The European Workplace:
The Right to Privacy and Data Protection

by

Michael Foutouchos

Send correspondence to:mfouto80@yahoo.gr

Preface*

One of the main aims of this paper is to assess the protection of employees' rights to privacy in Europe as a whole. Therefore data protection and the jurisprudence of the European Convention on Human Rights are presented together. Additionally, there is an attempt to link data protection law with human rights, and in particular with the right to privacy; and that is because not only they complete each other, but because only together they provide effective protection to workers' rights.

Each society produces the laws that it needs; if we lived in a perfect society, there would be no need for legislators to create criminal law. Accordingly, the fact that there is legal protection to the privacy rights of employees means that these rights were and are in danger. Hopefully, this paper helps the reader to understand not only how these rights are protected now, but also why they need protection.

1.1. Defining Privacy

* I would like to thank Bob Watt for earlier comments on this draft, however any mistakes or opinions expressed are solely mine. Additionally, I would like to thank my family that not only funded me but supported me all throughout.

Privacy is notoriously difficult to define; and if a practical definition is given, a legal one is even more difficult to formulate. One of the first definitions, and apparently one of the most broadly accepted, is that privacy is "the right to be let alone"[1]. Simple as it might sound this definition is less than fully satisfactory. A more legalistic approach is that

> [privacy is] the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information[2].

Difficulties with the full legal definition of privacy have led to the belief that "an interference with privacy is not even like an elephant, of which it can be said that it is at least easy to recognise if not define"[3].

Courts in their attempt to fully define privacy, which they are to protect, have come up with scaled definitions; i.e. arguably there are three 'zones' of privacy in need of protection, the first one which has to do with territorial or spatial aspects (e.g. privacy within somebody's home), secondly issues that have to do with the person and the last 'zone' of privacy refers to information[4]. However, in our time, which has come to be known the information age, it might be more necessary to focus on information issues (the third 'zone' of privacy)[5]. Furthermore, privacy has also been defined as "the claim of individuals, groups or institutions to define for themselves when, how and to what extent information about them is communicated to others"[6] or alternatively, the right to know about and to control what information is being held on an individual[7] or similarly, "the individual's ability to control the circulation of information relating to him"[8].

It has also been decided that:

---

[1] S. D. Warren and L. D. Brandeis, *The Right to Privacy*, (1890) 4 HarvardLR 193.
[2] David Calcutt, QC in the *Report of the Committee on Privacy and Related Matters* in 1990 (Cmnd. 5012).
[3] *Per* Lord Woolf in *R v Broadcasting Standards Commission ex parte BBC* [2000] 3 WLR 1327, p. 1332.
[4] *Per* La Forest J in *R v Dyment* [1998] 2 SCR 417, p. 428 (case from the Canadian Supreme Court).
[5] C. Fried, *Privacy*, (1968) YaleLJ 480, p. 482.
[6] A. Westin, *Privacy and Freedom*, (London, Bodley Head, 1967), p. 7.
[7] J. Michael, *Privacy*, in D. Harris and S. Joseph (eds.), *The International Covenant on Civil and Political Rights and United Kingdom Law*, (London, Clarendon Press, 1995), pp. 267-272.
[8] A. R. Miller, *Assault on Privacy: Computers, Data Banks and Dossiers*, (Michigan, MichiganUP, 1971), p. 40.

> [t]he scope of the right to respect for private life is such that it secures to an individual a sphere within which he can freely pursue the development of his personality. In principle, whenever the state enacts rules for the behaviour of the individual within that sphere, it interferes with the respect for private life[9].

Additionally, privacy is a right complementary to all other sorts of rights, in the sense that if not enjoyed freely there can be chilling effects to the exercise of other kinds of rights[10]. However, the list of possible definitions of privacy seems to be endless[11].

Despite all these possible definitions of privacy it seems that sometimes a comprehensive understanding of this concept is so difficult that British jurists would be unable to define and thus protect such an abstract right[12]. This lack of comprehension of the right to privacy seems so strong in the British legal thinking that only in early 2004 was the right to privacy firstly established in a House of Lords case[13] in British courts[14].

It is estimated that between £150-300 million per year are spent on CCTVs in the UK[15]. In Newham, software that can scan faces against a database of millions of photographs in seconds, which is meant to be used for the identification of criminals, has been developed[16]. In the employment environment things seem to be even more complicated and privacy even more threatened. With 75% of IT managers thinking that monitoring the employers is an absolute necessity[17]; 67% of employers admitting that they engage in electronic surveillance of their employees[18]; over one third of employees being monitored secretly[19]; companies already having fingerprint and face

---

[9] *André Deklerck v Belgium*, Application No 8307/78, DR 21, p. 16.
[10] J. Michael, *Privacy and Human Rights: An International and Comparative Study, With Special References to Developments in Information Technology*, (Dartmouth: UNESCO Pub., Aldershot: Paris, 1994), p. 4.
[11] See J. Velu, *The European Convention on Human Rights and the Right for Private Life, the Home and Communications,* in A. H. Robertson (ed.), *Privacy and Human Rights*, (Manchester, MUP, 1973), pp. 27-31: definitions of privacy from different points of view.
[12] Younger Committee on *Privacy in the United Kingdom* in 1972 (Cmnd. 5092), paras 57-73 and 665.
[13] *Campbell v MGN plc* [2004] EMLR 15.
[14] This reluctance should be seen under the generally traditional prism of disbelief towards constitutional form of rights of the UK judiciary; e.g.: "[t]ypically English law fastens not upon principles but upon remedies", *per* Lord Wilberforce in *Davy v Spelthrone BC* [1984] AC 262 at 276F; see also supra n. 10, p. 1.
[15] D. Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Laws and Developments*, (London, Privacy International, 2000), p. 41.
[16] Ibid., p. 42.
[17] Referring to UK companies, http://news.bbc.co.uk/1/hi/business/1370956.stm
[18] Referring to US companies, P. Skyte, *The Protection of Privacy at Work*, in R. Blanpain (ed.), *On-line Rights for Employees in the Information Society*, (London, Kluwer Law International, 2002), p. 1.
[19] Referring to US companies, ibid.

images stored in their data bases for millions of individuals[20]; and finally, with specialised monitoring software already in the market[21], privacy in the workplace resembles an endangered species.

The particularities of the right to privacy in the workplace are obvious when somebody takes into account the nature of employment. For example, the employers have property rights over the equipment that the employees use, and thus their monitoring interest. Additionally, employers have the right to manage their business in the manner they wish (managerial prerogative) within legal limits[22]. Furthermore, the employer is the person to be held responsible to damage to third parties in case the employee is negligent[23]. Finally, there is the relatively new concept of theft of time: employees are paid for the time that they work; if they are not productive enough they 'steal' paid time from the company. The latter concept seems that it emerged during the '80s in the US[24].

Everyone seems to accept, including trade unions and employees, that the right to privacy within the workplace is "partly abandoned in the sense that the employer can control personal behaviour of employees"[25] or as it has been said "[t]he civil liberties cease to exist when they enter the private sphere of the labour market, regulated by the contract of employment"[26]. On the other hand, the right to privacy has obtained constitutional status in most European countries and cannot simply be left aside when someone enters the premises of his employer.

Therefore, there are three main legal instruments that regulate the issue on a European level: (i) the European Convention on Human Rights (ECHR) and namely Article 8, which protects the right to privacy; (ii) Directive 95/46/EC[27] *on the Protection of Individuals with Regard to the Processing of Personal Data and on the*

[20] Namely the American company Polaroid, ibid.
[21] http://news.bbc.co.uk/1/hi/technology/2984922.stm
[22] See generally S. D. Anderman, Labour Law, *Management Decisions and Workers' Rights*, (London, Butterworths, 2000).
[23] *National Rivers Authority (Southern Region) v Alfred McAlpine Homes East Ltd* [1994] EnvLR 198.
[24] "Time theft steals money as sure as someone picking your pocket. ... It is America's biggest crime, and until its victims -the owners and managers of American industry- decide to do something about it, we'll continue to be stolen blind": quoted in L. Snider, *Theft of Time: Disciplining Through Science and Law,* [2002] 40 Osgoode Hall LJ 89, p. 90.
[25] F. Hendrickx, *Privacy and Employment Law: General Principles and Application to Electronic Monitoring*, in R. Blanpain (ed.) supra n. 18, p. 49.
[26] Prof. B. Hepple QC, *The Impact on Labour Law*, in B. Markesinis (ed.), *The Impact of the Human Rights Bill on English Law*, (Oxford, OUP, 1998), p. 63.
[27] OJ L281, 23.11.1995, p. 31.

Free Movement of such Data, creating the legal notion of personal data and protecting them; and (iii) the rest of the EC regulatory framework with Directive 02/58/EC[28] *concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, which partially creates the legal framework for the protection of personal data in the workplace. All three legal instruments are ratified by the member states of the European Union and nowadays they are binding law. However, two of them are EU legislation while the ECHR has a different legal background. In order to understand better the common nature and aims of the legislation it would be useful to, briefly, go through their history.

1.2. The Right to Privacy and Data Protection: Common Ancestry

Article 12 of the Universal Declaration of Human Rights is the first international legal document, in 1948, that mentions the right to privacy.

> No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks on his personal honour and reputation. Everyone has the right of the protection of the law against such interference or attacks[29].

The spirit of the era was one of restoration of democracy and compensation for the wrongs of the past; "[it] expressed the wish for the whole world to be politically organised on the basis of mutual, joint recognition of the individual's essential and permanent rights"[30]. The world tired from two global wars was in need for some fundamental rights so as to be able to live without fear of arbitrary interference from the states[31].

The Council of Europe (COE) came up with the ECHR only two years later. The relative right was to be construed in two paragraphs, as all the rights in the ECHR, one would contain the right itself and one the derogations. It was also to be directly enforceable only against public bodies. So Article 8 reads:

---

[28] OJ L201, 31.07.2002, p. 37.

[29] There seems to be a debate about whether the Universal Declaration is binding law or not, however, L. B. Sohn, *The Universal Declaration of Human Rights*, (1968) Journal of the International Commission of Jurists, Special Issue, pp. 25-26, supports that it is; however see also I. Brownlie, *Basic Documents in International Law*, (Oxford, Clarendon Press, 1995), p. 255.

[30] P. Vegleris, *Twenty Years' Experience of the Convention and Future Prospects*, in A. H. Robertson (ed.) supra n. 11, p. 340.

[31] For a very brief European perspective see D. Lasok and J. W. Bridge, *Law and Institutions of the European Communities,* (London, Butterworths, 1991), pp. 1-3.

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

"From the outset it should be noted that Article 8 does not protect the right to privacy *per se*"[32]. This simply means that the Article is so construed that certain infringements might not be addressable. But on the other hand, since 'respect' is referred to, the signatory States can be found to have positive and negative obligations under Article 8. Article 8 was construed that way, so as to broaden the responsibility of the state[33].

The general tendency for the evaluation of the fundamental right of privacy can be seen by the Commission's prisoners' related case law. In the early years of the application of the ECHR invasion of privacy would be largely justified under Art 8(2)[34]. However, as years went by and the right to privacy was considered more and more fundamental, and thus generally applicable, the scope broadened. In cases such as *Golder*[35] and *Silver*[36] the Court would show less tolerance with state interference with the Art 8 right.

The jurisprudence of the European Court of Human Rights started including issues relative to the working environment and to the right to private life. The landmark case of *Klass*[37], which will be analysed further on, demonstrated that clearly. The limits of labour law were for the first time faced with the limits of the right to privacy. Private life is about personal data, personal information; in many of the definitions examined above this is obvious. If personal life is to be protected, personal information should be protected as well, of course counterbalanced with other principles.

---

[32] J. Kingston, *Introduction to Privacy*, in L. Heffernan and J. Kingston (eds.), *Human Rights, A European Perspective*, (Dublin, Round Hall Press in association with Irish Centre for European Law, 1994), p. 153.
[33] D. J. Harris, M. O'Boyle and C. Warbrick, *Law of the European Convention on Human Rights*, (London, Butterworths, 1995), p. 303.
[34] *X v United Kingdom*, No 8231/78, Vol. 28D&R, pp.38-39 and *X & Y v Switzerland*, No 8166/78, Vol. 13D&R, p. 243.
[35] (1979-1980) 1 EHRR 524.
[36] (1984) 6 EHRR CD62.
[37] *Klass v Federal Republic of Germany* (1979-80) 2 EHRR 214.

"…[C]oncern about the potential effect of automatic data processing upon the right to privacy began to grow during the early 1960s and the early 1970s"[38]. European states started introducing legislation, on a national basis, about the protection of personal data and thus of private life. The independent and sporadic legislation however, created a problem: companies need information to operate at full efficiency and this information must be able to flow freely in a market; the existing legal background lacked homogeneity and thus created problems in the free flow of information[39].

On a European level three main institutions attempted to solve this problem: (i) the Council of Europe (COE), that had the experience in protecting privacy with the ECHR; (ii) the Organisation for Economic Co-operation and Development (OECD); and (iii) the, then, European Economic Community (EEC), which mainly had economic orientation.

The debate was focused on the issue whether the same kind of protection should be afforded for natural and legal persons[40]. The COE presented a resolution in 1973 that "[was] to lead to the later divergence between data protection laws over the protection given to legal as well as natural persons"[41]: "[i]n many cases individuals realise their rights through the intermediary body having legal personality"[42]. It seems that principal reasons for the deviation in the two sets of legislation (privacy-data protection) can be found in the early 1970s.

The EEC firstly addressed the issue of data protection in 1973 and the European Parliament kept itself busy by trying to find ways to protect personal data. Within the next ten years the OECD and the COE were co-operating so as to produce a single legal document, while the EEC and the European Parliament were debating so as to come up with a piece of legislation that would protect personal data in the private sphere.

The co-operation of the OECD and of the COE was fruitful and came up with the *Convention for the Protection of Individuals with Regard to Automatic Processing*

[38] Supra n. 10, p. 32.
[39] The French government of the day had requested from the OECD to take measures towards the international harmonisation of the relative national legislations, ibid. pp. 31-32.
[40] Supra n. 11, pp. 18-19.
[41] Supra n. 10, p. 33.
[42] Resolution (73)22, *On the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector*, adopted by the Committee of Ministers 26 September 1973.

of Personal Data, in 1980. Reading the Preamble is essential to understand the spirit of the document:

> The Member States of the Council of Europe, signatory hereto,
> Considering that the aim of the Council of Europe is to achieve greater unity between its Members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms,
> Considering that it desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing,
> Reaffirming at the same time their commitment to freedom of information regardless of frontiers,
> Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples…

Why is this Preamble so important? Because it clearly shows that there are many scholars and jurists that see no real difference between the essence of data protection law and human rights law; these people "…consider the whole effort as a part of the international human rights movement, and particularly as a measure to protect the privacy of natural persons" [43]. This realisation will be absolutely essential when relevant case law is analysed. This paper will try to support that the right to privacy and data protection are two sides of the same coin: the one is meant to be applicable to the public sector whilst the other to the private one.

