How to measure IT security awareness of employees: a comparison to e-mail surveillance at the workplace

Franziska Boehm, Tim Hey and Robert Ortner [1]

Cite as Boehm F., Hey T., & Ortner R., "How to measure IT security awareness of employees: a comparison to e-mail surveillance at the workplace", in European Journal of Law and Technology, Vol 7, No 1, 2016.

1. ABSTRACT

Measuring and improving IT security awareness of employees is of crucial importance considering the damages that occur through attacks on the IT security of companies each year. The paper presents a German research project, which intends to improve the IT security awareness of employees while at the same time considering the rights of individuals concerned. The authors address one specific labour law issue dealing with the question of how to ensure that there will not be an adverse impact on the employees' rights while clandestinely testing their IT security awareness. A parallel will be drawn to the case of e-mail surveillance at the workplace under EU and German law and its findings transferred to the project scenario. On this basis, suggestions for lawful test methods measuring the employees' IT security awareness will be made.

Keywords: IT-security awareness; Critical infrastructures; Penetration testing; Surveillance at the workplace; Surveillance of business e-mail accounts; Privacy by design; Fundamental rights of employees

2. INTRODUCTION

Attacks on IT security have been threatening computer networks since their very first establishment. Such attacks are constantly increasing and they quickly adapt to countermeasures, which can lead to high economic losses for companies and institutions concerned, mainly through the theft of personal data or trade secrets. [2] Often critical infrastructure - for instance in the fields of public health, telecommunication, transportation and security service [3] - is targeted. [4] In these cases, attacks are especially harmful due to societies' dependency on these infrastructures.

For this reason, technical features of IT systems are continuously tested to evaluate their level of IT security and to check their vulnerability. The most prominent testing method is typically the so-called penetration testing carried out by professional hackers. Yet, these tests are limited to the checking of technical gaps of IT systems. They do not consider risks being created by the user of the IT system, for instance, due to his insufficient awareness for IT security or through his inappropriate reaction to a security warning of his computer. So far, the existing test methods do not consider sufficiently the 'human factor' as a risk for IT security.

This deficit is the starting point of a research project addressing the user's IT security awareness. A detailed description of the project will be given in the first part of this paper (part three). It will be followed by an introduction of the basic principles of employee privacy and its legal requirements (part four). Afterwards we will analyse a situation which is - concerning its legal issues - similar to the project scenario, namely the observation of the employee's e-mail account (part five). In part six, the results will be compared to the project scenario in order to balance the employee's and the employer's rights and interests.

3. PRESENTATION OF THE PROJECT [5]

To improve the IT security awareness of employees, a new software tool has been developed by computer scientists, psychologists and lawyers, which will be used to clandestinely test the employees in a big hospital in Northern Germany. To put it simply, the software will simulate IT attacks by imitating phishing e-mails, which will be sent to the employees who are being tested.

The reaction of the employee regarding such an e-mail will be electronically protocolled and provides information about his or her IT security awareness. For instance, the fact that the employee opens the e-mail or clicks on a link inside the e-mail can indicate low security awareness whereas an immediate deletion will be a sign for a higher awareness level.

It is planned to run the test during a normal operation day, without informing the employees about the ongoing testing, in order to gain precise and genuine results. The tests are supervised by psychologists, data protection experts and lawyers monitoring the respect of labour law provisions.

The analysis of the results will serve as a basis for the next steps of the project. Specific training on IT security awareness for the tested employees will be developed and carried

out. The training will be followed by a second clandestine test comparable to the first one. After the second test, the employee's reaction will be analysed again. Based on these results the most effective methods to improve the IT security awareness of users will be developed.

4. CONFLICTING INTERESTS

Evidently the tests provided in the project scenario lead to various legal questions, especially in the field of labour law. In this context one of the major legal issues relates to the conflicting interests of the employee and the employer: the goal of the latter is to gain as much information about the employee's behaviour when confronted with attacks on IT infrastructure, whereby the employee has a valid interest in his privacy and data protection rights.

