ROGER BLANPAIN

Use and monitoring of e-mail, intranet and inter facilities at work

An analysis under Belgian Law

Introductory remarks

The digital society offers unimaginable possibilities in terms of on-line communication. Yesterday the building-blocks of this horizonless world were the telephone, teletext, fax and video. Today we are conquering the universe with e-mail, the internet and company intranets, and mobile phones. The opportunities are enormous. This is just the beginning.

It goes without saying that clearly agreed arrangements on the use of digital means of communication at work and on the monitoring of that use are necessary in order to avoid any misunderstanding and establish the rights and obligations of those concerned as plainly as possible. The right balance has to be found between the company's interests on the one hand and the employees' interests on the other.

The establishment of these rules needs to start out from clear basic principles. A determining factor here is the legal characterization of the employer/employee relationship, and more specifically labour law.

§1. LABOUR LAW IN GENERAL: THE EMPLOYER/EMPLOYEE RELATIONSHIP

I. Rights and obligations of the employer and the employee

A. Employee

In the case of the employee, the starting principles include the following:

• during the performance of the contract of employment the employee must observe decency and moral conduct (Article 16, 1978 Contracts of Employment Act);

• the contract of employment must be performed in good faith; in other words, tools and equipment supplied by the company, such as digital communications facilities, must be applied and used to promote the company's objective, and the employee is under an obligation "to perform his work carefully, honestly and conscientiously, at the time and place and in the manner agreed";[1]

• the employee also performs his work subject to the employer's authority (direction and supervision).[2] He is under an obligation "to act in accordance with the orders and instructions given to him by the employer or the employer's agents or appointed representatives for the purposes of the performance of the contract of employment";[3]

• both during the contract of employment and after it has ended, the employee is under an obligation "to refrain from:

a) divulging any trade secrets, business secrets or secrets connected with personal or confidential matters that he comes to know in the course of performing his work;
b) engaging or collaborating in acts that constitute disloyal competition";[4]

• the employee is under an obligation "to return in good condition to the employer all tools and equipment entrusted to him and any unused materials".[5]

• avoidance of sexual harassment: "sexual harassment means any form of verbal, non-verbal or bodily conduct of a sexual nature whose perpetrator knows or ought to know that it violates the dignity of men and women at work";[6]

• violence and bullying at work are likewise prohibited. These concepts are defined as follows in the Act of 11 June 2002 on protection against violence, bullying and sexual harassment at work...[7]

(1) "violence at work: any act of violence whereby an employee or other person ... is mentally or physically harassed, threatened or attacked in the course of performing their work";

(2) "bullying at work: any unlawful and persistent conduct, outside or within the company or establishment, which may express itself especially in

[1] Article 17(1) of the Contracts of Employment Act of 3 July 1978.
[2] Articles 2 and 3 of the Contracts of Employment Act of 3 July 1978.
[3] Article 17(2) of the Contracts of Employment Act of 3 July 1978.
[4] Article 17(3) of the Contracts of Employment Act of 3 July 1978.
[5] Article 17(5) of the Contracts of Employment Act of 3 July 1978.
[6] Article 1 of the Royal Decree of 18 September 1992 on employee protection against sexual harassment at work (*B.S.* 7 November 1992).
[7] *B.S.* 29 June 2002.

forms of behaviour, words, threats, actions, gestures and biased written statements and is aimed at or has the effect of damaging the personality, dignity or physical or mental integrity of an employee or other person ... or the performance of their work, jeopardizing their employment or creating a threatening, hostile, insulting, humiliating or upsetting atmosphere";

(3) "sexual harassment at work: any form of verbal, non-verbal or bodily conduct of a sexual nature whose perpetrator knows or ought to know that it violates the dignity of men and women at work".

B. Employer

In the case of the *employer* the starting principles include the following:

• the employer is under an obligation "to provide such assistance, tools and equipment and materials as are necessary for the performance of the agreed work".[8]

This means that it is the employer who decides what digital equipment and communications facilities are provided for employees and the manner in which these may be used. An employer may, of course, also decide that an employee is not to be granted access to on-line communications facilities. However, this is not a discretionary right. It is clear that an employee has the right to use the company's digital facilities where this is normally necessary for the purposes of carrying out his duties. It is also self-evident that a decision on the part of the employer unilaterally to modify access to particular digital communications facilities may constitute a unilateral variation of the terms and conditions of employment, which could lead to unilateral breach of the contract of employment on the part of the employer;[9]

• the employer has the right to direct the employee's performance and exercise managerial authority, i.e. to issue instructions and supervise the work.[10] It follows from this provision, again, that the employer can determine the details of the use of digital means of communication and monitor that use;

• it is also up to the employer to ensure the continuity of the service supplied by the company. This means, *inter alia*, that it has to be possible to access certain data that an employee or other worker has received via e-mail or stored,

[8] Article 20(1) of the Contracts of Employment Act of 3 July 1978.

[9] Article 1134, Belgian Civil Code ("All agreements that are entered into lawfully are binding, in accordance with the law, on those who have entered into them") applies to contracts of employment. This stipulation means that, unless it has been agreed otherwise, an employer may not unilaterally vary or retract the contractual terms and conditions. The power relationship that is exclusive to the contract of employment does not constitute grounds for doing so (Belgian Supreme Court 23 June 1997, *J.T.T.* 1997, 333).

