

5401/01/EN/Final WP 55

Working document

on the surveillance of electronic communications in the workplace

Adopted on 29 May 2002

Comments:

* national chapters might be further changed in agreement with national delegations

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

The secretariat is provided by Directorate A (Functioning and impact of the single market - Coordination - Data protection) of the European Commission's, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995¹,

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

has adopted the present working document:

Official Journal no. L 281 of 23/11/1995, p. 31, available at:

http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

Article 29 Working Party Working document² on surveillance and monitoring of electronic communications in the workplace

Draft Executive Summary

This working document complements Opinion 8/2001 on the processing of personal data in the employment context³ and contributes to the uniform application of the national measures adopted under the Data Protection Directive 95/46/EC⁴. It does not prejudice the application of national law in related areas to data protection.

The Article 29 Working Party has set up a subgroup to examine this question⁵ and has adopted an **extensive document** which can be found on the Internet in the following address⁶:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

The Article 29 Working Party has examined in this working document the issue of the monitoring and surveillance of electronic communications in the workplace, in other words, the monitoring by the employer of e-mail and Internet use by workers.

In the light of the jurisprudence of the European Court of Human Rights on Article 8 of the Convention for the protection of Human Rights and Fundamental Freedoms,

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf. This opinion contains an in-depth analysis of the application of the provisions of the Data Protection Directive (and in particular Articles 6, 7, and 8) to the processing of personal related to employment activities.

The Article 29 Working Party is an advisory group composed by representatives of the data protection authorities of the Member States, which acts independently and has the task, inter alia, of examining any question covering the application of the national measures adopted under the Data Protection Directive in order to contribute to the uniform application of such measures;

Opinion approved on 13 September 2001 and accessible in the following url address:

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.95, p. 31

The following supervisory authorities have contributed to the work of this subgroup: AT, BE, DE, ES, FR, IRL, IT, NL, UK.

The document includes an annex of the most relevant data protection legislation in the Member States with some impact on the activities surveillance and monitoring of electronic communications in the workplace.

other relevant international texts and the provisions of Directive 95/46/EC, this working document offers guidance and concrete examples about what constitute legitimate monitoring activities and the acceptable limits of workers' surveillance by the employer. Please note that in some Member States, legislation may establish higher standard of protection of those contained in this working document.

Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace. They do have a legitimate expectation of a certain degree of privacy in the workplace as they develop a significant part of their relationships with other human beings within the workplace. However, this right must be balanced with other legitimate rights and interests of the employer, in particular the employer's right to run his business efficiently to a certain extent, and above all, the right to protect himself from the liability or the harm that workers' actions may create. These rights and interests constitute legitimate grounds that may justify appropriate measures to limit the worker's right to privacy. The clearest example of this would be those cases where the employer is victim of a worker's criminal offence.

However balancing different rights and interests requires taking a number of principles into account, in particular proportionality. It should be clear that the simple fact that a monitoring activity or surveillance is considered convenient to serve the employer's interest would not solely justify any intrusion in worker's privacy. Before being implemented in the work place, any monitoring measure must pass a list of tests, which are extensively detailed in this working document.

The following questions may summarise the nature of this assessment:

- a) Is the monitoring activity transparent to the workers?
- b) Is it necessary? Could not the employer obtain the same result with traditional methods of supervision?
- c) Is the processing of personal data proposed fair to the workers?
- d) Is it proportionate to the concerns that it tries to ally?

Focusing on the practical application of these principles, this working document provides guidance on the minimum content of companies' policies on the use of email and the Internet which employers and workers can take as a minimum for further elaboration (taking into account the peculiarities of a given company, its size and the national legislation in related areas to data protection).

When considering the use of the Internet for private purposes, the Article 29 Working Party takes the view that **prevention should be more important than detection**, in other words, that the interest of the employer is better served in preventing Internet misuse rather than in detecting such misuse. In this context, technological solutions are particularly useful. A blanket ban on personal use of the Internet by employees does not appear to be reasonable and fails to reflect the degree to which the Internet can assist employees in their daily lives.

The Working Party would like to stress that it is essential that the employer informs the worker of (i) the presence, use and purpose of any detection equipment and/or

apparatus activated with regards to his/her working station and (ii) any misuse of the electronic communications detected (e-mail or the Internet), unless important reasons justify the continuation of the secret surveillance⁷, which is not normally the case. Prompt information can be easily delivered by software such as warning windows, which pop up and alert the worker that the system has detected and/or has taken steps to prevent an unauthorised use of the network.

As a practical working document, employers may consider providing workers with two e-mails accounts:

- a) one for only professional purposes, in which monitoring within the limits of this working document would be possible,
- b) another account only for purely private purposes (or authorisation for the use of webmail), which would only be subject to security measures and would be checked for abuse in exceptional cases.

The Article 29 Working Party has noticed some divergences between the national laws in related areas to data protection, mainly dealing with the derogations allowed to the fundamental right to secrecy of correspondence and related to the scope and effect of collective worker's representation and co-decision. The Article 29 Working Party has not, nevertheless, noticed divergences between the national laws in the area of data protection which may serve as major obstacles to a common approach and therefore has issued this working document which will be reviewed during the years 2002-2003 in the light of the experience and further developments in this area.

⁷ Cases of justified covert monitoring would be a good example for that.

1. SURVEILLANCE AT THE WORK PLACE. A CHALLENGE TO SOCIETY.

The surveillance of workers has recently drawn considerable media attention and is presently the subject of public debate in the Community. Indeed the gradual introduction throughout the Community of e-mail in the workplace has drawn the attention of both, employers and workers, to the risk of invasion of their privacy within the workplace.

In considering the question of surveillance, it must always be borne in mind that while workers have a right to a certain degree of privacy in the workplace, this right must be balanced against the right of the employer to control the functioning of his business and defend himself against workers' action likely to harm employers' legitimate interests, for example the employer's liability for the action of their workers.

While new technologies constitute a positive development of the resources available to employers, tools of electronic surveillance do present the possibility of being used in such a way so as to intrude upon the fundamental rights and freedoms of workers. What should not be forgotten is that with the coming of the information technologies it is vital that workers should enjoy the same rights whether they work on-line or off-line.

It must be emphasised moreover that the conditions of work have evolved in the way that it becomes more difficult today to clearly separate work hours from private life. In particular, as "home office" is developing, many workers continue their work at home using computer infrastructure provided by the employer for that purpose or not.

The human dignity of a worker overrides any other considerations. In considering this issue it is important to bear this fact in mind and the resulting negative effects that such actions can have on the quality of a workers relationship with their employer and on their work itself.

In view of all these factors it is unsurprising that this issue is at the forefront of public debate and there is an urgent need to contribute to a uniform interpretation of the provisions of Directive 95/46/EC and national laws transposing it in the light of the recent jurisprudence of the European Court of Human Rights.