This Convention, both structurally and materially speaking as well as from the point of view of its legal ideas, is a landmark for the evolution of data protection law in Europe. (i) It sets out the principles that should be adopted by the Member States[44]; (ii) specific rules were laid out for the international flow of data[45]; and (iii) a consulting procedure was also created for the case of non enforcement[46]. The principles, however, set out in Article 5 would be a very strong influence for the later Directive 95/46/EC, which read:

> Personal data undergoing automatic processing shall be:
>
> a. obtained and processed fairly and lawfully;
> b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

[43] Supra n. 10, p. 34.
[44] Article 5 - Quality of data.
[45] Article 12 – Transborder flows of personal data and domestic laws.
[46] Chapter V - Consultative Committee.

> c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
> d. accurate and, where necessary, kept up to date;
> e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

It is noteworthy that these principles, with some slight additions, were endorsed by the 95/46/EC Directive. At this point it should also be noted that the then EEC and later the European Union (EU) was a little bit hesitant in producing relevant legislation. This was for two reasons: (i) the COE and the COED were more than active on the issue; and (ii) the competence of the EEC on such kind of issues was questionable[47]. However, in 1979 the European Parliament's Legal Affairs Committee published a report on *Community Activities to be Undertaken or Continued with a View to Safeguarding the Rights of the Individual in the Face of Developing Technical Progress in the Field of Automatic Data Processing*[48]. In 1981 a Recommendation[49] was addressed to the Member States that they should sign the COE Convention. The Member States did sign the Convention but only six had ratified it by 1990[50]. So, in the early 1990s the EU got worried about the discrepancies among national data protection laws that disrupted the function of the common market. Therefore, it produced Directives such as 95/46/EC and 02/58/EC to solve this problem and to harmonise national legislations on the issue.

As it has been seen privacy law and data protection law have emerged from a common point of view; they both tried to protect the right to privacy of the individual, either against the state (ECHR) or against the private sector (EU and COE legislation). However, there is a difference that is of crucial importance: data protection laws emerged not only for the protection of the individual, but also for the free flow of data among the European countries, that is so much needed for the undisrupted function of the common market. In other words, data protection law did have the essence of protection of a fundamental right (privacy), but also it was meant to be company (employer) friendly.

2.1. The 95/46/EC Directive

[47] I. J. Lloyd, *Information Technology Law*, (London, Butterworths, 2000), paras 4.38-4.39.
[48] PE 56.386/fin Doc 100/79.
[49] OJ L246, 29/08/1981, p. 31.
[50] Denmark, France, Germany, Luxemburg, Spain and the UK.

Data protection law is predominantly a European phenomenon[51]; there are of course other countries with data protection laws (e.g. Canada, Australia), but the legislation does not have the breadth and the intensity that it does in Europe.

The two main European Union instruments that affect labour law in connection with the right to privacy are Directives 95/46/EC and 02/58/EC. The first Directive establishes the meaning of personal data and relevant ways of protection. Actually, it has been argued that a data protection/privacy law should consist of two parts: "(i) a definition of the circumstances in which third parties have the right to collect, use and disseminate personal information about others and (ii) a mechanism for preventing collection, use and dissemination outside those limits"[52].

The 95/46 Directive copes mainly with the latter characteristic. The objective of the Directive is dual, and once again the close affiliation of data protection law and the fundamental right of privacy is obvious:

> (1) In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
> (2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph (1)[53].

It entails eight principles that are meant to harmonise national legislations; five out of the eight principles are exactly the same with the five principles established in the 1981 COE Convention. It would be good however to see, how these principles are endorsed in national legislation. The UK Data Protection Act 1998 will be used as an example.

So, the 'fair and legal' principle means that processing of personal data is not going to be treated as legal if at least one of the conditions of Schedule 2[54] is met. When it comes to sensitive personal data, at least one of the conditions of Schedule 3[55] should be met. Fair processing is defined at Schedule 1, Part II, paragraphs 2 and

[51] C. Reed and J. Angel (eds.), *Computer Law*, (Oxford, OUP, 2003), p. 417; see Appendix 1.
[52] C. Reed, *Internet Law: Text and Materials*, (London, Butterworths, 2000), p. 227.
[53] Chapter 1, Article 1.
[54] Conditions Relevant for Purposes of the First Principle: Processing of Any Personal Data. The first principle in the Directive is at Section I, Article 6, para 1(a).
[55] Conditions Relevant for Purposes of the First Principle: Processing of Sensitive Personal Data.

3. For the British legal reality, common law notions come into play when legality is to be defined.

In the UK there seem to be three common law types of unlawfulness: (i) breach of confidence; (ii) breach of the *ultra vires* doctrine; and (iii) breach of a legitimate expectation[56]. It seems thus, that the criteria of unlawfulness are following exactly the same rationale that applies for a claim against a public authority for judicial review[57]. General guidance for the application and interpretation of the concept of unlawfulness has been provided by the Data Protection Registrar[58]. Unlawfulness is applicable in case of breach of statute law as well[59].

The second principle, that the data should be stored for specified and legitimate purposes and not used in a way incompatible with those purposes (the finality principle), is found in Schedule 1, Section 1, paragraph 1 of the Act[60]. These purposes can either be made known directly to the data subject or they can be specified by Notification to the Data Commissioner[61].

As according to the third principle the personal data should be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed[62]. In *Community Charge Registration Officer of Runnymede Borough Council v Data Protection Registrar*[63] the Court addressed the issue of interpretation of this principle.

The fourth principle if found at paragraph 4 of Part I of Schedule 1: "personal data shall be accurate and, where necessary, kept up to date"[64]. Section 70(2) sets the limits of inaccuracy: "for the purposes of this Act data are inaccurate if they are incorrect or misleading as to any matter of fact". It is worth noting at this point that accuracy is a prerequisite for the data controller, however the keeping up to date of the personal data is discretionary.

---

[56] Data Protection Registrar, *Private Lives and Public Powers: A Guide to the Law on the Use and Disclosure of Information about Living Individuals by Public Bodies*.
[57] This point has been addressed at M. Foutouchos, *ECHR Case Law and Data Protection: Developing and Completing*, 2nd Term Essay for LW 656, Essex University, 2004, p. 3.
[58] (The then Information Commissioner) *Guidelines*, Third Series, Nov. 1994, ODPR.
[59] Statute law unlawfulness: see R. Jay and A. Hamilton, *Data Protection: Law and Practice*, (London, Sweet & Maxwell, 1999), pp. 51-52.
[60] Section I, Article 6, para 1(b) of the Directive.
[61] Sections 18 and 17 of the Act respectively.
[62] Schedule 1, Part 1, para 3; Section I, Article 6, para 1(c) of the Directive.
[63] Case DA/90, 24/49/3 October 27, 1990.
[64] Section I, Article 6, para 1(d) of the Directive.

The fifth principle reads "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"[65] [66]. The UK Information Commissioner has provided relative guidance: i) data users should delete data that are no longer required for the prescribed purposes; (ii) data users who have a substantial databases may adopt a systematic deleting data policy; and (iii) if the data have been collected due to a special relationship between the data controller and the data subject these data should be deleted when the particular relationship ceases to exist (e.g. relationship between an employer and an employee)[67].

These are the five principles explicitly mentioned in the Directive. However, the British Act includes another three that are implied all throughout the Directive. Namely that the data should be processed in accordance with all the rights awarded to the data subject[68]. The seventh principle in the 1998 Act reads: "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"[69], passing on the responsibility for the security of the data to the controller. The eighth principle has to do with transborder data flow, which is forbidden "outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data"[70].

The Directive also provides for the creation national supervisory authorities (in the UK the Information Commissioner's Office, ICO[71]), which have the responsibility for the application of the national legislations and provide for guidance in case it is necessary[72]. Additionally, the Directive created a Working Party that will

[65] Schedule 1, Part 1, para 5.
[66] Section I, Article 6, para 1(e) of the Directive.
[67] Supra n. 59, p. 64.
[68] Schedule 1, Part 1, para 6, the rights that are confirmed by sections 7, 10-12 of the 1998 Act. In the Directive the rights are found in Section II, Article 7(a): unambiguous consent of the data subject for the processing; Section IV, Article 10: information relative to the data controller should be passed on to the data subject; Section V, Article 12: right of the data subject to access the relative data; Section VII, Article 14: right of the data subject to object.
[69] Schedule 1, Part 1, para 7; Section VIII, Article 16: confidentiality; Article 17: security; Chapter III includes remedies and liabilities, in the Directive.
[70] Schedule 1, Part 1, para 8; Chapter IV of the Directive.
[71] Which can be found at http://www.informationcommissioner.gov.uk/.
[72] See for example: http://ico-cms.amaze.co.uk/DocumentUploads/110603prelease.pdf, *Information Commissioner Spells out the Do's and Don'ts for Workplace Monitoring*, and most importantly:

monitor continuously the application of data protection laws and shall suggest for modifications and amendments[73].

Generally speaking, the 1995 Directive created not only a euphoria to the human rights supporters within the EU that for years they had been asking for more constitutionality[74], but it also provided effective protection of employees against intrusive surveillance and monitoring. It should also be noted however, that it was meant for wider application (commercial reasons etc) and not specifically for labour law issues; additionally it did not make specific reference for the swiftly changing sector of electronic communications.

2.2. The 02/58/EC Directive and Relevant Legal Issues

Directive 02/58/EC replaced Directive 97/66/EC[75]. The 1997 Directive brought about many essential changes in labour law, amongst others, and it was implemented in the UK simultaneously with the 1995 Directive. The 1995 Directive was implemented as the Data Protection Act 1998, and the 1997 Directive was implemented under s. 2(2) of the European Communities Act. Two more legislative measures were implemented in the UK in the light of the changes in data protection law: the Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations[76], both of which created the necessary space so that some forms of surveillance and monitoring would be legal, precise and accessible to everyone[77].

2.2.1. The 02/58/EC Directive

---

http://www.informationcommissioner.gov.uk/eventual.aspx?pg=SR&cID=446, *Codes of Practice*, which cover all the aspects of employment from recruitment to monitoring at work.

[73] Chapter VI, Article 29 and 30 of the Directive.

[74] See for example P. Alston and J. H. H. Weiler, *An 'Ever Closer Union' in Need of a Human Rights Policy*, p. 3 and M. P. Maduro, *Striking the Elusive Balance Between Economic Freedom and Social Rights in the EU*, p. 449, in P. Alston, M. Bustelo and J. Heeman (eds.), *The EU and Human Rights*, (Oxford, OUP, 1999).

[75] OJ L24, 30.01.1998, p. 1.

[76] SI 2000/2699.

[77] For the status of UK law before these changes see below the *Halford* case, additionally see *Malone v UK* (1991) 13 EHHR 448.

Even though the debates about the 1997 and the 1995 Directive had started at the same time, the complexity of the first one delayed its drafting for two more years[78]. In the meanwhile the changes in the information technology market were so rapid that by the time of the implementation of the 1997 Directive, talks about a new Directive had already begun[79] [80]. Subsequently, only five years after the voting of the 1997 Directive, it was repealed, not amended, and substituted by the 02/58/EC. Did it effectively change anything in connection with labour law?

Well, the only difference is that in Article 5, concerning confidentiality of the communications, it has an additional paragraph (para 3) coping with confidentiality of electronic communications. So, the second question is what were the significant points for labour law in the 97/66/EC Directive?

The 1997 Directive extended the protection of data protection to legal persons[81]; the restriction on the process of data acquired through communications is even greater than the general duty for fair and legal process of personal data. Generally speaking however, it was a piece of legislation additional to the 1995 Directive and it was oriented to market issues[82] (the relationship of consumers and service providers), rather than to labour law issues.

2.2.2. National Additional Legislation

The 1995 Directive was so radical and it included such fundamental issues that most of the Member States had to implement a series of laws (daughter legislation) so as to make their legal systems compatible[83]. The UK was no exception and the 95/46 Directive brought about new pieces of legislation. The Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations were introduced at that point.

---

[78] Supra n. 47, para 4.41.
[79] R. Jay and A. Hamilton, *Data Protection: Law and Practice*, (London, Sweet & Maxwell, 2003), para 26-01.
[80] Additionally, the wording of the Directive created problems, mainly for the legal treatment of e-mails: see supra n. 48 p. 453 and supra n. 76, para 26-01. For guidance on the issue of the e-mails see: Article 29 Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace*, 5401/01/EN/Final WP55, Adopted on 29 May 2002, p. 20, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_en.pdf
[81] Repeated in the 2002 Directive in Article 1(2).
[82] Namely: (i) the service provider and his customers/ subscribers; (ii) the subscriber and the real/ direct user of the service; (iii) users; and (iv) users and the state.
[83] Supra n. 47, para 4.47, and supra n. 51, p. 430.

Their role was to make some cases of interception of communications legal and compatible with 1995 Directive under Article 13[84]. Additionally, this daughter legislation provided for the necessary legal clarity on the issue that, up to then, it was absent; disrupting, thus the rule of law.

3. Data Protection Case Law

3.1.1. *Bodil Lindqvist v Åklagarkammaren i Jönköping*[85]

3.1.2. Opinion of Advocate General[86]:

Mrs Lindqvist was a part time, voluntary catechist in a parish in Sweden. She set up a web-page of the parish, so that information was easily accessible to the parishioners; there was also a direct link for the web-page of the parish in the home page of the Swedish church. The web-page contained information about the parish including: the names, and in some occasions the full names, of other employees and herself; her colleagues' jobs and hobbies; telephone numbers and other personal information was included; additionally, it was mentioned that one of her colleagues was a part-timer because she had health problems. Mrs Lindqvist did not notify her colleagues about the web-page neither did she inform the *Datainspektionen*[87]. The web-page was removed promptly. However, the *Hovrätten di Götaland* (Court of Appeal) referred seven questions to the European Court of Justice (ECJ) for preliminary ruling, concerning the interpretation and the scope of Directive 95/46/EC. The questions were the following:

> 1) Is the mention of a person on a web-page an action which falls within the scope of the Directive? Does it constitute the processing of personal data by automatic means to list on a web-page a number of persons with comments about their jobs and hobbies etc?
> (2) If the answer to the first question is no, can the act of setting up on a web-page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute a breach within the meaning of Article 3(1)?
> If yes:

[84] The Member States were given the power to do so under Art 13(1) and in connection with the reasons mentioned thereof.
[85] Case C-101/01.
[86] Opinion of Advocate General Tizzano, delivered on 19-09-2002.
[87] Information Commissioner for Sweden.

(3) Can the act of loading such information onto a private web-page which is accessible to anyone who knows its address be regarded as outside the scope of the Directive, under the exceptions in Article 3(2)?
(4) Is information on a web-page stating that a named colleague has injured her foot and is on half-time on medical grounds personal data concerning health which, according to Article 8(1), may not be processed?
(5) If a person in Sweden uses a computer to load personal data onto a web-page stored on a server in Sweden does that constitute a transfer of data to a third country within the meaning of the Directive?
(6) Can the provisions of the Directive, in a case such as the above, be regarded as contradictory with the general principles of freedom of expression or other freedoms and rights, which are applicable within the EU and are enshrined in *inter alia* Article 10 of the ECHR?
(7) Can a Member State, as regards the issues raised in the above questions, provide more extensive protection for personal data than the Directive, even if none of the circumstances described in Article 13 exists?