[10] Articles 2 and 3 of the Contracts of Employment Act of 3 July 1978.

in the event that the employee or other worker concerned is ill, on holiday or otherwise unavailable or has unlawfully withheld the data in question;

• as a general rule, the company is the owner of the tools and equipment made available to employees and other workers by the employer; the company is also liable for any damage caused to third parties in the course of its use;[11]

• the employer is responsible for any damage which an employee causes to third parties in the performance of his contract of employment. This is because the employee is an appointed agent of the employer or company.[12] In other words, the employer is responsible for employees' e-mail and intranet and internet use. Furthermore, the prevailing rule is that "in the event of damage or injury caused to the employer or a third party by an employee in the performance of his contract of employment, he shall be liable only if he is guilty of deliberate deception or gross negligence or has committed a serious offence. In cases of a lesser offence he shall be held liable only if that offence is of a repeated rather than an incidental nature";[13]

• the employer is likewise responsible for the prevention of bullying, violence and sexual harassment at work;[14]

• the employer is also responsible for the confidentiality of data entrusted to him by customers, as in the case of banks;

• responsibility for the company's image, which could be tarnished by racist, vulgar or similar messages, also rests with the employer;

• as mentioned earlier, the company needs to protect itself against hackers, spammers, viruses, theft of data (as in the case of industrial espionage), terrorist attacks, etc.;

• the legislation on copyright has to be observed when documents are downloaded;

• the company also has to keep a watch out for the smooth operation of its communications system. It is for example, a fact that excessive personal use not only costs time and money but can also result in a slowing-down of the company's system. Enormous savings can be achieved by regulating the matter appropriately.[15]

---

[11] Article 1384, Belgian Civil Code, first paragraph ("A person shall be liable not only for damage caused by acts of their own but also for damage caused by the acts of individuals in respect of whom that person must be held answerable or matters in the charge of that person.").

[12] Article 1384, Belgian Civil Code, third paragraph.

[13] Article 18, first and second paragraphs, of the Contracts of Employment Act of 3 July 1978.

[14] Act of 11 June 2002 on protection against violence, bullying or sexual harassment at work.

[15] A survey of Nordic companies by Computer Associates revealed that only 40% of corporate bandwidth was being used for work-related activities (Douglas Hayward, "Balancing the risk against the risqué", *Financial Times*, 2 October 2002).

II. Rights and obligations of employee representatives

In the case of *employee representatives*, the starting principles that apply are as follows:

• we live in an industrial-relations culture of information and consultation. This is expressly regulated in some cases, one example being in connection with the planning and introduction of new technologies.[16] There is direct employee involvement regarding every issue of relevance to the well-being of employees in carrying out their work for which their direct participation has been stipulated;[17]

• "the trade union delegation shall be permitted to issue all such oral and written communications as are useful to the workforce, provided this does not disrupt the organization of work";[18]

• in National Collective Agreement No 5 the employees recognize "the necessity of legal managerial authority being vested in the heads of companies and undertake as a point of honour to carry out their work dutifully";[19]

• consultation of the works council in connection with the organization of work;[20]

• the works council must be consulted when new technologies are being introduced;[21]

• "defining the forms of serious misconduct that constitute just cause for dismissal without notice,[22] disciplinary penalties, the amount and use of fines and the shortcomings for which they are imposed";[23]

• stipulation in the Decree on VDUs: "no use may be made of any quantitative or qualitative monitoring mechanism without the knowledge of the employees concerned";[24]

---

[16] Royal Decree of 3 May 1999 on the responsibilities and functioning of workplace health and safety committees (*B.S.* 10 July 1999), as amended by Royal Decree of 10 August 2001 (*B.S.* 22 September 2001).

[17] *Ibid.*, Article 31bis.

[18] Article 23 of National Collective Agreement No 5 of 24 May 1971 on the status of the workplace trade union delegation (*B.S.* 1 July 1971).

[19] *Ibid.*, Article 2, first paragraph.

[20] Article 15a) of the Act of 20 September 1948 on the organization of business (*B.S.* 27/28 September 1948), as amended on numerous occasions, and Article 10 of National Collective Agreement No 9 of 9 March 1972 regulating national agreements concluded within the National Labour Council and collective agreements on works councils (*B.S.* 25 November 1972).

[21] National Collective Agreement No 39 of 13 December 1983 on information and consultation regarding the consequences for employees of the introduction of new technologies (*B.S.* 8 February 1984).

[22] Article 6(4) of the Works Rules Act of 6 April 1965.

[23] Article 6(6) of the Works Rules Act of 6 April 1965.

[24] Chapter 3, "The man/computer interface". Annex to the Royal Decree of 27 August 1993 on working with VDUs.

• well-being at work: the workplace health and safety committee also has a contribution to make via the information and consultation procedure;[25]

• Article 7 of National Collective Agreement No 81 of 26 April 2002 on the protection of employees' personal privacy with respect to the monitoring of electronic on-line communications data[26] provides as follows: "an employer intending to install a system for monitoring electronic on-line communications data shall inform the works council of all aspects of that monitoring, as specified in Article 9, §1 of this agreement, in accordance with the provisions of National Collective Agreement No 9 of 9 March 1972 regulating national agreements concluded within the National Labour Council and collective agreements on works councils. In cases where there is no works council this information shall be given to the workplace health and safety committee or, in the absence of such a committee, to the workplace trade union delegation or, if no such delegation exists, to the employees themselves".

The specific question that arises is whether employee representatives themselves have the right to use intranet, internet and e-mail facilities for communications to and from employees? Are they able to demand a special Web site for the works council for the purposes of circulating the agenda and minutes of works council meetings? Are works council members entitled to contact each other, work out stances in preparation for meetings and maintain contact with their rank-and-file members and the unions to which they belong via e-mail or the company interanet?

It is clear that these points are not as yet regulated by law and are established at company level by the parties concerned, i.e. the employer and employee representatives.

Summing up

Without a shadow of doubt, the use of electronic on-line communications both offers opportunities and presents challenges for all the parties concerned (the company, its employees and their representatives). All this calls for clear agreement between employer and employees at company level.

It is clear that, subject to observance of the duty to inform and consult, the employer has the right to regulate the use of on-line communications and to monitor that use. This follows from the rights and obligations of employer and employee described above.

[25] Article 31bis of the Royal Decree of 3 May 1999 on the responsibilities and functioning of workplace health and safety committees.

[26] Pronounced generally binding by Royal Decree of 12 June 2002 (*B.S.* 29 June 2002).

The employer, it has been established, is the owner of the digital equipment concerned and as such bears full responsibility for it. The employee is under an obligation to obey the employer's orders and instructions and to perform his work carefully, honestly and conscientiously.

