INFORMATION TECHNOLOGY AND WORKERS' PRIVACY: THE GERMAN LAW

Hans-Joachim Reinhard†

I. INTRODUCTION

A. The Lack of a Uniform Code of Labor Law

In Germany, the widespread use of computers and the Internet has caught the legal system by surprise. Most of its sources date back to the end of the 19th century, so the statutes and codes relate more to the physical exchange of goods and to manual work, than to the processing of huge quantities of data that are nothing more than electronic impulses. Courts do their best and apply these existing norms as well as they can, but a lot of questions have still to be answered. Thus, judgments are sometimes controversial, and appeals are taken to the superior courts. Most of these judgments relate to e-commerce, crimes (such as the distribution of illegal pornography), and defamation. However, although the computer is the daily means of work for millions of German employees, there have not been many judgments of the labor courts relating to the use and storage of personal data and those that there are have only dealt with some minor problems. There are no "leading cases" that provide guidelines for both employers and employees.

This lack of leading cases might be a consequence of the specific character of German labor law. This law has never been a comprehensive and coherent system of rules. It is rather a bundle of scattered rules that were developed from a few sections of the 1900 Civil Code (*Bürgerliches Gesetzbuch—BGB*), which were primarily aimed at regulating the rights and duties of household servants and of blue-collar workers in a newly industrialized society. Throughout the years, there have been plans to bring the various sources together in a Uniform Code of Labour Law (*Arbeitsgesetzbuch—AGB*) and several

† Referent, The Max Planck Institute for Foreign and International Social Law, Munich, Germany.

initiatives have been taken in this respect by governments of both the Conservative and the Social Democratic Parties. On some occasions, these got as far as discussions in Parliamentary Committees and work groups; but, in practice, neither political party taken the creation of a Labour Law Code to be one of its main priorities.[1]

B. The Most Relevant Laws in the Area of Privacy for Workers

The following laws and regulations are the most important with respect to the computer surveillance of employees and the processing of employees' personal data:

- The Constitution (*Grundgesetz* or GG)[2] establishes some general rules that protect both the dignity of human beings and their right to privacy.
- The Civil Code (*Bürgerliches Gesetzbuch* or BGB)[3] regulates the main features of employment contracts.
- The Industrial Relations Act (*Betriebsverfassungsgesetz* or BetrVG)[4] regulates the rights of employees and of the Works Council: In particular, the right of the Works Council to receive certain information from employers. The BetrVG does not apply to work in the public sector,[5] but this is covered by very similar provisions in the various Laws on Worker Representation (*Personal-vertretungsgesetze* or PersVG).
- The Law on Redundancy Dismissals (*Kündigungs-schutzgesetz* or KüSchG)[6] obliges employers to make a fair selection among the employees if they want to make dismissals for economic reasons.

1. The main reason for this is the Parties' wish to avoid the difficult conflicts with employers or trade unions that the development of a Code would inevitably provoke. The most recent attempt at codification was in 1990, at the time of the reunification of Germany. From its foundation, East Germany had had a very sophisticated Labour Law Code and, with the removal of particular political elements, this could have served as a sound basis for a Universal Code of Labour Law for all Germany. Indeed, in the Unification Treaty, the East German delegation saw this as a chance to preserve part of their legal system and so Article 30 of the Unification Treaty required the Legislature to codify German labor law as soon as possible. However, there have been no significant developments since then, so this area of law remains very uneven and is found in many different laws and regulations.

2. Grundgesetz für die Bundesrepublik Deutschland of May 23, 1949, last revised on Dec. 19, 2000.

3. Bürgerliches Gesetzbuch of Aug. 18, 1986, last revised on Feb. 16, 2001.

4. Betriebsverfassungsgesetz [Industrial Relations Act] (BetrVG), v. 28.7.2001 (BGB1. I S.2518), ¶ 130.

5. *Id.* ¶ 130.

6. Kündigungsschutzgesetz of Aug. 25, 1969, last revised on Mar. 30, 2000.

- The Telecommunication Act (*Telekommunikationsgesetz* or TKG)[7] regulates all forms of telecommunications, including the use of the Internet.
- The Federal Data Protection Act (*Bundesdatenschutzgesetz* or BDSG)[8] regulates the processing of personal data and the access to such data by data subjects. The Commissioner for Data Protection (*Bundesdatenschutzbeauftragter*) is independent of government and may investigate cases where misuse of personal data is suspected. Similar laws and commissioners exist at the level of the Federal States within Germany (the *Länder*).
- The Telecommunications Services Act (*Teledienstegesetz* or TDG),[9] the Law on Data Protection in Telecommunications (*Teledienste-Datenschutzgesetz* or TDDSG)[10] and the Regulations on Data Protection in Telecommunications Enterprises (*Telekommunikations-diensteunternehmen-Datenschutzverordnung* or TDSV)[11] together regulate matters relating to privacy in the field of telecommunications.
- The Criminal Law Code (*Strafgesetzbuch* or StGB)[12] provides criminal sanctions for the misuse of personal data and for the unjustified breach of the laws on privacy.
- The Social Security Act, Volume 10 (*Sozialgesetzbuch X* or SGB X)[13] regulates the use of personal data by social security institutions.