The Swedish court had taken the view that undoubtedly there was processing of personal data. The data would link to certain, identified or identifiable, living individual(s) and the uploading onto the web-page would be considered as processing. The issue was whether the processing would be within the scope of the Directive; and, most importantly, whether the specific activity would fall within the scope of Community law[88].

Advocate General Tizzano, firstly assessed the question whether the activity would fall outside the scope of the Directive if: (i) the course of activity falls outside the scope of Community law; or (ii) if carried out by a natural person as a personal activity. Mrs Lindqvist had claimed that since the Directive was adopted on the basis of Article 95 EC, (ex- 100a), could not be regulated at a Community level because that would be contradictory with the values found in Article 5 EC[89].

The Commission's view on the subject was that the Directive should be interpreted broadly so as to include such kinds of activities, and added that Article 6 EC specifically mentioned that EU is to respect fundamental rights, bringing thus the present situation within the jurisdiction of Community law. Secondly, the Commission claimed that Mrs Lindqvist's activity was not a purely personal one because: (i) the web-page was accessible to the public at large; and (ii) the activity

[88] Issues that would fall outside the scope of Community law would be: the activities provided for by Titles V and VI of the TEU, additionally processing operations concerning public security, defence, State security and finally the criminal law-related States' activities.
[89] Para 29.

itself did not have a nature confined to Mrs Lindqvist, but included other people[90].

Advocate General's view was concurring with the opinion of the Swedish government in the fact that Mrs Lindqvist's activity was not purely a household one[91]; but on the other hand he found, agreeing with Mrs Lindqvist's argument, that the activity at issue was outside the scope of Community law since it was not an economic one[92]. On this basis, he found that the arguments of the Commission were flooded, in the sense that if non economic activities were to fall within the scope of Community law the meaning of Article 3(2) of the Directive would be rendered void[93].

The true scope of the Directive 95/46/EC was summed up:

> "…the Community legislature wanted to establish a level of protection equivalent in all Member States in order to remove obstacles to flows of personal data resulting from the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy"[94].

The Advocate General went on to underline that the Directive was construed in such a way that it did take into account the Article 8 right of the ECHR but "all this was conceived in the course of … the free movement of personal data inasmuch as it held to be vital to the internal market"[95] and "no Treaty provision confers on the Community institutions any general power to enact rules on human rights"[96].

With these observations, he concluded that the activity at issue was outside the scope of Community law and therefore it would not be necessary to answer the rest of the questions[97].

3.1.3. Comment:

Advocate General Tizzano adopted in his approach the narrowest possible interpretation of the Directive. Not only the dual target was disregarded, focusing only on the free flow of data and not on human rights issues, but the general aim of the EU was overlooked as well. EU is trying to instil common constitutional values in the

[90] Para 33.
[91] Para 34.
[92] Paras 35-36.
[93] Paras 37-39.
[94] Para 39.
[95] Para 40.
[96] Para 43.
[97] Paras 45-46.

member states so as to make European integration a feasible target and not merely an academic wish[98]. The experiment of the EU, common constitutional values without a common state, would be rendered void if rationale like the one adopted by Advocate General was to be accepted.

Additionally, the Data Protection Directive is clearly a constitutional piece of legislation[99], which of course takes into account the need of the common market (which also is another means for European integration[100]), enforcing only its common market scope would be a grave mistake.

Practically speaking, personal data of employees were processed. Finding that this processing was outside the scope of Community law would render the scope of the Directive void. All managers could have part-time staff or volunteers to process the data of their employees and all this would not be covered from Community regulation. Data protection, given its breadth and implications, needs clarity and cohesion. If the final judgement of the Court would follow Advocate General's reasoning there would be no clarity or cohesion creating problems with the common market aim of the Directive as well; the homogenisation of data protection laws of the member sates would not be possible due to the different interpretations of the Directive.

3.1.4. Judgement[101]:

The ECJ approached each question separately. For the first question (whether it was personal data within the meaning of the Directive) the Court established that: (i) the data referred to were personal, since they could be linked to a recognisable individual; and (ii) bearing in mind the contemporary technological conditions the processing was automated[102]. Since the first question was answered to the affirmative there was no need to assess the second question (whether under the given facts there

[98] F. C. Mayer, *Europe and the Internet: The Old World and the New Medium*, EJIL 2000 11(149), p. 162.

99 Data protection has been treated as a constitutional value by Germany since a very long time: R. Massey and K. Tauber, *Privacy and Personality, Politicians and Stars*, E-Law 1.2(5), p. 5; and A. Utley, *Pilot Angry at Terror Slur*, The Times Higher Education Supplement, 28-11-2003.

[100] R. Badinter, *A European Constitution: Perspectives of a French Delegate to the Convention*, IJCL ICon 1.2(363).

[101] Case C-101/01, Judgement of the Court delivered on 6-11-2003.

[102] Paras 24-27.

was a breach under Article 3(1))[103].

The third question (whether the present case was outside the scope of Community law), which was the one that made Advocate General answer negatively, was answered in scales and with a reasoning that seems to be relatively simple. The activity of Mrs was a religious, charitable one[104]. On the other hand, the exceptions afforded by the Directive at Article 3(2) have to do with national defence, national security etc. All these activities are carried out either by the State or State agencies and in no occasion they could be held activities of individuals[105]. Additionally, the fact that the activities of Mrs Lindqvist were religious or charitable does not make them personal since the data were uploaded onto a web-page, and thus millions of people had potential access to this. This activity is not comparable with an individual who has a directory of addresses or phone numbers[106]. Finally, the Court underlined that if a contrary interpretation was adopted this would create reverse effects from the ones aimed by the Directive; i.e. a case to case approach instead of a unification of data protection laws, and instead of free flow of data among member states to a halt in the flow of this data[107].

For the fourth question (medical data) the Court suggested a wide interpretation and thus another affirmative answer was given to the Swedish Court of Appeal.

The fifth question (transfer to third countries), seemed a little bit more complicated. The Court had to take into account several factors including that

> "[t]he ubiquitous nature of that information is a result *inter alia* of the fact that the technical means used in connection with the Internet are relatively simple and becoming less and less expensive"[108].

The Court seems to have followed the rationale that since the changes in the IT market are so rapid the present Directive could not have possibly covered such a kind of 'transfer'[109], and thus found that there was no transfer within the meaning of the Directive.

---

[103] Para 28.
[104] Para 39.
[105] Paras 43-44.
[106] Paras 45-46.
[107] Para 41.
[108] Para 58.
[109] Paras 59-70.

As far the sixth question was concerned (contradiction with other freedoms: namely Article 10 of the ECHR), the Court gave the answer that it was a matter of interpretation of the national courts, and that in principle the Directive was not contradictory with any freedom, notwithstanding its breadth[110].

The final question of the Swedish court was whether the member states could provide greater protection than the one afforded by the Directive. The answer of the Court was a reasonable one. The scope of the Directive is a dual one: protection of privacy and free flow of data; as long as these two remained protected member states could do whatever they wished[111], even to extend the scope of the Directive in areas of law not covered by it[112].

3.1.5. Comment:

The decision of the Court seems generally balanced. However, there is a point that can be partially criticised: the assessment of transfer of data to third countries. This is part of the broader academic and industry debate about the nature of the Internet. There are two possible approaches about the Internet: (i) it has to do with access to information (connectivity); and (ii) Internet should be treated as a body of information[113].

If Internet is about information then the Internet Service Providers (ISPs) should have the legal liabilities of publishers. Practically, this is the mode that is being followed. On the other hand, if Internet is about access to information the legal liability that might arise from the uploaded material lies solely to the person that uploaded the material[114]. Additionally, the latter view is implemented by a series of jurists[115]. Having these in mind, the Court was correct when it found no liability of the ISP for transfer of data to third countries. However, the reasoning of the decision seems relatively flooded when it comes to the liability of Mrs Lindqvist. It is striking that nobody was found responsible for transferring the data to third countries, since

[110] Paras 83-90.
[111] Para 97.
[112] Para 98.
[113] Y. Benkler, *Internet Regulation: A Case Study in the Problem of Unilateralism*, EJIL 2000 11(171), p. 176.
[114] As it was the case in *R v Perrin* [2002] EWCA Crim 747 (CA).
[115] See for example W. Dutton (et al.), *Cyberculture: The Key Concepts*, (Routledge, 2002); additionally, this is the view of Article 19 (pro freedom of speech UK NGO): ISPs should be treated as journalists and not as publishers.

this data was uploaded on the www and it was accessible through the home page of the Swedish church to all Internet users worldwide.

Finally, the ECJ had a more than satisfactory approach to the last question of the Swedish court. Member states were given the freedom to adjust Directive 95/46/EC to their needs, as long as its dual aim was achieved, and this was a firm reply to sovereignty-reasoned eurosceptics[116].

3.2.1. *Data Protection Registrar v PLP Motors Ltd*[117]

PLP Motors recruited an employee that used to work for a competitor company. The employee had in his possession names and details of customers of his ex-employer which he passed on to the managing department of the defendant company. The relevant details were used in advertising campaign by the defendant company and the Data Protection Registrar (now Information Commissioner) received a complaint from an individual who received the advertisement material. The defendant company was fined for unlawfully obtaining personal data.

3.2.2. Comment:

This is the use of data protection law as an alternative to proceedings for breach of confidence. The rationale of the case seems to coincide with the views of Advocate General Tizzano, in the sense that the data was used in the course of an economic activity and at the same time the processing of the data was intrusive to the right to privacy of the data subjects.

3.3.1. *Rechnungshof v Österreichischer Rundfunk and Others*[118]

3.3.2. Opinion of Advocate General[119]:

The Austrian constitution authorised the Austrian Court of Auditors (ACA) to audit several Austrian public companies, partially public or local authorities. As according to paragraph 8 of the Federal Constitutional Law (FDL) the bodies liable to

[116] See for example: R. Smith, *One Charter for All?*, Law Society Gazette, Vol 100, No 48, p. 11, 19-12-2003.
[117] Decision given on 24 April 1995 (unreported), quoted from supra n. 48, pp. 408-409.
[118] Case C-465/00 and joined cases C-138/01 and C-139/01.
[119] Opinion of Advocate General Tizzano, delivered on 14-11-2002.

be audited by the Court of Auditors should inform the Court for the salaries or pensions of persons that were over a certain limit. The aim of the legislation was to provide clarity and scrutinise public spending. This list should include the names and the salaries/pensions of the relative individuals. Several public bodies refused to provide the relevant list; other public bodies provided the list but in an anonymous form. The Austrian Court submitted a dual question to the ECJ:

> 1. Are the provisions of Community law, in particular those on data protection, to be interpreted as precluding national rules which require a State body to collect and pass on data on income for the purpose of publishing the names and income of employees?
> 2. If the answer to at least part of the above question is in the affirmative: Are the provisions precluding the abovementioned national rules directly applicable, in the sense that persons obliged to disclose data may rely on them in order to prevent the application of conflicting national rules?[120]

The two joined cases had to do with two employees of the aforementioned companies that denied providing their data (name and salary). The questions of the Court were exactly the same as in Case C-465/00.

Advocate General Tizzano considered whether the Directive was applicable, and his assessment started by a recapitulation of the points of the parties. The Austrian Court had inescapably linked the process of data at issue in connection with the free movement of workers (Article 39 EC). Under this presumption the defendants and the Court considered that the audit activities fall within the scope of Community law. The concept was that Article 39 EC would come into play because the employees would have absolute freedom in negotiating a new contract of employment with a new, potentially non Austrian, employer. Additionally, foreign workers would be deterred from working for these companies/entities in Austria under the fear of the audit[121]. The issue would become more complex about those economic entities that had to compete in the European or international market (National Bank of Austria and Austrian Airlines)[122].

The Commission, at the hearing, submitted that there were five main processes involved: (i) collection of data by the entities subject to audit; (ii) passing those data to the ACA; (iii) the ACA's inclusion of them in its report; (iv) the sending of the

[120] Para 19.
[121] Paras 30-32.
[122] Para 33.

report to the Parliament; and (v) publication of the report. The four latter processes would be outside the scope of the Directive, as they were within the powers of the state and thus outside the scope of Community law. However, the first process would be within the scope of the Directive because it did interfere with the free movement of workers (Article 39 EC), and it did have other social implications (Article 141 EC)[123].

The Advocate General accepted the five processes argument of the Commission and he went on to assess whether these five different forms of process would be covered by the scope of the Directive[124].

He found that the five processes would fall outside the scope of Community law, because they had to do with the managing of finances within the sovereign powers of the member states[125]. Additionally, he brought down the Article 39 EC by saying that these rules would apply equally to foreign and national workers without creating discriminatory conditions or other impediments to the free movement of workers[126].

Furthermore, the argument used by the defendants that Article 8 of the FDL would be implementing or furthering the aims of the 1995 Directive was also brought down. The rationale was that this Article would not set down general rules for the processing of personal data but instead it would be an administrative provision that would make sure that public funds were spent cautiously[127].

Advocate General Tizzano went on explaining his reasoning by referring to his Opinion on the *Lindqvist*[128] case. He underlined that the main aim of the Directive was to create an equivalent level of data protection and helping thus the common market[129]; it was not meant to be a human rights instrument:

> "The safeguarding of the fundamental rights constitutes…an important value and a requirement taken into account by the Community legislature in delineating the harmonised system needed for the establishment and functioning of the internal market, but it is not an *independent* objective of the Directive. If it were, it would have to be accepted that the Directive is intended to protect individuals with respect to the processing of personal data even quite apart from the objective of encouraging the free movement of such data, with the incongruous result that even

[123] Para 39.
[124] Paras 41-42.
[125] Paras 43-44.
[126] Paras 46-47.
[127] Para 48.
[128] Supra n. 85.
[129] Para 51.

forms of processing carried out in the course of activities entirely unrelated to the establishment and functioning of the internal market would also be brought within its scope"[130].

Accordingly, he found that forms such as these referred to in the present case would fall outside the scope of Community law within the meaning of Article 3(2) of the Directive; and additionally he found that the ECJ had no jurisdiction to rule whether the relevant legislation is compatible with the EU data protection principles.

3.3.3. Comment:

Advocate General Tizzano adopted exactly the same reasoning and rationale as he did in the *Lindqvist*[131] case. Once again his reasoning was such that would try to limit EU legislation to a core of financial-based legislation based upon national sovereignties and undermining, thus, the constitutional impact of European legislation.

The Advocate General seemed influenced by the judgement in *Internationale Handelsgeselschaft*[132]: "[t]he protection of [human] rights, whilst inspired by the constitutional tradition common to the Member States, must be ensured within the framework of the structure and objectives of the Community"[133]. The implementation of human rights in the legal framework of the EU should be advanced, but on the other hand "[r]espect for human rights is a condition of the lawfulness of Community acts"[134]. It is obvious from Community case law that as years go by respect for human rights becomes more and more a trend in the decisions of the ECJ[135].