This is the legal basis for the employer's right to carry out monitoring both of the content of messages and of internet use, certainly in cases where that use takes place for work-related purposes.

§ 2. THE ROLE OF THE NATIONAL LABOUR COUNCIL: NATIONAL COLLECTIVE AGREEMENTS[27]

I. CCTV surveillance in the workplace: National Collective Agreement No 68[28]

National Collective Agreement No 68 of 16 June 1998 concerns the protection of employees' personal privacy with respect to CCTV surveillance in the workplace. CCTV surveillance is defined as meaning: "any surveillance system incorporating one or more cameras which is used to keep a watch on certain places or activities in the workplace from a point that is geographically at a distance from those places or activities, with or without a view to storing the visual data that it collects and transmits".

CCTV surveillance is permitted only for the purposes of:

- health and safety;
- protecting the company's property;
- monitoring the production process;
- monitoring the employee's work.[29]

The employer must explain the purpose of CCTV surveillance clearly and explicitly.

Information on the matter must be given in advance to the works council and, where there is no works council, to the health and safety committee, to the workplace trade union delegation or, where none exists, to the employees themselves. The required information covers:

---

[27] Those agreements, when rendered generally binding by a Royal decree apply to the private sector as a whole and to all employers and employees. They are sanctioned.

[28] P. HUMBLET, "Labour Court disallows video evidence of employee theft", *De Juristenkrant*, 12 February 2003, 1, 13, discussing a Supreme Court judgment of 27 February 2001 which rules a concealed camera to combat theft to be admissible and an Antwerp Labour Court judgment of 6 January 2003 which rejects this on the basis of National Collective Agreement No 68. HUMBLET also takes the line that the use of cameras should be regulated not by collective agreement but by law, which would then also apply to the public sector.

[29] This is not intended to mean filming the employee permanently. The monitoring in question may only be temporary.

- the purpose of such surveillance;
- whether or not the visual data will be stored;
- the number and siting of the camera(s);
- the period or periods for which the camera(s) will operate.

If implications for employees' privacy seem likely the works council, or where appropriate the relevant health and safety committee, must be consulted.

II. Monitoring of on-line communications: National Collective Agreement No 81

In Belgium, National Collective Agreement No 81 of 26 April 2002 on the protection of employees' personal privacy with respect to the monitoring of electronic on-line communications data, concluded within the National Labour Council and pronounced generally applicable by Royal Decree of 12 June 2002,[30] is the only instrument which deals specifically with access to and use of on-line communications facilities at work and the monitoring of such use.

However, this agreement regulates only one aspect of the problem, namely *safeguarding the employee's right to the protection of privacy in cases where at his workplace electronic communications data are collected for the purpose of monitoring and processing to make it possible to attribute such data to an individually identifiable employee*. In such cases it involves both work-related and private use by the employee.

As concerns National Collective Agreement No 81 specifically, it must be repeated that it applies only to the private sector, and hence not to the public sector. This clearly leaves a loophole.

Next, it cannot be emphasized too strongly that, as stipulated in Article 51 of the Collective Agreements and Joint Agreements Act of 5 December 1968, a collective agreement – even when it has been decreed generally applicable – cannot derogate from legislative provisions that constitute matters of public policy or mandatory law. That means, in this particular case, that when National Collective Agreement No 81 starts out from the assumption that, say, the Telecom Act and Article 314bis of the Criminal Code are applicable, the agreement itself cannot derogate from them, and this is also the case with respect to employees' work-related use of on-line communications facilities.

Unless, that is, we assume that the social partners who signed the agreement implicitly accept that the 1978 Contracts of Employment Act can be regarded as a law which permits derogation from the Telecom Act and from Article 314bis of the Criminal Code. In point of fact, the statement made in the agreement, after it has been established that the Telecom Act is and remains applicable, reads as follows: "Lastly, the principles laid down in Articles 16,17

[30] *B.S.* 26 September 2002.

and 18 of the Contracts of Employment Act of 3 July 1978 continue to apply as the pre-eminent expression of employer and employee obligations in the context of the employment relationship. The agreement must, of course, be interpreted in accordance with these fundamental rules".

As an agreement that has been decreed generally applicable, National Collective Agreement No 81 is legally enforceable, on pain of criminal sanctions. We have to ask ourselves whether it is really appropriate that all national collective agreements decreed generally applicable should automatically be enforceable under criminal law in this way? Actually, a great many of the provisions laid down in these agreements, and No 81 is just one such example, are extremely vague or even ambiguous, something which should prompt a certain degree of caution in the application of criminal law. Clearly, a distinction should be made here according to the (mandatory) nature of the obligations laid down in an agreement.

To conclude, in response to the criticism that no *travaux préparatoires* are available for national collective agreements which could clarify their interpretation certain such agreements have for some considerable time now contained commentaries on their Articles and some have included a preliminary statement. This raises the question of the legal force of commentaries and statements. The Belgian Supreme Court has ruled that "a commentary given by the National Labour Council that has not been incorporated into the actual text of a national collective agreement as pronounced generally applicable by Royal Decree cannot alter the scope and meaning of the agreement".[31]

The Court also stated that: "the courts interpret a national collective agreement at their absolute discretion, taking into account the shared intentions of its signatories".[32] Besides, we must not lose sight of the fact that provisions which carry a criminal sanction have to be given a restrictive interpretation.

III. Analysis of National Collective Agreement No 81

A. Scope

The objective of National Collective Agreement No 81 is to safeguard the fundamental right of employees to have their personal privacy respected in the employment context by specifying, while at the same time taking account of what is required for the company's efficient operation, the purposes for which a system for monitoring electronic on-line communications data may be installed, the conditions of proportionality and transparency with which it must comply and the rules governing the permissibility of individualizing such data.

---

[31] Supreme Court of Justice 14 April 1980, *R.W.* 1980–81, 113.

[32] Supreme Court of Justice 11 March 2002, R. BLANPAIN, *Wetboek Arbeidsrecht [Code of Labour Law]*, E. Story-Scientia, Ghent *s.d.*, 2.II.B.1–7.

