible nor can it be expected of the employee in cases:

- not only about petty offences

[99] Kania, in: Röller, Whistleblowing, recital 2a.
[100] Federal Labor Court, ruling of 05.02.1959 – 2 AZR 60/56.
[101] Federal Labor Court, ruling of 03.07.2003 – 2 AZR 235/02.

- when the employee would be subjected to criminal prosecution himself (§ 138 German Criminal Code – "Omission to bring planned criminal offences to attention of the authorities")
- when the employer commits an administrative offence or crime/felony himself
- where the employee is subject to an administrative offence or a crime
- when there is only a little chance to clarify the situation internally

In such cases, external whistleblowing is no reason to justify a dismissal.

Other reasons for the protection of whistleblowers include the following situations: The employee is obliged as a civic duty to testify in cases of an initiated investigation by the police or the public prosecution's office. If the employee gives a burdensome but true testimony against the employer this cannot lead to a dismissal, hence the whistleblower is protected for such cases. If the given testimony against the employer is untrue or false, this will certainly be seen as a reason for a behavioral dismissal.[102] Furthermore, every employee has the right to file a complaint in certain cases and will be protected against dismissal, e.g. in cases of violations of labor standards and employment protection provisions or violations of the Act on Protection of Health see here for § 17 (2) Workplace Health and Safety Act (Arbeitsschutzgesetz).[103]

To give an example for a case in which whistleblowing could not lead to a dismissal: A German geriatric nurse claimed wrongdoings of her employer, before she approached public she even tried to talk to her employer, but he was not interested. Hence, she had tried to solve the problem internally first. But due to the fact that this did not lead to any success, she did not have much choice but to inform the public about the wrongdoings. When her employer found out about it, she was extraordinarily dismissed on grounds of her behavior. That is why she initiated legal proceedings, German courts turned down her complaint. Therefore, she filed a complaint at the European Court of Human Rights (ECtHR) which decided that the dismissal was illegal due to the fact that she fulfilled her civic duty. Hence the decision of the German court was wrong.[104] The ECtHR expressed that whistleblowing is protected by Art. 10 ECHR and that the

[102] Federal Constitutional Court, ruling of 02.07.2001 – 1 BvR 2049/00.
[103] Kania, in: Röller, Whistleblowing, recital 3b.
[104] ECtHR, ruling of 21.07.2011 – 28274/08. (Heinisch./. Germany).

interest of the public to be informed overweighs the interest of the employer to keep his business secrets.

2. No Protection of External Whistleblowers

Sometimes it is not necessary to do external whistleblowing. In cases where the wrongdoing was not caused by the employer or someone in a similar position, but another employee, an internal hint would be reasonable. The employer has a right to be informed about unknown wrongdoings in the company, which are not subject of being unknown due to gross negligence, before the information are made public.[105]

Whistleblowers are not protected from dismissals, when there is no legitimate right to whistleblow. This applies in cases when the whistleblower knowingly gives false or untrue evidence or plans to damage the employer on purpose by publicizing information. In such cases the employee commits an abuse of rights.[106]

An employee falsely claimed that his employer committed traffic offences during a business trip. That is why the employer lost his driving license. Later it came out that the claim was wrong hence the employee was dismissed extraordinarily on grounds of his behavior. The employee took legal action against the dismissal but the German Federal Labor Court agreed to the dismissal because of the harm this wrong information had caused to the employer.[107]

IV. Whistleblowing Systems and Reporting Obligations

Every employee is generally obliged to immediately inform either his supervisor or his employer about imminent harm or disruptions.[108] This is especially true if damages or disruptions may be caused by a colleague through theft, embezzlement or a breach of the safety regulations within the own area of work or team. But also, if such events occur in another area of work than the one of the whistleblower and in cases where she/he is also not responsible for this area of work, a reporting obligation may exist. But the whistleblower is only obliged to inform the supervisor/ employer about it, when