Under European law the employee is protected by Article 7 and Article 8 of the Charter of the Fundamental Rights of the EU which lays down the foundations of the right to privacy, respectively referring to the protection of personal and family life, home and communications and of personal data. In addition, Article 8 of the European Convention of Human Rights asserts the right to respect for private and family life, home and correspondence. While the protection of employees' personal data has been disputed for years at EU [6] as well as at national level [7] , draft Article 5 of the new general data protection regulation (GDPR) [8] names general principals safeguarding personal data applying also to processing of employees' personal data. Even though, the Member States may - according to draft Article 82 GDPR - provide more specific rules in the employment context, they must consider these principals.

Employee privacy in the EU has mainly been influenced and interpreted according to Article 8 of the European Convention of Human Rights (ECHR). In Niemitz v. Germany the European Court of Human Rights stated that there is no distinction between private and business life, since many people develop relationships with other people during their working time. In addition to that, exercising a profession could become a part of the person's life to such a relevant degree that it is impossible to distinguish between these two life spheres. [9] Thus, and due to social changes in the manner of working and the possibilities of surveillance technologies, the boundaries between business and private have become blurred. [10]Therefore, activities of employees in a business context are equally protected under Article 8.

Consequently, the Court decided in Halford v. United Kingdom that the employee has a reasonable expectation in his privacy when making calls from telephones provided by the employer even though the latter owns the used facilities. Thus, if the employer intercepts those calls, he interferes with the employee's rights under Article 8 ECHR. [11] In Copland v. United Kingdom the ECtHR ruled that the same applies to e-mail conversations. [12]

Furthermore, not only the content of a phone call or an e-mail is an issue under Article 8 ECHR. In Malone v. United Kingdom and in Copland v. United Kingdom the Court considered metadata, like the date or length of a phone call or the sending time of an e-mail as an "integral element of the communication" [13] and therefore also worthy of protection. [14]

Although Article 8 ECHR should at first protect the individual against interferences made by public authorities, it is essential for facilitating respect for private and family life that this right also includes positive obligations for the state [15] and thus, also between employees and employers in the private sector. [16]

In this context, attention must be paid to the fact that Article 8 ECHR is limited by other public or private interests, especially those which are legally protected. [17] The employer usually has an interest in securing his freedom to choose an occupation and conduct a business, guaranteed by Article 15 and 16 of the Charter of Fundamental Rights of the European Union [18] as well as in the protection of his property rights, guaranteed by Article 17 of the Charter as well as Article 1 of Protocol no. 1 to the Convention. [19]

Hence, in the testing scenario, there are on one hand the employer's property rights and the right to pursue his professional activity, whereas on the other hand there is the employee's right to respect for a private life. As none of the fundamental rights overrides the other, they have to be interpreted in such a way that the conflicting fundamental rights are consistent with each other. To achieve this, the competing interests have to be fairly balanced by weighing the different interests. [20]

In domestic German law the legal situation is comparable to the one at European level. The employee's interest in his privacy is protected by Article 2 paragraph 1 read in conjunction with Article 1 paragraph 1 of the German Constitution. The employer is safeguarded by his right to pursue a professional activity and his property rights guaranteed by Article 12 paragraph 1 and Article 14 paragraph 1 of the Constitution. Again the competing rights have to be settled fairly and evenly balanced to achieve an adequate balance of all interests at stake. [21]

Within the framework of the research project, these rights have to be taken into closer consideration, as they clearly establish the main threshold for the legitimation of any surveillance and testing measure. We want to evaluate preconditions for a lawful and adequate test design, respecting the privacy interests of the tested employees on the one hand and meeting the requirements to test IT security awareness on the other hand.

5. GENERAL FRAMEWORK FOR THE MONITORING OF EMPLOYEES' BUSINESS E-MAILS IN THE EU AND IN GERMANY

First, the general legal requirements for the monitoring of employees' business e-mail accounts are analysed to draw a parallel to the testing scenario. Such conditions can serve as an example for the requirements applied to secret electronic surveillance methods such as the clandestine testing foreseen in the project context.