C. The Impact of Directive 95/46/EC on German Law

After lengthy discussions, Directive 95/46/EC was finally transposed into German law. The Directive should have been transposed by October 24, 1998, but the legislative process was delayed by disagreements between the various Ministries involved and by the elections of September 1998, which led to a change of government. Eventually, the Law of May 18, 2001[14] gave effect to the

7. Telekommunikationsgesetz of July 25, 1996, BGBl. 1996 I S. 1120.
8. Bundesdatenschutzgesetz of May 18, 2001, BGBl. 2001 I S. 904
9. Teledienstegesetz of July 22, 1997, BGBl. 1997 I S. 1870.
10. Teledienstedatenschutzgesetz of July 22, 1997, BGBl. 1997 I S. 982. For a discussion of the amendments proposed the by Government on May 17, 2000, *see* Koenig/Neumann K & R 2000, 417.
11. Telekommunikationsdiensteunternehmen-Datenschutzverordnung of July 12, 1996.
12. Strafgesetzbuch of May 15, 1871, last revised on June 19, 2001.
13. Zehntes Buch Sozialgesetzbuch—Sozialverwaltungsverfahren und Sozialdatenschutz—(SGB X) of Nov. 9, 1982, BGBl. 1982 I S. 1450, last revised on Jan. 18, 2001, BGBl. I S. 130.
14. Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom, v. 18.5.2001 (BGBl. 2001 I S. 904).

European Law by modifying the Data Protection Act, the Social Security Act, and some other legal instruments. German law was brought into line with the requirements of the Directive with the adoption of new terminology and with the widening of the rights and duties of the parties involved. Nonetheless, because German lawyers had played an important part in the process of developing the Directive itself, only a few major changes were required. For the most part, it was a question of modernizing the existing law so as to take account of the new technologies for data processing and surveillance.

D. An Overview of the German System of Jurisdictions

In employment disputes both employers and employees are entitled to go to court. The German court system is organized into several independent branches that deal with different areas of the law. In most cases, the Labour Courts have jurisdiction in matters involving employers, employees, and Works Councils; although, depending on the facts of the case, some matters must be taken before the Ordinary Courts (which have jurisdiction in matters of civil and criminal law) or the Social Courts (which mostly deal with social security matters). In rare cases, the Administrative Courts have jurisdiction. Within each branch of the court system, there are courts of first instance, courts of appeal in each state, and a Federal appeal court as the final authority. Thus, labor law cases go first to the Labour Court (*Arbeitsgericht* or ArbG), then to the State Labour Court (*Landesarbeitsgericht* or LAG), and finally to the Federal Labour Court (*Bundesarbeitsgericht* or BAG). Whereas the Arbeitsgericht and the Landesarbeitsgericht hear questions of fact and law, the Bundesarbeitsgericht considers legal questions only, so if a case turns only on questions of fact, proceedings end at the second level. Moreover, if the litigation concerns a sum of less than €600, appeals to the Landesarbeitsgericht and Bundesarbeitsgericht are only permitted if the courts accept them because of the legal importance of the case.

Before a contested claim is heard, a Labour Court judge must hold a conciliation hearing with the parties; only if this fails will the court procedures start. In practice, however, conciliation hearings are usually a formality to be followed immediately by the hearing. Cases are heard in the first instance by a mixed panel of professional and lay judges. The lay judges are appointed for a period of four years by employees and employers. In practice, most are representatives of trade unions and employers' associations, but this is not a condition

for being a lay judge. Court rulings may also be appealed to the Federal Constitutional Court (*Bundesverfassungsgericht* or BVerfG), although usually only the judgments of the final court of appeal in each area of law are considered. The Federal Constitutional Court is not itself a final court of appeal, but rather a court that deals with alleged infringements of fundamental rights. As such, it has the power to consider the constitutionality of both court rulings and legislation. In its fifty years, the Court has played an important role in the development of German law, especially with respect to new issues where the traditional legal rules are unable to provide a satisfactory solution.

II. COMPUTERS, SURVEILLANCE, AND PERSONAL DATA

The collection and processing of personal data is not a new issue in Germany. Employers have always collected personal data about their employees (for example, on their marital status, education, and skills) and the lawfulness of these practices has never been in question. Computers have, however, introduced new questions about the capacity and efficiency of data processing. In former times, when data were usually stored on file cards, the simple questions of space and manpower prevented excessive processing of personal data, as well as its long-term storage; but nowadays computers are able to store huge volumes of personal data and to process them in seconds. Moreover, employees themselves also accumulate data on their computers, and some of these may be confidential (for example, data collected by members of the Works Council in the course of their duties). This raises the question of who should be allowed to have access to personal data. Clearly, such access could be an important means of checking on employees, but it may also be a means of discovering the enterprise's secrets and of interfering with the work of a colleague. Moreover, in a globalized world, it is obvious that employee access to communications facilities cannot be denied by the employer. Indeed, because the cost of communications have fallen, most German employers allow—or at least tolerate to a certain extent—the private use of their communication facilities. In most enterprises this works on the basis of "gentleman's agreements," but in some cases, express rules have been drawn up in order to prevent abuse.