[105] Federal Labor Court, ruling of 03.07.2003 – 2 AZR 235/02 and Kania, in: Röller, Whistleblowing, recital 3b.
[106] Kania, in: Röller, Whistleblowing, recital 6a.
[107] Federal Labor Court, ruling of 18.12.1980 – 2 AZR 980/78.
[108] Federal Labor Court, ruling of 07.12.2006 – 2 AZR 400/05.

there is a risk of personal injuries or significant material damage. The whistleblower is not obliged to name the person.[109]

But if a company has compliance or ethical regulations and all employees are officially informed about it, they are obliged to report any violations against these regulations. Most of the time there is a certain “whistleblowing”-procedure on how the wrongdoing or misbehavior has to be reported, this is also called whistleblowing-system. The management implements something like that to make sure to be informed about every behavior that is not according to legal or companies standards. This prevents whistleblowers of publicizing wrongdoings on the one hand. On the other hand, it provides the whistleblower with a sanction free internal option of hints and legal certainty for the consequences of her/his doing. International companies have to make sure to include the works council in German subsidiaries about the implementation of such regulations due to data protection regulations.[110]

The German legislator suggests to include information about who should get access to what kind of information, how the information should be collected and processed in the compliance or ethical regulations. A company could e.g. establish anonymous telephone hotlines, ombudspersons, consulting and mediation institutions or others. But it is not allowed to force employees to denounce their colleagues.[111] Besides that, the regulations have to ensure that someone who is falsely denounced is protected and that no one abuses the system to damage an employee’s reputation or her/his dignity.

Question 8):

Are the (legal) consequences of postings over social media about the employer, superiors, colleagues, workplace conditions and so on an issue in your country? If yes, can such postings lead to a dismissal and / or slander claims?

[109] Kania, in: Röller, Whistleblowing, recital 11a.
[110] Federal Labor Court, ruling of 22.07.2008 – 1 ABR 40/07.
[111] Federal Labor Court, ruling of 23.10.2008 – 2 AZR 483/07.

I. Balance of interests (freedom of expression vs. protection of personal dignity)

First of all, it is important to know that courts have to balance different rights of the employer for one thing and the rights of the employee otherwise on a case-by-case basis. In the context of social media, there are some rights that come into question. Art. 1 (1) GG gives every person living in Germany the right of freedom of expression. This means every employee can express her/his opinion. On the other hand, every employer is protected by the right to the personal honour, which limits the right of freedom of expression according to Art. 1 (2) GG. If an employee insults the employer this can be seen as a violation of general personal rights, of the human dignity and of the right to freedom of economic activity of the employer.

In cases when the employee insults the employer and causes a violation of honour by it, this can justify an ordinary behavioural dismissal as well as an extraordinary one.[112] Usually it is necessary to warn an employee first, so that she/he gets a chance to change but in cases of a particularly serious violation of honour, a warning is dispensable. A behavioural dismissal can also be justified in cases when the employee spreads untrue facts about the employer or treason of business and trade secrets.[113]

But it is up to the courts to distinguish between an insult and an objective criticism about the employer, the last one does not lead to a violation of honour of the employer hence does not justify a dismissal.[114]

II. Criterion: During working hours or in spare time

Another important aspect that has to be taken into account is whether the employee uses social media on a private level during working hours or not. If she/he uses e.g. Facebook during working hours although the employer does not allow the private use of social media, this is seen as a violation of contractual duties and the employer's right to manage. Such a behavior can justify a dismissal.[115]

[112] Bauer, p. 67.
[113] Schockenhoff, p.18.
[114] Kort, p. 1322.
[115] Göpfert/Wilke, p. 83.

The situation differs when the employee uses social media during in her/his spare time. In such cases, other aspects like the following have to be considered as well:

III. Criterion: Availability of information (marked privately or published in chats)

If a comment about the employer in social media can justify a dismissal while using it privately, depends on whether the information is freely accessible or was expressed confidentially. If an employee uses technical privacy settings to prevent the publication of confidential information, she/he can trust on the confidentiality during a protection against dismissal procedure.[116] The problem lies in defining what means confidentiality/privacy of an expressed opinion and what means the publication of information in the age of social media and the internet.