The agreement is without prejudice to more favourable provisions at sectoral Joint Committee or company level (Article 1, §1).

It does not relate to rules on access to and/or use of a company's electronic on-line communications facilities, which are the prerogative of the employer. It therefore leaves intact any applicable company rules and practices on information and even consultation in this field.

It is also without prejudice to existing company rules and practices regarding trade union activities (Article 1, §2).

B. Definition

For the purposes of applying the agreement, "electronic on-line communications data" means electronic on-line communications data *sine loco*, irrespective of the carrier medium via which something is transmitted or received by an employee in the context of employment (Article 2).

C. Commitments undertaken

The signatories to the agreement, i.e. the recognized social partners, affirm the following principles:

– the employee side acknowledges the principle whereby the employer has the right to exercise control over tools and equipment and their use by employees in the context of the performance of their contractual obligations including, subject to the rules on applicability laid down in this agreement, circumstances where such use falls within the sphere of the employee's private life;

– the employer side respects the right of employees to the protection of their personal privacy in the employment context and the rights and obligations that result therefrom for each party (Article 3).

D. Rules on the monitoring of electronic on-line communications data

1. General provisions

Monitoring of electronic on-line communications data is permitted only in so far as it fulfils the principles of legitimate purpose and proportionality and also the principle of transparency, as ensured by the procedural conditions (Article 4).

2. Principles

a. Legitimate-purpose principle: objective of monitoring

The objective of monitoring is, obviously, the proper functioning of the company.[33] This is usually included in the codes of practice that companies have drawn up on the subject of use and monitoring.

National Collective Agreement No 81 goes along with this and states that monitoring is permitted for the purposes of keeping a check on "faithful observance of the policy and rules in force within the company on the use of on-line technologies" [Article 5, §1(4)].

Apart from this the agreement also permits monitoring for one or more of the following objectives, which in fact largely overlap with what is stated on the subject in the company codes of practice quoted in Part I of this book, more particularly:

"1) the prevention of unlawful or defamatory acts, acts that are contrary to good moral conduct or may violate another person's dignity;[34]

2) protection of such of the company's economic, commercial and financial interests as are confidential and also the discouragement of practices that conflict with them;

3) the security and/or efficient technical operation of the company's IT network systems, including associated cost control and also physical protection of the company's equipment"[35] [Article 5, §1,(1–3)].

---

[33] In the case of covert surveillance of electronic on-line communications data the provisions of the Criminal Code are applicable, and this form of surveillance can be introduced only in accordance with the rules laid down in the Code of Criminal Procedure (commentary on Article 5 of National Collective Agreement No 81).

[34] The commentary on the matter accompanying National Collective Agreement No 81 reads as follows: "Unlawful or defamatory acts, acts that are contrary to good moral conduct or may violate another person's dignity as referred to in §1(1) of this Article can consist in particular in computer hacking such as unlawfully gaining access to electronic on-line communications data relating to personnel management or confidential medical files, or in consulting pornographic or paedophile sites and sites which give incitement to discrimination, racial segregation, hatred or violence towards a group, community or the members thereof on the grounds of the race, colour, origin, religion or national or ethnic descent of those members or of some of them".

[35] The commentary on the matter accompanying National Collective Agreement No 81 reads as follows: "Practices that conflict with the company's economic, commercial and financial interests as referred to in §1(2) of this Article can take the form of, in particular, harmful advertising as defined in Article 23(6) of the Trade Practices and Consumer Information and Protection Act of 14 July 1991, the dissemination of files and the divulgement of business/trade secrets, including research and development, production processes and all potentially confidential data".

In addition, the commentary accompanying the agreement states that the possibility of monitoring electronic on-line communications data for *training purposes* remains unaffected, since it does not constitute surveillance.

In other words, contrary to what is stated in the first sentence of Article 5, §1 of the agreement this Article does not give a restrictive list of objectives but a very broad form of wording for them that permits the company to carry out necessary types of monitoring.

Article 5, §2 states that the employer must define the objective(s) of monitoring clearly and explicitly. In other words, the objectives must be explicitly included in the company code of practice.

b. Proportionality

The rule is clear: as much monitoring as is necessary, but no more. Article 22 of the Constitution is in fact applicable to the employment relationship and this principle may be departed from only where it is (legally) necessary, and only to that extent. National Collective Agreement No 81 rightly states, in its Article 6 under the heading "Proportionality principle", that the monitoring of electronic on-line communications data may not as a general principle entail any intrusion on the employee's personal privacy.

Where monitoring nonetheless entails an intrusion on the employee's personal privacy, this intrusion must be kept to a minimum.[36]

[36] The commentary on the matter accompanying the agreement states: "The principles embodied in this Article signify that the only electronic on-line communications data to be collected, and more specifically in this connection to be processed for the purposes of monitoring, are such data as are necessary for monitoring, i.e. those data which, given the justified objective of the monitoring concerned, entail the least possible intrusion on the employee's personal privacy. Application of this Article relates more particularly to the collection of generalized data by the company. Procedures for the processing or individualization of such data are not dealt with here but are regulated below in Part II of this agreement. In practice the present provisions cover, for example:

- as concerns the monitoring of internet sites, the collection of data on the connection time for each workstation but not individualization of the sites visited, which is regulated in Part II;
- as concerns the monitoring of electronic mail use, the collection of data on the number of outgoing messages for each workstation and their volume but not identification of the employee who sends them, which is regulated in Part II".

c. Informing employees – transparency

1) Advance information

a) There is a works council

An employer intending to install a system for monitoring electronic on-line communications data must inform the works council of all aspects of that monitoring (Article 7, §1), and more particularly:

"– the policy on monitoring and prerogatives of the employer and the supervisory staff;
– the objective(s) pursued;
– whether or not personal data are stored, and where and for how long they are stored;
– whether or not monitoring is to be permanent" (Article 9, §1).

b) No works council exists

In cases where there is no works council this information must be given to the workplace health and safety committee or, in the absence of such a committee, to the workplace trade union delegation or, if no such delegation exists, to the employees themselves (Article 9, §2).