The Working Party was therefore of the opinion that it would be useful to impart the following information and working documents to the public and private sector. It should be noted that this working document covers any activity related to the surveillance of electronic communications in the work place both real time surveillance and access to stored data.

2. INTERNATIONAL LEGAL INSTRUMENTS

2.1 ARTICLES 8 AND 10 OF THE EUROPEAN CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

Article 8.

- 1. Everyone has the right to respect for his private and family life, his home and correspondence.
- 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 10.

- 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
- 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

All Member States and the European Union are bound by the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms. These rights have traditionally been exercised vertically (i.e. the individual vis-à-vis the state) and the debate about the extent to which they can be exercised horizontally (i.e. as between individuals) is ongoing. However it is clear that these rights are, in general, present.

The Working Party is therefore of the view that when considering the application of the national measures adopted under Directive 95/46/EC in order to contribute to the uniform application of such measures, it is necessary to recall the main principles of the case-law as it currently stands, of the European Court of Human Rights in relation to this provision and, in particular, as regards the secrecy of correspondence.

In the judgements given to date, the Court has made it clear that the protection of "private life" enshrined in Article 8 does not exclude the professional life as a worker and is not limited to life within home.

The case **Niemitz v. Germany** concerned the search by a government authority of the complainant's office. The government tried to argue that Article 8 did not afford protection against the search of someone's office as the Convention drew a clear

distinction between private life and home, on the one hand, and professional and business life and premises on the other.

The Court rejected this approach by stating:

"Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not"

More precisely in the case of **Halford v. the United Kingdom** the Court decided that interception of workers' phone calls at work constituted a violation of Article 8 of the Convention. Interestingly enough, Ms Halford was provided with two telephones, one of which was for private use. No restrictions were placed on the use of these telephones and no guidance was given to her.

Ms Halford alleged that the interception of her telephone calls amounted to violations of Article 8 of the Convention. The Government submitted that telephone calls made by Ms. Halford from her workplace fell outside the protection of Article 8, because she could have had no reasonable expectation of privacy in relation to them. At the hearing before the Court, counsel for the Government expressed the view that an employer should in principle, without the prior knowledge of the worker, be able to monitor calls made by the latter on the telephones provided by the employer.

In the Court's view, however, "it is clear from its case-law that telephone calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 paragraph 1 (...).

There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls...".

The notion of "correspondence" includes not only letters in paper form but also others forms of electronic communications received at or originated from the workplace, such as telephone calls made from or received at business premises or e-mails received at or sent from the offices' computers.

Some interpreters point out that this seems to also imply as (although it was not specified in the judgement) that if a worker is warned in advance by an employer about the possibility of their communications being intercepted, then he may loose his expectation of privacy and interception will not constitute a violation of Article 8 of the Convention. The

-

⁸ 23 November 1992, Series A n° 251/B, par. 29; Emphasis added

⁹ 27 May 1997

Working Party would not be of the opinion that advance warning to the worker is sufficient to justify any infringement of their data protection rights.

More generally, three principles can be extracted from the case law on Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms:

- a) Workers have a legitimate expectation of privacy at the workplace, which is not overridden by the fact that workers use communication devices or any other business facilities of the employer.
 - However the provision of proper information by the employer to the worker may reduce the workers legitimate expectation of privacy.
- b) The general principle of secrecy of correspondence covers communications at the workplace. This is likely to include electronic e-mail and related files attached thereto.
- c) Respect for private life also includes to a certain degree the right to establish and develop relationships with other human beings. The fact that such relationships, to a great extent, take place at the workplace puts limits to employer's legitimate need for surveillance measures.

Article 10 is also relevant, to a lesser extent, as it governs the freedoms of expression and of information and outlines the right of the individual to receive and impart information and ideas without interference by a public authority. The relevance of Article 10 seems to be reflected in the Court's considerations in the case Niemitz v. Germany above mentioned. As the Court said, in the working place people develop a significant part of their relationship with the outside world and therefore their right to freedom of expression certainly would play a role in this context.

2.2 CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (ETS NO. 108)

The Convention opened for signature on 28 January 1981 and was the first legally binding international instrument in the data protection field. Under this Convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.¹⁰

Other important documents related to the Convention 108 also relevant in this context are:

• Council of Europe's Working document (89) 2 on the Protection of Personal Data used for Employment purposes. ¹¹

See as well the Council of Europe's Recommendation (89) 2 on the Protection of Personal Data used for Employment Purposes: http://cm.coe.int/ta/rec/1989/89r2.htm

http://cm.coe.int/ta/rec/1989/89r2.htm

- Council of Europe's Working document (97) 5 on the Protection of Medical Data¹²
- Council of Europe's Working document (86) 1 on the Protection of Personal Data used for Social Security Purposes. ¹³
- Council of Europe's Recommendation (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services

2.3. THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 7. Respect for private and family life.

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8. Protection of personal data.

- 1. Everyone has the right to the protection of personal data concerning him or her.
- 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- 3. Compliance with these rules shall be subject to control by an independent authority.

The Charter of Fundamental Rights of the European Union seems to follow the main lines of the ECHR and the concept of secrecy of correspondence has been widened to become the concept of new generation "secrecy of communications" which is aimed at affording electronic communication the same degree of protection that mail has traditionally received.

In addition to that, Article 8, by giving data protection a substantially differentiated nature, complements the protection afforded by Article 7. This result is of particular importance as regards the issue of e-mail monitoring.

-

http://cm.coe.int/ta/rec/1997/97r5.html

http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm

2.4. INTERNATIONAL LABOUR OFFICE (ILO)

The International Labour Office Code of Practice on protection of workers' personal data (1997).

- "5. General Principles
- 5.1. Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.
- 5.2. Personal data should, in principle, be used only for the purposes for which they were originally collected.
- 5.3. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretation caused by a change of context.
- 5.4. Personal data collected in connection with technical or organisational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.
- 5.5. Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.
- 5.6. Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance (...)

6.14.

- (1) If workers are monitored, they should be informed in advance of the reasons for monitoring, the time schedule, the method and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers.
- (2) Secret monitoring should be permitted only:
 - a) if it is in conformity with national legislation or
 - b) if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing
- (3) Continuos monitoring should be permitted only if required for health and safety or the protection of property (...)
- 12.2. The workers' representatives, where they exist, and in conformity with national law and practice, should be informed and consulted:
- a) concerning the introduction or modification of automated systems that process worker's personal data,

- b) before the introduction of any electronic monitoring of workers' behaviour in the workplace
- c) about the purpose, contents and the manner of administering and interpreting any questionnaires and tests concerning the personal data of the workers".

3. SURVEILLANCE AND MONITORING OF ELECTRONIC COMMUNICATIONS IN THE WORK PLACE UNDER DIRECTIVE 95/46/EC

The following Working document is based on an application of the principles contained in Directive 95/46/EC to the question in hand taking into account Article 8 of the European Convention for the protection of human rights and fundamental freedoms which requires respect of the correspondence as well as the private life.