Some German labor law experts differentiate between where the comment was made. Was the comment made on the so-called Facebook-wall of the user her-/himself or did the employee leave a message on the Facebook-wall of someone else or was the comment made within a chat?

Some experts use this criterion to figure out to whom the information was accessible, therefore aspects such as how many Facebook friends the person has and how many of them are colleagues, are taken into account.

The labour court Hagen decided that no comment about the employer can be confidential, when 50 or more percent of the circle of friends are colleagues.[117] Comments in such an environment are public within the company and can be compared with a notice board within in the company.

Furthermore, the reason for making a comment has to be considered. It makes a difference whether the fact about the employer was given spontaneously (by commenting something or clicking the “I like” button Facebook provides its users with) or the comment was made in the heat of the moment or on the employee’s own initiative.[118]

[116] Kort, p. 1321-1323.
[117] Labor Court of Hagen, ruling of 16.05.2012 – 3 Ca 2597/11.
[118] Scheid/Klinkhammer, p. 6 and p. 9.

The labor court Duisburg decided that the behavioral dismissal was not lawful.[119] The employee was angry with his colleagues because they denigrated him before his employer. That was why he called them “smartasses” and “rolls of fat” on his Facebook page, but he did not mention their names. When the employer heard about it, he dismissed him. Even though the comment was marked „private“, the confidentiality argument did not apply because most of his Facebook friends were colleagues. But due to the fact that he only posted those comments after he heard what his colleagues had done, the court decided that he acted in the heat of the moment. Besides that, the employee did not mention any names in particular hence no colleague could be identified.

Other experts opine that differentiations between who is able to access the information are unnecessary because comments made on Facebook can never be considered as confidential. They justify their opinion by arguing that the internet is an unpredictable medium hence anyone has to be aware of the fact that any kind of detail can published at any time.

These different approaches show that there is no general rule to apply, when it comes to the expression of opinion in social media. At the end, it always depends on the individual case. Anyhow, it is recommended to be aware of the scope and the addressees of an insult.[120]

Due to the complex aspects which play a role in such cases, a judgement by the State Labor Court of Hamm shall be given as an example:[121]

An employee described her employer as “oppressor” and “exploiter” on her Facebook-wall. The court interpreted these comments as insults. Besides that, the comments were accessible to everyone (made public) hence they were intended to stay online for a longer period of time. Hence she was extraordinary dismissed due to her behavior because these comments were of reputational risk to the employer. The court agreed to the dismissal of the employer. Warnings as well as personal dialogues were dispensable in this case.

[119] Labour Court Duisburg, ruling of 26.09. 2012 – 5 Ca 949/12.
[120] BeckOK-ArbR/Stoffels, § 626 BGB, recital 106 a.
[121] State Labour Court of Hamm, ruling of 10.12.2012 – 3 Sa 644/12.

IV. Criterion: Compliance with Data Protection Regulations

Another important aspect in judging whether a comment made in social media can lead to a dismissal or not, has to do with data protection regulations. Most companies do research on their corporate image. When they come across comments of employees during such research, this is in accordance with legal regulations to use data for business reasons § 28 (1), 1 No. 3 FDPA (Federal Data Protection Act, mentioned above).

But if the employer obtains access to the social media account of an employee by fraud or forces the employee to give him access by e.g. faking an identity, this is seen as a violation against the FDPA hence any evidence obtained by one of the described methods cannot be used during a dismissal protection procedure.[122]

Courts have to balance the interests of employee's general personal rights on the one hand and the employers exploiting interest on the other, in cases of a breach of the data protection guidelines § 32 FDPA. To avoid situations like that the employer should access such information only through legal methods e.g. by revealing her/his true identity in social media.

