The INTERNATIONAL JOURNAL OF COMPARATIVE LABOUR LAW *and* INDUSTRIAL RELATIONS

Wolters Kluwer
Law & Business

Editorial Office Marco Biagi Foundation
University of Modena and Reggio Emilia
Largo Marco Biagi 10, 41121
Modena, Italy
Tel.: +39-059 2056 042
Fax: +39-059 2056 068
E-mail: rymkevitch@unimore.it

Publisher Ewa Szkatuła

Journal's world wide web site: http://www.fmb.unimore.it/on-line/Home/Ricercaepubblicazioni/TheInternationalJournalofComparativeLabourLawandIndustrialRelations.html

Annual subscription Kluwer Law International, P.O. Box 316, 2400 AH
Alphen aan den Rijn, The Netherlands, http://www. kluwer-law.com.

Published by:
Kluwer Law International
PO Box 316
2400 AH Alphen aan den Rijn
The Netherlands
Website: www.kluwerlaw.com

Sold and distributed in North, Central and South America by:
Aspen Publishers, Inc.
7201 McKinney Circle
Frederick, MD 21704
United States of America
Email: customer.service@aspenpublishers.com

Sold and distributed in all other countries by:
Turpin Distribution Services Ltd.
Stratton Business Park
Pegasus Drive, Biggleswade
Bedfordshire SG18 8TQ
United Kingdom
Email: kluwerlaw@turpin-distribution.com

The International Journal of Comparative Labour Law and Industrial Relations is published quarterly (March, June, September and December).

Subscription rates, including postage (2011): Print subscription prices: EUR 296/USD 395/GBP 218
Online subscription prices: EUR 274/USD 366/GBP 202 (covers two concurrent users)

The International Journal of Comparative Labour Law and Industrial Relations is indexed/abstracted in the *European Legal Journals Index*.

Printed on acid-free paper.

ISSN 0952-617X

The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy

Shelley Wallach*

The nature and scope of modern technology poses a growing threat to employee privacy in the workplace and, as a result, presents new challenges and a greater need for clearer rules and boundaries for both actors in the workplace: the employer and the employee. This article focuses on various aspects of surveillance and monitoring of employees regarding the internet, e-mail, phone calls and location data. It examines the problems and conflict of interests that arise and outlines various legal responses in hard law and soft law, including legal rulings. Different approaches to these topics are presented, mainly the approach of the American legal system versus the European ones, and some examples of cases in various countries are considered. It is argued that by learning from each other and the various solutions adopted, we should strive to preserve, as far as possible, the employee's right to privacy.

1. Introduction

The use of modern technology in the age of digital media gives rise to privacy issues in an unprecedented manner. Modern technology, in all its forms, is virtually everywhere, and its use is only spreading and getting more sophisticated. The risks it poses to our individual freedom are clearly not limited to the workplace, but in this article the focus is on issues regarding the world of work and the employment relationship.

It is hard to imagine a workplace today in which no use is made of digital media, by which I mean the use of computers (internet and e-mail), mobile phones (and land-lines), and all kinds of surveillance and monitoring equipment including Closed Circuit Television (CCTV) and all forms of cameras. The only places in which such technology is not used are in the 'low tech' sectors, and even those are dwindling.

Privacy has many facets and can be examined in connection with many matters such as job interviews, various tests, and personal data protection,[1] but the issues addressed in this article are surveillance and monitoring. Should an employer be entitled to use such measures, and if so, when and what kind of limitations should be imposed on his right to do so?

Employers have always been able to monitor the whereabouts of their employees, but in the past it was expensive and time consuming to get information, store and retrieve

* Magistrate in the Tel-Aviv Labour Court, Israel.

[1] This article is a sequel to the previous one, S. Wallach, 'Who's Info Is It Anyway? Employee's Rights to Privacy and Protection of Personal Data in the Workplace', *The International Journal of Comparative Labour Law and Industrial Relations* 23, no. 2 (2007): 189–219.

Wallach, Shelley. 'The Medusa Stare: Surveillance and Monitoring of Employees and the Right to Privacy'. *The International Journal of Comparative Labour Law and Industrial Relations* 27, no. 2 (2011): 189–219.

it from files or folders. In addition, most surveillance and information-gathering activities could hardly be done without the knowledge or awareness of the employee. Digital technology has changed all that dramatically. Today, it is possible at minimal cost and often using devices already installed in the workplace, such as computers and phones, to carry out surveillance and monitoring of an employees' activities starting from their presence in the workplace, their activities, their level of output, whom they communicate with at work, and the contents of any communications, including internet use and e-mails.

Moreover, when electronic monitoring is carried out, whether regarding computer usage, internet, e-mails or phone calls, or by means of surveillance camera, the electronic eye, unlike the human eye, never tires and never looks elsewhere. As long as its function and angle has not been changed by the operator, it is a stare that continues in a constant and unlimited timeframe, and this stare, fixed on the object of surveillance, the employee, is ever-present, following the employees at all times, leaving them without a shred of privacy. It can also take place without employees being aware of its presence at all. Therefore I call this electronic surveillance 'the Medusa Stare' after the creature of ancient Greek mythology that turns all those who look at it to stone.