There are many forms of surveillance available to the employer within the workplace, all of which create their own individual problems. Two forms, to which similar principles apply, will be dealt with in this paper; e-mail monitoring and surveillance of Internet access.

The starting point is the confirmation of the point made in Opinion 8/2001 that Directive 95/46/EC applies to the processing of personal data in the employment context as in any other context ¹⁴. In addition to the general Directive 95/46/EC, the Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector might also be relevant. This Directive particularises and complements Directive 95/46/EC with respect to the processing of personal data in the telecommunications sector. As well as falling within the scope of Directive 95/46/EC, monitoring of electronic communications by employers, including e-mail and Internet access, might also fall within the scope of Directive 97/66/EC, which is presently being revised in the context of the review of the community legal framework on telecommunications. In the cases in which this Directive applies, its Article 5 (dealing with confidentiality of the communications) and Article 6 (on traffic and billing data) can play a particularly important role.

3.1 GENERAL PRINCIPLES APPLYING TO E-MAIL AND INTERNET MONITORING

The following data protection principles are derived from Directive 95/46/EC and should be complied with when considering the processing of personal data that is involved in such monitoring. Compliance with all the following principles is necessary for any monitoring activity being lawful and justified.

3.1.1. NECESSITY

This principle means that the employer must check if any form of monitoring is absolutely necessary for a specified purpose before proceeding to engage in any such activity. Traditional methods of supervision, less intrusive for the privacy of individuals, should be carefully considered and where appropriate implemented before engaging in any monitoring of electronic communications.

It would only be in exceptional circumstances that the monitoring of a workers mail or Internet use would be considered necessary. For instance, monitoring of a worker's e-mail may become necessary in order to obtain confirmation or proof of certain actions on his

13

-

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf

part. Such actions would include criminal activity on the part of the worker insofar as it is necessary for the employer to defend his own interests, for example, where he is vicariously liable for the actions of the worker. These activities would also include detection of viruses and in general terms any activity carried out by the employer to guarantee the security of the system.

It should be mentioned that opening an employee's e-mail may also be necessary for reasons other than monitoring or surveillance, for example in order to maintain correspondence in case the employee is out of office (e.g. sickness or holidays) and correspondence cannot be guaranteed otherwise (e.g. via auto reply or automatic forwarding).

The principle of necessity also means that an employer should only keep the data no longer than is necessary for the specified purpose of the monitoring activity.

3.1.2. FINALITY

This principle means that data must be collected for a specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes. In this context the "compatibility" principle means, to use an example, that if the processing of data is justified on the basis of the security of the system, this data could not then be processed for another purpose such as for monitoring the behaviour of the worker.

3.1.3. TRANSPARENCY

This principle means that an employer must be clear and open about his activities. It means that no covert e-mail monitoring is allowed by employers except in those cases where a law in the Member State under Article 13 of the Directive allows for that ¹⁵. This is most likely to be the case where specific criminal activity has been identified (being necessary to obtain evidence and subject to the respect of legal and procedural rules of the Member States) or in those cases where national laws providing the necessary safeguards, authorise the employer to take certain actions to detect infractions in the workplace.

Furthermore, this principle can be divided into two aspects:

3.1.3.1. THE OBLIGATION TO PROVIDE INFORMATION TO THE DATA SUBJECT

This is, perhaps, the most relevant example of the principle of transparency in practice to the question at hand. It means that the employer has to provide his workers with a readily accessible, clear and accurate statement of his policy with regard to e-mail and Internet monitoring.

Workers need to be provided with full information as to what specific circumstances would justify such an exceptional measure and as to the breadth and scope of such monitoring. Elements of this information should be:

Article 13 of the Directive allows Member States to adopt legislative measures to restrict the scope of the obligations and rights provided for in certain articles of the Directive when such a restriction constitutes a necessary measures to safeguard important public interests such as national security or the prevention, investigation, detection and prosecution of criminal offences, or the protection of the data subject or of the rights and freedoms of others.

- 1. E-mail/Internet policy within the company describing in detail the extent to which communication facilities owned by the company may be used for personal/private communications by the employees (e.g. limitation on time and duration of use).
- 2. Reasons and purposes for which surveillance, if any, is being carried out. Where the employer has allowed the use of the company's communication facilities for express private purposes, such private communications may under very limited circumstances be subject to surveillance, e.g. to ensure the security of the information system (virus checking).
- 3. The details of surveillance measures taken, i.e. who? what? how? when?
- 4. Details of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them.

The Working Party would like to stress at this point that it is advisable from a practical point of view that the employer immediately informs the worker of any misuse of the electronic communications detected, unless important reasons justify the continuation of the surveillance¹⁶, which is not normally the case. Prompt information can be easily delivered by software such as warning windows, which pop up and alert the worker that the system has detected an unauthorised use of the network. Quite a lot of misunderstandings can also be solved in this way.

A further example of the transparency principle, is the practice of employers to inform and/or consult worker representatives before introducing worker-related policies. It should be stressed that decisions on monitoring of workers, including surveillance of electronic communications of workers, are covered by the recently adopted Directive 2002/14/EC provided that the enterprise or undertaking concerned falls within its scope of application. In particular, this Directive provides for information and consultation of employees on decisions likely to lead to substantial changes in work organisation or in contractual relations. National legislation or collective agreements may lay down arrangements, which are even more favourable to employees.

Collective agreements may not only oblige the employer to inform and consult with worker representatives before implementing surveillance systems, but may moreover make such implementation subject to the worker representatives' prior agreement.

Collective agreements may also set out the scope and extent of the Internet and email use by employees that is allowed as well as details of the monitoring of such use.

3.1.3.2. THE OBLIGATION TO NOTIFY SUPERVISORY AUTHORITIES BEFORE CARRYING OUT ANY WHOLLY OR PARTLY AUTOMATIC PROCESSING OPERATION OR SET OF SUCH PROCESSING OPERATIONS

-

¹⁶ Cases of justified covert monitoring would be a good example for that.

This is another way of providing transparency as workers can always check in the Data Protection registers, for instance, what categories of data, for what purposes and for what recipients is the employer supposed to process the personal data of their employees.

3.1.3.3. RIGHT OF ACCESS

A Worker, as any other individuals under the Directive¹⁷, has a right of access to the personal data related to him processed by his employer and where appropriate, request its rectification or erasure or blocking which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data.

Worker's access to employers' files <u>without constraint</u> at reasonable intervals and without excessive delay or expense is a powerful tool that workers individually can exercise to make sure that the monitoring activities in the workplace remain lawful and fair to the workers. Access to employer's files, however, might be problematic in exceptional circumstances as for example access to the so-called evaluation data.

The Working Party has already taken a first view on this issue¹⁸ and may provide further guidance in the future in the light of the experience.