V. Criterion: Treason of business and trade secrets

The treason of business and trade secrets can harm companies seriously, especially when those secrets are made available to the general public. Sometimes employees are not aware of such treasons, often a publication of such information happens due to a negligent handling of very sensitive facts, e.g. during a heated debate in chats. But even if the comment was irresponsible and made in the heat of the moment, it is a serious violation of the obligation of secrecy of business and trade secrets of the employee under § 241 (2) German Civil Code. That is why this can lead to an extraordinary behavioral dismissal. Furthermore, a treason of business and trade secrets can lead to claims for damages. The treason of business and trade secrets can harm the employer seriously hence he may claim for such damages.

[122] Kort, p. 1324.

Literature

Bauer/Günther: Kündigung wegen beleidigender Äußerungen auf Facebook, NZA 2013, p. 67ff

Bayreuther: Einstellungsuntersuchungen, Fragerecht und geplantes Beschäftigtendatenschutzgesetz, NZA 2010, p. 679ff

Beckschulze, Internet und E-Mail-Einsatz am Arbeitsplatz, Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen DB 2009, p. 2097ff

Boecken/Düwell/Diller/Hanau/Brink (Ed.), Gesamtes Arbeitsrecht, 1. Edition Baden-Baden 2016

Dann/Gastell, Geheime Mitarbeiterkontrollen: Straf- und arbeitsrechtliche Risiken bei unternehmensinterner Aufklärung, NJW 2008, 2945ff

Däubler, Das Arbeitsrecht II, 1. Edition, Reinbeck, 2009 (referred to as: Däubler, ArbR)

Däubler/Hjort/Schubert/Wolmerath (Ed.), Arbeitsrecht, 3. Edition, Frankfurt a.M. 2016 (referred to as: Däubler/Author)

Däubler/Kittner/Klebe/Wedde (Ed.), Kommentar zum BetrVG, 15. Edition, Frankfurt a.M. 2016

Epping/Hillgruber (Ed.), Beck'scher Online Kommentar GG, 31. Edition, München 2016 (referred to as: BeckOK/Author, Art. GG)

Forgo/Helfrich/Schneider/Schoof (Ed.): Betrieblicher Datenschutz, 1. Edition, München 2014.

Freckmann, Versteckte Kameras, seitenlange Protokolle bei Discounter Lidl, BB 22/2008, p. M 1

Freckmann/Wahl, Überwachung am Arbeitsplatz, BB 2008, p. 1904ff

Frings/Wahlers, Social Media, iPad & Co. im Arbeitsverhältnis, BB 2011, p. 3126ff

Fülbier/Splittgerber, Keine (Fernmelde-)Geheimnisse vor dem Arbeitgeber?, NJW 2012, p. 1995ff

Gola/Schomerus (Ed.): Bundesdatenschutzgesetz, Kommentar, 12. Edition, München 2015 (referred to as: Gola/Schomerus BDSG)

Göpfert/Wilke: Facebook-Aktivitäten als Kündigungsgrund, in: Arbeit aktuell 2011, p. 79ff

Grau/Dzida: Verwertung von Beweismitteln bei Verletzung des Arbeitnehmerdatenschutzes, NZA 2010, p. 1201ff

Herrmann/Soiné, Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, NJW 2011, p. 2922ff

Herzog/Herdegen/Scholz/Klein (Ed.) Maunz/Düring, Grundgesetz. Kommentar, Stand September 2016, 78. Ergänzungslieferung, München (referred to as: Maunz/Dürung/Author)

Joussen, Mitarbeiterkontrolle: Was muss, was darf ein Unternehmen wissen?, NZA-Beil. Nr. 1 2011, p. 35ff

Kopp/Sokoll: Wearables am Arbeitsplatz – Einfallstore für Alltagsüberwachung, NZA 2015, p. 1352ff

