12.6 Summary and Conclusions

European legislation relevant in the context of data protection in the workplace is quite complex, as the overview in section 12.2 shows. In this chapter three case studies illustrating relevant application scenarios for profiling in the workplace were introduced and analysed.

In the first case the use of private e-mail at the workplace was elaborated concerning two relevant European Directives and the existing instruments for e-mail monitoring and analysis. If the employer offers the employee an account for private as well as business e-mails, monitoring e-mail communication is for the most part legally prohibited. As a result, employers should strictly discriminate between e-mail accounts that are used for private e-mail at or from the workplace and those that are used for e-mail on behalf of the employer only. Different approaches to implement these different types of accounts have been suggested.

The second case study analyses the use of human resource and skill management. Relevant questions in this context proved to be appropriate legal grounds to run such a system, transparency of the system’s operations and purpose binding for the use of the results.

In the third case study the use of profiling for fraud prevention in retail was explored. In addition to the elaboration of reliable legal grounds for the introduction and application of fraud prevention systems, limitations on data to be collected and analysis were suggested and discussed. Especially in this case, the collection and use of data beyond the scope of the system needs to be prevented by technical and organisational means. This should include co-operation with, e.g., works counsels.

12.7 Reply: The Use of Labour Law to Regulate Employer Profiling: Making Data Protection Relevant Again

Paul De Hert*

The strength of data protection as a legal framework for the balanced application of profiling techniques in employment situations should be assessed with prudence. As a set of rules and guarantees focusing on the individual person, it does not fit well in an area of society where power differences between the parties concerned are considerable. The only legal vocabulary that is accepted and recognised is the one used in collective labour law, where union and employee-representatives discuss most issues, including the ones that concern individual rights. The success of data protection will depend on its ability to find its way into this collectivised vocabulary. But how strong is the vocabulary of labour law?

* Vrije Universiteit Brussel (VUB) and Tilburg Universiteit, Tilburg Instituut for Law, Technology and Society (TILT)
12 Profiling in Employment Situations (Fraud)

12.7.1 The General Framework: An Empty Shell\textsuperscript{185}

The work relationship between employer and employee is characterised by an unequal balance of power. Negotiation and consultation procedures between employers and employees aim to ease the consequences of this unequal relationship. The employer cannot assert his authority with regard to all aspects of the employee’s personality and activities. The context of the working conditions presents specific characteristics that have been described by the European Court of Human Rights. Thus, in the case Niemitz v. Germany: “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.”\textsuperscript{186}

Employers should therefore accommodate workers’ privacy. Not accommodating privacy in the workplace can result in a lack of employee trust, creativity and health (Business for Social Responsibility Education Fund, 2001). In many cases, workplace monitoring can seriously compromise the privacy and dignity of employees. Surveillance techniques can be used to harass, discriminate and create unhealthy dynamics in the workplace (PHR, 2004). Usually the answer given to these challenges is based on the principles of data protection. Employers are recommended to accommodate data protection rights for their employees. This includes notice, employee participation in drafting a monitoring policy and employee access to information collected under the policy. This is also the core of Leopold’s and Meints’ analysis, be it that their analysis is clearly European. In practice, this means that recommendations are presented as a result of an analysis of legal texts. They are more than just recommendations, they are law. Employers in Europe do not have a moral but a legal duty to accommodate data protection rights, it is more than just good will or enlightened management.

What strikes the reader is the complexity of the analysis. We learn that in European countries the collection and processing of personal information is protected by the EU Data Protection and the Telecommunication Privacy Directives.

\textsuperscript{185}Most of the articles quoted by the author can be viewed on http://www.vub.ac.be/LSTS/.

\textsuperscript{186}23 November 1992, Series A nr. 251/B, par. 29. See also the case Halford v. United Kingdom, 27 May 1997, ECR 1997-III, par. 44: “In the Court’s view, 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 para. 1 (art. 8-1) (see the above-mentioned Klass and Others judgment, loc. cit.; the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, p. 30, para. 64; the above-mentioned Havig judgment, loc. cit.”
The latter provides for confidentiality of communications for “public” systems and therefore does not cover privately owned systems in the workplace. In these cases the former applies. The result is unsatisfactory. There are two different protection regimes depending on technicalities and we are advised to consider a distinction between private and professional use of e-mail services. Leopold and Meints conclude their analysis under ‘Example 1’ with the suggestion that the complete restriction of the private use of e-mail for the entire staff might be one of the practical solutions. This recommendation - promoting medieval privacy protection - is illuminating but contradicts the spirit of the Court’s findings in Niemitz, viz., that in modern life it is not always possible to clearly distinguish which of an individual’s activities form part of his professional or business life and which do not.