3.3.4. Judgement[136]:

The ECJ started the analysis by referring to the submission of observations by

[130] Para 53.
[131] Supra n. 85.
[132] Case 11/70 [1970] ECR 1125.
[133] Ibid., p. 1134, paras 3-4.
[134] Opinion 2/94 [1996] ECR 1-1759, para 34.
[135] See comparatively *Geitling* joined cases 36/38 and 40/59 [1960] ECR 423: Community law "does not contain any general principle, express or otherwise, guaranteeing the maintenance of vested rights", p. 439 and *Stauder v City of Ulm* Case 26/69 [1969] ECR 419, that a balance between supremacy of EU law and human rights was struck; see additionally: L. Betten and N. Grief, *EU Law and Human Rights*, (London, Longman, 1998), pp. 58-67.
[136] Case C-465/00 and joined cases C-138/01 and C-139/01, judgement delivered on 20-05-2003.

member states and the Austrian court[137]. If the specific kind of process was to be justified under Articles 6(b), (c), Article 7(c) or (e) of the Directive, the usual ECHR considerations should take place: (i) in accordance with the law; (ii) necessary in a democratic society for the pursuit of a legitimate aim; and (iii) proportionate to the aim pursued[138]. On the other hand, the defendants submitted that the interference could not be justified under Article 8(2) of the ECHR[139]. Additionally, the defendants supported that the measure was aimed at people who were not public figures[140]. Moreover, one of the defendant entities, claimed that "if the legislature attache[d] real importance to the reasonableness of the remuneration received by the employees of certain bodies, it is then necessary to publish the income of all employees, regardless of its amount"[141].

The Court went on to underline that

> "[t]he Union shall respect fundamental rights, as guaranteed by the [Convention] and as they result from the constitutional traditions common to the Member States, as general principles of Community law"[142].

Then the dual task of the Court, in connection with the first question, was proclaimed[143]: (i) did the relevant legislation provide for interference with the right to privacy? And if yes (ii) was the interference justifiable under 8(2) of the ECHR?

The ECJ started by the realisation that the European Court of Human Rights (ECourtHR) included in its scope matters of business, employment nature[144]; and found, however, given the character of the Austrian legislation, that it was up to national courts to establish whether the publication of the names was necessary or not[145].

The ECourtHR reasoning was applied fully and the ECJ came up with the result that the task to assess the proportionality of the interference, which takes place in the pursuance of a legitimate aim is upon the national courts and not upon the

[137] Denmark, Austria, Italy, Netherlands, Finland, Sweden, the Commission and the Austrian court submitted observations for the case.
[138] Para 50.
[139] Para 59.
[140] Para 60.
[141] Para 62.
[142] Article 6(2) EU, quoted at para 69.
[143] Para 72.
[144] *Amann v Switzerland* (2000) 30 EHRR 843, and *Rotaru v Romania* 8 BHRC 449 2000 WL 1151470; quoted at para 73.
[145] Paras 78-79.

ECJ[146]. So, if the national courts were to find that the legislation at issue was incompatible with Article 8(2) of the ECHR only then it would also fall foul of the proportionality threshold as set out in Articles 6(b), (c), Article 7(c) or (e) of the Directive[147]. In case it was found compatible (i.e. by not mentioning the names of the individuals), the national courts would still have to assess the foreseeability of the legislation[148]. Additionally, national courts should make such attempts so as to

> "interpret any provision of national law, as far as possible, in the light of the wording and the purpose of the applicable directive, in order to achieve the result pursued by the latter and thereby comply with the third paragraph of Article 249 EC"[149].

The ECJ concluded, in connection with the first question, Articles (1)(c) and 7(c) and (e) of Directive did not preclude the national legislation under consideration provided that the display of the names of the individuals was necessary and appropriate to the legitimate objective pursued (management of public funds); and this can only be a task for the national courts[150].

The second question imposed to the ECJ was whether individuals could refer directly to the Directive in case national legislation was conflicting with the scope of it. The Court replied to the affirmative by referring to its case law[151] and by underlying that the Directive was clear and precise enough so as to be possible to individuals to refer to it in national courts[152].

3.3.5. Comment:

The ECJ followed a typical ECourtHR approach, making thus clear the constitutional character of the Directive. This case and the *Lindqvist*[153] case make clear that the ECJ is willing to apply a blanket policy upon the 1995 Directive; meaning that it provides the maximum protection to the individuals and through this way the national laws are being harmonised.

---

[146] Paras 87-90.
[147] Para 91.
[148] Para 92.
[149] See Case C-106/89 *Marleasing* [1990] ECR I-4135, paragraph 8; quoted at para 93.
[150] Para 94.
[151] Case 8/81 *Becker* [1982] ECR 53, paragraph 25, and Case C-141/00 *Kügler* [2002] ECR I-6833, paragraph 51.
[152] Paras 99-101.
[153] Supra n. 84.

It is particularly striking, however, that the ECJ in this case followed the pattern set out by the ECourtHR: respect to the margin of appreciation, the national courts have the competence to appreciate several matters to a better degree but the triple principle test (legality, necessity in a democratic society and proportionality) is to be irreconcilable. Even the fact that all national legislation is to be read in the light of the Directive so as to be found compatible[154] is a typical ECHR characteristic[155]. Once again the ECJ manifestly showed the constitutional character of the Directive and that it is a much wider legislation than a Directive that merely aims at the preservation and the protection of the common market. The fact that the arguments of Advocate General were not adopted proves this beyond any doubt. The ECJ seems to appeal to the general plead for more constitutionality within the EU[156].

4. ECourtHR Case Law

Due to lack of specified legislation from the EU for many years the ECourtHR was meant to absorb most of employment-privacy related case law. Issues like surveillance and monitoring (employment related but not necessarily on employers' premises), the right to sexual orientation (with its legal implications e.g. dress code) and several other have since long been brought under the attention of ECourtHR, which has piled up specific case law and has relatively framed an area of privacy within the working environment. In most cases it is established that the right to privacy and the question is whether this interference was justified under Article 8(2).

4.1.1. *Klass v Federal Republic of Germany*[157]

German legislation allowed telephone tapping and inspection of mail by relevant authorities. Five German lawyers brought a claim to the Court that this legislation was infringing, among others, their Article 8 right. This legislation existed so as to protect the State against 'imminent dangers' putting at risk the 'free

[154] Supra n. 145.
[155] See Section 3(1) of the Human Rights Act 1998: "so far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights".
[156] E. U. Petersmann, *Proposals for a New Constitution for the EU*, (1995) 32 CMLR 11 23.
[157] (1979-80) 2 EHRR 214.

democratic constitutional order' and 'the existence or the security' of the State[158].

The administrative frame of the legislation precluded that approval of the supreme Land authority should have been granted beforehand or a designated federal Minister should supervise the operation, on the application of a relevant security agency. Every three months the surveillance authorities had the right to renew the order. Only in case the purpose of the operation was not put at risk could the surveillance subject be notified about it, after the end of the operation; a commission would monitor the whole operation for illegalities. An independent judicial authority would supervise the operation for illegalities. A report on the operation should be handed in by the responsible Minister to an all-party parliamentary committee; whilst the commission should firstly approve the surveillance desired by the Minister.

It was accepted that there was an interference with the Article 8 right and the issue was whether it was justifiable under the derogative 8(2). The German Constitution provided for such kind of interference on the condition that this was done according to a relevant statute. Article 1(1) of the G 10[159] allowed certain authorities to perform such activities. According to Art 1(9)(5) of the G 10: "... there shall be no legal remedy before the courts in respect of the ordering and implementation of restrictive measures".

The triple principle ECourtHR test was applicable; legality, necessity in a democratic society and proportionality. As far as to the first part the Court found that:

> "[t]his requirement is fulfilled in the present case since the interference results from Acts passed by Parliament, including one Act which was modified by the Federal Constitutional Court"[160].

Consequently, the Court had to assess the second part of the test. The applicants contested that there were not enough safeguards against the abuse of such a measure even though it was precluded that it would be applicable only in occasions of "imminent dangers" threatening "the free democratic constitutional order".

A dual point was brought up at this point by the Court: the complexity and character of contemporary societies would allow for some interference with

[158] It should be noted that this case was brought up only six years after a terrorist attack at the Olympic Games that were hosted by Munich in 1972 and only one year after the actions of the Baader-Meinhof Group (Red Army Faction, RAF) came to an end in 1977.
[159] Restrictions on the Secrecy of the Mail, Post and Telecommunications Act.
[160] Supra n. 157, p. 231.

individuals' rights on the provision that this would be for the benefit of the society at large; and secondly, the ECourtHR could not override national sovereignty in several issues[161].

> "The Court, being aware of the danger such a law [G10] poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate"[162].

The margin of appreciation is accompanied by the fear that the Conventional rights might come into nullity. The Court assessed the security barriers that were included: members of the parliament would scrutinise the operation, independent judicial authorities would provide supervision to the acts of the police, whilst only in urgent cases the Minister would not ask for relative permission by the supervisory commission.

The Court concluded that even thought here was some potential interference with the right to privacy, this interference was compatible with the triple principle test and additionally: "[s]ome compromise between the requirements for defending democratic society and individual rights was inherent in the Convention"[163].

4.1.2. Comment:

This case, even though not employment-related strictly speaking, provides for an ideal example for the way that the ECourtHR approaches issues related with the Article 8 right. The German laws invoked were the equivalent of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (even though, the relevant British legislation is mainly employment oriented.

However, what is extremely essential in this case in connection with labour law is that for the first time telephone conversations are included within the ambit of the right to privacy[164]. So, monitoring of phone calls is within the jurisdiction of the ECourtHR and it needs to be regulated accordingly. However, the big issue remains: reconciliation of human rights with the State's needs. And "as Grotius put it, if some

[161] At p. 232.
[162] Ibid.
[163] At p. 217.
[164] Supra n. 33.

aspects of being a person cannot be sold without our ceasing to be persons, then it should fall to the law to decide what is alienable and what is not"[165].

At this point, it is worthy to give some elements of German legal thinking that has influenced the privacy law as no other. The right to personality, and not a right to privacy that is narrower, is constitutionally granted to the German people[166]. Accordingly the same right remains intact in the workplace[167] and this has largely been achieved by the labour courts that have imposed the duty to respect this right to private sector employers, as well[168]. For the German legal reality this right has been defined as:

> "a right to be respected as a person, not to have one's individuality infringed, in one's right to express oneself (in appearance, writing, and speech), in one's social standing (honour), and in the private and intimate spheres of one's existence"[169].

For a German jurist the right to privacy is a means for achieving the right to personality and therefore when it comes to appreciate the former right the broadest possible definition and interpretation should be afforded so as to be possible for the latter right to exist.

Under these clarifications it is easier to proceed to the assessment of the relevant case law by the ECourtHR.

4.2.1. *Niemietz v Germany*[170]

The mail of a given political group would be forwarded to the office of the applicant, who was a lawyer. This political group cooperated with another political group, the Anti-clerical Working Group. A telefax was sent to a judge, signed by a Klaus Wegner, who probably was a fictitious person, on behalf of the latter group. This telefax had to do with the proceedings of a trial and expressed the opposition of the signatory party in an offending way for the judge.

A warrant was issued so as to locate and bring Klaus Wegner to trial. The

---

[165] Quoted in M. W. Finkin, *Information Technology and Workers' Privacy: Part IV: The Comparative Historical and Philosophical Context: Menschebild: The Conception of the Employee as a Person in Western Law*, 23 CompLabL&Pol'yJ 577, p. 633.
[166] Article 2(1) of the Basic Law (*Grundgesetz*).
[167] Supra n. 165, p. 581.
[168] Ibid., pp. 581-582.
[169] Quoted ibid.
[170] (1993) 16 EHRR 97.

German Constitution provides for the inviolability of the home[171], and this provision had traditionally been interpreted broadly by the German courts so as to include business premises. As regards to the warrant, statute prescribed that the home and other premises of a person, who is not suspected of a criminal offence may be searched only in order to arrest a person charged with an offence, to investigate indications of an offence or to seize specific objects and provided that there were relative indications. Relevant statute was also covering the case that an individual wanted to bring proceedings against the lawfulness of a warrant or the manner of execution. Additionally, lawyers in Germany have the right not to testify for anything that relates with their professional capacity. The applicant followed the relevant proceedings to challenge the legality of the warrant, but his application was rejected by the relevant authorities on the grounds that his case was not justifiable. Finally, he brought a claim before the ECourtHR, amongst other things, for violation of his Article 8 right.

The issue was whether there was interference with the Article 8 right. The German government contested that here was a fine line drawn in the ECHR that separated the notion of family life and home from that of professional life and professional premises. The Court however, in a pioneer approach considered that:

> "[t]here appears … to be no reason … why … the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is … 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"[172]

and additionally "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"[173]. And the court went on to stress that "a narrow interpretation of the words 'home' and 'domicile' could therefore give rise to the same risk of inequality of treatment as a narrow interpretation of the notion of 'private life'"[174]. Such considerations led the ECourtHR to the firm belief that there was interference with the right to privacy[175].

The next step of the Court was to assess if the interference was in accordance

[171] Article 13(1) of the Basic Law.
[172] Para 29.
[173] Ibid.
[174] Para 31.
[175] Para 33.

with the law and in pursuance of a legitimate aim. In both the Court answered to the affirmative since (i) the reasons and the procedure for the warrant existed in statute and (ii) the prevention of crime and the protection of the rights of others (the honour of the judge) were legitimate aims[176].

So, it all came up to whether the interference was proportional and necessary in a democratic society. The Court found that the particular context in which the warrant was drawn and its phrasing (it ordered a search for and seizure of 'documents' without any limitation) were to be found disproportionate[177]. And on this ground the ECourtHR found violation of Article 8.

4.2.2. Comment:

The labour law significance of his case is more than obvious. The right to privacy was extended for the first time to cover employment premises. A paradoxical gap of the law was covered. A human being is indivisible, and accordingly so should their rights. A person cannot give up their rights because they entered employment premises, especially under the complexity of the working conditions nowadays.

> "The predefined working hours is considered obsolete as a concept … [t]he employees work impressively more hours than prescribed by law, they work on weekends and Bank Holidays without the relevant payment"[178].

Under these working conditions personal rights cannot be excluded from the workplace. The ECourtHR in *Botta v Italy*[179] went so afar as to say: "... private life ... includes a person's physical and psychological integrity".

On the other hand the ECourtHR did not take any specific view in relation with labour law issues; it seems that "it is easier to identify rather than to establish a possible contribution of the Convention to the workplace"[180]. But this characteristic has to do with the nature of the Court itself: it is not a legislative body with broad powers; it is a Court that examines individual cases and it is according to the needs of the societies that these cases are adjudicated. This argument is not meant to go into

[176] Paras 34-36.
[177] Para 37.
[178] Δ. Χαριτόπουλος, *Μοντέρνες Δουλειές*, Τα Νέα, 07-12-2002 (D. Charitopoulos, *Modern Jobs*, Ta Nea).
[179] (1998) 26 EHRR 241, para 32.
[180] K. D. Ewing, *The Human Rights Act and Labour Law*, (1998) 27 ILJ 275, p. 280.

the issue of judicial interpretative powers[181]; however, it is clear that as times change the judiciary feels like interpreting some clauses of the Convention more liberally or broadly. Apparently, we are going through times of changes; it is not only the Courts that have to reassign their point of view, it is the police, as well, that has to reassess its approach to several issues[182].

The limit of legitimacy seems to be proportionality, which quickly becomes a dominant value in the legal system. The state no more may utter: "Me the State, I am the people"[183]. Fourteen workers were suspended in Edinburgh for smoking in the toilets of the Burton's Biscuits factory. They were caught by a CCTV and they went through disciplinary proceedings for gross misconduct even though there was no notice for the camera[184]. The principles of proportionality and necessity in a democratic society seem more than relevant when assessing such issues under the ECHR.