This use of communications facilities gives employers the right, and in particular cases (such as those related to the obligation to provide evidence) the duty, to make records. Nevertheless, access to

such records must be restricted to authorized persons only, and the records themselves must be cancelled or destroyed within an appropriate time-scale. The same is true for records of computer use. And to the extent that the surveillance of employees constitutes the processing of personal data, it comes under the law in this area; for example, surveillance of employees without their knowledge is only justified in very extreme circumstances, such as where there are suspicions of criminal activities. As to personnel records, although much of the personal data they contain are banal or already well-known, there may be some information that employees do not want to be made public (such as information about illegitimate children and divorces). This data must be protected in the same way as other sensitive personal data.

III. THE SURVEILLANCE OF WORKERS THROUGH THE EMPLOYER'S COMPUTER SYSTEM

A. Introduction

The introduction of computers into the workplace means an important change in the position of the employees. They may be confronted with new technologies that they do not have sufficient skills to operate and so may feel overwhelmed and even tempted to refuse to use the new equipment. They may also regard the computer as an instrument of control and surveillance. Elderly workers may fear that they will not be able to adapt to an ever-faster process of production and thus lose their jobs. All this raises the question of whether employers may equip a workplace with computers when this is against the express will of the employees and whether they may transfer employees from a workplace without computers to one that is so equipped. Although such questions frequently arise (and not just with respect to computers, but with respect to the introduction of new equipment in general), there is hardly any caselaw on this subject in Germany. The law recognizes that employers have the right to decide the main lines of administration and management in the enterprise, and that employees have a duty to follow these decisions as long as they are reasonable and do not affect their personal integrity and human dignity. This means that employees may not refuse to work with a computer. Indeed, the Federal Labour Court has ruled that employers have the right to introduce computers if they see fit to do so. Nevertheless, employers must take the abilities of each particular employee into account. If, for example, employees are unable to use a computer (perhaps because they have no knowledge of English) then

the employer must seek a solution, either by making changes in the workplace or by re-training the employee. Only if these strategies fail is the employer entitled to change the employment contract.

This in turn raises the question of whether employers are obliged to pay for re-training in such circumstances. Although there is no legislation or caselaw on this question, the employer's paying for necessary qualifications is generally thought of as being implied by the employment contract, and this is supported by the legislation that rules that employers may not dismiss employees for reasons of redundancy if the latter can be re-trained for other positions within the enterprise.[15] Moreover, employers are legally obliged to create "humane" workplaces and to promote the professional development of their employees.[16] This duty to provide vocational training is, however, limited according to the needs of the employee and the workplace: Employees are not entitled to training that would result in their being overqualified for their jobs. Such training is part of the employee's working time and must not be done in free time. If a training course takes place outside regular working hours, employees are entitled to monetary compensation or equivalent time off. Except in a few cases (such as being of advanced age), employees are obliged to take any training course that is related to their tasks within the enterprise.

It may be that an employer does not equip all workplaces with computers or provides access to communications facilities to certain employees only. In such cases, the other employees may feel excluded or may think that the employer does not have confidence in their abilities and trustworthiness. They might ask for access too. In such circumstances employers are obliged under German law to observe the principle of equal treatment. This means that they must have justification for distinguishing between employees. It could be that only a certain category of employees need access for their work or it could be the status of the employees (it would, for example, be justified to provide computer access only to managers). It would, however, be unfair, and thus in breach of German labor law, to exclude any employee who belongs to the same category or who has the same status as other employees who do have such access.

15. Law on Redundancy Dismissals, *supra* note 6, ¶ 1 Abs. 2 S. 3.

16. Industrial Relations Act, *supra* note 4, ¶ 75 Abs. 2; Grundgesetz [Federal Constitution] (GG), art. 12.

B. New Grounds for Concern

When employers install computers or new computer programs at the workplace, the Works Council has various rights with respect to this change.[17] It has the right to supervise the installation of new equipment in order to ensure that employers respect all of the laws designed to protect employees. This clearly includes the various laws on the protection of personal data (BDSG, TKG, TDDSG) which are all laws of a protective nature. As part of its supervision, the Works Council may make investigations, talk to employees, and make random tests to see whether control mechanisms and safety procedures are being observed. Such tests may be made at any time and there is no need for there to be any actual suspicion of non-compliance with the law. Employers must inform the Works Council, comprehensively and in advance, of any new technical equipment that they intend to introduce; they must provide all the information that the Works Council needs in order to exercise its right of supervision.[18] This requirement covers the introduction of any computer equipment and networks and access to the Internet or to an intranet: All of these are considered to be "technical equipment" covered by this law.[19]