The principles of data protection rights laid down in the two European Directives are general in scope and linked to many subtleties. Every principle seems to have its exception and every exception gives birth to new exceptions, this time with the emphasis on the scope of the exception. Their application to workplace privacy issues is not always clear. Close your eyes and try to recall what Leopold and Meints have to say on their three examples (surveillance of e-mail-communication and Internet access; human resource and skill management; fraud prevention in retail). The taste in our mouth is technical and procedural. Substantive solutions or answers did not make it into our legal memory. Does data protection have anything to say on substantive issues regarding profiling?

Through the years I have lost a part of my passion for the European data protection regulations and the analysis carried out in terms of data protection. The threats are usually aptly identified and there is a good amount of lip-reading done of the privacy and data protection rights but how about the outcome of the exercise? In 2001 the Registratiekamer, the Dutch Data Protection Registrar, published a lengthy list of guidelines for employers planning to implement online employee monitoring systems in the workplace, based on the (then) new Personal Data Protection Act, signed on July 6 2000. These included requirements that a company must discuss the entire system and its usage with the relevant unions and work councils, as well as publishing details of the discussions and the system to the staff. Interestingly, the Dutch Data Protection registrar skated around the contentious issue of personal e-mail at work, saying that, if possible, personal and professional e-mail should be kept separate but, if this cannot be carried out, then monitors should attempt to ignore obviously personal e-mail (Gold, 2001; De Hert, 2001). This kind of legal output has a chilling effect on the reader, at least on this reader. The mountain brings forth a mouse. Employers have nothing to fear with regard to data protection, they can push through as far as they want. Employers, who are open and willing to respect data protection ‘rights’ must feel like they are sacrificing competitiveness and business advantages. This is even more so when they start reading in newspapers about their colleagues in other countries. With the American Management Association finding that nearly 3/4 of major businesses monitor
their employees\textsuperscript{187} and with the 2000 U.K RIP Act allowing for most employers to monitor without consent (Crichard, 2001), it must be difficult to explain to employers on the European continent that they cannot monitor their employees at will, as do their American and British colleagues. One of the challenges of European data protection will be to overcome a “race to the bottom” - development in the area of human rights as a consequence of internationalisation. Whereas good communication to parties involved about differences in the legal systems with countries outside the EU will probably lead to more acceptance of the EU legislation, less is true about differences in legal systems within the EU. It is striking to note that the preamble of the 1995 Directive discusses internal market problems due to privacy restrictions in certain EU countries, but does not consider the race to the bottom problems due to the lack of privacy guarantees in certain EU countries. At one time the Commission envisaged a new Directive to harmonise differences in data protection regulation regarding workers (De Vries, 2002) but apparently and sadly this initiative lost momentum.

\textbf{12.7.2 The Data Protection Move Towards Labour Law Instruments: Transcending Technicalities}

There are several models for data protection regulation: comprehensive or sectoral laws; self-regulation and regulation through technology (PHR, 2004). The European approach to regulation is well known: general laws on the European and national level that govern the collection, use and dissemination of personal information by both public and private sectors with an overseeing body that ensures compliance. Traditionally, this approach is contrasted with the United States preference for sectoral laws, governing, for example, video rental records and financial privacy, enforced through a range of mechanisms. Although many European and American authors express strong attachment to the European approach\textsuperscript{188} there are alternative viewpoints (Blôk, 2001 and 2002: Bergkamp, 2002). Equally, there are reports showing that successful strategies against excessive camera surveillance are driven by the citizens using administrative enforcement mechanisms, rather than by the data protection authorities using data protection mechanisms (Bennett & Bayley, 2005). In recent writings we have therefore applauded the development at the EU level, and at the level of the member states to draft sectoral laws used to complement

\textsuperscript{187} For a helpful overview of workplace privacy issues, mainly in the United States, see the Electronic Privacy Information Centre (EPIC)’s Workplace Privacy Page \texttt{http://www.epic.org/privacy/workplace/}; and Solove & Rotenberg, 2003.