Kort: Soziale Netzwerke und Beschäftigtendatenschutz, NZA 2012, p. 1321ff

Kort: Das Dreiecksverhältnis von Betriebsrat, betrieblichem Datenschutzbeauftragten und Aufsichtsbehörde beim Arbeitnehmer-Datenschutz, NZA 2015, p. 1345ff

Kratz/Gubbels, Beweisverwertungsverbote bei privater Internetnutzung am Arbeitsplatz, NZA 2009, p. 652ff

Maties, Arbeitnehmerüberwachung mittels Kamera?, NJW 2008, p. 2219ff

Müller-Glöge/Preis/Schmidt (Ed.): Erfurter Kommentar zum Arbeitsrecht: 17. Edition, München 2017 (referred to as: ErfK/Author)

Richardi/Kortstock, Videoüberwachung am Arbeitsplatz – allgemeines Persönlichkeitsrecht – Grundsatz der Verhältnismäßigkeit, RdA 2005, p. 383ff

Rolfs/Giesen/Kreikebohm/Udsching: Beck'scher Online-Kommentar Arbeitsrecht, 42. Edition, Munich 2017 (referred to as: BeckOK-ArbR/Author)

Röller (Ed.): Personalbuch 2015 Arbeitsrecht, Lohnsteuerrecht, Sozialversicherungsrecht, 22. Edition 2015.

Schaub/Koch/Linck (Ed.): Arbeitsrechts-Handbuch, 15. Edition, München 2013 (referred to as: ArbeitsR-HdB)

Simitis (Ed.): Bundesdatenschutzgesetz, Kommentar, 8 Auflage, München 2014.

Thüsing/Lambrich, Das Fragerecht des Arbeitgebers – Aktuelle Probleme zu einem klassischen Thema, BB 2002, p. 1146ff

Vogel/Glas, Datenschutzrechtliche Probleme unternehmensinterner Ermittlungen, DB 2009, p. 1747ff

Wiese/Kreutz/Oetker/Raab/Weber/Franzen/Gutzeit/Jacobs (Ed.): Gemeinschaftskommentar zum Betriebsverfassungsgesetz: 10. Edition, München 2014 (referred to as: GK-BetrVG)

Wolf/Mulert, Die Zulässigkeit der Überwachung von E-Mail-Korrespondenz am Arbeitsplatz, BB 2008, p. 442ff

Zöller/Greger (Ed.), Kommentar zur ZPO, 31. Edition Frankfurt a.M. 2016

Appendix: Relevant German Provisions in English Language

Art. 1, 2 German Constitution

Article 1
Human dignity – Human rights – Legally binding force of basic rights

(1) Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.

(2) The German people therefore acknowledge inviolable and inalienable human rights as the basis of every community, of peace and of justice in the world.

(3) The following basic rights shall bind the legislature, the executive and the judiciary as directly applicable law.

Article 2
Personal freedoms

(1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.

(2) Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant to a law.

§§ 1, 4a, 6b, 32 FDPA

§ 1 FDPA
Purpose and scope

(1) The purpose of this Act is to protect the individual against his/her right to privacy being impaired through the handling of his/her personal data.

(2) This Act shall apply to the collection, processing and use of personal data by

1. public bodies of the Federation,

2. public bodies of the Länder in so far as data protection is not governed by Land legislation and in so far as they

   a) execute federal law or,

   b) act as bodies of the judicature and are not dealing with administrative matters,

3. private bodies in so far as they process or use data by means of data processing systems or collect data for such systems, process or use data in or from non-automated filing systems or collect data for such systems, except where the collection, processing or use of such data is effected solely for personal or family activities.

(3) In so far as other legal provisions of the Federation are applicable to personal data, including their publication, such provisions shall take precedence over the provisions of this Act. This shall not affect the duty to observe the legal obligation of maintaining secrecy or professional or special official confidentiality not based on legal provisions.

(4) The provisions of this Act shall take precedence over those of the Administrative Procedures Act in so far as personal data are processed in ascertaining the facts.