3.1.4. LEGITIMACY

This principle means that any data processing operation can only take place if it has a legitimate purpose as provided for in Article 7 of the Directive and the national legislation transposing it. Article 7(f) of the Directive is particularly relevant to this principle in that in order for processing a workers data to be allowed under Directive 95/46/EC, it must be

¹⁷ Article 12: Member States shall guarantee every data subject the right to obtain from the controller:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purpose of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with b), unless this proves impossible or involves a disproportionate effort.

a) without constraint at reasonable intervals and without excessive delay or expense:

¹⁸ See recommendation 1/2001 on employee evaluation data.

for the purposes of legitimate interests pursued by the employer and it must not infringe upon the fundamental rights of the workers.

The need of the employer to protect his business from significant threats, such as to prevent transmission of confidential information to a competitor, can be such a legitimate interest.

The processing of sensitive data in this context is particularly problematic, as Article 8 of the Directive does not allow for a balance of interest within the meaning of Article 7 (f) of the Directive. However, the second paragraph, letter b) of Article 8 makes reference to "processing necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards".

The processing of sensitive data connected to monitoring activities and surveillance is a difficult issue, which is not only relevant for the employment context. Indeed is a general issue on which the Working Party may provide some guidance in the future.

As a matter of fact, unless specifically authorised by national law providing for adequate safeguards, monitoring activities directly aimed at the processing of sensitive data of workers would not find a legitimisation under the provisions of Directive 95/46/EC and would not be acceptable. However, preventing or making very difficult any monitoring activities (which in many cases are not only lawful but even also desirable such as those directly aimed at guaranteeing the security of the system), by the simple fact that the processing of certain sensitive data might be unavoidable involved, does not seem acceptable either.

3.1.5. Proportionality

This principle requires that personal data including those involved in monitoring must be adequate, relevant and not excessive with regard to achieving the purpose specified. The company policy in this area should be tailor made according to the type and the degree of risk, which the particular company faces.

The proportionality principle therefore rules out blanket monitoring of individual e-mails and Internet use of all staff other than where necessary for the purpose of ensuring the security of the system Where the objective identified can be achieved in a less intrusive way the employer should consider this option (for example, he/she should avoid systems that monitor automatically and continuously).

The monitoring of e-mails should, if possible, be limited to traffic data on the participants and time of a communication rather than the contents of communications if this would suffice to allay the employers concerns. If access to the e-mail's content is absolutely necessary, account should be taken of the privacy of those outside the organisation receiving them as well as those inside. The employer, for instance, cannot obtain the consent of those outside the organisation sending e-mails to his workers. The employer should make reasonable efforts to inform those outside the organisation of the existence of monitoring activities to the extent that people outside the organisation could be affected by them. A practical example could be the insertion of warning notices regarding

the existence of the monitoring systems, which may be added to all outbound messages from the organisation.

Technology gives the employer much opportunity to assess the use of e-mail by his workers by checking, for example, the number of mails sent or received or the format of any attachments and therefore the actual opening of mails is disproportionate. Technology can further be used to ensure that the measures taken by an employer to safeguard the Internet access he provides to his workers from abuse are proportionate by utilising blocking, as opposed to monitoring, mechanisms. ¹⁹

Systems for the processing of electronic communications should be designed to limit the amount of personal data processed to a strict minimum²⁰.

On the question of proportionality it should be highlighted that the mechanism of collective bargaining can be very useful in deciding what actions are proportionate to what risk faced by what employer. A consensus can thus be reached between the employer and the workers regarding how the balance of interests can be struck.

3.1.6. ACCURACY AND RETENTION OF DATA

This principle requires that any data legitimately stored by an employer (after consideration of all the other principles in this chapter) consisting of data from or related to a workers e-mail account or their use of the Internet must be accurate and kept up to date and not kept for longer than necessary. Employers should specify a retention period for e-mails in their central servers based on the business needs. It is hard to see that a retention period longer of three months would be normally justified.

3.1.7. SECURITY

This principle obliges the employer to implement appropriate technical and organisational measures to ensure that any personal data held by him is secure and safe from outside intrusion. It also encompasses the right of the employer to protect his system against viruses and may involve the automated scanning of e-mails and network traffic data.

The Working Party is of the opinion that, in view of the importance of maintaining a secure system, such automated opening of e-mails should not be considered as violating the worker's right to privacy, provided that appropriate safeguards are put in place. For

- Internet: some companies use a software tool, which can be configured in order to block any connection to predetermined categories of websites. The employer can, after consultation of the aggregated list of websites visited by his employees, decide to add some websites to the list of those already blocked (possibly after notice to the employees that connection to such site will be blocked except if the need to connect to that site is demonstrated by an employee).

- E-mail: other companies use an automatic redirect facility to an isolated server, for all e-mails exceeding a certain size. The intended recipient is automatically informed that a suspect e-mail has been redirected to that server and can be consulted there.

 $^{^{19}}$ Many examples can already be taken from the practice as to this use of technology.

²⁰ Draft Directive 97/66, Recital 30

example, employers may now avail of automated technologies, which serve their security interests without infringing on the workers rights to privacy.

The Article 29 Working Party draws attention to the role of the system administrator, a worker who holds important responsibilities from the data protection point of view. It is of great importance that the system administrator and anyone else who has access to personal data about workers in the course of monitoring, is placed under a strict duty of professional secrecy with regard to confidential information, to which they have access.

4. E-MAIL MONITORING

4.1. THE SECRECY OF CORRESPONDENCE

As explained earlier in the working document, the Working Party is of the view that online and off-line situations should not be treated differently without reason and as such emails benefit from the same protection of fundamental rights as traditional paper mail ²¹. The jurisprudence of the European Court of Human Rights has provided some guidance on the application of the principle of the right of secrecy of correspondence in a democratic society. However, Member States' legal systems interpret this principle slightly differently, in particular as regards its scope of application to professional communications, both as regards its content and the traffic data. From the data protection issue it does have important consequences when considering the degree of tolerable intrusion in workers' e-mail.

The Article 29 Working Party is of the view that <u>electronic communications made from business premises may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 paragraph 1 of the European Convention.</u> There is little margin for interpretation as this respect as this issue has been clearly settled by the Court in the case **Halford v. the United Kingdom** mentioned above.

What remains to be seen and indeed allows for certain margin of interpretation is to what extent this principle can be subject to derogations or limitations in particular when it is confronted with the rights and freedoms of others similarly protected by the Convention (e.g. legitimate interests of the employer). In any case, location and ownership of the electronic means used do not rule out secrecy of communications and correspondence as laid down in fundamental legal principles and constitutions.

The Article 29 Working Party would like nevertheless to recall that this is not a specific problem for the processing of personal data in the employment context but a general one, which arises from the fact that data protection laws and regulations do not apply in abstract. Data Protection rights are supposed to apply to different legal systems with other laws in place stipulating other rights and obligations for individuals (e.g. employment law). The Article 29 Working Party is nevertheless convinced that the solutions proposed in this working document can be useful when conducting this difficult balance of interest.