\textsuperscript{188} “A major drawback with this approach is that it requires that new legislation be introduced with each new technology, so protections frequently lag behind. The lack of legal protection for individual’s privacy on the Internet in the United States is a striking example of its limitations. There is also the problem of a lack of an oversight agency” (PHR, 2004). For more detail about the different approaches, see De Hert, 2002b.
comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records.

The turn in data protection writings and practices towards labour law, not quite theorised but nonetheless present in Leopold’s and Meints’ analysis, is to be understood along the same lines. Through it, there is an attempt to benefit from the advantages of both sectoral laws and self-regulation, in addition to enjoying the advantages of a general framework.

At first sight this turn is not evident: the European data protection framework is of a general nature and it provides for general concepts and proper enforcement machinery. However, more is needed to penetrate social sub-spheres such as labour law and labour practices. The demonstration of Leopold and Meints convincingly shows that data protection has at least something to say about profiling at the workplace but not much insight is given about the enforceability of the solutions and recommendations they arrive at. Based on my knowledge of the European, Belgian and Dutch case law - showing unfamiliarity with data protection concerns or preferential treatment of employer interests, there is no reason to be cheerful (De Hert, 2002a; de Vries, 2002; De Hert & Loncke, 2005; De Hert & Gutwirth, 2006). Hence, the use of labour law and its self-regulatory characteristics: absence of time-consuming formal procedures needed for ‘real’ or formal legislation, ability for easy adaptation to changing circumstances, creation of rules, build on values that the relevant parties are already familiar with, more awareness due to self-legislation and more willingness to comply (Koops, et al., 2006).

105In a recent Dutch case, the applicant requested a court order for a bank (‘Dexia’) to supply relevant personal data. He demanded to be provided with a complete overview of all processed personal data, including information about the purposes of the processing, the recipients of the data and the sources of the data. Further, the applicant demanded copies of: the lease contract, the risk profile, certificates of the shares referred to in the contract, certificates of dividend payments, the credit-worthiness survey (‘credit-score’), written reports about telephone calls and every other document that concerned him. The court was of the opinion that the applicant had no right to obtain a copy of the contract. However, Dexia had to give information about the contract data, to the extent that they could be defined as personal data. The same was true for the requested copies of the dividend payments. The court stressed that Dexia had to submit information about all personal data, irrespective of the existence of a legal obligation to process these data. There was for example, no obligation for Dexia to set up a risk profile. But if data are processed to construct such a profile, they have to be included in the overview provided to the data subject. However, the court decided that Dexia could make use of one of the exemptions provided by the Act, namely that a controller is not obliged to provide an overview of the personal data if this implies a disproportionate administrative burden for him. Dexia demonstrated to the court that their duty to respond to a similar request had seriously upset its organisation and had already cost more than a hundred thousand euros. For this reason the court rejected the applicant’s request and decided that in this instance Dexia would not have to provide the overview of the personal data. Dexia v applicant, 12 July 2005. The decision (in Dutch) is published on www.rechtspraak.nl under number LJN AS2127. See Jos Webbink and Gerrit-Jan Zwenne, ‘The scope of Access Rights under the Dutch Data Protection Act’, via http://www.twobirds.com/english/publications/articles/Access_Rights_under_the_Dutch_Data_Protection_Act.cfm. We learn from the Dexia case that profiling in an employment situation aiming to prevent further or establish fraud committed by employees is regarded as individual profiling covered by the Directive when it aims to identify the fraud. On the contrary, data mining techniques to generate insight on fraudulent behaviour and methods will be justified by group profiling when the information is not convertible to any particular person. The real purposes regarding the application of the data processing are decisive.
12.7.3 The Turn of Data Protection to Labour Law Instruments: Transcending Individuality and Individual Consent