2) Information when the monitoring system is being installed

a) Nature of the information[37]

When a system for monitoring electronic on-line communications data is being installed, the employer must inform the employees concerned of all aspects of that monitoring:

"– the policy on monitoring and prerogatives of the employer and the supervisory staff;
– the objective(s) pursued;
– whether or not personal data are stored, and where and for how long they are stored;
–whether or not monitoring is to be permanent" (Article 9, §1).

[37] "The purpose of the information procedure referred to in this Article is to increase transparency regarding the monitoring of electronic on-line communications data and to facilitate a dialogue between the employer and those he employs, at individual level, so that surveillance can be set up in a climate of trust" (commentary accompanying Article 9 of National Collective Agreement No 81).

The information must also cover:

- the use of equipment made available to the employee for the purposes of performing his work, including restrictions on use in the context of the particular post occupied;
- the rights, duties and obligations of employees with respect to use of the company's electronic on-line communications facilities, and any bans imposed;
- the disciplinary penalties specified in the company's works rules for failure to observe the rules on use (Article 9, §2).

b) Quality of the information

The information must be effective, comprehensible and kept up to date. The choice of method for conveying the information is for the employer to decide (Article 8, §2).[38]

c) Good faith

This information procedure does not release the parties from the obligation to perform contracts and agreements in good faith (Article 8, §3).

d) Consultation

In addition, monitoring systems that have been installed must be evaluated at regular intervals either, depending on the circumstances, within the works council or the health and safety committee or in consultation with the workplace trade union delegation, with a view to suggestions for adapting them to technological developments (Article 10 of National Collective Agreement No 81).

[38] "The information referred to in §2 of this Article can be provided, for example:
- as part of general instructions (circulars, displayed notices, etc.);
- by mentioning it in the staff handbook of works rules;
- by mentioning it in the individual contract of employment;
- through instructions given each time equipment is used (messages on the screen when the workstation is turned on and/or particular programs are activated).

Naturally, the relevant regulatory provisions stipulating the mandatory content of a company's work rules, such as information on disciplinary penalties, continue to apply in the case of §2 of this Article" (commentary accompanying Article 8 of National Collective Agreement No 81).

e) Individualization of on-line communications data

Part II of Chapter IV of National Collective Agreement No 81 lays down rules on the individualization of electronic on-line communications data.

1) Definition

For the purposes of the agreement, the "individualization" of electronic on-line communications data means an action whose purpose is to process data of this kind collected during monitoring installed by the employer so as to make it possible to attribute such data to an identified or identifiable person (Article 12, §1).

Depending on the objective of the monitoring system installed by the employer, the individualization of electronic on-line communications data takes place:

– as a direct procedure, in accordance with Article 15;
– as an indirect procedure, in accordance with Articles 16 and 17.

An indirect procedure is one that is combined with a prior notification phase (Article 12, §2).

2) Principles

The principles relating to monitoring are repeated here again.

a) Legitimate-purpose principle

Article 13 stipulates that in individualizing electronic on-line communications data the employer must act in good faith and in accordance with the objective(s) of the monitoring concerned (§1).

If the electronic on-line communications data collected are processed for purposes other than that for which the monitoring system was installed, the employer must ensure that everything which is done is compatible with the original objective and take all necessary steps to avoid any forms of misinterpretation (§2).

b) Proportionality principle

The employer may not individualize electronic on-line communications data collected during monitoring in a manner that is incompatible with the objective(s) specified in Article 5, §1[39] (Article 14, §1).

Electronic on-line communications data necessary for the purposes of the objective(s) pursued may be individualized. Such data must be, in the light of the objective(s) concerned, adequate, relevant and not excessive (Article 14, §2).

c) Procedural conditions[40]

1) Direct individualization

Direct individualization of electronic on-line communications data is permitted in cases where monitoring is aimed at one or more of the objectives specified in Article 5, §1(1–3)[41] (Article 15).

The purpose of this Article is to offer an employer who in pursuing the objectives listed here detects an irregularity the opportunity of proceeding directly, in the light of the general data available to him, to the individualization

[39] "1. The prevention of unlawful or defamatory acts, acts that are contrary to good moral conduct or may violate another person's dignity.

2. Protection of such of the company's economic, commercial and financial interests as are confidential and also the discouragement of practices that conflict with them (harmful advertising, dissemination of confidential information, divulgement of business/trade secrets, ...).

3. The security and/or efficient technical operation of the company's IT network systems, including associated cost control and also physical protection of the company's equipment (overloading/slowing- down of the system, spread of viruses, ...).

4. Faithful observance of the policy set out in this document in connection with the use of on-line technologies."

[40] "The enforcement of these rules may not create a situation in which the guarantees provided for employers and employees by this agreement are rendered ineffective through the categorization of all electronic on-line communications data as being exclusively of either a work-related or a private nature.

This Part II of the agreement is not applicable to the subject and content of electronic on-line communications data for which no indication has been given by the employee that they are not of a work-related nature" (Article 11 of National Collective Agreement No 81).

[41] "1. The prevention of unlawful or defamatory acts, acts that are contrary to good moral conduct or may violate another person's dignity.

2. Protection of such of the company's economic, commercial and financial interests as are confidential and also the discouragement of practices that conflict with them (harmful advertising, dissemination of confidential information, divulgement of business/trade secrets, ...).

3. The security and/or efficient technical operation of the company's IT network systems, including associated cost control and also physical protection of the company's equipment (overloading/slowing- down of the system, spread of viruses, ...)."

of electronic on-line communications data in order to be able to trace the identity of the person or persons responsible.

In practice, potential irregularities may be detected in the course of routine consultation of the electronic on-line communications data collected within the company (statistical data, for example) or by making use of any other source of information (commentary accompanying Article 15).

2) Indirect individualization

a) Notification phase

In cases where the objective of monitoring is that specified in Article 5, §1(4),[42] the individualization of electronic on-line communications data is permitted only if the requirement for a prior notification phase is fulfilled (Article 16, §1).

