Opinion of the Netherlands Trade Union Federation [Federatie Nederlandse Vakbeweging - FNV] on European Directive No 95/46/EC

1. INTRODUCTION

The Personal Data Protection Act [Wet bescherming persoonsgegevens - WBP] came into force on 1 September 2001, in implementation of Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

The FNV has always been satisfied with the WBP as such.

As pointed out in the FNV package of April 2000\(^1\) entitled "Meer respect voor grondrechten van werknemers" ["More respect for employees' basic rights], the FNV thinks the WBP is of major importance for the protection of privacy. It is pointed out that the significance of this framework law for labour relations can be fleshed out in a code of practice, which could be based on the ILO Code of Practice on the Protection of Workers’ Personal Data, for example.

Unfortunately, it did not prove possible to draw up a code of practice of this kind. The FNV has now published its own specimens at its website: http://www.fnv.nl/02werkgeld/arbo/wetgeving/privacy/ModelPrivacyreglement/model_privacyreglement1.htm.

The FNV models are intended as an aid for works councils when drawing up privacy rules for the business in question. The FNV mentioned "protection against unrestricted monitoring of e-mail and Internet traffic by employers, the use of detective bureaux to investigate the movements of workers, and the use by employers of evidence they have obtained by illicit means" as questions requiring further attention with the aid of the WBP.

The FNV did not directly call for specific provisions in the Civil Code [Burgerlijke Wetboek - BW] on protecting the privacy of employees. It was thought that the WBP would merge better with the system of labour law than the Data Protection Act (Wet op de persoonsregistraties - WPR):

a. The protection of privacy is now more a question of labour relations than it was in the days of the WPR, as can be seen from things such as the increase in the number of disputes and requests for information submitted to the Data Protection Board [College Bescherming Persoonsgegevens - CBP], the number of judgments published, and the attention this subject has received from the media and the works councils.

b. The parties in an labour dispute can now formulate the issues more tangibly and thereby "oblige", as it were, judges to make a concrete rulings.

c. A new and active player has appeared on the field: the works councils. Privacy protection is high on their list of favourite subjects.

d. The role of the Data Protection Authority [Registratiekamer] or the CBP has changed. These supervisory authorities have developed information material that is increasingly tailored to labour relations. Examples include: a checklist for works councils, rules on the

---

\(^1\) In an updated summary of the FNV note of March 1999 entitled "Onder geen beding" [On no account].
monitoring of employees’ e-mail and Internet use, a framework arrangement for e-mail and Internet use, general rules on camera surveillance and monitoring of telephone conversations.

e. The two sides of industry, VNO-NCW [the result of the amalgamation in 1995 of the Federation of Dutch Enterprises (VNO) and the Dutch Christian Federation of Employers (NCW)], members of the FNV, and the FNV itself have developed models that translate the WBP into a general framework law on labour relations. Judging from the response, the FNV specimens, which are published at the website, are being used by works councils, employers and lawyers.

Even though the WBP has only been in force for a short time, a number of shortcomings can already be detected:

1. Compared with those in France and Germany, judges in the Netherlands continue to be somewhat more reticent about recognising a right to privacy at the place of work. In comparable cases, the employer is protected in the Netherlands while the employee is protected in France and Germany.

2. Dutch judges, including those of the Supreme Court [Hoge Raad], hardly ever, if at all, make pronouncements as to whether privacy has been infringed in specific cases, even if it blatantly has been. They prefer merely to check against the familiar labour-law standards.

   This reproach does not apply only to the judges, but also to the lawyers in question, who fail to oblige the judges to make carefully reasoned rulings by presenting the facts and asking the right legal questions.

3. Dutch judges attach no consequences to infringements of privacy by employers if it comes to light as a result of the infringement that an employee had been misbehaving. Even if employers have committed punishable acts in such cases (in practice, usually computer crime) they are out of harm’s way. The other employees in the company whose privacy has been infringed will not take the matter to court. We have yet to see the first case of an employee bringing action against an employer for computer crime.

   In other countries, such as France, judges may not use evidence that has been illicitly obtained in cases of this kind.