4.3.1. *Halford v United Kingdom*[185]

Ms Halford, the applicant, was a police officer. As an employee she had her own office and two telephones, one for personal use, one for business. The telephones were not connected to the public telephone network but they were connected with the internal network. The applicant had been reassured by her employer that she could freely use her personal use telephone. The applicant claimed that while there was a pending dispute with her employer (discrimination proceedings) her phone was intercepted, so as to provide evidence for that dispute; consequently, she brought a claim under Article 8, amongst others, before the ECourtHR.

The Interception of Communications Act 1985 was adopted after the

---

[181] See for example S. Leader, I*mpartiality, Bias and the Judiciary*, in A. Hunt (ed.), *Reading Dworkin Critically*, (NY/Oxford, Berg, 1992), p. 243; R. Dworkin, *A Bill of Rights for Britain*, (London, Chatto & Windus, 1990), p. 23; I. Harden & N. Lewis, *The Noble Lie: The British Constitution and the Rule of Law*, (London, Hutchinson, 1986), p. 213; K. A. Ewing & C. A. Gearty, *Freedom Under Thatcher: Civil Liberties in Modern Britain*, (Oxford, Clarendon Press, 1990), p. 274.
[182] N. Taylor, *Policing, Privacy and Proportionality*, (2003 Special Issue: Privacy) EHRLR 86, p.100.
[183] F. Nietzsche, *Thus Spoke Zarathustra*, translated by T. Common, http://www.eserver.org/philosophy/nietzsche-zarathustra.txt
[184] J. Duffy, *Cig Brother*, Daily Record, 16-01-2001.
[185] (1997) 24 EHRR 523**.**

Malone[186] case and it provided for interception of communications of a public network. The Court established that since the applicant was assured about the security of her personal line at work, and that since there was no written law that prescribed interception of communications on a private, closed network, there was unjustified violation of her Article 8 right.

4.3.2. Comment:

After this case the British government introduced the Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations. Their introduction coincided with the implementation of the 96/46/EC Directive in the Data Protection Act 1998. These two legislative instruments provide for a full scale under which (tele)communications can be intercepted lawfully.

Additionally, this case brought up another important issue: expectation to privacy would give rise to a right to privacy. This practically means that if an employer warns an employee that there is no such expectation their communications can be intercepted freely. Susan Singleton, famous privacy lawyer, goes so far as to say that "[i]n sectors where staff are very hard to recruit, stringent e-mail policies and what might be seen as an infringement of personal liberties could lead to an exodus of key people"[187]. This practically means that privileged people (those who are difficult to recruit usually are paid better) should remain privileged in the sense that their rights can be respected; no reference is made in Singleton's book about the non privileged: are their rights to be compromised or are their human rights are of less quality?

This is a typical case that the wording of the Court or the particular facts of the case can provide jurists and lawyers with many problems. Is *Halford* unique due to the facts of the case or is it generally applicable? This is part of a more general debate. Of course there are lawyers who believe that this case was harmful for the

[186] *Malone v United Kingdom* (supra n. 77). In this case it was established that in order for the interference with Article 8 to be legitimate it must be prescribed by law (written or unwritten); this law should be accessible, and if it was a 'norm it should be precise enough so that it would be feasible for the individual to comply. Interception of communications would, up to then, take place under an administrative instrument that was neither precise nor accessible. After this case Interception of Communications Act 1985 was adopted.

[187] S. Singleton, *E-Commerce: A Practical Guide to the Law*, (Aldershot, Gower, 2001), p. 8.

protection of privacy[188], others who believe that "in law context is everything"[189]; others who believe that only it is a harmful but has far reaching effects[190] and others that simply disagree with the concept of privacy in the workplace[191]. The question cannot be answered in a safe and secure manner by anyone. It is even more striking however, that an employee inside his office might be deprived of his right to privacy whilst in *Peck*[192] the ECourtHR took the view that an individual might have the expectation of privacy in the middle of a public road in the broad daylight.

5. Surveillance Methods: CCTVs, E-mail and Internet Monitoring

It is generally believed that surveillance is as old as work[193]. Everybody agrees that employers should be able to supervise or monitor their staff[194]. The issue is however, that nowadays technology seems to be much more effective –and definitely more intrusive- than surveillance methods used to be in the past[195]. With word processing packages maintaining record of the time spent on documents[196] and with chair sensors, so that an employer can know how long an employee spends at their desk[197] new technologies change the nature of surveillance. Moreover, "it is all too easy in today's technological societies to rely on surveillance and monitoring of

[188] A. McColgan, *Do Privacy Rights Disappear in the Workplace?*, (2003 Special Issue: Privacy) EHRLR 120, p. 122.
[189] *R (on the application of Daly) v Secretary of State for the Home Department*, HL [2001] 2 WLR 1622, para 28; suggested amongst others in M. Ford, *Two Conceptions of Workers Privacy*, [2001] IJL 135, p. 140.
[190] See G. Morris, *Fundamental Rights: Exclusion by Agreement*, [2001] 30 ILJ 49.
[191] A. Westin, *Privacy in the Workplace: How well Does American Law Reflect American Values?*, (1996) 72 Chi-KentLR 271, p. 276: "employees who enter employer's premises to do paid work have left 'private' space and entered a 'public' arena".
[192] (2003) 36 EHRR 41.
[193] M. Ford, *Surveillance and Privacy at Work*, http://www.ier.org.uk/pr_ford.htm, or alternatively surveillance "is as old-established as society": supra n. 47, para 3.3.
[194] H. Oliver*, Email and Internet Monitoring in the Workplace: Information Privacy and Contracting Out*, [2002] 31 IJL 321, pp. 324-326; see additionally M. Jeffery, *Information Technology and Workers' Privacy: A Comparative Study: Part II: National Studies: The English Law*, 23 CompLabL&Pol'yJ 301, p. 305: comment on the Lawful Business Practice Regulations 2000.
[195] Even though it has been argued that "the uses to which technology is put may be invasive, just as the uses of human supervision may be invasive": M. Finkin, *Employer Monitoring of Employee Electronic Mail and Internet Use*, (1999) 72 Chi-KentLR 221, p. 226.
[196] Supra n. 47, para 3.6.
[197] K. D. Ewing (ed.), *Human Rights at Work*, (London, Institute of Employment Rights, 2000), p. 38.

their workers without considering whether this is truly necessary"[198]. The most common methods of surveillance are CCTVs and the monitoring of Internet use and e-mails. The EU has specific suggestions over these issues.

5.1. CCTVs Monitoring

Even though CCTVs and constant filming are considered as magical appliances by employers that will boost productivity and they decrease to the minimum the loss of time[199], the rest of the people consider it:

> "not only personally repugnant to employees but it has such an inhibiting effect as to prevent employees from performing their work with confidence and ease. Every employee has occasion to pause in the course of his work, to take a breather, to scratch his head, to yawn, or otherwise to be himself without affecting his work. An employee, with reason, would hesitate at all times to so behave, if his every action is being recorded on TV. To have workers constantly recorded on TV is… reminiscent of the era depicted by Charlie Chaplin in 'Modern Times' and constitutes… an affront to the dignity of man"[200].

Or as it has been put by the mouth of the British judiciary: "[i]t is common knowledge … that every day there are periods when a worker is on his employers premises but he is not expected or required to be actually working"[201]. In order to resolve this tension between the managerial prerogative and the employees' right to privacy the Article 29 Data Protection Working Party (established by Directive 95/46/EC) has published the Opinion 4/2004 on the *Processing of Personal Data by Means of Video Surveillance*[202].

The Working Party, even though recognises that for several purposes CCTVs might be really helpful (i.e. detection of crime), goes on to recognise that a dual threat exists[203]: (i) disproportionate, unjustified restrictions on citizens' rights and fundamental freedoms; and (ii) this means of surveillance possibly entails discrimination dangers.

---

[198] Oliver, supra n. 194,p. 330.
[199] http://www.asginvestigations.com/security_cameras/: advertising CCTVs "many of our clients find that the money they save on their liability insurance premiums pay for the system within the first year!"
[200] *Per* Delaney (American case) in *Re Electronics Instrument Company and International Union of Electrical Workers* (1965) LA 563.
[201] *Per* Lord Reid in *Post Office v Crouch* [1974] ICR 378.
[202] 11750/02/EN WP 89, adopted on 11-02-2004, accessible at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp89_en.pdf
[203] Ibid., pp. 4-5.

The general regulatory framework for CCTVs should be that of Directive 95/46/EC. This means that the case law of the ECJ on data protection is applicable for CCTVs as well. However, there are some occasions that fall outside the scope of Community law[204]; i.e. issues of public safety, security etc, or actions done by an individual in the course of a personal or household activity[205]. The definition of data obtained by filming with CCTV is the broadest possible, covering all possible applications of technology[206].

Additionally, CCTV regulations are guided by the generally applicable Opinion 8/2001 on the *Processing of Personal Data in the Employment Context*[207]. This Opinion includes all the key principles that must prevail any processing of employee data[208]: (i) finality, meaning data should be collected for specified purposes only; (ii) transparency, which refers to the fairness of the data collecting procedure and to the right of access of the data subject; (iii) legitimacy, collection of data should be as according to national law; (iv) proportionality, the data and the methods for their collection should be proportionate to the aims; (v) accuracy and retention of the data, the data should be accurate and when necessary kept up to date; (vi) security, the employer should provide for organisational and technical measures so that the data will remain secure; (vii) awareness of the staff, on any occasion the staff should be informed that they are being monitored. Most importantly, the Working Party, taking into account the inequality of bargaining powers between employees and employers, suggests that consent should be a reason for legitimisation of surveillance only when there is a "genuine free choice and [the employee] is subsequently able to withdraw the consent without detriment"[209].

Of course it is not suggested how the latter balance is to be struck; i.e. when does an employee have a really free to choice to give consent? On this issue, collective bargaining seems to be a more than positive view, meaning that trade unions could bargain collectively this issue on behalf of their members[210]. However,

[204] See Recital 16 of the Directive.
[205] See Recital 12 of the Directive.
[206] Supra n. 200, p. 15.
[207] 5062/01/EN/Final WP48, adopted on 13-09-2001, accessible at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf
[208] Ibid., p. 3.
[209] Ibid.
[210] C. Jones (Institute of Employment Rights), *Are British Bosses Turning to Big Brother?*, Guardian Saturday Review Pages, p. 2, 03-07-1999.

it is a given fact that even still there will, and there are, problems in this area[211].

5.2. E-mail and Internet Monitoring

The Article 29 Working Party has also published a paper relative to monitoring of e-mail and Internet use: *Working Document on Surveillance of Electronic Communications in the Workplace*[212], which is supposed to suggest specific measures and principles under which e-mail and Internet use may be monitored. It is striking that the introduction of the paper states: "[w]orkers do not abandon their right to privacy and data protection every morning at the doors of the workplace"[213] and goes on to underline that "[t]he human dignity of the worker overrides every other consideration"[214]. This statement clearly shutters the foundations of the belief that managerial prerogative is above all.

5.2.1. E-Mail Monitoring:

The Working Party firstly recapitulates the values of the ECourtHR as extracted by the case law that has already been examined[215]: (i) privacy rights are not overridden by the property rights of the employer (only with a consensual agreement the expectation for privacy might be limited); (ii) right to respect for the secrecy of communications is likely to cover e-mails and attached files; and (iii) human relationships developed in the workplace are, arguably, limiting the employers' right to monitor. Bearing in mind that the ECourtHR case law is applicable the Working Party underlines the principles that should characterise the possible surveillance of e-mails of employees[216].

(i) Necessity of interception, the issue here is whether the interception is absolutely necessary or the same result could be obtained with a less intrusive method of surveillance; (ii) finality, meaning that the data should be collected and processed for a specified, legal reason; (iii) transparency, which has three aspects: a. information

[211] E.g. employers will not consult with unions for surveillance issues: T. Wyatt, *Union Anger at 'Big Brother'*, Council UK Newsquest Regional Press - This is Bradford, 22-03-2004.
[212] 5401/01/EN/Final WP 55, adopted on 29-05-2002, accessible at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_en.pdf
[213] Ibid., p. 4.
[214] Ibid., p. 6.
[215] For the case law see supra ECourtHR Case Law; ibid., p. 9.
[216] Ibid., pp. 13-19.

given to the data subject (effectively this means that the company should have a known, cohesive and clear policy on e-mails), b. notification of relative authorities as defined by the duties of the data controller found in the 1995 Directive, and c. the data subjects should have unrestricted access to the data (emphasis added); (iv) legality, within the meaning of Article 7 of the Directive; (v) proportionality; (vi) accuracy and retention of data; and (vii) security.

The Working Party takes a view that can solve the queries and debates found in a big part of the academic literature (especially in connection with the *Halford*[217] case): "electronic communications made from business premises may be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8"[218]. Generally speaking, the views of the Working Party, when it comes to e-mail use, are the most liberal and pro employee possible, with a braveness that even trade unionists might not have expressed them. It should be noted that the Working Party suggests that two e-mail accounts should be given to employees; one for business and one for personal use[219]. This is a measure that only indirectly has been put forward by R. Blanpain[220]. Some companies already provide their employees with their own home Internet connection[221], why should not they give them a second e-mail account for personal use, as well?

On 15th March 2002 Ms Goudie was dismissed by the Royal Bank of Scotland on the grounds that she had misused the company's Internet policy, in fact she would send e-mails with pornographic material to her colleagues[222]. The complaint of the Bank was not related with the time she spent sending these e-mails but that she sent e-mails which fell foul of the company's Internet policy. It is always fair that an employer has a well regulated Internet policy, and that they would not like to be found liable for the employees' activities. On the other hand, it is a given practice that employees will exchange e-mails, and some of them might contain material which could be pornographic. If the company had provided Ms Goudie with an e-mail for

[217] Supra n. 185.
[218] Supra n. 212, p. 20.
[219] Ibid., p. 5.
[220] R. Blanpain, *Employment and Labour Law Aspects. Setting the Scene. Asking the Right Questions?*, in supra n. 18, pp. 38-43; even though he recognises that "[n]o-one would agree that on-line rights of workers means that every employee is entitled to surf and e-mail during working hours as he wishes", p. 43.
[221] T. Barber, *Siemens to Launch Euro 1bn Network. Digital Platform Plan to Speed Shift from Old Economy*, Financial Times, 11-10-2000.
[222] *The Royal Bank of Scotland v Goudie* 2004 WL 62015.

private use, she would not have been dismissed, the company would not have had to pay damages for unfair dismissal and most probably they would not even have to pay for a special matrix that filters all e-mails. This argument is not meant to suggest that employees should exchange e-mails with pornographic material, especially if they fall foul of obscenity or copyright laws; the aim is to save the two sides (employees-employers) from unnecessary frictions and possible expenses (see Appendix 2).