Where the members of the Works Council do not themselves have the knowledge or skills necessary to assess the information—as may well be the case with the introduction of new computer technologies—they have the right to ask for help from an expert, who may be from the enterprise itself or external to it. The costs of this expert advice are borne by the employer. The Works Council may then make suggestions on the manner in which the new equipment should be introduced and used and the employer is legally obliged to consider these. Moreover, any complaints from the employees affected must be discussed by the Works Council and the employer. If they are unable to find a solution that satisfies the employee, the complaint may be taken to an independent committee

17. According to the BetrVG, a Works Council should be created in all enterprises with at least five permanent employees (three of whom must be eligible for election to the Council). Any three employees may initiate this process. Employers may not prevent the election of a Works Council and any attempt to do so is punishable with up to a year in prison and a fine. In practice, employers sometimes try to avoid the creation of a Works Council by putting indirect pressure upon employees. This is particularly the case in small and medium-sized firms, where the employers still think of themselves as owners and bosses. Although the trade unions often attempt to enforce the law in such firms, the effectiveness of any resulting Works Council remains questionable, given that this depends very much on the cooperation of the employer.

18. Industrial Relations Act, *supra* note 4, ¶ 80 Abs. 1 Nr.

19. *Id.* ¶ 90.

(*Einigungsstelle*) for it to decide, a forum of arbitration.[20] If the Works Council finds that the employer is not following the laws on the protection of employees (for example, by the unlawful storage of personal data), it must first talk to the employer directly and seek a solution. If this fails to end the unlawful activity, the Works Council may then inform the appropriate state authorities and ask them to take action. It has no powers to take direct action itself, *i.e.* to call a work stoppage.

The Works Council must also be informed by the employer of any redeployment or re-training of employees that the employer is planning as a consequence of the introduction of the new technological equipment and it has the right to participate in any actual decisions on redeployment, recruitment, and training, as well as on any substantial modification to the organization of the enterprise or of working methods.[21] Its consent is needed before the employer may lawfully introduce such changes (and may be refused where the Works Council considers that such changes could detrimentally affect the health or the physical or mental condition of the workers involved).[22] Moreover, if the Works Council has not been consulted properly the employees have the right to refuse to use the new equipment.

What all of this means in practice, however, is usually that employers make the main decisions and the Works Council is only able to alter some of the details. Clearly, all of this depends on the presence of a Works Council. Where no such Council exists, and nobody takes the initiative to create one, it is up to the individual employees to defend their own rights. In this, they can ask the help of any trade union of which they are a member or they may go to the Labour Court.

1. The Use of the Employer's Resources, Especially Time

As we have seen, there is very little caselaw in Germany that deals specifically with the use of computers at work. Nonetheless, with respect to questions on the private use of employers' resources, the courts have developed some general rules in cases involving other means of communication, such as telephones. The employment contract itself does not entitle employees to make private use of the employer's equipment (except in exceptional circumstances, such as

20. *Id.* ¶ 76.
21. *Id.* ¶¶ 96, 99.
22. *Id.* ¶ 90.

where there has been an accident in the employee's family). In general, employers are free to allow or to forbid the use of work equipment for private purposes and if they decide to allow it they may impose conditions, for example by allowing private use but only outside of working hours. Such a policy may take different forms: Employers may modify some of the employment contracts, and thus allow private use by certain employees only; or they may simply make a general announcement. A more usual approach is for employers to make an agreement with the Works Council, which is then binding on all employees.[23] However, in most firms in Germany, private use is allowed through a *de facto* policy. The fact is that, in practice, employers tolerate private use, at least to a certain extent. Where an employer tolerates private telephone calls in this way, employees may take it for granted that the private use of e-mail and Internet facilities is also tolerated. (Indeed, unlike telephone calls, the private use of computer facilities does not usually imply any extra cost.) Employers may withdraw this tacit consent at any time; but, if consent was formally agreed (in the employment contract or in an agreement with the Works Council) then the employee or the Works Council will have to agree to the change.

Even where private use is allowed or tolerated, excessive private use may nevertheless be in breach of the employment contract. Much depends here on the facts of each individual case in assessing what may be considered excessive use. One factor may the time spent; for example, one hour of private use of the e-mail or Internet facilities in the course of a month might not be considered excessive, but a quarter of an hour every day might. Another factor may be the kind of work that the employee has to do: If it is continuous work, then private use may affect efficiency, but if it is a discontinuous task or if the employee does not have fixed working hours, then as long as the job gets done it might not be excessive for employees to use quiet moments for making private communications. If an employee makes excessive private use of the computer communications facilities then the employer will usually have to give a written warning to that employee; only if the behavior continues will a dismissal be lawful.