See http://europa.eu.int/comm/internal market/en/dataprot/wpdocs/wp6en.pdf

The Internet Task Force Paper, most important document adopted by the Working Party on privacy in the Internet, insisted on this idea in its Chapter number 3, page 21:

See http://europa.eu.int/comm/internal market/en/dataprot/wpdocs/wp37en.pdf

20

_

One of the first recommendations issued by the Working Party, Recommendation 3/97 "Anonymity in Internet", already said that on-line and off-line situations should be treated in the same way.

4.2. LEGITIMISATION UNDER DIRECTIVE 95/46/EC

E-mails contain personal data covered by the provisions of Directive 95/46/EC and therefore employers must have a legitimate ground for processing this data. As it was extensively explained in Opinion 8/2001, consent of workers must be freely given and fully informed and employers should not rely on consent as a general means of legitimising such processing.

The most likely legitimisation for e-mail monitoring can be found in Article 7 (f) of the Directive, that is, where processing is necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed. Before considering the application of this provision to the points at issue, it must be pointed out that such legitimisation cannot override fundamental rights and freedoms of the worker. This includes, where applicable, the fundamental right to secrecy of correspondence.

The Working Party has already taken the view that²²:

"Where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment"

Given that e-mails contain personal data of both the sender and the recipient, and employers can only generally obtain the consent of one of these parties without major difficulty (unless the e-mails comprise inter-staff correspondence), the possibility of legitimising the monitoring of e-mails on the basis of such consent is very limited. Similar considerations apply to Article 7 (b) of the Directive as one of the parties to the letter would never have a contract with the data controller within the meaning of this provision, i.e. to monitor the mail.

It should at this juncture, be pointed out, that where a worker is given an e-mail account for purely personal use or is allowed access to web-mail account, opening of e-mails in this account by his employer (apart from scanning viruses) can only be justified in very limited circumstances²³ and cannot under normal circumstances be justified on the basis of Article 7 (f) because it is not in the legitimate interests of the employer to have access to such data. Instead the fundamental right to secrecy of correspondence prevails.

Therefore, the question of the extent to which Article 7 (f) allows the monitoring of emails depends on the application on a case by case basis of the fundamental principles explained in Chapter 3.2. As already indicated in chapter 3.1.4 (legitimacy) when

.

See paragraph in a framework in page 23 of Opinion 8/2001.

Such actions would include criminal activity on the part of the worker insofar as it is necessary for the employer to defend his own interests, for example, where he is liable for the actions of the worker, or where he is the victim of the criminal activity.

conducting this balance test proper account should be taken of the privacy of those outside the organisation affected by the monitoring.

4.3 RECOMMENDED MINIMUM INFORMATIONTHAT THE COMPANY SHOULD PROVIDE TO ITS WORKERS

In drawing up their policy employers must comply with the principles set out in Chapter 3.1.3 under the general Transparency principle²⁴, in the light of the necessities and the size of the organisation.

And more specifically in relation to e-mail the following points should be addressed;

- a) Whether a worker is entitled to have an e-mail account for purely personal use, whether use of web-mail accounts is permitted at work and whether the employer recommends the use, by workers, of a private web-mail account for the purpose of using e-mail for purely personal use (see Chapter 4.4).
- b) The arrangements in place with workers to access the contents of an e-mail, i.e. when the worker is unexpectantly absent, and the specific purposes for such access.
- c) When a backup copy of messages are made, the storage period of it.
- d) Information as to when e-mails are definitively deleted from the server.
- e) Security issues
- f) The involvement of representative of workers in formulating the policy.

It should be noted that there is a continual obligation on the employer to ensure that his policy is kept up to date in line with technological developments and the opinion of his workers.

4.4 WEBMAIL²⁵

24

- 1. E-mail/Internet policy within the company describing in detail the extent to which communication facilities owned by the company may be used for personal/private communications by the employees (e.g. limitation on time and duration of use).
- 2. Reasons and purposes for which surveillance, if any, is being carried out. Where the employer has allowed the use of the company's communication facilities for express private purposes, such private communications may under very limited circumstances be subject to surveillance, e.g. to ensure the security of the information system (virus checking).
- 3. The details of surveillance measures taken, i.e. who? what? when?
- 4. Details of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them
- Webmail is a web e-mail system, which provides web based e-mail from any POP or IMAP server, which is generally user name and password protected.

The Working Party is of the opinion that such a policy of allowing workers the use of a private account or web-mail could contribute to a pragmatic solution of the problem at issue. Such a working document on the part of the employer would clarify the distinction between e-mails for professional and for private use, and would reduce the possibility of employers invading their workers' privacy. Furthermore it would involve no, or minimal, extra cost to the employer.

If an employer adopts such a policy then it would be possible, in specific cases where there is a serious suspicion about the behaviour of a worker, to monitor the extent to which that worker is using their PC for personal purposes by noting the time spent in webmail accounts. In this way the employers interests would be served without any possibility of worker's personal data, and in particular, sensitive data, being disclosed.

Furthermore such a policy may be of benefit to workers as it would provide certainty for them as to level of privacy they can expect which may be lacking in more complex and confusing codes of conduct. Having said that, it is also necessary to stress that:

a) the fact that the use of web-mail or private account is allowed does not prejudice the full application of previous sections of this chapter to other e-mail accounts in the workplace

- b) when allowing the use of web-mail, companies should be aware that their use might challenge the security of companies' networks, especially as regards the spreading of viruses.
- c) workers should be aware that sometimes servers of web-mail are located in third countries where there could not be adequate protection of the personal data of individuals.

It should be born in mind that these considerations apply to standard employer-employee relationships. Special rules might need to be applied to the communication of those employees who are bound by obligations of professional secrecy.

5. MONITORING OF INTERNET ACCESS

5.1 PRIVATE USE OF THE INTERNET AT WORK

First and foremost it should be emphasised that it is up to the company to decide if workers are allowed to use the Internet for personal reasons and the extent to which this is permissible.

That point considered however, the Working Party is of the opinion that a blanket ban on personal use of the Internet by employees may be considered to be impractical and slightly unrealistic as it fails to reflect the degree to which the Internet can assist employees in their daily life.

5.2. PRINCIPLES RELATING TO INTERNET MONITORING

There are some principles, which can be applied when considering the question of monitoring workers access to the Internet.

Wherever possible **prevention should be more important than detection**. In other words the interest of the employer is better served in preventing Internet misuse through technical means rather than in expending resources in detecting misuse. To the extent reasonably possible Internet policy should rely on technical means to restrict access rather than on monitoring behaviour, i.e. by having some sites blocked or installing automatic access warnings.

The delivering of prompt information to the worker on the detection of a suspicious use of the Internet is important in order to minimise problems Even if a necessary measure, any monitoring must be **a proportionate response** to the risk faced by the employer. In most cases Internet misuse can be detected without the necessity of analysing the content of the sites visited. For example, a check on the time spent, or a check on the sites most frequently visited by a department may suffice to reassure an employer that their facilities are not being misused. If these general checks reveal possible misuse of the Internet, then the employer may consider the possibility of additional monitoring of the area at risk.