5.2.2. Internet Use Monitoring:

The argument suggested above for the use of e-mails seems that already becomes a trend about the use of Internet. The Working Party appears to have a reasonable position about that, as well: "…it should be emphasised that it is up to the company to decide if employees are to use Internet for personal reasons and the extent to which this is permissible"[223]. The employers know that 52% of the employees book holidays on the Internet at work; 41% perform research for hobbies; 28% go on shopping on-line; and 27% occupy themselves with sports; they also know that 60% of all on-line shopping takes place at work[224]. On the top of all these companies provide their employees with free subscription for porn web-sites[225] or they give free computers for home use, printers and Internet subscription[226]; on the top of all these, 90% of employees that use the Internet, agree that it is addictive.

All the above seem weird; the position of the Working Party, the figures about the use of Internet at work and then the reaction of the companies is to give free home-access-Internet to employees. The answer is simple: trust. Companies themselves have started realising that lawyers and disciplinary procedures do not boost productivity; happy employees do! Actually, this is evidenced by relative survey[227].

If employees spend time on the web watching sites with pornographic material[228] employers prefer to give them free access at home, so they can go on

[223] Supra n. 212, p. 24.
[224] All figures can be found at: http://news.bbc.co.uk/1/hi/business/1370956.stm
[225] Danish firm gives free porn to their employees: http://www.theregister.co.uk/2004/05/27/danish_free_porn/
[226] F. Warner, *Ford Motors Gives PC to All Employees*, The Wall Street Journal Europe, 4,5-02-2000.
[227] *The 1998 Workplace Employee Relationship Survey: First Findings*, accessible at: http://www.dti.gov.uk/er/emar/ffind.pdf
[228] *Parr v Derwentside District Council,* Newcastle-Upon-Tyne Employment Tribunal (23-09-98, Case No. 2501507/98); *Dunn v IBM UK Ltd*, (South) London Employment Tribunal (01-07-98, Case No.

working while at work. If employees want to browse the web, it is more lucrative for the companies to provide them with Internet at home, rather than having them browsing at work for non-business purposes. There is no reason why "staff [should] be treated like they are the company's greatest enemy"[229]: "trust is at the core of corporate values"[230]. The alternative is an aggressive policy towards the employees and costly filtering software[231].

So, since it has already been seen were the evolution of the market forces are leading in connection with the use of Internet at work, it would be useful to see the positions of the EU on the issue. The Article 29 Working Party generally suggests that Internet use is at the disposal of the employer. However, it is recognised that a blanket policy forbidding the use of Internet would not only be impractical, but unrealistic, as well[232]. Apart from the general principle of transparency (which is equally applicable for the use of e-mails) it is underlined that prevention should be preferred to detection[233]. Proportionality and cautiousness are also to be important principles. The employees should be notified about any specific policies or filtering software[234]. The principles of the 1995 Directive and of the Opinion 8/2001[235] are also applicable both to the e-mail and Internet use monitoring.

6.1. Is the Protection of Employees' Privacy Adequate? Are There Any Other Alternatives?

> "It is hoped that uncertainties which characterise the present position [regarding the law in the UK,] will be redressed so that both employers and their workers will have a clearer picture of the boundaries of legitimate conduct"[236].

2305087/97); *Humphries v V.H. Barnett & Co (a firm)*, (South) London Employment Tribunal (10-07-98, Case No. 2304001/97); are just very few of the cases that visiting web-sites with pornographic material ended up to dismissal.

[229] Peter Skyte MSF Union, supra n. 224.

[230] Prof. M. Kets de Vries, *Beyond Sloan: Trust Is at the Core of Corporate Values*, Financial Times, 02-10-2000.

[231] It should be added however, that for every 2,000 employees there is one who uses company IT infrastructure to run his own business, P. Rutherford, spokesman of the filtering firm Clearswift: http://news.bbc.co.uk/1/hi/technology/2984922.stm

[232] Supra n. 212, p. 24.

[233] Ibid.

[234] Ibid.

[235] Supra n. 207.

[236] G. Morris, *English Law*, in supra n. 18, p. 146.

Even though the human need for privacy is as old as the formation of societies, the legal framework for its protection in the workplace dates back only a few years. The traditional concept of 'master and servant' as found in cases like *Turner v Mason*[237] has definitely become obsolete[238], but this does not mean that the values of privacy-related-labour law have been absorbed. The employers only recently started realising that the duty of co-operation[239], considered to be implied in a British contract of employment, is meant to go both ways. Moreover, only relatively recently, "[companies] discovered that government still has authority, even in the new economy"[240]. Therefore, this new legislation needs time for its effectiveness to be assessed[241].

Generally speaking, the legislation and the case law seem to be satisfactory. This does not mean that possible problems are not meant to come out. The data protection rights of job applicants[242], or their right to privacy[243] [244], as well as the right of privacy of employees who have to through drug tests[245], or their data protection rights[246], even the rights to privacy of cross dressers[247] and the rights to privacy of homosexuals[248] (the two last cases have to do with other pieces of legislation, as

[237] [1845] 14 M&W 112.
[238] For the contemporary application of the idea see Lord Steyn in *Malik v BCCI* [1998] AC 20.
[239] *Secretary of State for Employment v Associated Society for Locomotive Engineers and Firemen (No 2)* [1972] 2 QB 455.
[240] V. Haufler, *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*, (Washington, CEIP, 2001), p. 100.
[241] It is noteworthy that the *Codes of Practice* of the Information Commissioner (revised, so as to include the latest European legislation) were only published in June 2004: http://www.informationcommissioner.gov.uk/eventual.aspx?pg=SR&cID=446
[242] For relative guidance see: Information Commissioner, *Codes of Practice: The Employment Practices Data Protection Code, Part 1*, pp. 18-37; accessible at: http://www.informationcommissioner.gov.uk/cms/DocumentUploads/The%20Employment%20Practices%20Data%20Protection%20Code%20Part%201%20Recruitment%20and%20Selection.pdf
[243] See *Vogt v Germany* (1996) 21 EHRR 205, para 44.
[244] For an academic perspective: supra n. 187, pp. 56-57; see also Sir G. Lightman and J. Bowers, *The Incorporation of the ECHR and Its Impact on Employment Law*, (1998) EHRLR 560, footnote 28: "[j]ob candidates in the private sector appear wholly unprotected…", even though it should be considered outdated.
[245] See *X v Commission of the European Communities* [1995] IRLR 320 ECJ (a covert HIV test was foul of Article 8 of the ECHR), and for relative guidance see *UK Laboratory Guidelines for Legally Defensible Workplace Drug Testing*, accessible at: http://www.wdtforum.org.uk/pdfs/wdtgde~1.pdf
[246] For relative guidance see: Information Commissioner, *Codes of Practice: The Employment Practices Data Protection Code, Part 4: Information about Workers' Health*, pp. 22-26; the guidance includes genetic testing and blood types, accessible at: http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Part%204%20-%20v0.9a.pdf
[247] *Kara v United Kingdom* [1999] EHRLR 232.
[248] *Smith and Grady v United Kingdom* [1999] IRLR 734.

well[249]); and finally, the question whether the ECourtHR jurisdiction is applicable to the private sector and relevant implications[250].

The existing privacy related legislation is far from being impeccable; nevertheless, it must be credited that European legal authorities are doing a lot in regards to the protection of the workers' privacy. However, there are alternative ways for regulating the right to privacy or data protection issues, apart from the ECHR and EU legislation.

6.2.1. The ILO

The International Labour Organisation was established with the treaty of Versailles (28-06-1919) and was re-established after World War II in 1946 under the general prism of re-establishing the United Nations (up to then League of Nations)[251]. The ILO is treaty based, i.e. it produces treaties that once ratified by the signatory states, they are incorporated into the national legal system and they become actionable at national courts. The signatory states themselves have the responsibility for the enforcement of the legislation; the ILO investigates specific complaints and requests for specific reports in connection with the implementation. However, it is not a body like the EU with its own Court and jurisprudence. "The ILO model rests on what we might call a 'conventional' state-centric model of international governance"[252], under the trend of most international organisations it does not interfere with national sovereignty issues[253]. Additionally, it should be noted that in the '80s and the '90s British trade unions preferred to pursue their grievances in the ILO, rather than in the ECourtHR[254].

The ILO Code of Practice on Workers' Protection of Personal Data (1997) is referenced as international data protection law by the Working Party in two occasions:

---

[249] Employment Equality (Sexual Orientation) Regulations 2003 SI 2003/1661, Sex Discrimination (Gender Reassignment) Regulations 1999 SI 1999/1102.
[250] G. Morris, *The Human Rights Act and the Public/Private Divide in Employment Law*, [1998] 27 ILJ 293; Sir S. Sedley, *Public Law and Contractual Employment*, [1994] 23 ILJ 201; and Sir J. Laws, *Public Law and Employment Law: An Abuse of Power*, [1997] PL 455.
[251] I. Hurd, *Labour Standards through International Organisations: The Global Compact in Comparative Perspective*, Journal of Corporate Citizenship, September 2003 No 11, 99.
[252] Ibid.
[253] Unlike the EU and, arguably the WTO.
[254] Supra n. 244, p. 568.

the Opinion 8/2001[255] and the Working Document on Surveillance of Electronic Communications in the Workplace[256].

"5. General Principles

5.1. Personal data should be processed lawfully and fairly, and only for several reasons directly relevant to the employment of the worker.
5.2. Personal data should, in principle, be used only for the purposes for which they were originally collected.
5.3. If personal data are to be processed for purposes other than those which they were collected, the employer should ensure that they are not used in a manner which is incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretation caused by a change of context.
5.4. Personal data collected in connection with technical or organisational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.
5.5. Decisions concerning a worker should no be based solely on the automated processing of that worker's personal data.
5.6. Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance(…)
6.14.
(1) If workers are monitored, they should be informed in advance of the reasons for monitoring, the time schedule, the method and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers.
(2) Secret monitoring should be permitted only:
a) if it is in conformity with national legislation or
b) if there is suspicion on reasonable grounds of criminal activity
or other serious wrongdoing
(3) Continuous monitoring should be permitted only if requires for health and safety or the protection of property (…)

12.2 The workers' representatives, where they exist, and in conformity with national law and practice, should be informed and consulted:
a) concerning the introduction or modification of automated systems that process worker's personal data,
b) before the introduction of any electronic monitoring of workers' behaviour in the workplace
c) about the purpose, contents and the manner of administering and interpreting any questionnaires and tests concerning the personal data of workers."

All these principles are more or less familiar with those formulated by the 1995 Directive, and additionally they cover both the private and public sector. The ILO Code of Conduct provides an adequate level of protection but lacks enforcement powers. On the contrary, the EU relevant regulatory framework, not only has a Court

[255] Supra n. 207.
[256] Supra n. 212.

where relevant violations can be adjudicated, it also has obtained the international profile of the ILO legislation[257] [258].

6.2.2. Industry Regulation

A country that traditionally regulates data protection with industry regulation is the USA. For a European studying workers' privacy, it might be difficult to follow the combined character of the regulations in the USA:

> "[t]he United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin"[259].

An insight would be more than helpful to understand the attitude towards data protection at the other side of the Atlantic[260]:

> "[T]his bill places unnecessary and complicating obligations on employers and may be likely to lead to litigation by affected employees over whether the required notice was provided and whether it was read and understood by the employee. I support reasonable privacy protections for employees in the workplace, but not at the price of undue regulatory burdens and potential legal exposure to business for doing what any employee should assume in the employer's right when they expect employment"[261].

This is the concept of some legislators for the workers' right to privacy. It is more or less parallel to the dual aim of the 1995 Directive: we want workers' privacy but not to the expense of business efficiency. However, there is a fundamental

---

[257] E. U. Petersmann, *European and International Constitutional Law: Time for Promoting 'Cosmopolitan Democracy' in the WTO*, in G. de Búrca and J. Scott, *The EU and WTO: Legal and Constitutional Issues*, (Oxford, Hart Pub., 2001), pp. 95-96: the EU diffuses its constitutional values with the countries that has any kind of relationships. See also the 'Safe Harbor' (accessible at: http://www.export.gov/safeharbor/) agreement between the EU and the USA.

[258] It is remarkable however, how an organisation like the ILO that supports workers rights, does not have an on-line accessible document of these rights. If an employee wants to learn about the rights that ILO suggests, they can only *buy* the ILO magazine that refers to workers' privacy rights or workers' data protection rights (probably the right to access to information is not yet in the agenda of the ILO).

[259] Introduction to the Safe Harbor: http://www.export.gov/safeharbor/index.html

[260] For the situation of workers' rights in connection with data protection in the USA see Appendix 3.

[261] Message of Gov. G. Davis vetoing SB No 1822 (30-09-2000), quoted in M. Finkin, *United States Law*, in supra n. 18, p. 249.

difference; the Working Party has come to endorse the values of the ECHR and of the relevant case law[262].

The main kinds of policies of self industry regulation can be summed up in the followings: (i) 'official use only' principle, combined with no restraint on the employers' right to access/disclosure; (ii) accessibility for any legitimate business purpose (by the employer); (iii) emphasis on employees' privacy with employers having the right to access on a case-by-case basis; and (iv) rules on types of access and disclosure by the employer with additional notice/approval by the employees[263].

The continuous pressing of American NGOs for stronger state regulation on e-privacy[264] and the direct doubting of the EU towards US standards of privacy at work create scepticism about the quality of industry regulation. Additionally, industry regulation is created by companies which are not willing to impose unnecessary burdens on themselves. This practically means that such regulation will comply with the minimum protection of the employees and the maximum protection of the companies[265], compromising thus values that, in theory at least, are not to be compromised.

6.3. Other Alternatives

6.3.1. The WTO:

There are other international bodies besides the ILO that would be willing to take over labour issues. For example the World Trade Organisation (WTO), probably in an attempt to calm down its innumerable critics, has timidly suggested that labour issues might come into the agenda[266]. However, it is recognised that it is highly controversial and the truly responsible body is the ILO. The WTO even though it is a trade organisation, and in no way specialised in labour issues, it does have high

[262] For the US equivalent of *Niemietz* (supra n. 167) see *O'Connor v Ortega* 480 US 709 (1987); the limit of protection for workers' privacy followed the general principle of reasonableness: "an expectation of privacy that the society is prepared to consider reasonable", p. 715.
[263] Supra n. 261, p. 248.
[264] Supra n. 240, p. 90.
[265] For the equivalent in consumers' privacy protection see J. Heilemann, *The Truth, the Whole Truth and Nothing but the Truth: The Untold Story of the Microsoft Antitrust Case*, Wired Vol. 8 No. II pp. 260-321.
[266] M. Matsushita, T. Schoenbaum and P. Mavroidis, *The World Trade Organization: Law, Practice and Policy*, (Oxford, OUP, 2003), pp.602-604.

enforcement abilities[267] and it is highly authoritative and influential[268]. However, its members in 1996 did promise to recognise some "core labour standards"[269], which most probably will not have to do with the workers' privacy but with more basic issues related to trade.

6.3.2. The ISO:

It has been academically suggested that possibly the International Standards Organisation could expand its powers by granting certificates for labour standards[270]. The ISO produces certificates on standards on a variety of different products and services. But lately it

> "has broadened its scope with forays into the area of 'quality' broadly defined (the ISO 9000 initiative) and of environmental standards (ISO 14000). With these steps … its work has steadily shifted into the public eye and into the kinds of issue normally associated with corporate codes of conduct"[271].