Inappropriate use may also be sanctioned. An example here could be the downloading of pornography from the Internet using the employer's computers.[24] If the employee keeps such pornography for personal use only, then an official warning will usually be the

23. *Id.* ¶ 77.
24. ArbG Hannover, NZA (2001), 1022

appropriate sanction. On the other hand, a dismissal might be appropriate if the employee uses the pornography to annoy or harass other employees, if the contents are illegal (as would be the case with child pornography),[25] or if the employee has not taken any steps to ensure that minors do not have access to the pornography.

2. The Efficient Operation of the Computer System

Employees must use all work equipment in a correct manner and must do their best to prevent any damage to it. Where computers are concerned, this, for example, means that they must use virus scanners where requested to do so and should not use any data that might contain a virus. Similarly, where employees are allowed to use the computer facilities for private purposes they must not damage the system by overloading it (for example, by downloading huge files from the Internet or by printing very large documents). Above all, employees must not hamper the correct and efficient operation of the computer system. If they do, they may be legally required to compensate the employer for any direct or indirect damages they cause and, depending on the circumstances, the employer may have the right to give them an official warning or to dismiss them.

3. Industrial Relations

Employees must respect the intimacy and privacy of their colleagues, of their employer, and of third persons with whom they may come into contact in the course of their work. We have already seen that where the downloading and use of pornography breaks this rule the employee may be lawfully disciplined or dismissed. Similarly, the sending of annoying or insulting e-mails may lead to discipline or dismissal.[26] This does not affect the employees' right to express their opinions on workplace matters through any medium, including computer communication facilities, even if these opinions are contrary to the employer's. Such communications must, however, be truthful and must only be accessible to people within the enterprise. If such opinions are accessible to the public, employees must ensure that they do not disclose information that is confidential or that dishonors the employer.

25. ArbG Braunschweig, NZA-RR (1999), 192–194 (where the manager of a kindergarden downloaded 60 files with child pornography and had stored them at home).

26. ArbG Frankfurt, RDV (2001), 189; ArbG Wesel, NZA (2001), 786.

4. The Security of Confidential Information

Employees must observe appropriate security standards for confidential information. Thus, they must keep their passwords secret and must not provide access to the computer system to others who are not entitled to access. This obviously includes persons from outside the enterprise, but may also include other employees if particular information (such as details of a new product) is restricted to certain employees only. Employees must not look for or use any confidential information to which they should not have access,[27] and if they happen to discover such information by accident, they must keep it secret and not use it for their own purposes.[28] One of the few cases decided in this area concerned a policeman who had access to the police database and who used it in order to check whether certain friends of his daughter had been in trouble with the police. Because consulting this database was a normal part of his job, the policeman was not punished under the criminal law (for an invasion privacy), but he was nonetheless liable for a small fine under administrative law.[29]

5. Civil and Criminal Liability

As we have seen, if employees damage their work equipment, they may be obliged to pay compensation to their employer. German civil law follows the principle of physical replacement.[30] This means that, unless the injured party agrees otherwise, the party responsible for the damage must replace the damaged thing *in specie* (which may, for example, mean that the employee is obliged to buy a new computer). There may also be liability for financial losses if the damage meant that the enterprise was unable to function as usual;[31] but such damage can only be expressed in monetary terms. There is no compensation for things such as loss of expectations and good will. In general, there is no liability for non-physical damage,[32] except in exceptional cases such as a breach of copyright and compensation for pain and suffering. (The latter is only awarded if the health of the victim was directly affected by the unlawful act, so there is no compensation for insults or sexual harassment unless direct damage to

27. LAG Köln, RDV (2001), 30

28. Verwaltungsgericht [Administration Court] (VG) Frankfurt/Main, RDV (2000), 279.

29. Bayerisches Oberstes Landesgericht [Court of Appeals for Selected Matters in Bavaria] (BayObLG), CF, 3 (1999), 32.

30. Bürgerliches Gesetzbuch [Civil Code] (BGB), ¶ 249.

31. *Id.* ¶ 252.

32. *Id.* ¶ 253.

health can be shown; and, even if it is, the amount of compensation is usually very low.)[33]

Liability for physical damage to work equipment will depend on the degree of the employee's negligence.[34] In cases of slight negligence, employees are not liable to pay compensation. In cases of medium-scale negligence, the costs of the damage are shared between the employer and the employee, according to the circumstances, the financial situation, and the ratio between the employee's salary and the damage done. And, in cases of gross negligence, the employee is in principle liable for all of the damages caused,[35] although in practice, such a ruling is hardly ever made because it would lead to the financial ruin of the employee. Employees are also fully responsible for willful damage, but this is usually difficult to prove. And of course, employees are, like any other person, liable for damages caused to third parties. This may include the destruction of data or equipment, the breach of copyright, the defamation of individuals or organizations, and sexual and racial harassment.