On the one hand, monitoring the employee's business e-mail account to verify his performance at work is considered as a legitimate purpose of the employer. [22] Knowing the professional interactions of his employees is a valid interest since, for instance, the writing of private e-mails during work time may indicate that little attention is paid to work-

related activities. [23] The collection of data such as the senders' or recipients' address, the subject heading, date and volume, as well as the content represent suitable instruments to reveal a misuse or at least give an initial indication for misuse. [24]

On the other hand, the interests of the employee need to be taken into account as well. When monitoring the employee's business e-mail account, jurisprudence has developed certain categories to balance the different interests at stake. Firstly it has to be differentiated between traffic and content data since it is assumed that they show a different level of privacy relevance, which has to be considered and analysed. [25] Secondly, it needs to be distinguished between employers prohibiting and employers allowing the private use of the business e-mail accounts. In the latter case, the employee has a higher expectation of privacy. [26]

5.1. CASE LAW IF THE PRIVATE USE OF THE BUSINESS E-MAIL ACCOUNT IS FORBIDDEN BY THE EMPLOYER

5.1.1. MONITORING OF TRAFFIC DATA

According to Directive 2002/58/EC, traffic data are inter alia the duration, time or volume of a communication, as well as the sender's and recipient's number or address. [27] Even though these data provide personal information about the employee, for instance, about his localization or his contacts, [28] recent ECtHR case law indicates that monitoring of traffic data is lawful. [29] If the private use of the business account is forbidden, the employer proceeds on the assumption that the employee's business account does not entail privacy related e-mails. [30] In addition to that, by using the account for private purposes, the employee would violate provisions of his work contract making the private use unlawful. [31]

5.1.2. MONITORING OF CONTENT

The surveillance of e-mail content is a more serious intervention in the employee's general right of privacy. [32] The e-mail content might include confidential or intimate information. For instance, no employee wants his employer to read an e-mail reminding him to participate in the next meeting of his alcoholics anonymous group. Reading the content of employee's e-mails is therefore sometimes regarded as illegal. [33]

However, if proceeding on the assumption that private e-mail use is forbidden, similar arguments as with regard to traffic data apply. In addition, although the reading of content is clearly more privacy invasive [34], the employer has a right to randomly control compliance of his work instructions, including possible violations of the contract concerning the prohibition of private e-mail use. [35] For this purpose, courts consider the monitoring even of the content of the employee's e-mails as lawful. [36] However, if the employer discovers private use during his controls, for instance by the private nature of the subject line or the recipient, further investigation is not allowed and the employer has to stop reading the particular e-mail immediately. Otherwise, he would overstep the boundaries of his right to control. [37]

5.2. CASE LAW IF THE PRIVATE USE OF THE BUSINESS E-MAIL ACCOUNT IS ALLOWED BY THE EMPLOYER

A different setting is given when the employer allows the private use of the business e-mail account. The employer authorizes the employee to deal with private concerns and by doing so he has to respect the additional privacy granted to the employee. [38] Therefore, the employer creates, metaphorically speaking, a sort of private space.

5.2.1. MONITORING OF TRAFFIC DATA

This private space granted to the employee leads to a higher expectation of privacy and one could argue that, in contrast to the former scenario, monitoring of traffic data should be regarded as illegal due to the permission of private use. [39] In this scenario, the employer has indirectly agreed to restrict himself in his monitoring rights, which leads to a lower weighting of his interests while, in most of the cases, the interests of the employee prevail. [40]

Nevertheless, there are certain situations in which the employer's interest may dominate, for instance when he has a reasonable suspicion that his employees violate their work contracts by spending excessive time on private e-mails or by activities damaging his reputation. [41]

5.2.2. MONITORING OF CONTENT

Taking into account that monitoring of traffic data is not lawful, this interdiction must a fortiori apply to the controls of e-mail content. [42] Only in very limited situations, is the employer allowed to monitor the content of private e-mails, for instance, when he has a reasonable and well-founded suspicion that the employee is committing a crime or harms the employer's interests in other very serious matters. [43]

6. BALANCING OF INTERESTS IN THE TESTING SCENARIO

After having clarified the general framework for e-mails surveillance, we will now focus on the concrete balancing of interests in the testing scenario. Firstly, we address the issue of the clandestine testing approach, followed by a view on the theoretical consequences for the employee including possible dismissals, if his reactions in the test do not fulfil the employer's criteria. Last but not least, regard will be paid to the privacy relevance of the collected data within the tests and how they can be designed to minimally interfere with the employee's rights. Therefore, the principles mentioned above shall serve as a basis.