(5) This Act shall not apply in so far as a controller located in another Member State of the European Union or in another state party to the Agreement on the European Economic Area collects, processes or uses personal data, except where such collection, processing or use is carried out by a branch in Germany. This Act shall apply in so far as a controller which is not located in a Member State of the European Union or in another state party to the Agreement on the European Economic Area collects, processes or uses personal data in Germany. In so far as the controller is to be named under this Act, information is also to be furnished on representatives established in Germany. Sentences 2 and 3 shall not apply in so far as data storage media are employed solely for the purposes of transit through Germany. Section 38 (1) first sentence shall remain unaffected.

§ 4a FDPA
Consent

(1) Consent shall be effective only when based on the data subject's free decision. Data subjects shall be informed of the purpose of collection, processing or use and, in so far as the circumstances of the individual case dictate or upon request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance.

(2) In the field of scientific research, a special circumstance pursuant to sub-Section 1 third sentence above shall also be deemed to exist where the defined purpose of research would be impaired considerably if consent were obtained in writing. In such case the information pursuant to sub-Section 1 second sentence above and the reasons from which considerable impairment of the defined purpose of research would arise shall be recorded in writing.

(3) In so far as special categories of personal data (Section 3 (9)) are collected, processed or used, the consent must further refer expressly to these data.

§ 6b FDPA
Monitoring of publicly accessible areas with optic-electronic devices

(1) Monitoring publicly accessible areas with optic-electronic devices (video surveillance) is allowable only in so far as it is necessary

1. to fulfil public tasks,

2. to exercise the right to determine who shall be allowed or denied access or

3. to pursue rightful interests for precisely defined purposes

and if there are no indications that the data subjects' legitimate interests prevail.

(2) The fact that the area is being monitored and the controller's identity shall be made discernible by appropriate means.

(3) Data that have been collected under sub-Section 1 above may be processed or used if this is necessary for the pursued purpose and if there are no indications that the data subjects' legitimate interests prevail. They may only be processed or used for another purpose if this is necessary to avert dangers to state security or public safety or to prosecute crimes.

(4) Where data collected through video-surveillance are attributed to an identified person, this person shall be informed about such processing or use in conformity with Sections 19a and 33.

(5) The data shall be deleted without delay, if they are no longer needed for the pursued purpose or if the data subject's legitimate interests stand in the way of any further storage.

§ 32 FDPA

Data collection, processing and use for employment-related purposes

(1) Personal data of an employee may be collected, processed or used for employment-related purposes where necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract. Employees' personal data may be collected, processed or used to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the collection, processing or use of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in excluding the collection, processing or use, and in particular the type and extent are not disproportionate to the reason.

(2) Sub-Section 1 shall also be applied when personal data are collected, processed or used without being processed by automatic procedures nor processed, used in or from a non-automated filing system, nor collected in such a filing system for the purpose of processing or use.

(3) The rights of participation of staff councils shall remain unaffected.

§ 87 WCA

§ 87 WCA
Right of co-determination

(1) The works council shall have a right of co-determination in the following matters in so far as they are not prescribed by legislation or collective agreement:

1. matters relating to the rules of operation of the establishment and the conduct of employees in the establishment;

2. the commencement and termination of the daily working hours including breaks and the distribution of working hours among the days of the week;

3. any temporary reduction or extension of the hours normally worked in the establishment;

4. the time and place for and the form of payment of remuneration;

5. the establishment of general principles for leave arrangements and the preparation of the leave schedule as well as fixing the time at which the leave is to be taken by individual employees, if no agreement is reached between the employer and the employees concerned;

6. the introduction and use of technical devices designed to monitor the behavior or performance of the employees;

[…]

(2) If no agreement can be reached on a matter covered by the preceding subsection, the conciliation committee shall make a decision. The award of the conciliation committee shall take the place of an agreement between the employer and the works council.