The possible criminal liability of employees in this area is governed both by the Criminal Law Code and by Administrative Law. In all cases, employers must apply for permission to initiate prosecution (unless it is a case of public interest, in which case it will be dealt with by the public prosecutor). The wrongful deletion, destruction, or alteration of computer data (or any attempt to do any of these things) is punishable by up to two years in prison and by a fine.[36] If these actions have disrupted the functioning of the enterprise or of a public authority, or if hardware was destroyed, damaged, removed, or modified, this penalty may be up to five years' imprisonment. In addition, any person who, without authorization, searches for information among data that are stored electronically or magnetically may be punished by up to three years in prison or a fine.[37]

33. The amounts granted as compensation for pain and suffering are always a point of discussion in Germany, in particular in cases of severe injuries caused by accidents. Normally, compensation does not exceed €500. The highest compensation ever granted in a very exceptional case was about €125,000.

34. For details *see* 2 WOLFGANG DÄUBLER, ARBEITSRECHT § 6.3.3.1 (1998).

35. BGB, ¶ 611.

36. Strafgesetzbuch [Penal Code] (StGB), ¶ 303.

37. *Id.* ¶ 202.

C. Reasonable Surveillance

There is no doubt that under German law, employers are entitled to check on the efficiency of their employees, and to prevent any misuse of the enterprise's equipment. Nevertheless, the employees' right to privacy must always be taken into account. Although this right is a Constitutional one—meaning that it focuses on the relationship between the individual and the state—the courts have recognized that it may also be considered in relationships between private parties. So although it is not directly applicable, it would seem to be common sense that the Constitutional protection of the privacy of the weaker party results in some generally applicable limits. Thus, all the relevant facts and circumstances must be considered when employers exercise their right to check on their workers. We shall look at these under four headings: Workplace policies, notification, the nature and extent of the surveillance, and special considerations.

1. Workplace Policies

As we have seen, employers are not obliged to allow the private use of their equipment and, if they do, they may set different conditions of access for different employees, as long as there are reasonable grounds for making such distinctions. The mere fact that private use does not impose any additional costs to the employer does not entitle the employee to make such use.

2. Notification

Employers may not read the employees' e-mails or watch their Internet activities unless the employees have been informed about this beforehand. In general, this requirement will be satisfied if the employer makes a general announcement that computer monitoring may occur. However, if employers wish to monitor employees' activities because they suspect misuse of the work equipment, the Works Council must become involved. In procedures for disciplinary dismissals, employers may not use any data as evidence if these were collected without the consent of the Works Council.

3. The Nature and Extent of the Surveillance

Where employers permit the private use of their computer communication facilities, they may record the beginning and the end of such activities, but may not monitor the contents of the

communications; indeed, in such circumstances, employees have the right to encode their private messages. On the other hand, where employers do not permit such private use, they may then lawfully install devices such as filters in order to enforce this restriction. Special rules apply to certain employees such as psychologists, physicians, lawyers, journalists, and priests. These employees are under a legal obligation not to disclose to any third parties any confidential information that they discover in the course of their work. For these purposes, employers are considered to be third parties. This means that the employers of such people may not check on or store the e-mail addresses of their employee's clients. For employees with a legally independent status, such as judges and certain scientists, the law is even stricter. In order to safeguard their independence, the employers of such people may not monitor or store any data that might help to identify the other party to the employee's communications. Employers may set reasonable limits upon the use of the communications facilities (for example, in terms of costs) and they may ask for an explanation if such limits are exceeded, but they may not forbid such employees to communicate with any given individual, group, or organization.

4. Special Considerations

Employers are obliged at their own cost to provide the Works Council with access to the means of communication that are usually used to communicate with employees within the enterprise, insofar as this is necessary for the functioning of the Works Council.[38] However, the Federal Labour Court ruled that computer communications facilities are not automatically to be considered "necessary." The Works Council must demonstrate that access to such facilities is needed in order for it to perform its functions or in order for it to exercise its rights of supervision. (In general, it seems that the bigger the enterprise, the more likely that the use of computers will be deemed necessary.)[39] This decision was heavily criticized by commentators[40] and, indeed, the decisions of the lower courts (particularly the State Labour Court of Baden-Württemberg) had been far more generous towards Works Councils.[41] Because under

38. Industrial Relations Act, *supra* note 4, ¶ 40.

39. BAG, NZA (1998), 954; BAG, NZA (1999), 1209.

40. For example, *see U. Fischer,* BB (1999), 1921; Klebe/Wedde DB (1999), 1954.

41. LAG Hamm, BB (1997), 1361; LAG Baden-Württemberg, LAGE ¶ 40; Industrial Relations Act, *supra* note 4, Nr. 51; the same tendency may also be seen in LAG Düsseldorf, BB (1995), 879.