When assessing Internet use by workers employers **should try to exercise caution in coming to conclusions**, taking into account the ease with which websites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading banner advertising and miskeying. In any case, workers must have the facts presented to them and be given full opportunity to contest the misuse alleged by the employer.

5.3 RECOMMENDED MINIMUM CONTENT OF COMPANY'S INTERNET POLICY

- 1. The information specified in Chapter 3.1.3 under the Transparency principle²⁶.
 - And more specifically in relation to Internet use in particular the following points should be addressed:
- 2. The employer must set out clearly to workers the conditions on which private use of the Internet is permitted as well as specifying material, which cannot be viewed or copied. These conditions and limitations have to be explained to the workers.
- 3. Workers need to be informed about the systems implemented both to prevent access to certain sites and to detect misuse. The extent of such monitoring should be specified, for instance, whether such monitoring may relate to individuals or particular sections of the company or whether the content of the sites visited is viewed or recorded by the employer in particular circumstances. Furthermore, the policy should specify what use, if any, will be made of any data collected in relation to who visited what sites.
- 4. Inform workers about the involvement of their representatives, both in the implementation of this policy and in the investigation of alleged breaches.

26

- 1. E-mail/Internet policy within the company describing in detail the extent to which communication facilities owned by the company may be used for personal/private communications by the employees (e.g. limitation on time and duration of use).
- 2. Reasons and purposes for which surveillance, if any, is being carried out. Where the employer has allowed the use of the company's communication facilities for express private purposes, such private communications may under very limited circumstances be subject to surveillance, e.g. to ensure the security of the information system (virus checking).
- 3. The details of surveillance measures taken, i.e. who? what? when?
- 4. Details of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them.

CONCLUSION

The Working Party has drafted this working document to contribute to the uniform application of the national measures adopted under Directive 95/46/EC on the area of surveillance and monitoring of electronic communications in the workplace. (Please see summaries of national legislation in Annex to this document).

The Working Party has noticed some divergences between the national laws, mainly in related areas to data protection dealing with the derogations allowed to the fundamental right to secrecy of correspondence and related to the scope and effect of collective representation and co-decision. The Article 29 Working Party would like to stress, nevertheless, that any divergences between Member States' laws implementing Directive 95/46/EC do not serve as major obstacles to a common approach, which is contained in the principles and good practices outlined in this working document.

The Subgroup on Employment shall keep this working document under review in the light of the experience and further developments in this area during the years 2002- 2003.

Done at Brussels, 29 May 2002

For the Working Party

The Chairman

Stefano RODOTA

ANNEX TO THE WORKING DOCUMENT

NATIONAL LEGISLATION ON SURVEILLANCE AND MONITORING OF ELECTRONIC COMMUNICATION IN THE WORKPLACE

6.1.1 Belgium

Article 22 of the Belgian Constitution guarantees the right to privacy.

Article 2,s.1 of the collective agreement nr. 13 of 13 December 1983 provides that "once an employer has decided to invest in new technology...which has important collective consequences for...working conditions he must before the beginning of the introduction of the new technology provide information about the nature of the new technology, about the factors that justify it's introduction and it's consequences and consult with the representatives of the employees on the introduction of the new technology".

Furthermore, the principle of secrecy of correspondence is guarded by Article 109 d of the law of 21 March 1991 on the reform of certain economic public companies which states that "save with consent....it is prohibited for anybody, whether carried out by oneself or through a third person, to take cognisance of the existence of data of all kinds that have been transferred by means of telecommunication and that originate from and are destined to other persons".

The Belgian Data Protection Authority has also addressed the issue of e-mail and Internet monitoring in an Opinion in 2000 (Opinion no.10/2000 of 3 April 2000). Regarding the monitoring of e-mails, the Belgian Commission is of the opinion that an employer should not gain access to the content of an e-mail as such an action is not a proportionate response to any interests that the employer may wish to protect. The Commission has recommended that instead employers should monitor on the basis of a list of e-mail traffic and use software designed to identify inordinately large messages or chain messages.

Regarding the monitoring of Internet use, the Commission is of the view that continual monitoring of individuals is inappropriate. The Commission recommends that an employer makes a general review of all web sites visited by his workers (without identifying which individuals have visited what site) and following such an investigation, assess possible areas of risk and take individual action accordingly.

6.1.2 Denmark

Monitoring and surveillance in the workplace is mainly dealt with through collective agreements and especially the so-called 'basic agreement'. As a central part of this basic agreement is the recognition that the employer is allowed monitor the work done in the workplace. However, in case law it has been recognised that this right is subject to the obligation on employers to act responsibly and not to abuse their powers.

According to the Annex to the Basic Agreement between the Danish Confederation of Employers and the Danish Confederation of Trade Unions of 24 April 2001, the employer is obliged to inform the employees of any specific monitoring activities that he plans to carry out two weeks in advance of any such monitoring being introduced.

This agreement is typical of those in place in Denmark.

Monitoring of telecommunications is contrary to s.263 (1)(3) the Danish Criminal Code regardless of whether the communication is private or professional. However, whether email is included within this prohibition is unclear, and private Internet use is not.

The Danish Data Protection Agency has in some cases found that an employer may record/log the employee's use of the Internet. The following conditions have to be complied with.

The recording and examination of the log file has to be necessary for the legitimate interests of the employer, and the interests of the employee may not override this interest. Legitimate interests can be technical and security interests as well as interests of the employer to monitor the employee's use of the Internet.

In a clear and unambiguous way, the employer shall normally in advance inform the employee of the recording and that the recording may be checked on suspicion of the workers misuse of the Internet according.

Concerning e-mail, the Danish Data Protection Authority has found that a company may draw up a security copy of the e-mails of the employee's and examine this copy by suspicion of misuse of the e-mail system. The following conditions have to be complied with:

The security copy and the possible examination of the e-mail of the employee may only take place if it is necessary for the legitimate interests of the employer and the interests of the employee do not override these interests.

The legitimate interests can be interests of the operation of the business, security, reestablishment of the e-mail, documentation and monitoring.

Both concerning monitoring of the use of Internet and monitoring e-mail the employer is obliged to process data in accordance with good practices for the processing of data.

6.1.3 Germany

Article 10 of the Constitution guarantees privacy of posts and telecommunications. Additionally s85 of the Telecommunication Act obliges everybody who provides telecommunication services to maintain the secrecy of telecommunications.

The degree of protection is different between private and official use of electronic communications. The control of official mails is allowed. But without consent it is not allowed to use surveillance of (official) e-mail as a means for control of employees' efficiency. An employer/works council agreement is necessary for this. It is in any case forbidden to control and particularly to read private e-mails. The best practical solutions for this problem are separate e-mail accounts for private and official mails.

If the use of the Internet is possible at the work place the problems are the same. The regulations for data protection in the field of teleservices (Teleservices Data Protection Act, in its recently amended version) do not apply for official use of the Internet at the workplace. But they do apply to the private use of the Internet as far as it is allowed.