---

2 In the United Kingdom protection of the privacy of employees amounts to even less than it does in the Netherlands and for some multinationals this even seems to be reason to relocate from France to the UK. This is remarkable because one of the very purposes of Directive 95/46/EC was to combat competition between Member States on the basis of differences in the extent of protection of personal data. In the periodical "Privacy & informatie“, Dr Paul de Hert of the Catholic University of Brabant has written (in an article entitled "Kenbaarheid van bedrijfscontrole op e-mail en internetgebruik: Factoren die spelen bij de chaos rond dit leerstuk" [Recognisability of monitoring by employers of use of e-mail and the Internet: factors affecting the chaos surrounding this doctrine]): “How far can employers go with the checks they would like to make in the light of employees’ basic rights? Admittedly European basic rights draw a few clear boundaries, but rarely do authors or judges take them as a basis for issuing satisfactory guidelines for legitimate restrictions of basic rights by employers. In each specific case many of them, in legal doctrine and case law, weigh the interests of the employers against the interests of the employees. (...) Not infrequently they use open labour-law notices (...). Referring to these open labour-law standards is not without risk. There is just the question of whether the values underlying Article 8 of the ECHR are served. In Dutch labour law, for example, Volume 7, Title 10 of the Civil Code, which deals with work contracts, contains no provisions on the privacy of employees at the place of work, but does provide for a general investigation right for the employer. Thus the open standards are not impartial.”

3 In the February 2002 issue of the periodical entitled "Privacy & informatie" ("Rechtspraak over 'mailen en surfen'“ [Case law on e-mail and surfing“]), Hester de Vries, a lawyer who has worked at the Hugo Sinzheimer Institute, the Data Protection Authority and the law firm "Kennedy Van der Laan", is one of the major experts on the protection of the privacy of employees in the Netherlands, expressed amazement at the fact that “at the beginning of 2001, the media nevertheless devoted considerable attention to the implications of this law, or at least how it has been translated into the general rules on monitoring e-mail and Internet drawn up by the Data Protection Board [College Bescherming Persoonsgegevens] (then still known as the 'Registratiedienst'). Moreover, the organisations representing the interests of both employers and employees have given the matter considerable attention at their websites and, inter alia, developed specimen codes of practice.
4. In the Netherlands cantonal judges make completely different rulings in comparable cases.
5. The works council still fails to make sufficient use of its right of consent of matters concerning the protection of personal data.

2. **SPECIFIC PROTECTION OF PERSONAL DATA ON EMPLOYEES**

In the article mentioned above, Hester de Vries wrote that "if we look at how widely the situation varies from one Member State to another [where the protection of the privacy of employees is concerned], despite the EU Directive on the protection of personal data, we realise why the European Commission is considering a sectoral Directive on the protection of personal data on employees. The FNV also inclines in this direction."

In practice, the right to privacy as one of the fundamental human and (hence) workers' rights still receives insufficient emphasis in labour relations.

There is a lot to be said for a stricter formulation the principle whereby personal data must never be used for purposes other than the one for which they were collected. The criterion set out in Directive 95/46/EC, according to which the purposes of processing further to collection must not be incompatible with the purposes as they were originally specified, is too vague and repeatedly leads to differences in interpretation between employers and employees.

The principle of transparency should also be formulated more strictly. Admittedly, employees have the right to know what data are kept on them, but they rarely avail themselves of this right. After all, what should they inquire about? The alternative, which has in fact already been described in the ILO code of Practice (8.3 and 11.1), is better, therefore: employers must periodically (each year) actively inform employees and their representatives of all the data being kept on them.

In many countries, the legislation based on Directive 95/46/EC is a paper tiger. Employers can invade the privacy of their employees with impunity, as they know the employees will not bring (criminal) action against them. The judges in the civil courts in the Netherlands admit evidence obtained illicitly through infringement of privacy in cases where employers want to get rid of an employee. The Directive should stipulate that evidence obtained illicitly through infringement of privacy must not be used in legal proceedings, including civil cases.

It should also be possible for the supervisory organisations to impose a civil penalty for the infringement of rules that are directly based on a European Directive.

Finally, the use of *privacy enhancing technologies* prescribed by the Member States for that purpose should be promoted through tax or other measures.