German law the rulings of superior courts are not binding on lower courts, the situation would still seem to be that the more common the use of computers becomes, the greater the probability that a court will consider access "necessary" for the Works Council. Moreover, the Industrial Relations Act (as revised in 2001) now explicitly states that employers must provide Works Councils with information and communication media.[42]

Where the Works Council is given computer access, this must be via a machine to which only the members of the Council have access. For reasons of privacy, employers may not require them to share a computer that is also used for other purposes. The use of this computer must be limited to what is necessary for performing the functions of the Works Council.[43] It still remains to be settled whether the Works Council may set up its own homepage on this computer. Most commentators argue that such a homepage may be set up if it is for internal use within the enterprise, but may not if it is accessible externally.[44]

Special consideration must also be given to the activities of the trade unions. The rights of trade unions are protected by the German Constitution.[45] They have the right to have physical access to an enterprise in order to provide information to the employees and to recruit new members.[46] It is still unclear whether this right of access includes a right to use facilities such as an intranet and e-mail.[47] Some commentators argue that it does not, on the grounds that the employer may have to bear certain costs (such as those arising from the printing of e-mails); others argue in favor of an interpretation of the law that would allow unions to make reasonable use of e-mail and intranet, an opinion that was supported by a decision of the Federal Constitutional Court, according to which the Constitutional protection of trade unions covers all activities that are necessary for the maintenance of trade unionism. It is, however, understood that this right to inform employees through the employer's computer system is subject to certain limits, for example, employees must download and read the information from the union in their own time.

42. Industrial Relations Act, *supra* note 4, ¶ 40 Abs. 2.

43. LAG Hamburg, AuR (1997), 301 (addressing whether the Work's Council may send provocative but not insulting criticism of the employer).

44. For a decision along these, *see* ArbG Paderborn, DB (1998), 678.

45. Art. 9 Abs. 3 GG.

46. Industrial Relations Act, *supra* note 4, Art. 2 Abs. 2.

47. LAG Schleswig-Holstein, AuR (2001), 71 (addressing the case of an employee who sent information on trade union activities from his private computer to colleagues in the enterprise).

IV. PERSONAL DATA ABOUT THE WORKER

A. Introduction

The processing of personal data is a very sensitive subject in Germany, about which many people feel very strongly. This concern dates from the beginning of the 1980s, when a comprehensive national census was undertaken by the Federal Government. Many German citizens refused to disclose their personal details and, after much controversy, the matter finally arrived at the Federal Constitutional Court, which ruled that the protection of personal data is a fundamental right under the Constitution.[48] According to the judgment, this fundamental right, *"generally guarantees the power of the individual to determine the publication and the use of his personal data. Restrictions of this right of 'data self-determination'* [Recht auf informationelle Selbstbestimmung] *are only permitted if there is an overriding public interest."* Thus, in German law, all data subjects should have as much freedom as possible to decide for themselves the use that is to be made of their personal data and should only have a duty to disclose such data where this is absolutely necessary. Although officially this ruling only applies to the relationship between the citizen and the state, it has nevertheless had an enormous impact on the discussion of data protection in the private sphere, including in matters of labor law. It is generally agreed that all personal data must be protected and must not be published without the formal consent of the data subject, except in cases where the public interest or the interests of third parties prevail.

B. The Legal Regulation of Personal Data at Work

Some general rules on the protection of personal data are found in the TKG and the TDDSG. According to this legislation, the data controller must establish safeguards against unauthorized access to communications.[49] Where data controllers provide a public service (such as the provision of timetables or phone numbers) they may only store data for accounting and billing purposes, but may not store any data on the identity of individual users. More important here are the requirements of the Data Protection Act, which were revised in order

48. BVerfG, decision of Dec. 15, 1983; *cf.* Reinhold Baumann, *Stellungnahme zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 15.12.1983 zum Volkszählungsgesetz*, DVBl, 612–619 (1984).

49. TKG *supra* note 7, ¶ 87.

to bring them into line with the requirements of Directive 95/46/EC.[50] According to this legislation, the collection and processing of personal data is only permitted when specifically authorized by legislation, or when the data subject gives consent. All data subjects must be informed of the identity of the data controller who wishes to process their personal data, of the purpose of the processing, and, if applicable, of the categories of third party to whom it might be disclosed.[51] With a few exceptions, the consent of the data subject must be voluntary and in writing; the written text must be clearly formulated and understandable and must be kept separate from any other documents that the data subject has to sign (such as employment contracts).[52]

1. The Data That May Be Stored

German law requires the processing of personal data to be kept to a minimum: Only data that are absolutely necessary for the stated purpose of the processing may be used. In defining what is necessary, much will depend on the circumstances; the more intimate the information the less likely it is that an individual will be obliged to disclose it. For example, employers may not ask a female job applicant if she is pregnant (except in the case of dangerous work or night work, when the law requires them to do so, because it prohibits such work being done by pregnant workers). If the employer may legitimately collect and store the personal data, it should, wherever possible, be encoded and made anonymous.[53]

2. The Subject of the Data

Employers may store personal data on all persons with whom they have (or have had) professional relations, if these data are necessary for the creation or execution of a contract.[54] Thus, employers may store personal data about job applicants, employees, and former employees, as long as these people were properly informed about the use of their data and did not object to it. In the revised version of the Data Protection Act, which came into force on May 23, 2001, a new principle was established: *"the configuration and selection of data processing systems must aim at collecting, processing*

50. *Supra* note 14.
51. *Supra* note 8, ¶ 4.
52. *Id.* ¶ 4(a).
53. *Id.* ¶ 3(a).
54. *Id.* ¶ 28 Abs. 1.

and using no personal data, or as few personal data as possible." Consequently, employers may only store personal data about their employees that are absolutely necessary and they are required to delete any superfluous data.