Surveillance or monitoring is allowed without consent as far as necessary to ensure the systems effective operation (for example, virus check).

6.1.4 Greece

The Hellenic Constitution of 1975, as revised in April 2001, contains a set of fundamental rules covering privacy and the broader right to personality.

Furthermore, Greece has constitutional provisions, which deal with respect for, and the protection of, human value that cannot be waived by the individual. Under Greek law contract, which excessively curtails the freedom of the individual is void.

Articles 178 and 179 of the Civil Code state that any legal act contrary to good morals is void and Greek law also states that a legal act is also void when it excessively curtails another's freedom. The term "freedom" is taken to mean the provisions on human rights set by the Constitution, which includes the right to privacy.

These provisions could be used to invalidate a monitoring of e-mails by employers as such an action curtails the employees right to privacy.

Law 1767/1988, as amended by Law 2224/1994, grants worker's councils powers to jointly decide with the employer on certain issues including surveillance.

Furthermore the Hellenic Data Protection Authority has produced a decision on monitoring in the workplace.

6.1.5 Spain

The Spanish Constitution states in Article 18 the secrecy of communications regarding private communications – either postal, telegraphic or telephonic. It also states the limit to the use of data processing, established and developed by law, in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.

Article 5 of the 1995 Labour Act refers to the obligation of the employees of accomplishing with their labour obligations according to the good faith and diligence. Otherwise it is considered a breach of contract (Article 54.2)

Article 18 of the Labour Act states that "Inspections of the employee's person, lockers and personal belongings shall only be carried out when necessary for the protection of the company assets and those of the rest of the company employees, inside the workplace and in labour time. The dignity and privacy of the employee shall be respected to the utmost

during inspection and it will be carried out in the presence of a legal employee representative or, in his absence, another company employee, whenever this is possible"

Article 20 of the Labour Act is referred to the power of managing, inspecting, organising and controlling of the employer. The employer may adopt any appropriate measures to verify and control the performance of the employees' duties, always respecting human dignity.

The 1995 Labour Hazards Prevention Law refers to the employer's duty to consult the employees, in due advance, about the adoption of decisions related to, among others, the planning and organisation of work in the company and the introduction of new technologies, and everything connected with their consequences for the employees' safety and health, derived from the election of the equipment, the definition and adequacy of working conditions, and the impact of environmental factors at the workplace.

The Labour Act and the 1985 Union Freedom Act develop the employees' right to collective representation as their right to participate in the company through collective representative bodies (Personnel Delegates and Company Committees) and Union representatives.

The Civil Code states in Article 1903 that employers are responsible face to face with third parties of the damages caused by their employees in the carrying out or their tasks.

The Criminal Code punishes in Article 197 to take possession of someone else's private correspondence when the purpose is to disclose a personal secret or the private life.

6.1.6 France

Article 9 of the French Civil Code guarantees each individual the right to respect for his private life, even during and in the place of work.

According to the 1991 law on secrecy of communications, an employer cannot access the private communications of its workers except under the authority of a judicial warrant or when the interception is made in 'good faith'. The latter term has been interpreted by the CNIL (the French data protection authority) as permitting the monitoring of the volume and size of messages together with the format of attached documents but not the reading of e-mails.

Under Article L. 121-8 of the French Labor Code, an employer cannot collect personal information concerning an employee without informing the employee. This means that workers must be informed of the existence of surveillance devices introduced by their employer.

Further, in the Neocel case [Cass. Soc. 20/11/91 (RDS 1992(2), 77)], it was affirmed that the Civil Code prohibits the surreptitious surveillance of employees.

In the course of a recent appeal by Nikon France it was decided on 2 October last by the French Supreme Court (Social Chamber) that an employee has the right to have his privacy respected and this implies that his employer cannot have access to the content of personal messages sent or received by the employee.

In the case in question the employee had sent a personal e-mail through the computer he used for the purposes of his work despite the fact that his employer had specifically

prohibited personal use of the system. The court found that despite the fact that the employee had disobeyed the employer, this did not justify the reading of the mail by the employer.

The Court was of the opinion that limited daily use of e-mail/Internet should be allowed, provided that such a use does not affect the daily professional life of the employee. It was also recommended that messages should always contain a description as to whether they are personal or professional.

After public consultations on drafted detailed principles on cyber-surveillance, which started in March 2001, the French national data protection authority (CNIL) adopted conclusions on 5 February 2002, which recommend - among other things - the solution of the question of surveillance in the workplace through further negotiation and the designation of a specific personal data protection official by the social partners.

6.1.7 Ireland

Art. 40.3.1 of the Irish Constitution guarantees that the State will, in it's laws, respect and, as far as practicable, by it's laws, defend and vindicate the personal rights of the citizen. These 'personal rights' of the citizen, or 'unnumerated rights' as they have been referred to in the Irish case law, are ever evolving. The right to privacy has already been recognised in Irish case law as being one of the personal rights of the citizen.

6.1.8 Italy

Under Italian law a judicial order is required for accessing employee's e-mail messages.

Article 15 of Italian Constitution guarantees the freedom and secrecy of correspondence and 'any other form of communication'.

The importance of this provision has been recognised by the Italian Garante (Data Protection Authority) in the context of e-mail surveillance. They stated, in an Opinion of 12 July 1999, that e-mails attract the same confidentiality privilege as traditional mail and they also stressed that an Act of 1993 (no. 547) on computer related crimes and a decree of 1997 (no. 513) on electronic documents referred to the need to safeguard e-mail in the same way as traditional mail.

More specifically, this Opinion ruled that electronic messages circulated via restricted access newsgroups and mailing lists using an employer's equipment were to be regarded as private correspondence and could not be accessed by the employer.

The Garante is currently considering the possibility of issuing guidelines in the area of email surveillance in light of any working documents made by the Working Party.

The Italian Data Protection legislation (Law No. 675/1996) states under section 43(2) thereof, that is does not affect existing employment legislation relating to workers rights (Law No. 300/1970). Article 4 of the latter Act outlaws surveillance of workers per se and only allows technology which could indirectly result in the surveillance of workers if the appropriate trade union agrees to same and there are specific requirements in connection with organisation, production and/or occupational security.

6.1.9 Luxembourg

No section contributed as yet.

6.1.10 Netherlands

Article 10 of the Dutch constitution states that everyone has the right to have their privacy respected.

The constitutional imperative can be used to interpret Section 660 of the Civil Code.

This section states that employers must do or refrain from doing, that which a good employer would do or refrain from doing, in similar circumstances. Furthermore section 611 of the Civil Code deals with the relationship and good performance of employer and worker. This section, in light of the constitutional guarantee, could be interpreted as guaranteeing employee privacy.

Article 5.1-5.3 of the Working Conditions Act provides that workers have to be informed in case of employee monitoring, and that the worker's councils and trade unions have to be informed, and in some cases, agree to any such measures. In particular the Working Council Law underlines that the work council should be informed, heard and agree concerning monitoring at the workplace.