There are however more than ‘language’ factors accounting for this striking turn from data protection law to labour law. In particular we draw attention to the collective dimension of privacy. The distinction between first, second and third generation human rights has never been very solid. First generation rights also serve collective interests. Freedom of assembly, for instance, laid down in article 11 of the European Convention on Human Rights contains a straightforward illustration of this proposition: “Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests”. In a similar vein, does the protection afforded by the privacy right benefit groups? The right to have a certain name given to a child offers protection to persons belonging to certain minority groups (Gilbert, 1992). We saw above the recognition of the right to privacy in Niemitz as a right to develop relationships with the outside world. The legal and material environment needed for such a development cannot be the creation of one individual. It is a collective good that should in principle be open to everyone. To claim rights with such a strong collective basis, associations of all kinds are far better placed than individual ones (De Hert & De Schutter, 1998). If privacy has a future, the legislation behind privacy will, so we believe, have to allow associations defending privacy by opening privacy procedures for associations. This will contribute to an objectivation of privacy and data protection conflicts and provide solutions when individuals are not willing to take up their rights (with a heavy collective dimension). We note that this call for recognition of the collective dimension of privacy is not new in international human rights law. Rights are defined in a certain context and this context changes or may change. New refugee patterns have brought legal scholars to recognise that today’s society is in need of a set of refugee rights that are not only accorded to the individual refugee but in certain cases also to refugee groups in need of protection (Jackson, 1991; Hathaway & Neve, 1997; Parrish, 2000; Fitzpatrick, 1996).

Partly, data protection regulation recognises this collective dimension of privacy through its administrative features: special watchdogs are created and delicate processing activities are subjected to notification and checking procedures. Contempory data protection, viz. data protection after the 1995 Directive, has shifted away from this by replacing a system of regulation based

\[100\] These procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the data protection principles. In order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplifications are allowed, except in cases where certain processing operations are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies. In addition a system of prior checking is made possible for risky processing operations and in the course of the preparation of new legislation regarding the protection of personal data.
on the idea that processing activities need to be legitimate by a system based on the idea that processing activities need consent. It would not be feasible to analyse this in great depth but the 1995 Directive, inspired by Dutch pragmatism and its ability to conceive everything as a potential candidate for trade, has amended some of the basis intuitions of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data by making consent a valuable option in almost all cases. In practice, this implied a complete redrafting of some national data protection bills of older date that did not recognise consent as a legal ground for the legitimate processing of data (Leonard & Poulet, 1999). We are, for that reason no great admirers of the 1995 EU Directive boasting in its preamble that “the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981” (comp. with Gutwirth, 2002).

Leopold and Meints rightly consider consent of the data subject as one of the most problematic criteria of Art. 7 of the 1995 Directive when being applied to the workplace context. According to Article 2 para (h) of the Directive, consent has to be defined as a freely given and informed indication of the wishes by which the data subject signifies his agreement to personal data relating to him being processed. Many companies traditionally use consent as the legal basis to process workers’ personal data to a third country. Workers are then asked to sign a so-called ‘consent form’ agreeing to the processing. Such forms often concern a whole list of personal data and rarely give explanations as to the consequences of not agreeing to the processing by the worker. In fact, these forms are habitually seen by the employers as a formality: “let the workers sign and then it is OK” (Blas, 2002). The foolishness of the European legislator when introducing consent as a legal ground in the sphere of human rights has provoked some reaction from the member states. The Dutch Data Protection Law defines consent as any freely given, specific and informed indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed (Article 1, letter i of the WBP). Again, this is not much help for the regulation of the working sphere. The Working Party rightly takes the view that where consent is required from a worker and where there is a real or potential prejudice that arises from not consenting, the consent is not valid in terms of satisfying either article 7 or 8 of the Directive, as it is not freely given. If it is not possible for the worker to refuse, it cannot be considered as consent, as this must at all times be freely given. A worker must therefore be able to withdraw consent without prejudice. The Working Party underlines the fact that where, as an 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 consent without detriment (Working Party, Opinion 8/2001).

Blas has brilliantly identified the elements that should be taken into consideration for the correct interpretation of the requirements regarding consent
(Blas, 2002).\textsuperscript{191} Consent for profiling operations should be freely given and has to be specific. This means in particular that it should specifically be given for each individual profiling operation, not for profiling in general. The requirement for information implies that the data subject should be aware or made aware of the particular risks of the profiling operation. The consent will only be valid if the data subject has been sufficiently informed. If the relevant information is not provided this exception will not apply. It is not sufficient if the data subject has been informed about the intended profiling operation and has not objected to it (opt-out construction). This is not a clear indication of the wishes of the data subject. Because the consent must be unambiguous, any doubt about the fact that the consent has been given would also render the exception inapplicable.