3. The Time for Which Data May be Stored

This principle also applies to the time for which personal data may be stored. The law does not establish a time limit for the storage of data. Because such data may only be stored if they are necessary for their stated purpose, they will have to be deleted as soon as this purpose is achieved or is no longer applicable.[55]

4. The Quality of the Information

Data controllers must ensure that the personal data they hold are correct. Thus, the law does not require regular updating, but it does require that personal data be corrected as soon as they become out-of-date or inaccurate.[56] Data subjects have the right to be informed upon enquiry of what personal data about them are being stored or processed, and what the purpose of this processing is.[57] If, for reasons of public policy, this information may not be given to the data subject, they may nonetheless ask for the reason to be given to a Commissioner for Data Protection.[58] All such information about the use of personal data must be provided free of charge. If data subjects suffer damage as a result of the unlawful processing of their personal data, they may claim compensation. In such cases, the burden of proof lies with the data controller.

5. The Use of the Data

Only the persons that have collected the personal data are allowed to make use of them. It is absolutely forbidden for persons who work with personal data to process or use such data without lawful permission. The data controller must oblige all such persons to respect the confidentiality of the data and they must sign an undertaking to this effect before they start working. Their duty to

55. *Id.* ¶ 20 Abs. 2 Nr. 2.
56. *Id.* ¶ 20 Abs. 1 Satz 1.
57. *Id.* ¶ 19 Abs. 1.
58. *Id.* ¶ 19 Abs. 6.

respect the confidentiality of the data continues even after they have stopped working for the data controller.[59]

6. The Use of Personal Data by Third Parties

In general, personal data must not be disclosed to third parties. However, in exceptional cases the law allows this. The most important example is the transfer of data to the authorities responsible for the Social Security and tax systems. In this case, employers are obliged to disclose certain personal data about their employees (such as their Social Security number, salary, and marital status). Special rules apply to data processing by these authorities. Legislation creates detailed regulations that establish which authorities may make use of what kind of personal data and the measures that must be taken in order to protect the privacy of data subjects.[60]

7. Enforcement

The Commissioners for Data Protection have the task of supervising the storage and processing of all personal data in Germany. For constitutional reasons, there are commissioners both at the Federal level and at the level of the 16 states. The rules on the election and legal status of all the commissioners are similar. The Federal Commissioner for Data Protection is elected by a simple majority in Parliament, following the proposal of a candidate by the Government.[61] He or she must be at least 35 years old, is elected for five years, and may be re-elected once. The Commissioner is independent and not obliged to follow orders from the government.[62] Anyone may ask a Commissioner for assistance.[63] Commissioners have the power to monitor any collection or processing of personal data and, to do this, they may enter public-sector premises at any time.[64] If they find unlawful data processing they must report this to the data controller. Every two years, they must make a general report to Parliament in which they must also refer to developments in the private sector with respect to data protection.

59. *Id.* ¶ 5.
60. Sozialgesetzbuch [Social Insurance Code] (SGB), ¶¶ 67-85(b).
61. *Supra* note 8, ¶ 22 Abs. 1.
62. *Id.*
63. *Id.* ¶ 21.
64. *Id.* ¶ 24 Abs. 4.

Public and private sector organizations that employ at least five persons and use automatic processing for personal data—or that employ at least twenty persons and use other forms of personal data processing—must appoint in writing an officer who will be responsible for data protection within the organization.[65] This appointment must be made within one month of starting the processing. If the organization does not comply, it may be fined up to €25,500. In general, the unlawful collection and processing of personal data and breaches of the law on privacy may be punished with up to two years in prison or a fine of up to €25,500, in addition to any further provisions of the Criminal Law Code.[66]

V. CONCLUSION

In Germany, the privacy of employees is protected by both public and private law. Public law, such as the Data Protection Act and the Social Security Code, restrict the collection, storage, and processing of personal data. Infringements may be dealt with by the administrative courts or Social Security courts. Under labor law, employers may restrict the private use of their computing facilities, but if they do not make an express prohibition, or if they usually allow it in practice, then such private use will not be a lawful justification for a disciplinary dismissal (unless there is also criminal misuse of these facilities, sexual harassment, or excessive use of the employer's time or other resources, such as printers). Despite the importance of computer technologies in everyday working life, there are very few reported cases in this area in German law. According to some surveys, the reason for this might be that most enterprises settle disputes about such matters at an informal and local level, without involving the law: Because the computer processing of personal data is a very sensitive subject in Germany, enterprises may fear a loss of public credibility if they are perceived of as having abused computer technologies in this way.

65. *Id.* ¶ 36.
66. *Id.* ¶¶ 43-44.