Under Article 8 of their Data Protection Act monitoring is only allowed when the employees have given their unambiguous consent, or the processing is necessary for the performance of the labour agreement, or for the fulfilment of a legal obligation of the employer, or for the purposes of the legitimate interest pursued by the employer.

In a 1999 decision of the Dutch Data Protection Authority it was decided that continuous monitoring of e-mail is not allowed, as there is no specified and legitimate purpose to such monitoring. This decision applies even where the employer's policy clearly states that the worker should have no expectation of privacy.

In a judgement of the regional Court of Harlem of 16 June 2000, it was referred to the concept of "privatisation of the workplace" meaning that the boundaries between private life and work life are not clear anymore. In this context private contacts at work should be allowed.

6.1.11 Austria

Article 8 of the European Convention on Human Rights, which deals with the right to privacy, is directly applicable in Austria and has been given the status of a constitutional guarantee in the Austrian legal system. Furthermore, Article 1 of their Data Protection Act of 2000 (Datenschutzgesetz 2000), which creates the right of individuals to have their data protected, also has the status of a constitutional right.

Data protection in the workplace is subject to the fundamental right of data protection regulations laid down in the Austrian Data Protection Act of 2000 (Datenschutzgesetz 2000).

There is an explicit provision concerning the use of sensitive data in the workplace-s.9, ss.11. Under this section "interests in secrecy" of the Data subject are not infringed when the use of their sensitive personal data is required by an employer according to his rights and duties in the field of employment law and is legitimate according to specific legal provisions.

Under Art. 96 of the Arbeitsverfassungsgesetz (Federal Law Gazette No. 22/1974) certain measures cannot be undertaken by an employer without the consent of the relevant labour council. These include introducing control measures and technical installations if such measures impinge upon human dignity. Furthermore this consent of the worker's council is necessary even if in individual employment contracts the employee agrees to such measures.

6.1.12 Portugal

The Portuguese Constitution is quite forward thinking in its approach. Rather than having a general Article in their constitution on privacy, Article 35, deals with data protection in relation to the use of computerised data. The Portuguese Constitution also contains article about the intimacy reservation of private life and the protection of personal dignity (Article 26) and assures the secrecy of correspondence and other means of private communication (Article 34 paragraph 1). Article 34 paragraph 4 prohibits the intrusion of public authorities in correspondence, in telecommunications and other means of communication, with the exception of the cases set by law within criminal procedure.

According to Article 18 these constitutionally guaranteed rights have to be respected both in the public and private sector, meaning they also have to be protected in private labour relationships.

Under Article 54 of the Constitution, workers' councils are given the right to receive information and be consulted in relation to any change in working conditions.

In a 1998 decision of the Portuguese Data Protection Commission, the Commission ruled directly on the issue of Secrecy of Correspondence. The decision concerned the refusal of a telecommunications company to comply with a request for information from the courts. The Commission pointed out that under Article 34 paragraphs 1 and 4 of the Portuguese Constitution the right to secrecy of correspondence is recognised, and decided that this right covered both the traffic of the communication and the contents.

The Labour Agreement Act, in its article 39.1, recognises to the employer the right to establish the terms, in which the work shall be rendered, and shall do so within the bounds settled by the labour agreement and its own regulation. Whenever the working conditions or the number of employees justifies it, the employer may elaborate rules of procedure, containing the "organisation and working discipline rules" (article 39.2). The working council, in case it exists, shall be previously heard on the rules of procedure, which are approved and verified by the labour inspection services (cf. article 39.3 and article 13 c) of the above mentioned Act (DL 219/93 of 16/6).

Besides the duty of obedience, the employee shall "watch over the good maintenance and use of the goods related to his work, entrusted by the employer (article 20 e) of the Act).

The employer is forbidden to oppose, in anyway, to the employee to exercise his rights (art.21.1 a) of the Act).

The decree-law 5/94 of 11 January states— in the sequence of the Directive 91/533/EC — the obligation of the employer to inform the employee about the applicable conditions on the labour agreement or on the working relationship. The obligation to inform is established in article 3, disposing article 2 that the employer shall inform the employee about "other rights and duties within the labour agreement". The information shall be provided in written and signed by the employer (article 4).

6.1.13 Finland

On 1 October 2001, the Finns introduced an act on the protection of privacy in working life, which will supplement their Personal Data Act. The Act applies to both, the public and private sectors, and includes job applicants.

Section 9 of the Act deals specifically with surveillance of workers. The aim of the law is not to create rights or obligations related to technical surveillance or the use of information networks, but to encourage the establishment of policies dealing with it within the workplace.

The law emphasises that the employer must not endanger the secrecy of private e-mails by his actions. Any data collected through surveillance must be necessary from the viewpoint of the employment relationship. The Act also places an obligation on employers to consult with their employees before implementing policies relating to e-mail surveillance.

After the employer has engaged in this consultation he is obliged to define the purpose of the surveillance, the methods used and the principles pertaining to the use of e-mail and information networks.

With regard to collective bargaining, the Finnish Co-operation Act gives a right of consultation to employees and places a duty on the employer to inform employees when deciding on any forms of surveillance.

6.1.14 Sweden

Under Chapter 2, Section 6 of the Swedish Constitution citizens are protected from the examination of mail and covert recording of confidential communications (this right however is capable of being limited by legislative enactment).

Further, Article 9 and 10 of their Personal Data Act provides that the monitoring of workers e-mail and use of the Internet should only be performed for specific purposes of which the workers are informed. Also Article 11 Lag (1976:580) om medbestammande i arbetslivet stipulates that trade union organisations must be consulted prior to introducing any form of employee surveillance.

6.1.15 The UK

The **Regulation of Investigatory Powers Act 2000** became law in Britain in October 2000 and made it unlawful for employers and others to intercept employee telephone calls and e-mails without the consent of both the senders and the recipients of the correspondence.

However, pursuant to section 4 (2) of the Act, the **Telecommunications** (**Lawful Business Practice**) (**Interception of Communication**) **Regulations 2000** were introduced which authorised employers to undertake such interception *without consent* monitoring and recording communications in order to;

- 1 Establish the existence of facts relevant to the business
- 2 Ascertain compliance with relevant regulatory or self-regulatory practices and procedures

- 3 Ascertain the standards achieved by employees
- 4 Prevent or detect crime
- 5 Investigate or detect unauthorised use of the telecommunications system
- 6 Ensure the system's security and effective operation

The exceptions to the consent requirement are wide. The employer must however make all reasonable efforts to inform every person who may use the system that communications transmitted by means thereof may be intercepted (section 3.2).

Employers undertaking monitoring that, as will generally be the case, involves the processing of personal data are still required to comply with the Data Protection Act 1998. The Information Commissioner has issued a draft code of practice for consultation. This sets out how the requirements of the Act apply in practice to monitoring in the workplace.