The shift into labour issues, however, still seems dramatic and there are many practical problems to be faced[272]. It is truthful that "[s]tandards make an enormous contribution to most aspects of our lives"[273], and it should not be a surprise if in some years' time ISO came into labour issues, as well. However, generally speaking, these issues remain in the hands of bodies that have some sort of political decision-making character.

6.3.3. The European Constitution:

The idea of a European Constitution that for too long had been a nice dream lately has started taking flesh and bones. In early summer 2004 the political leaders of

---

[267] "The WTO's sharpest teeth are its dispute settlement body and its cross-retaliation provisions, both of which enable it to force nations to comply with WTO rules": B. Balanya [et al.], *Europe Inc: Regional and Global Restructuring and the Rise of Corporate Power*, (London, Pluto Press in association with Corporate Europe Observatory, 2000), p. 124.
[268] G. de Búrca and J. Scott, *The Impact of the WTO on the EU Decision-making*, in G. de Búrca and J. Scott supra n. 257, pp. 1-30.
[269] http://www.wto.org/english/thewto_e/whatis_e/tif_e/bey5_e.htm
[270] Supra n. 251.
[271] Ibid.
[272] National sovereignty surely being one amongst them.
[273] http://www.iso.org/iso/en/aboutiso/introduction/index.html

Europe came up with a Draft Treaty Establishing a Constitution for Europe[274]. The argument put forward here is that if the right to privacy is constitutionally recognised in Europe then this particular right will have the catholic treatment that it has in Germany[275]. Accordingly, the right to privacy shall become a prerequisite into the European labour law and not an added extra that causes academic debates and puzzles to jurists because they cannot define it.

7. Why Do We Want a Right to Privacy in the Workplace?

One of the arguments that is constantly being put forward by the employers is that the infrastructure and operational cost of data protection is too high. Actually, only for the UK it is estimated that the starting cost for the first year for the private sector will would be around £ 863 million and the recurring cost around £ 630 million[276]. On the other hand, companies in the UK do evade taxes, and apparently this costs the British government £ 18 billion a year[277]. In this case it seems that there is more cash than necessary to cover the costs of data protection.

It has already been suggested that a new principle is crawling into the workplace: trust. It is high time that the employers of Europe realised that the times of the big social clashes are done away with. However, tension in the workplace is more than inevitable: employers will always ask that the employees will work as much as possible for as little payment as possible, and employees will always ask to be paid as much as possible for the smallest possible amount of work.

The EU had to force the employers to accept the concept of consultation within the limits of their managerial prerogative[278], the French government just went further on passing a law on life long vocational training and social dialogue[279], whilst the British government just published the regulations that they will be implementing

[274] http://european-convention.eu.int/docs/Treaty/cv00850.en03.pdf
[275] See above Comment on the *Klass* case, pp. 28-29.
[276] Supra n. 47, p. 61.
[277] G. Duncan, *International Tax Task Force to Be Set up*, The Times, Saturday 24-04-2004.
[278] For a quite general appreciation of the issue see H. Collins, *Market Power, Bureaucratic Power and the Contract of Employment*, [1986] 15 ILJ 1, p. 4, for a practical application see Council Directive 94/45/EC OJ L254 , 30.09.1994 p. 64 on the Establishment of a European Works Council or a Procedure in Community-scale Undertakings and Community-scale Groups of Undertakings for the Purposes of Informing and Consulting Employees.
[279] European Labour Law Bulletin, Issue of July/August 2004, p. 1., accessible at http://www.freshfields.com/practice/epb/publications/newsletters/labourlaw/9052.pdf

the 2002/14/EC Directive[280] concerning the informing and consulting of employees[281]. Practically speaking the concept of managerial prerogative is being shattered. It is time that employees and employers actually co-operate and share, partially, the same rights in the workplace; and as employers enjoy their right to privacy, employees are to enjoy it too. Good employees and bad employees will always exist, and monitoring in the workplace will never stop, but in the meantime the majority of the employees should have the freedom to enjoy it. And any one is entitled to ask: why?

Because "[m]an is an end. [E]very rational being exists as an end in himself. Whatever he may do, involving only himself or other rational beings, he must always be valued as an end, not merely as means to be used at the whim of this or that will"[282], because man's value does not rest solely on our desires[283]; because "only morality and humanity … have dignity. Skill and hard work have a market value … [b]ut keeping one's promises and helping others … have inherent values"[284]. Because the supreme law is this: "always act on a maxim which you can at the same time will to be a universal law"[285].

Privacy is more important if one thinks that "…there is no injustice in the greater benefits earned by a few provided that the situation of persons not so fortunate is thereby improved"[286]. The never ending debates about human rights are always applicable. Do rights go one way only? No; rights entail duties, and should not be seen cut off from them[287]. The right to privacy, as seen already, is part of the general right to personality. And one person in order to be able to develop their personality free from arbitrary powers they should be given some free space and some free time. The right to privacy is not a new whim of the employees so that they can produce less work; it is the proof for respect to the human dignity.

---

[280] On *Establishing a General Framework for Informing and Consulting Employees in the European Community*, OJ L80, 23.03.2002, p. 29.
[281] Supra n. 280, p. 2.
[282] B. E. A. Lidell (translation and commentary), *Kant on the Foundation of Morality (a Modern Version of the Grundlegung)*, (Bloomington, & London, IUP, 1970), p. 155.
[283] Ibid.
[284] Ibid., p. 173.
[285] Ibid., p. 180.
[286] J. Rawls, *A Theory of Justice*, (Oxford, OUP, 1999), p. 13.
[287] See J. Finnis, *Natural Law and Natural Rights*, (Oxford, OUP, 1982), pp.197-202; Sir J. Laws, *The Limits of Human Rights*, (1998) PL 254.

Bentham many years ago had come up with the idea of the *Panopticon*[288]. The Panopticon would be a monitoring device: a cylinder built out of glass; the cylinder, in the middle, would have another cylinder, built out of bricks but would have many openings and windows with shades so that the people from the inner building could see those in the outer one but the people from the outer building could not see those in the inner one. Additionally, a system of pipes would transmit all sounds from the outer building to the inner one. Bentham, even though he would not have imagined that, could work as an industrial architect or interior designer nowadays. M. Foucault talking about Bentham's device and commenting on the idea of discipline has written: "[i]s it surprising that prisons resemble factories, schools, barracks, hospitals, that all resemble prisons?"[289]

Monitoring and surveillance in modern workplaces have far reaching effects, and it is simplistic to say that they just form part of the managerial prerogative. Foucault comments about the *Panopticon* again:

> "it makes it possible to perfect the exercise of power. It does this in several ways: because it can reduce the number of those who exercise it, while increasing the number of those on whom it is exercised … it gives power of mind over mind"[290].

Furthermore, psychologists Dr Babiak and Professor Hare warn that many psychopaths manage to come up to managerial positions, and this is due to the structure of contemporary societies and companies[291].

The aforementioned issues, inevitably, involve the concept of legal and moral norms. Sometimes it is the deriving of a 'must' from an 'ought to' that makes the difference[292]: the legislators do not 'have to', strictly speaking, protect the workers' right to privacy; however, "legal norms based on moral reasons gain a supreme position"[293]. Morality underlines legality. This is part of the ancient clash of moral norms with legal norms, manifestly put in Sophocles' *Antigone*. There is no clear

---

[288] J. Bentham (edited and introduced by M. Bozovic), *The Panopticon Writings*, (London, Verso 1995).
[289] M. Foucault (translated by A. Sheridan), *Discipline and Punish: The Birth of the Prison*, (London, Penguin, 1977), p. 228.
[290] Ibid., p. 206.
[291] Three links of the BBC analysing the survey and interviewing the psychologists: http://news.bbc.co.uk/1/hi/health/3579402.stm; http://news.bbc.co.uk/1/hi/wales/3395443.stm; and http://news.bbc.co.uk/1/hi/business/3392233.stm.
[292] See generally M. D. A. Freeman, *Introduction to Jurisprudence*, (London, Sweet & Maxwell, 2001), pp. 96-103.
[293] A. R. Oquendo, *Deliberative Democracy in Habernas and Nino*, OJLS 2002.22(189).

answer to the question which of the two norms should fully prevail. The aim is to achieve a balance between the two[294]. What is suggested in this paper is that this balance, as far the workers' right to privacy is concerned, is to be struck with co-operation.

The history of Europe is more troubled than it looks like nowadays. In the late '60s, when legislation about data protection started emerging, southern Europe was under dictatorships (Spain, Portugal and Greece, without mentioning countries under the Soviet influence); whilst northern Europe was either going[295] or was soon meant to go[296] through social agitation. In Greece up to the '70s if an individual was to be employed he had to present the Social Beliefs Certificate, signed by the police, mentioning that he did not belong to trade unions and that his political beliefs were 'patriotic' and people who were unlucky enough to have a member of their family in the, illegal, Communist party, could never work in the public sector.

The EU and the ECourtHR are building stable foundations for democracy and this inevitably has to go through the workplace. Data protection law and the right to privacy protect the integrity of the worker and there is nothing wrong about that, nor should these values be compromised.

[294] D. D. Raphael, *Problems of Political Philosophy*, (Hampshire, Palgrave, 1990), pp. 118-119.
[295] Riots of the 1968 May in France; the RAF and Brigadi Rossi in Germany and Italy respectively, were at full power.
[296] The 1980s social reforms in the UK.

APPENDICES

Appendix 1

The Diffusion of Data Protection Legislation by Region

	1970s	1980s	1990s
W. Europe	Sweden (1973) W. Germany (1978) Denmark (1978) Austria (1978) France (1978) Norway (1978) Luxembourg (1978)	Iceland (1981) UK (1984) Finland (1987) Ireland (1988) Netherlands (1988)	Portugal (1991) Spain (1992) Switzerland (1992) Belgium (1992) Monaco (1993) Italy (1996) Greece (1997)
E. & C. Europe			Slovenia (1990) Hungary (1992) Czech Rep. (1992) Russia (1995) Estonia (1996) Lithuania (1996) Poland (1997) Slovak Rep. (1998) Latvia (2000)
N. America	United States (1974)	Canada (1982)	
S. America			Chile (1999) Argentina (2000)
Australasia		New Zealand (1982) Australia (1988)	
Middle East and Asia		Israel (1981) Japan (1988)	S. Korea (1994) Hong Kong (1995) Taiwan (1995) Thailand (1998)

Source:
http://www.essex.ac.uk/RCPR/events/jointsessions/paperactive/edinburgh/ws11/RaabBennett.pdf

Appendix 2

Model Company's Policy on Privacy in the Use of the Internet and E-mail

The undersigned:
1. ..... (fill in the name of the company),
having its registered office at ……, being the employer, hereby represented by
Mr/Mrs/Ms.....,
management,

and

2. The works council of . (fill in the name of the company), hereby represented by
Mr/Mrs/Ms……....., chairperson of the works council.

Purpose of the agreements

The protocol contains agreements about the way in which the company addresses aspects such as registration, collection and monitoring of data concerning use of e-mail and the Internet that can be traced back to an individual. The aim of the protocol is to find the right balance between responsible use of the Internet and e-mail and protection of the employees' privacy in the workplace.

Article 1. *General assumptions*

1. Data that can be traced back to an individual shall not be registered, collected, checked, combined or adapted in a different way from that agreed in this protocol.
2. Personal data shall only be used for the purpose for which they have been collected.
3. Registration of data that can be traced back to an, individual shall be kept to a minimum. In this respect, the objective is to achieve maximum protection of employees' privacy in the workplace.

Article 2. *Use of e-mail*

1. Employees are authorized to use the e-mail system for non-commercial transactions in order to send and receive personal e-mail messages, both internally'; and externally, provided that this does not interfere with their day-to-day work commitments.
2. The following conditions apply to the employee's right to send and receive personal e-mail messages:

- the e-mail must contain a disclaimer,
- it is not permitted to send threatening, sexist or racist messages.
-…….
-…….

3. The employer shall not read the content of either personal or commercial e-mail messages. Neither shall personal data with regard to number of e-mails, e-mail addresses or other relevant data be registered and/or checked. This does not affect his right to carry out occasional checks based on compelling reason that are in the interest of the company. Such checks shall be reported to the works council.

Article 3. *Use of the Internet*

1. Employees are authorized to use the Internet system for non-commercial: transactions, provided that this does not interfere with their day-to-day work commitments.
2. It shall not be permitted deliberately to consult sites that contain pornographic or racist matter.
3. The employer shall not register and/or check on personal data concerning use of the Internet, such as the time spent browsing and the sites that are visited. This does not affect his right to carry out occasional checks based on compelling reasons that are in the interest of the company. Such checks shall be reported to the works council.

Article 4. *Employees' rights*

1. Right of inspection: employees have the right to inspect any data registered about them. Requests for inspection shall be granted within four weeks.
2. Right of copy: employees are entitled to a copy of the data registered about them within four weeks following their request.
3. Right of correction: employees have the right to correct factually incorrect details in the data registered, to have them corrected or to add to them. Decisions about requests for correction or addition shall be taken within four weeks. The corrections shall be carried out immediately if a request for correction or addition is granted.
4. Right of removal: employees have the right to remove and destroy data registered about them that are not or no longer relevant, or that are in breach of the protocol or any statutory regulations. A decision about a request for removal and destruction shall be taken within four weeks. Removal and destruction shall be carried out immediately if such a request is granted.

Article 5. *Complaints procedure*

If the employee feels that he has been treated unfairly with regard to his rights under this protocol, he can submit an appeal to the works council. The company shall subsequently appoint an appeals committee, which shall consist of an employer's and an employees' representative.

1. This protocol is an agreement Art 32, para 2, of the Dutch Works Council and the management shall sent a copy of it to the Bedrijfcommissie (=appeals committee).
2. This protocol shall not affect the work council's powers or provisions that ensue from the Act, the collective agreement or any other regulations in force.
3. The employer and the works council shall be able to amend this protocol by mutual agreement. Adaptations or amendments shall be laid down in writing, signed and sent to the Bedrijfcommissie.

Agreed and signed by,

Date:……..
At:…….

Employer:	Chairperson works council:
……..	……

Explanatory Notes:

Article 1.1

It is possible to speak of personal data if the person linked to the information, in all fairness, can be identified. The fact that the name of the person in question is not linked to the details is not always important. An employee can be traced by through, for example, a personal identification number or a login name.

Article 2.2 and Article 3.2

Personal use of the Internet and e-mail can be made subject to certain conditions. The employer can shorten or extend the list of conditions in consultation with the works council.

Article 2.3 and 3.3

Secret observation shall be permitted on occasion. In this case there must be good reason to suspect or presume that an offence or wrongful act has been committed by one or more employees, which would justify such action. All other remedies must have been tried and the interest of the company should be seriously at stake. Furthermore, company employees should be aware that, in exceptional cases, computer use will be monitored and that specified types of behaviour will not be tolerated.

Article 4

These rights ensue from the Dutch Data Protection Act.

This is a model Internet and e-mail policy suggested by FNV Bondgenoten, the biggest Dutch trade union.

Source: R. Blanpain (ed.), *On-line Rights for Employees in the Information Society*, (London, Kluwer Law International, 2002), pp. 122-124.