6.1. CLANDESTINE TESTS

The clandestine approach of the tests has a particular, highly intrusive effect [44] , but seems to be necessary for the project's success. If the user is informed about upcoming tests, his IT security awareness would be highly increased, possibly leading to inaccurate results. Moreover, informing employees beforehand might lead to the effect that only compliance to the companies' IT security guidelines is measured, instead of actual IT security awareness.

In order to safeguard the employees' interests a first method is to inform them as far as this information has no effect on the test results. For instance, it is possible on the one hand to inform employees about general tests of IT security and the collection of personal data in this context, but on the other hand to conceal the fact that the user's awareness of IT security awareness will be addressed. A second method is to inform work councils, union groups, or other employee representatives before the tests to involve the employee's interests in the conception phase. [45] Shortly after the realization of the tests, the tested employees need to be transparently informed about it. The information must include details on the purpose of collection and the use of their data, including their right of access and deletion and the right to object to future processing. [46]

A further possibility for the employer to test its employee's IT security awareness is to create a sort of trap by using phishing e-mails. In addition to the secret evaluation of the employee's work performance, he establishes an artificial testing scenario, which provokes a mistake of the employee and puts him in a situation that restricts his general freedom of action. Using traps to test the employee's work performance is not per se regarded as unlawful according to German case law. For instance, clandestine test-purchases by the head of a supermarket to control how carefully his cashiers check the carts for hidden items is regarded as lawful. [47] However, certain conditions, such as informing the work council and a transparent information policy must be fulfilled. Drawing a parallel to our testing scenario, a clandestine test approach could be legally carried out when certain conditions are respected.

6.2. EMPLOYMENT CONSEQUENCES

To avoid labour law related consequences for employees like negative entries in personal files or, in the worst-case, dismissals, if the employee's reaction does not meet the employer's expectations, protective measures must be in place. The goal of the test plays a crucial role in this context. In contrast to e-mail account surveillance, the tests relating to the IT security awareness are not intended to be used for a sanctioning of the tested employee; instead the employer wants to know how he is able to improve this factor. To ensure that test results are not misused, the collected data could be anonymized, which would, however, prohibit the possibility to link the results from the first and the second test making it impossible to evaluate, which training method was the most effective one to enhance IT security awareness. Pseudonymization is therefore another possibility to prevent the employer to allocate the results to each employee. In this case, a third trustworthy and independent partner or third party administering the key, such as, for instance, an independent data protection authority, is however necessary.

6.3. PRIVACY RELEVANCE

The differentiation between traffic and content data regarding the surveillance of e-mail accounts illustrates that the scope of the employer's right to monitor his employees depends on the extent to which the particular piece of data enables conclusions about the data subject's personality.

A major question is how intensely the project's tests affect the employee's privacy. A low impact would make it easier to argue for the lawfulness of tests. [48] One can distinguish two things: The intent to gether information about the employee's level of IT security awareness does not permit his employer to draw considerable conclusions about his personality. But the fact that an employee reads a phishing e-mail not only provides information about his IT security awareness, but also about him being interested in the content of the particular e-mail. If the employee clicks on an e-mail, which seems to be about football, family planning or diseases, his behaviour allows conclusions about his personal situation and might therefore lead to an intrusive interference of his personal rights.