One could question the wisdom of the European legislator in inserting consent as a general legal ground, knowing that Europe is a continent of workers rather than autonomous Greek Gods. Overseeing these requirements regarding consent makes one realise that consent is difficult to apply when the profiling envisaged would cover the data of numerous data subjects (Blas, 2002). In such a case, the information has to be given in a complete and appropriate way to all the data subjects and consent has to be obtained from all of them in order to enable profiling. In addition to the fact that this whole operation can be time consuming and might involve considerable expense (for instance if the data subjects are in different locations), the use of consent for this kind of case shows some other practical inconveniences. For instance: what does the controller do if some of the data subjects give their consent and others do not?\textsuperscript{192} Also, what does the controller do if some of the data subjects decide to withdraw their consent at a later stage?\textsuperscript{193} Strategically, the turn to labour law can be understood as a way to overcome the burdens of consent for the employer willing to profile more than one employee. Freedom implies the possibility of choice, as Leopold and Meints rightly note, but what is left for the individual worker to choose when worker representatives have decided upon their rights?

\textbf{12.7.4 Assessing the Role of Labour Law}

The foregoing casts some shadow on the role of labour law in the area of privacy and data protection.\textsuperscript{194} One could respond to this that this new role for representative

\textsuperscript{191}In the following we stay close to the analysis of Blas (regarding transfers of workers’ data to third countries) but we transpose her analysis to our subject matter.

\textsuperscript{192}“If workers are free to say ‘yes’ or ‘no’ to the envisaged transfer there might be a considerable amount of workers opposing the profiling operation”. Blas, 2002.

\textsuperscript{193}“It should be borne in mind that data subjects (or where applicable their legal representatives) are free to withdraw their consent at any time. The decision to withdraw consent does not have a retroactive effect but the processing of the data of that data subject will have to be terminated from that moment on”: Blas, 2002.

\textsuperscript{194}Our finding that privacy is a collective good that needs to be upheld by collective means certainly does not imply that workers should give their rights away to representative workers bodies.
‘individualisation’ is possible without mediation. Recourse to general monitoring is only made obligatory in situations of minor importance. Elsewhere we have identified the events of September 11 as a driver behind the privacy unfriendly provisions in Collective Labour Agreement 81. The workers’ representatives at the negotiation table obviously did not do a good job. This was partly due to a lack of case law in favour of employee’s interests. Only after the conclusion of the Agreement, the news spread that the French Court of Cassation had rendered an important judgment in favour of workers’ privacy with regard to the use of the Internet and e-mail. This judgement immediately provoked more privacy friendly judgements in Belgium but did not have an impact on the drafting of Collective Labour Agreement no. 81. It is therefore often heard that this agreement is a product of the period after 9/11 and before the judgement of the French Court of Cassation.

With this observation, we return to our description of models of regulating data protection. Labour law in some way allows for forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. In theory, there is nothing wrong with this, especially not in the light of our finding that the general provisions of the EU Directive regarding consent do not fit into the reality of the working sphere. However, in many countries, especially the United States, efforts to achieve more balanced outcomes for data protection through self-regulation have been disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problems with these approaches. Industry codes in many countries have tended to provide only weak protections and lack enforcement (PHR, 2004). We wrote that judges are often unfamiliar with data protection and the work of the data protection authority. Most significant in this respect is the important judgment of the Belgian Court of Cassation (27 February 2001), omitting all reference to international and national data protection and the Collective Labour Agreement no. 68 of 16 June 1998. Both areas of law with their specific but complementary legal instruments were ignored and evidence gathered through secret monitoring by the employer was legally accepted in court. Is data protection really better off with labour law in its stable? Of course but in a legal system that refuses to distinguish between secret profiling and legitimate or transparent profiling, labour law will not do what data protection law is unable to do. Elsewhere in this volume, Gutwirth and I have defended the view that stronger allies (such as criminal law prohibitions) are needed to realise transparency and other key values of data protection. The fact that human rights are at stake does not make self-regulation or regulation through labour law actors illegitimate – public interest can be very well served by these models of regulation - but it does force the central legislator to be more alert and to intervene if necessary (Koops, et al., 2006).