The purpose of the notification referred to in §1 is to inform the employee(s) clearly and comprehensibly that an irregularity exists and that electronic on-line communications data will be individualized if any recurrence of a similar irregularity is detected (§2).

The notification referred to in §2 of this Article must consist in a reminder or more detailed explanation of the principles and rules laid down in the company, so that any future irregularity of the same nature is prevented (commentary accompanying Article 16).

b) Interview[43]

An employee who as a result of the indirect individualization procedure referred to in Article 16 is held responsible for an irregularity in the use of electronic on-line communications facilities must be invited by the employer to an interview to discuss the matter (Article 17, §1).

This interview takes place prior to any decision or assessment that can affect the employee individually.

The purpose of the interview is to give the employee the opportunity to voice any objections to the proposed decision or assessment and to justify his use of the electronic on-line communications facilities provided.

---

[42] "4. Faithful observance of the policy set out in this document in connection with the use of on-line technologies."

[43] "The purpose of this Article is to make it possible, in an interview which the employee is invited to attend by the employer, to forestall any possible misunderstandings and to ensure that trust is restored between the employer and employee.

In practice the interview takes place when the employee who is responsible for an irregularity is identified, and therefore goes hand in hand with the individualization of data" (commentary accompanying Article 17).

This procedure does not apply during suspension of performance of the contract of employment, for whatever reason (Article 17, §2) (annual holiday, illness, ...), "to avoid making it even more difficult to observe the period of grace of three working days allowed for evoking just cause for summary dismissal".[44]

f) Assistance

The agreement is without prejudice to the application of National Collective Agreement No 5 of 24 May 1971 on the status of workplace trade union delegations and more specifically here its Article 13[45] (commentary accompanying Article 17).

g) Final provisions

National Collective Agreement No 81 has been concluded for an unspecified period. It can be revised or terminated at the request of any of the signatory parties, subject to observance of a notice period of six months.

The organization taking the initiative for revising or terminating the agreement must state the reasons for doing so and put forward proposals for its amendment. The other organizations undertake to discuss these within the National Labour Council within one month of their receipt (Article 18).

[44] VBO, *op. cit.*, p.7.

[45] "Any individual complaint should be submitted through the usual line-management channels by the employee concerned, who at his request is assisted by his trade union delegate. The trade union delegation shall have the right to be heard in connection with any individual grievance or dispute that has proved impossible to resolve through these channels."

IV. Critical assessment of National Collective Agreement No 81[46]

A. Validity

1. Only in the case of work-related use by employees

A collective agreement regulates individual and/or collective relations between employer(s) and employees (Article 5 of the Collective Agreements Act of 5 December 1968). For the purposes of that Act "employee" means an individual who by virtue of a contract of employment or otherwise than by virtue of a contract of employment performs work subject to another person's authority (Article 2, §1 of the 1968 Act).

In other words, National Collective Agreement No 81 applies only to employees while they are working in performance of their contract of employment and are at the same time subject to an employer's authority. In short, when an employee is using the company's on-line facilities for private purposes he is not acting subject to authority.[47] Consequently, the agreement cannot be valid with respect to the employee's private activities. This means that the agreement is applicable only to the employee's work-related activities. To that extent, National Collective Agreement No 81 is wide of the mark. What is stated in the agreement regarding employees' private use of company's facilities has no legal substance.

Although employees' private use of company facilities certainly involves some kind of contractual relationship between employer and employee or non-contractual relationship (when private use takes place without permission), under no circumstances does it involve an employment relationship.

---

[46] As regards the constitutionality of National Collective Agreement No 81 and more particularly whether a collective agreement can regulate the right to privacy, see the question by Senator V. VAN QUICKENBORNE, No 2-788, *Hand.* Senate 23 May 2002. The Minister for Employment replied that the agreement does not regulate employees' right to privacy but merely specifies it in more detail and consequently, according to the Minister, a formal statute is not necessary. See also F. HENDRICKX, *op. cit.*, p.120 et seq. According to L. MONSEREZ the agreement is unconstitutional because in accordance with the case-law of the Court of Arbitration a formal statute is necessary in every case where the Constitution stipulates that a matter must be regulated "in" or "by law". If the Crown adopts a measure, it should be confirmed in law by the legislators within a reasonable time-limit. The agreement does more than merely specify the right to privacy in more detail: it actually defines the cases in which and the conditions under which an employee can invoke the secrecy of communications, as one of the facets of the right to respect for private life ("A legally valid collective agreement?", *De Juristenkrant*, 5 June 2002, 2).

[47] *Cf.* the case-law of the Belgian Supreme Court of Justice stating that "an employee is not deemed to be performing his contract of employment when, with his employer's permission, he is using a company car for private purposes (Belgian Supreme Court 7 May 1996, *R.W.* 1996–97, 657).

2. Other users

The agreement is equally invalid in the case of other users who do not perform their work subject to the employer's authority, such as self-employed persons who work for the company, consultants or any clients who may use the company's on-line communications facilities, and in their case with respect, what is more, to work-related use as well as private use. Here too, although contractual or non-contractual relationships exist between the parties, there are no relationships of subordination to the employer's authority and hence no employment relationships.

B. Contrary to mandatory law

The agreement starts out from the assumption that the Act of March 1991 on the reform of certain state enterprises continues to apply – and in particular its Article 109terD prohibiting third parties from examining or making use of data transferred by telecommunications, except with the consent of all the persons involved in the communications concerned.

A similar prohibition is also contained in Article 314bis of the Belgian Criminal Code.

These legislative provisions are of a mandatory nature, i.e. they constitute *jus cogens* which cannot be derogated from by agreement, not even in the form of a collective agreement that has been decreed generally applicable. This is made very plain by Article 51 of the Collective Agreements and Joint Committees Act of 5 December 1968, where collective agreements that have been decreed generally applicable are ranked in second place, after "mandatory legal provisions". If, in short, the social partners within the National Labour Council take the view that this legislation applies to the employment relationship, no examination or use of such data by third parties is lawful without the consent of all the persons involved in the communications concerned. Yet National Collective Agreement No 81 permits the employer, albeit subject to certain conditions, to examine employees' on-line communications without the consent of all the parties involved in the communications concerned. Logically, this is quite wrong.