As mentioned above in the context of the surveillance of business e-mail accounts, the employer is not allowed to read private e-mails even if private use is prohibited. He may look in the employee's mailbox but he has to stop reading when discovering private content. Therefore, when monitoring employee behaviour it has to be ensured that access to private information is limited to a minimum. Thus, the phishing e-mails in the project must be designed in a way hindering the testers to draw conclusions about private concerns of the tested persons. One possibility to meet this requirement could be the development of neutral phishing e-mails, which, for instance, can be e-mails appearing as a query of the system administrator of a web mail provider to disclose passwords to him. In this case, besides the tested IT security awareness, conclusions can be drawn about the fact that the employee owns an account at this provider, but not about the employees' personal situation. Another example for a test design, which does not enable conclusions about the employee's personality, could be an e-mail containing only fictitious characters.

The test requirements might however be different, if the private use of the business IT infrastructure is allowed. At least in the case of e-mail surveillance, the employer's power is restricted. This is based on the argument that the employee was granted some sort of private space, which the employer must respect. As a consequence, the impact on the employees' personal rights is higher. [49] Since the use of phishing e-mails including private content is prohibited even where private use is forbidden, they are even less lawful when private use is allowed.

The restriction of the employer's monitoring power is based on the assumption that there might be private information inside the monitored data pool. Thus, this restriction is only necessary when there is indeed any private information inside the granted space. If it can be guaranteed that the employer will not find any privacy related information, because there is none, the permission of private use does not restrict the employer's right to look inside that space.

Transferring this assessment to the project scenario and providing that the phishing e-mails are designed in a way that they do not allow conclusions about the employees' personality, a restriction of the employers monitoring power is not necessary, even if private use is allowed. This leads to the result that the legal requirements for the project's phishing e-mails are identical with the ones in the scenario where the private use is forbidden making no difference for the project tests' implementation whether the private use of the institutions' IT-infrastructure is allowed or not. In contrast to the surveillance of the employee's e-mail

account, the so designed phishing e-mails would be lawful, even if the private use is allowed.

7. CONCLUSION

It follows from the foregoing, that the measuring of the IT security awareness of employees can be realized without excessive or undue impact on the employees' right to privacy. By drawing a parallel to the possibility of e-mail surveillance at the workplace under ECHR, EU and German law, suggestions for lawful test methods measuring the employees' IT security awareness were made. An example is the use of carefully prepared phishing e-mails, which are constructed in a way that the employee's reaction permits no conclusions about his personal situation. In addition, even a clandestine testing scenario can be lawful, if work councils are fully informed before the tests. Additionally, the tested persons must be informed afterwards. Further, tests results should be pseudonymized and keys need to be stored at a trusted and independent third party.

Overall, this paper presents one of several approaches to test the IT security awareness in a work context in a lawful way. By reducing the privacy relevance of the collected data in a first step and the use of anonymization and pseudonymization techniques in a second step, the proposed approach should serve as one example to design a privacy-friendly method to test the IT security awareness of employees.

8. BIBLIOGRAPHY

Journals

Bayreuther, Frank (2012), 'Zulässigkeit und Verwertbarkeit heimlicher Videoaufzeichnungen am Arbeitsplatz', Der Betrieb, pp. 2222-2226

Beckschulze, Martin/Henkel, Wolfram (2001), 'Der Einfluss des Internets auf das Arbeitsrecht', Der Betrieb, pp. 1491-1506

Beckschulze, Martin (2003), 'Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz - Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen', Der Betrieb, pp. 2777-2786

Gola, Peter (2012), 'Beschäftigtendatenschutz und EU-Datenschutz-Grundverordnung', Europäische Zeitschrift für Wirtschaftsrecht, pp. 332-336

Joussen, Jacob (2011), 'Mitarbeiterkontrolle: Was muss, was darf das Unternehmen wissen?', Neue Zeitschrift für Arbeitsrecht-Beilage, pp. 35-42

Mengel, Anja (2004), Kontrolle der E-Mail- und Internetkommunikation am Arbeitsplatz, Betriebs-Berater, pp. 2014-2021

Mitrou, Lilian/Karyda, Maria (2006), 'Employees' privacy vs. employers' security: Can they be balanced?', Telematics and Informatics, pp. 164-178

Books

Däubler, Wolfgang (2010), 'Gläserne Belegschaften', (Frankfurt: Bund)