Appendix 3

Computer Surveillance: Internet Connections Monitored (a 2000 US survey)	
Any such practice	54.1%
All employees	42.2%
Selected categories	11.9%
Ongoing	12.6%
Occasional	19.2%
Routine	9.2%
Specified	11.6%
Electronic Mail: Messages Stored and Reviewed (a 2000 US survey)	
Any such practice	38.1%
All employees	32.3%
Selected categories	5.8%
Ongoing	6.8%
Occasional	13.5%
Routine	4.6%
Specified	13.9%
Computer Surveillance: Files Stored and Reviewed (a 2000 US survey)	
Any such practice	30.8%
All employees	23.4%
Selected categories	7.4%
Ongoing	5.5%
Occasional	11.2%
Routine	4.1%
Specified	10.7%

Source: R. Blanpain (ed.), *On-line Rights for Employees in the Information Society*, (London, Kluwer Law International, 2002), pp.

REFERENCES - BIBLIOGRAPHY

Books:

- A. Westin, *Privacy and Freedom*, (London, Bodley Head, 1967).
- D. Harris and S. Joseph (eds.), *The International Covenant on Civil and Political Rights and United Kingdom Law*, (London, Clarendon Press, 1995).
- A. R. Miller, *Assault on Privacy: Computers, Data Banks and Dossiers*, (Michigan, MichiganUP, 1971).
- J. Michael, *Privacy and Human Rights: An International and Comparative Study, With Special References to Developments in Information Technology*, (Dartmouth: UNESCO Pub., Aldershot: Paris, 1994).
- A. H. Robertson (ed.), *Privacy and Human Rights*, (Manchester, MUP, 1973).
- D. Banisar, *Privacy and Human Rights 2000: An International Survey of Privacy Laws and Developments*, (London, Privacy International, 2000).
- R. Blanpain (ed.), *On-line Rights for Employees in the Information Society*, (London, Kluwer Law International, 2002).
- B. Markesinis (ed.), *The Impact of the Human Rights Bill on English Law*, (Oxford, OUP, 1998).
- D. Lasok and J. W. Bridge, *Law and Institutions of the European Communities,* (London, Butterworths, 1991).
- L. Heffernan and J. Kingston (eds.), *Human Rights, A European Perspective*, (Dublin, Round Hall Press in association with Irish Centre for European Law, 1994).
- D. J. Harris, M. O'Boyle and C. Warbrick, *Law of the European Convention on Human Rights*, (London, Butterworths, 1995).
- I. J. Lloyd, *Information Technology Law*, (London, Butterworths, 2000).
- C. Reed and J. Angel (eds.), *Computer Law*, (Oxford, OUP, 2003).
- C. Reed, *Internet Law: Text and Materials*, (London, Butterworths, 2000).
- R. Jay and A. Hamilton, *Data Protection: Law and Practice*, (London, Sweet & Maxwell, 1999).
- R. Jay and A. Hamilton, *Data Protection: Law and Practice*, (London, Sweet & Maxwell, 2003).
- W. Dutton (et al.), *Cyberculture: The Key Concepts*, (Routledge, 2002).
- L. Betten and N. Grief, *EU Law and Human Rights*, (London, Longman, 1998).
- A. Hunt (ed.), *Reading Dworkin Critically*, (NY/Oxford, Berg, 1992).
- R. Dworkin, *A Bill of Rights for Britain*, (London, Chatto & Windus, 1990).
- I. Harden and N. Lewis, *The Noble Lie: The British Constitution and the Rule of Law*, (London, Hutchinson, 1986).
- K. A. Ewing and C. A. Gearty, *Freedom Under Thatcher: Civil Liberties in Modern Britain*, (Oxford, Clarendon Press, 1990).
- F. Nietzsche, *Thus Spoke Zarathustra*, translated by T. Common, http://www.eserver.org/philosophy/nietzsche-zarathustra.txt.

- S. Singleton, *E-Commerce: A Practical Guide to the Law*, (Aldershot, Gower, 2001).
- K. D. Ewing (ed.), *Human Rights at Work*, (London, Institute of Employment Rights, 2000).
- V. Haufler, *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*, (Washington, CEIP, 2001).
- G. de Búrca and J. Scott, *The EU and WTO: Legal and Constitutional Issues*, (Oxford, Hart Pub., 2001).
- M. Matsushita, T. Schoenbaum and P. Mavroidis, *The World Trade Organization: Law, Practice and Policy*, (Oxford, OUP, 2003).
- B. Balanya [et al.], *Europe Inc: Regional and Global Restructuring and the Rise of Corporate Power*, (London, Pluto Press in association with Corporate Europe Observatory, 2000).
- B. E. A. Lidell (translation and commentary), *Kant on the Foundation of Morality (a Modern Version of the Grundlegung)*, (Bloomington, & London, IUP, 1970).
- J. Rawls, *A Theory of Justice*, (Oxford, OUP, 1999).
- J. Finnis, *Natural Law and Natural Rights*, (Oxford, OUP, 1982).
- J. Bentham (edited and introduced by M. Bozovic), *The Panopticon Writings*, (London, Verso, 1995).
- M. Foucault (translated by A. Sheridan), *Discipline and Punish: The Birth of the Prison*, (London, Penguin, 1977).
- S. Deakin and G. S. Morris, *Labour Law*, (London, Butterworths, 2001).
- S. D. Anderman, Labour Law, *Management Decisions and Workers' Rights*, (London, Butterworths, 2000).
- P. de Cruz, *Comparative Law in a Changing World*, (London, Cavendish Pub., 1999).
- J.-M. Servais, *Inviolability of the Trade Union Premises and Communications*, (Geneva, ILO, 1980).
- N. Humphreys, *Trade Union Law*, (London, Blackstone, 1999).
- IDS, *Trade Unions*, (London, Employment Law Handbook, 2000).
- S. Singleton, *E-Commerce: A Practical Guide to the Law*, (Aldershot, Gower, 2003).
- A. C. Neal, *Fundamental Social Rights at Work in the European Community*, (Aldershot, Dartmouth, 1999).
- R. Blanpain, *European Labour Law*, (London, Kluwer Law Int., 2000).
- P. van Dijk and G. J. H. van Hoof, *Theory and Practice of the European Convention on Human Rights*, (Deventen, Kluwer Law and Taxation Pub., 1990).
- I. Brownlie, *Basic Documents in International Law*, (Oxford, Clarendon Press, 1995).
- D. D. Raphael, *Problems of Political Philosophy*, (Hampshire, Palgrave, 1990).
- M. D. A. Freeman, *Introduction to Jurisprudence*, (London, Sweet & Maxwell, 2001).
- T. Campbell, *Justice*, (Hampshire, Macmillan Press, 2001).

Articles and Journals:

- S. D. Warren and L. D. Brandeis, *The Right to Privacy*, (1890) 4 HarvardLR 193.
- C. Fried, *Privacy*, (1968) YaleLJ 480.
- L. Snider, *Theft of Time: Disciplining Through Science and Law,* [2002] 40 Osgoode Hall LJ 89.
- L. B. Sohn, *The Universal Declaration of Human Rights*, (1968) Journal of the International Commission of Jurists, Special Issue.
- M. Foutouchos, *ECHR Case Law and Data Protection: Developing and Completing*, 2nd Term Essay for LW 656, Essex University, 2004.
- F. C. Mayer, *Europe and the Internet: The Old World and the New Medium*, EJIL 2000 11(149).
- R. Massey and K. Tauber, *Privacy and Personality, Politicians and Stars*, E-Law 1.2(5).
- A. Utley, *Pilot Angry at Terror Slur*, The Times Higher Education Supplement, 28-11-2003.
- R. Badinter, *A European Constitution: Perspectives of a French Delegate to the Convention*, IJCL ICon 1.2(363).
- Y. Benkler, *Internet Regulation: A Case Study in the Problem of Unilateralism*, EJIL 2000 11(171).
- R. Smith, *One Charter for All?*, Law Society Gazette, Vol 100, No 48, p. 11, 19-12-2003.
- E. U. Petersmann, *Proposals for a New Constitution for the EU*, (1995) 32 CMLR 11 23.
- M. W. Finkin, *Information Technology and Workers' Privacy: Part IV: The Comparative Historical and Philosophical Context: Menschebild: The Conception of the Employee as a Person in Western Law*, 23 CompLabL&Pol'yJ 577.
- Δ. Χαριτόπουλος, *Μοντέρνες Δουλειές*, Τα Νέα, 07-12-2002 (D. Charitopoulos, *Modern Jobs*, Ta Nea).
- K. D. Ewing, *The Human Rights Act and Labour Law*, (1998) 27 ILJ 275.
- N. Taylor, *Policing, Privacy and Proportionality*, (2003 Special Issue: Privacy) EHRLR 86.
- J. Duffy, *Cig Brother*, Daily Record, 16-01-2001.
- A. McColgan, *Do Privacy Rights Disappear in the Workplace?*, (2003 Special Issue: Privacy) EHRLR 120.
- M. Ford, *Two Conceptions of Workers Privacy*, [2001] IJL 135.
- G. Morris, *Fundamental Rights: Exclusion by Agreement*, [2001] 30 ILJ 49.
- A. Westin, *Privacy in the Workplace: How well Does American Law Reflect American Values?*, (1996) 72 Chi-KentLR 271.
- M. Ford, *Surveillance and Privacy at Work*, http://www.ier.org.uk/pr_ford.htm.
- H. Oliver*, Email and Internet Monitoring in the Workplace: Information Privacy and Contracting Out*, [2002] 31 IJL 321.

- M. Jeffery, *Information Technology and Workers' Privacy: A Comparative Study: Part II: National Studies: The English Law*, 23 CompLabL&Pol'yJ 301.
- M. Finkin, *Employer Monitoring of Employee Electronic Mail and Internet Use*, (1999) 72 Chi-KentLR 221.
- C. Jones (Institute of Employment Rights), *Are British Bosses Turning to Big Brother?*, Guardian Saturday Review Pages, p. 2, 03-07-1999.
- T. Wyatt, *Union Anger at 'Big Brother'*, Council UK Newsquest Regional Press - This is Bradford, 22-03-2004.
- T. Barber, *Siemens to Launch Euro 1bn Network. Digital Platform Plan to Speed Shift from Old Economy*, Financial Times, 11-10-2000.
- F. Warner, *Ford Motors Gives PC to All Employees*, The Wall Street Journal Europe, 4,5-02-2000.
- Prof. M. Kets de Vries, *Beyond Sloan: Trust Is at the Core of Corporate Values*, Financial Times, 02-10-2000.
- Sir G. Lightman and J. Bowers, *The Incorporation of the ECHR and Its Impact on Employment Law*, (1998) EHRLR 560.
- G. Morris, *The Human Rights Act and the Public/Private Divide in Employment Law*, [1998] 27 ILJ 293.
- Sir S. Sedley, *Public Law and Contractual Employment*, [1994] 23 ILJ 201.
- Sir J. Laws, *Public Law and Employment Law: An Abuse of Power*, [1997] PL 455.
- I. Hurd, *Labour Standards through International Organisations: The Global Compact in Comparative Perspective*, Journal of Corporate Citizenship, September 2003 No 11, 99.
- J. Heilemann, *The Truth, the Whole Truth and Nothing but the Truth: The Untold Story of the Microsoft Antitrust Case*, Wired Vol. 8 No. II pp. 260-321.
- G. Duncan, *International Tax Task Force to Be Set up*, The Times, Saturday 24-04-2004.
- H. Collins, *Market Power, Bureaucratic Power and the Contract of Employment*, [1986] 15 ILJ 1.
- European Labour Law Bulletin, Issue of July/August 2004.
- Sir J. Laws, *The Limits of Human Rights*, (1998) PL 254.
- A. Zinser, *International Data Transfer Out of the European Union: The Adequate Level of Data Protection According to the Article 25 of the European Data Protection Directive*, 21 JMarshallJComputer&InfoL 547.
- J. Craig, *Privacy in the Workplace and the Impact of the European Convention Incorporation on the United Kingdom Labour Law*, 19 CompLabL&Pol'yJ 373.
- A. E. Shimanek, *Do You Want Milk with These Cookies?: Complying with the Safe Harbor Privacy Principles*, 26 IowaJCorpL 455.
- G. Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards*, 25 YaleJInt'lL 1.
- A. Delaney, *Employee Privacy – Grasping the Nettle*, Emp. L.B. 2003, 56(Aug), 4-6.

- S. U. Ejike, *Workplace Privacy in Domestic and International Business: Employers' Rights and Liabilities*, IntTLR 2002, 8(1), 12-18.
- D. Christie, *Employee Surveillance*, EmpLB 2000, 38(Aug.), 2-4.
- D. Wisbey and S. Mirza, *Employee records-new pitfalls for employers*, NLJ 152.7061(1922).
- H. Oliver, *Email And Internet Monzitoring In The Workplace: Information Privacy And Contracting-Out*, ILJ 2002.31(321).
- D. Calow and C. Manley, *It's Okay to Talk Dirty by Office Email*, NLJ 152.7022(345).
- I. Smith, *From the Coalface*, NLJ 150.6961(1750).
- O. Ward, *Is Big Browser watching You?*, NLJ 150.6953(1414).
- A. R. Oquendo, *Deliberative Democracy in Habernas and Nino*, OJLS 2002.22(189).

URLs and Web-links:[*]

- http://news.bbc.co.uk/1/hi/business/1370956.stm
- http://news.bbc.co.uk/1/hi/technology/2984922.stm
- http://www.informationcommissioner.gov.uk/
- http://www.informationcommissioner.gov.uk/eventual.aspx?pg=SR&cID=446
- http://ico-cms.amaze.co.uk/DocumentUploads/110603prelease.pdf
- http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_en.pdf
- http://www.asginvestigations.com/security_cameras/
- http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp89_en.pdf
- http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp48en.pdf
- http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp55_en.pdf
- http://news.bbc.co.uk/1/hi/business/1370956.stm
- http://www.theregister.co.uk/2004/05/27/danish_free_porn/
- http://www.dti.gov.uk/er/emar/ffind.pdf
- http://news.bbc.co.uk/1/hi/technology/2984922.stm
- http://www.informationcommissioner.gov.uk/eventual.aspx?pg=SR&cID=446
- http://www.informationcommissioner.gov.uk/cms/DocumentUploads/The%20Employment%20Practices%20Data%20Protection%20Code%20Part%201%20Recruitment%20and%20Selection.pdf
- http://www.wdtforum.org.uk/pdfs/wdtgde~1.pdf
- http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Part%204%20-%20v0.9a.pdf
- http://www.export.gov/safeharbor/
- http://www.export.gov/safeharbor/index.html

[*] All were accessible up to 10-09-2004.

- http://www.wto.org/english/thewto_e/whatis_e/tif_e/bey5_e.htm
- http://www.iso.org/iso/en/aboutiso/introduction/index.html
- http://european-convention.eu.int/docs/Treaty/cv00850.en03.pdf
- http://www.freshfields.com/practice/epb/publications/newsletters/labourlaw/9052.pdf
- http://news.bbc.co.uk/1/hi/health/3579402.stm
- http://news.bbc.co.uk/1/hi/wales/3395443.stm
- http://news.bbc.co.uk/1/hi/business/3392233.stm
- http://essex.ac.uk/RCPR/events/jointsessions/paperactive/edinburgh/ws11RaabBennet.pdf