Moreover, the agreement should also comply with labour law and the essential characteristics of the contract of employment, and more particularly the position of subordination to the employer's authority that allows control and supervision with respect to employees' use of on-line communications facilities as well.

The agreement also fails both to take adequate account of the employer's rights of ownership and/or disposal over company information facilities and to take account of the rules on liability, i.e. the fact that the employer is

vicariously liable for employees' digital activities even where he has no say in them.

In short, the assumption from which National Collective Agreement No 81 starts out is wrong. The employer is not a third party. In accordance with the employment relationship, the employee in this respect forms part of and is representing the company. Article 109ter D of the Act of 21 March 1991 and Article 314bis of the Belgian Criminal Code do not, therefore, apply to the employer/employee (employment) relationship, nor to communications-connected relations between a company and self-employed users.

Unless, that is – as stated earlier[48] – we assume that the social partners who signed the agreement implicitly accept that the 1978 Contracts of Employment Act can be regarded as a law which permits derogation from the Telecom Act and from Article 314bis of the Criminal Code.

In point of fact, if these legislative provisions (the Telecom Act and Article 314bis of the Belgian Criminal Code) were really applicable it would prevent a compny from functioning properly, and that cannot have been the intention. "*Impossibilium, nulla est obligatio*" (nobody can be held under an obligation to do what is impossible)!!

C. A clear conception of privacy

Obviously, Article 22 of the Constitution is important and the employee's privacy must be guaranteed as far as is possible, as must observance of the principles enshrined in the Act of 8 December 1992 on the protection of privacy with respect to the processing of personal data, namely the principles of legitimate purpose, proportionality and transparency.

All this means that covert monitoring of on-line communications is prohibited and that appropriate information and consultation of employees is the order of the day; that monitoring may be carried out only for reasons connected with the efficient progress of the company's affairs and proper performance of the contract of employment; and, lastly, that monitoring of on-line communications use may take place only to the extent that is necessary.

It is, however, a prerequisite for the efficient operation of the company and proper performance of the contract of employment that the employer must have the right to examine the content of an e-mail message even in situations where no misuse is suspected, but simply because knowing what the message contains is necessary for the efficient operation of the company. It is unthinkable that a company should be unable to access e-mail addressed to an absent employee because this requires the consent not only of the employee concerned but also of possibly dozens of correspondents.

[48] See paragraph 266 above.

To that extent, the privacy conditions established in National Collective Agreement No 81 are too restrictive and incompatible with the mandatory provisions of labour law and the rights of ownership.

D. Individualization: overlapping objectives

The agreement makes a distinction between direct individualization and indirect individualization (Article 5, §1). Direct individualization is permitted in the following cases:

"1. The prevention of unlawful or defamatory acts, acts that are contrary to good moral conduct or may violate another person's dignity.

2. Protection of such of the company's economic, commercial and financial interests as are confidential and also the discouragement of practices that conflict with them (harmful advertising, dissemination of confidential information, divulgement of business/trade secrets, ...).

3. The security and/or efficient technical operation of the company's IT network systems, including associated cost control and also physical protection of the company's equipment (overloading/slowing-down of the system, spread of viruses, ...)".

Indirect individualization, i.e. combined with a prior notification phase and an interview with the employee concerned, is permitted only in the following case:

"4. Faithful observance of the policy and rules in force within the company on the use of on-line technologies" (Article 5, §1).

However, when we read through the company codes of practice studied here[49] we find that the principles and rules on use and monitoring in force within the company are also aimed at the first three objectives. How, then, is it possible in practice to make a distinction between direct and indirect individualization? It makes no sense, since the objectives of the two procedures overlap.

In short, National Collective Agreement No 81 is flawed on a number of essential points. To reiterate – the 1991 Act (Telecom Act) and Article 314bis of the Belgian Criminal Code cannot be applicable to work-related use of company facilities. It must be possible, albeit subject to observance of the principles of legitimate purpose, proportionality and transparency, for the employer to monitor the content of the on-line messages and files of employees and other workers.

Those of the agreement's provisions that do not conflict with mandatory law, such as the provisions on informing and consulting employees and so forth, are of course legally valid.

[49] See Part I above.

The grant of access to the use of communications facilities at work, and more particularly e-mail, the internet and company intranets, falls within the province of the employer's prerogative. Monitoring by the company of the use made of communications by employees and other users is likewise a must, including the monitoring of the content of communications and, for example, the particular Web sites visited. The recording of telephone conversations can be justified as an element of proof of the existence of certain agreements.

All this follows clearly and unambiguously from the system of Belgian labour law. An employee performs work in a position of subordination to the authority of the employer, who exercises direction and supervision of the employee's work performance. That performance can, may and must where necessary be monitored.

In point of fact the provisions of labour law, or more specifically Articles 16 and 17 of the Contracts of Employment Act of 3 July 1978, constitute an implicit legal exception to the Telecom Act and to Article 314bis of the Belgian Criminal Code, which prohibit any examination of on-line communications. Furthermore the employer is the owner of the on-line communications facilities concerned, if not the holder of the right of disposal over them, a fact which entitles him to lay down rules on their use and to monitor the use actually made of them.

Obviously, none of this may take place arbitrarily. The rules on privacy apply, and in particular the principles of legitimate purpose, proportionality and transparency have to be complied with.

This means that the company's policy on access, use and monitoring should be clear and unambiguous; proper agreements should be reached on the matter; and information and consultation are the order of the day. All users have the right to be given access to, and request the rectification of, data stored concerning their use of communications.

Privacy is a fundamental right, enshrined in Article 22 of the Belgian Constitution, which is directly enforceable at work and with respect to the employment relationship just as it is elsewhere.