Hanau, Peter/Hoeren, Thomas (2003), 'Private Internetnutzung durch Arbeitnehmer' (Munich: C.H. Beck)

Müller-Glöge, Rudi (2012) in Henssler, Martin/Krüger, Wolfgang (ed), 'Münchener Kommentar zum Bürgerlichen Gesetzbuch: BGB - Band 4; Schuldrecht, Besonderer Teil II, §§ 535-630' (Munich: C.H. Beck)

Hesse, Konrad (1999), 'Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland', (Heidelberg: C.F. Müller)

Kania, Thomas (2016) in Müller-Glöge, Rudi/Schmidt, Ingrid/Preis, Ulrich (ed), 'Erfurter Kommentar zum Arbeitsrecht' (Munich: C.H.Beck)

Kuner, Christopher (2007), 'European Data Protection Law, Second Edition' (Oxford: Oxford University Press)

Panzer, Andrea (2004), 'Mitarbeiterkontrolle und neue Medien' (Frankfurt: Peter Lang)

Richardi, Reinhard (2016) in Richardi, Reinhard (ed), 'Betriebsverfassungsgesetz' (Munich: C.H. Beck)

Thoma, Oliver (2013), 'Das Spannungsverhältnis zwischen Beschäftigtendatenschutz und IT-gestützter Compliance - Die Gefahren der Internet- und E-Mail-Kontrolle sowie des Datenscreenings für das informationelle Selbstbestimmungsrecht der Beschäftigten' (Hamburg: Dr. Kovac)

Thüsing, Gregor (2014), 'Beschäftigtendatenschutz und Compliance', (Munich: C.H. Beck)

Various

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

[1] Franziska Boehm is a Professor at the Karlsruhe Institute of Technology and at the Leibniz Institute for Information Infrastructure. Tim Hey and Robert Ortner are junior researchers at the University of Münster's Institute for Information, Telecommunication and Media Law. The authors are named in alphabetic order and contributed to this article to the same extent.

[2] The German inter-trade-organization estimates an economic loss about 51 billion Euro for German economy due to cyber attacks https://www.bitkom.org/Presse/Anhaenge-an-PIs/2015/04-April/Digitale-Angriffe-auf-jedes-zweite-Unternehmen/BITKOM-Charts-PK-Digitaler-Wirtschaftsschutz-16-04-2015-final.pdf.

[3] Compare the proposal for a common level of network and information security (NIS-Directive, COM(2013) 48 final) which uses the term "critical infrastructures" for systems and networks that are essential for the functioning of a society and economy.

[4] Symantec, Symantec Intelligence Report August 2015, http://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence-report-08-2015-en-us.pdf.

[5] For more information about the project and its partners: https://itsec.cs.uni-bonn.de/itsapt/

[6] Gola, 2012; compare also recital 124 of the proposed new data protection regulation.

[7] Cf proposal for an employee data protection Act in Germany, BT-Drucksache 17/4230, http://dipbt.bundestag.de/dip21/btd/17/042/1704230.pdf.

[8] Cf final draft of the new General Data Protection Regulation, http://www.statewatch.org/news/2015/dec/eu-council-dp-reg-draft-final-compromise-15039-15.pdf.

[9] Niemietz v. Germany [1992] ECHR 13710/88, recital 29, *http://www.bailii.org/eu/cases/ECHR/1992/80.html*.

[10] Mitrou/Karyda, 2005.

[11] Halford v. The United Kingdom [1997] ECHR 20605/92, recital 50, *http://www.bailii.org/eu/cases/ECHR/1997/32.html*.

[12] Copland v. The United Kingdom [2007] ECHR 62617/00, *http://www.bailii.org/eu/cases/ECHR/2007/253.html*; see also: Benediktsdóttir v. Iceland [2009] ECHR 38079/06, *http://www.bailii.org/eu/cases/ECHR/2009/1100.htm*.

[13] Malone v. The United Kingdom [1984] ECHR 8691/79, recital 84, *http://www.bailii.org/eu/cases/ECHR/1984/10.html*.

[14] Malone v. The United Kingdom [1984] ECHR 8691/79 for telephone; For e-mail metadata see: Copland v. The United Kingdom [2007] ECHR 62617/00.

[15] Cases: von Hannover v. Germany [2004] ECHR 59320/00, recital 57, *http://www.bailii.org/eu/cases/ECHR/2004/294.html*; Köpke v. Germany [2010] ECHR 420/07, *http://www.bailii.org/eu/cases/ECHR/2010/1725.html*; Benediktsdóttir v. Iceland [2009] ECHR 38079/06.

[16] Barbulescu v. Romania [2016] ECHR 61496/08, recital 52 f.

[17] von Hannover v. Germany [2004] ECHR 59320/00; Benediktsdóttir v. Iceland [2009] ECHR 38079/06.

[18] Article 15 coincides with Article 16 of the Charter, see: Joined Cases C-143/88 and C-92/89 Zuckerfabrik Süderdithmarschen and Zuckerfabrik Soest [1991] ECR I-415, paragraphs 72 to 77; Joined Cases C-184/02 and C-223/02 Spain and Finland/Parliament and Council [2004] ECR I-7789, paragraph 51.

[19] Köpke v. Germany [2010] ECHR 420/07.

[20] Köpke v. Germany [2010] ECHR 420/07; von Hannover v. Germany [2004] ECHR 59320/00.

[21] So called ‚practical concordance', first mentioned in Hesse, 1999, paragraph 72, recital 318 and applied by Federal Constitutional Court decision of 7 March 1990 - 1 BvR 266/86, 1 BvR 913/87 (= BVerfGE 81, 278, 292), Federal Constitutional Court decision of 6 October 2009, 2 BvR 693/09 (= BVerfGK 16, 267).

[22] Halford v. The United Kingdom [1997] ECHR 20605/92, recital 48, *http://www.bailii.org/eu/cases/ECHR/1997/32.html*; Kuner, 2007, recital 5.68; Mitrou/Karyda, 2005, p. 170.

[23] This was the case in many dismissal cases before court. For instance: Federal Labour Court decision 07 July 2005, 2 AZR 581/04 (=Neue Juristische Wochenschrift 2006, 540); Higher Labour Court Berlin-Brandenburg decision 16 February 2011, 4 Sa 2132/10 (=Neue Zeitschrift für Arbeitsrecht-Rechtsprechungsreport 2011, 342)

[24] In the case Higher Labour Court Hessen decision of 25 July 2011 - 17 Sa 153/11 (= Neue Zeitschrift für Arbeitsrecht-Reshtsprechungsreport 2012, 76) the employer verified a misuse by examining the metadata; In the case Barbulescu v. Romania [2016] ECHR 61496/08 the employer monitored the content.

[25] Malone v. The United Kingdom [1984] ECHR 8691/79, recital 84; Copland v. The United Kingdom [2007] ECHR 62617/00, recital 43; Data Protection Working Party, 2001, p.21.

[26] Halford v. The United Kingdom [1997] ECHR 20605/92, recital 45; Copland v. The United Kingdom [2007] ECHR 62617/00, recital 42; Barbulescu v. Romania [2016] ECHR 61496/08, recital 39.

[27] Directive 2002/58/EC, recital (15), Art. 2 (b).

[28] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014], EU:C:2014:238, recital 26-27.

[29] Barbulescu v. Romania [2016] ECHR 61496/08.

[30] Barbulescu v. Romania [2016] ECHR 61496/08, recital 57; Beckschulze, 2003, p. 2780; Thüsing, 2014, paragraph 9, recital 42; Weißnicht, 2003, p. 451.

[31] Labour Court Frankfurt decision of 2 January - 2 Ca 5340/01 (=Neue Zeitschrift für Arbeitsrecht 2002, 1093); Hanau/Hoeren, 2003, p. 61.