Departures from the "right to be left alone in peace", including the secrecy of communications, are possible only if they are justified, if they are proportionate to what is necessary – no more departures from the principle than are necessary – and if the policy on the matter has been made known beforehand.

This also applies at work. In other words, a company which intends to introduce a policy on access, use and monitoring with regard to the use made by its employees and other workers of the communications facilities it provides should draw up a policy which, after the requisite information and consultation procedures, is made available to them to read, and, preferably, to which they give their signed consent.

With a view to striking the right balance between the fundamental right to privacy on the one hand and safeguarding the efficient operation of the company on the other, National Collective Agreement No 81 on the protection of employees' personal privacy with respect to the monitoring of on-line electronic communications data was concluded within the National Labour Council on 26 April 2002 and subsequently pronounced generally applicable by Royal Decree.

This agreement is flawed on a number of points. To begin with, a collective agreement cannot regulate employee's private use of on-line communications. The fact is that a collective agreement can only give shape to the employment relationship between employer and employee, whereas when an employee is using on-line communications for private purposes there is no subordination to the employer's authority, no work performance and therefore no employment relationship.

For the legal characterization of private use we have to turn to ordinary law, to general legal principles and to what has been agreed between the parties. Private use involves a legal relationship between the owner of the communications facilities on the one hand and a user on the other in which mutual agreements apply, as is of course also the case for both work-related and private use of these communications facilities by non-employee users.

What is more, the agreement is not logically consistent. It starts out from an assumption of the applicability of the criminal-law ban on examining telecommunications without the consent of all the persons involved in the communications concerned (Telecom Act and Article 314bis of the Criminal Code) but then proceeds to derogate from these mandatory provisions through collective agreement, which is manifestly contrary to the hierarchy of sources of law as stipulated in Article 51 of the 1968 Collective Agreements and Joint Committees Act.

Unless, that is, we assume that the social partners who signed the agreement implicitly accept that the 1978 Contracts of Employment Act can be regarded as a law which allows an exception to the Telecom Act and to Article 314bis of the Criminal Code.

In short, the assumption from which National Collective Agreement No 81 starts out is wrong. The employer is not a third party in the employment relationship. Monitoring is a normal given, provided it meets the requirements of legitimate purpose, proportionality and transparency.

The National Labour Council should do its homework again and ask itself whether the development of rules on the use and monitoring of on-line communications by employees at work is not more a matter for the legislators, since it involves fundamental rights whose interpretation and implementation, and possible derogations from them, are best left to Parliament. All the more so since Article 22 of the Constitution stipulates that restrictions on privacy may be imposed only by law and that the conditions for such restrictions must also

be specified by law. Law here means a formal written statute. Such statutory restriction can, obviously, be either explicit or implicit. The National Labour Council's powers, of course, cover only the private sector and the public sector also needs an appropriate system of regulation.

It is now up to companies themselves, after information and consultation of employees and their representatives and possibly other users and always subject to compliance with the existing legislation,[50] such as that on disciplinary sanctions and a company's works rules, to develop a suitable code of practice that meets the requirements of their own particular situation. It goes without saying that for employers, employees and other users in a financial institution things are different from the situation in a construction firm, a hospital or a government department.

A code of practice needs to be all-encompassing: all aspects have to be covered; all the courses on the menu need to be catered for but each course undoubtedly has its own "taste and colour".

ROGER BLANPAIN

AZ E-MAIL, AZ INTRANET ÉS EGYÉB KOMMUNIKÁCIÓS ESZKÖZÖK HASZNÁLATA ÉS ELLENŐRZÉSE A MUNKAHELYEN

Elemzés a belga jog alapján

(Összefoglalás)

A tanulmány bemutatja a munkavállalók, a munkáltatók és a munkavállalók érdekképviseleti szerveinek jogait és kötelezettségeit az on-line kommunikáció ellenőrzésével összefüggésben. A szerző részletesen elemzi a 68. számú általános (országos) kollektív szerződést a munkavállalók magánéletének védelméről a munkahelyi CCTV megfigyelésre tekintettel és az on-line kommunikáció ellenőrzéséről szóló 81. számú általános (országos) kollektív szerződést.

[50] As also with the provisions of National Collective Agreement No 81, in so far as these are legally valid.

A munkáltató felelősséggel tartozik a tulajdonában lévő eszközök használatáért, következésképpen – meghatározott jogi feltételek között – jogosult szabályozni és ellenőrizni az elektronikus kommunikáció használatát. A CCTV megfigyelés megengedett, ha annak célja az egészséges és biztonságos munkavégzés, a vállalat tulajdona védelmének illetve a termelés és a munkavállalók munkája ellenőrzésének biztosítása.

Az elektronikus kommunikáció ellenőrzése jogszerű, ha érvényesülnek a törvényes cél, az arányosság és a transzparencia elvei, valamint megfelelő eljárási garanciák léteznek. Az ellenőrzés célja a vállalat megfelelő működésének fenntartásához kapcsolódhat, amelyet világosan és egyértelműen meg kell határozni. Az ellenőrzés a szükségesség követelményét nem sértheti. Az átláthatóság érdekében az ellenőrzésről előzetesen tájékoztatni kell a munkavállalót vagy a munkavállalók érdekképviseleti szerveit vagy a munkavállalók közösségét. Ezeket az elveket kell figyelembe venni a munka-vállaló azonosításakor is.

A 81. számú országos kollektív szerződés nem jelent teljes körű szabályozást. A hatálya csak azokra a munkavállalókra terjed ki, akik munkakörhöz kapcsolódóan használják a vállalaton belüli on-line lehetőségeket és a munkáltatói jogkör gyakorlójának illetékessége alá tartoznak.

Kritikaként fogalmazható meg, hogy a kollektív szerződés derogációra ad lehetőséget a Telekommunikációról szóló törvény és a Büntető Törvénykönyv tekintetében, ami ellentétes a jogforrási hierarchia elvével. Ezenkívül szabályai túl szigorúak és nem összeegyeztethetőek a munkajog és a tulajdonjog szabályaival.