[32] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014], EU:C:2014:238, recital 28; Federal Constitutional Court decision of 3 March 2004 - 1 BvR 2378/98, 1 BvR 1084/99 (=BVerfGE 109, 279); Federal Constitutional Court decision of 14 September 1989 - 2 BvR 1062/87(= BVerfGE 80, 367) Mitrou/Karyda, 2006, p. 171.

[33] Mitrou/Karyda, 2006, p. 171; cf: the surveillance of content can only be justified under Article 7 (b) of the Directive 95/46/EC in very limited cases, Data Protection Working Party, 2001, p.21; Kuner, 2007, recital 5.68: Däubler, 2010, recital 351.

[34] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others [2014], EU:C:2014:238, recital 28; C-362/14 Schrems [2015], ECLI:EU:C:2015:650, recital 94.

[35] Barbulescu v. Romania [2016] ECHR 61496/08, recital 57: Müller-Glöge, 2012, paragraph 611, recital 1062.

[36] Barbulescu v. Romania [2016] ECHR 61496/08, recital 39; Higher Labor Court Hamm decision of 16 January 2012 - 7 Sa 1201/11 (= Zeitschrift für Datenschutz 2012, 488); Beckschulze, 2003, p. 2779; Hanau/Hoeren, 2003, pp. 47, 61; Thüsing, 2014, paragraph 9, recital 50.

[37] Hanau/Hoeren, 2003, p. 54; Weißnicht, 2003, p. 451.

[38] Halford v. The United Kingdom [1997] ECHR 20605/92, recital 45; Joussen, 2011, p. 39; Thoma, 2013, p. 147; Thüsing, paragraph 9, recital 55.

[39] Mengel, 2004, p. 2018.

[40] Thoma, 2013, p. 147; Panzer, 2004, p. 274.

[41] Federal Labor Court decision of 27 April 2006 - 2 AZR 386/05 (= Neue Zeitschrift für Arbeitsrecht 2006, 977); Federal Labor Court decision of 7 July 2005 - 2 AZR 581/04, recital 37 (= Neue Juristische Wochenschrift 2006, 540); Labour Court Frankfurt decision of 2 January 2002 - 2 Ca 5340/01 (=Neue Zeitschrift für Arbeitsrecht 2002, 1093); Hanau/Hoeren, 2003, p. 65f.; Panzer, 2004, p. 284; Kuner, 2007, recital 5.78.

[42] Däubler, 2010, recital 368; Hanau/Hoeren, 2003, p. 47; Data Protection Working Party, 2001, p.21.

[43] Beckschulze/Henkel, 2001, p. 1494; Kuner, 2007, recital 5.78; Data Protection Working Party, 2001, p.21.

[44] *Federal Constitutional Court* decision of 11 March 2008 - 1 BvR 2074/05, 1 BvR 1254/07 (= BVerfGE 120, 378); decision of 4 April 2006, 1 BvR 518/02 (= BVerfGE 115, 320); decision of 2 March 2006, 2 BvR 2099/04 (= BVerfGE 115, 166); Bayreuther, 2012, pp. 2222f.; Thüsing, 2014, paragraph 3, recital 47, paragraph 11 recital 30.

[45] Richardi, 2016, paragraph 87, recital 8; Kania, 2016, paragraph 87 BetrVG, recital 48.

[46] This follows from the rationale of Art. 8 EMRK and Art. 2 paragraph 1 in conjunction with Art. 1 paragraph 1 German constitution: Leander v. Sweden [1987] ECHR 9248/81, *http://www.bailii.org/eu/cases/ECHR/1987/4.html*; Federal Constitutional Court decision of 15 december 1983, 1 BvR 209/83 (= BVerfGE 65, 1).

[47] *Federal Labor Court* judgment of 18 November 1999 - 2 AZR 743/98 (=BAGE 93, 1); *Labor Court* judgment of 3 August 2007 - 28 Ca 6745/07.

[48] Federal Constitutional Court decision of 13 June 2007 - 1 BvR 1783/05 (=BVerfGE 119, 1, 86 ff.); decision of 24 June 1993 - 1 BvR 689/92 (= NJW 1993, 2365).

[49] Thoma, 2013, p. 147.