By our very human nature we are not psychologically equipped to deal with such an invasion of our privacy.[2,3] The technology that makes such surveillance possible already exists, and we can safely assume that not only is it not going to disappear in the foreseeable future, but that it is more likely to become more widespread and sophisticated. The only way to limit such surveillance and protect the employee's right to privacy is to adopt legal provisions that impose limitations by legislation, codes of practice, guidelines, collective agreements and, where necessary, court rulings.

It should be stressed that the employee's right to privacy, albeit a fundamental right in a democratic society, is not an absolute right. Employers have rights as well: first and foremost property rights in the enterprise and managerial prerogatives to run the business as the employer sees fit and in a way that serves their best interests. We are dealing therefore with a conflict of rights and interests, giving rise to a balancing act in order to draw boundaries.

2. The Issue of Privacy in Various Legal Systems, Different Approaches and Legal Sources

The issue of privacy, including monitoring and surveillance, is perceived totally differently by the US legal system and the European ones (considering the differences

[2] For more in-depth discussion on the issue of technology in the workplace and the ramifications for employee's privacy, see M. Jeffery, 'Information Technology and Workers' Privacy: Introduction', *Comparative Labor Law & Policy Journal* 23 (2002): 251, 255–261.

[3] The notion of constant surveillance has also been called the Panopticon, a concept first coined by Samuel Bentham, who devised a physically constructed environment so that the people within it have the sense of constantly being watched and monitored. The idea is to enforce discipline in order to make the workplace more efficient. Henry Ford used it in his factories. See C. Pease-Watkin, 'Jeremy and Samuel Bentham – *The Private and the Public*', <www.ucl.ac.uk/Bentham Project/journal/cpwsam.htm>, 2002.

between European countries). Generally speaking, the US approach recognizes hardly any right to privacy, in strong contrast to the European approach.

2.1. The US legal approach

The US legal system does not define privacy as a value, and certainly not as a fundamental right that needs to be protected, and it can be said Categorically that there is almost no legal restriction imposed on a US employer wishing to monitor or use surveillance in the workplace. Only two states in the whole US have legal restrictions on electronic surveillance.[4]

Even the only Federal law on this issue, the Electronic Communications Privacy Act (ECPA), does not contain any restrictions on such surveillance as long as the employee's consent has been obtained (and this, as discussed below, is a problematic issue with regard to employment), or if it carried out in the 'ordinary course of business'.

US employees who receive good legal advice will be told that even if it is not really necessary, they should employ some means of surveillance, such as CCTV cameras, and they should monitor their employees internet activities or read their e-mails in order to be able to claim later that they are in the habit of doing so in the ordinary course of business to prevent a possible claim by an employee that such monitoring was not standard practice and was suddenly introduced, thus affecting their expectation of privacy. This gives an incentive to employers to resort to such surveillance in order to forestall a possible future claim by employees that their right of privacy has been infringed, and this is not a positive outcome.

Surprising as it may seem, privacy as a value does not appear at all in the US Constitution and is not protected by it. The legal source from which US courts derive their authority in cases in which the issue of privacy arises is the Fourth Amendment:[5]

> The right of people to be secure in their persons, houses, papers and effects against unreasonable search and seizure, shall not be violated, and no warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

The basic principle with regard to surveillance and employee privacy in the US legal system is that as long as the employer has informed the employee of the possibility of such surveillance or the intention to use it, and the employee has agreed to work, it is assumed that his consent has been given. More to the point: the stress is put on the employee's expectation of privacy and whether there was any. When such an expectation of privacy was not deemed to exist, for instance, when the employer has specifically made it known in advance that there is a possibility of surveillance, there are few restrictions,

---

[4] For a discussion of the US legal perspective, see M. Finkin, 'Information Technology and Workers Privacy: The United States Law', *Comparative Labour Law & Policy Journal* 23, no. 4 (2003): 501–508 and M. Finkin, *Privacy in Employment Law*, 3rd edn (Arlington, VA, USA: BNA Books, A division of BNA, 2009).

[5] The full text of the US Constitutional Amendments can be seen at <www.caselaw.if.findlaw.com/data/constitution/amendments.html>.

if any, on the employer conducting such surveillance. This gives rise to the incentive to conduct surveillance from time to time in order to make it part of the ordinary course of business so the employee is not able to claim a reasonable expectation of privacy.

2.2. The European Union and European Approaches

In sharp contrast to the US approach that refrains as far as possible from legislation on this issue, in European legal systems there are many legal sources that enshrine this right.

This fundamental difference between the US and European approaches depends on many factors that are outside the scope of this article, but, as a rule, whereas US citizens wish to be protected as far as possible from state interference in their affairs and display what may be described as an instinctive suspicion of such intervention by the state authorities, European citizens expect the government and the legislature to create legal safeguards that protect their rights from being violated by a system of binding legal arrangements.[6]

This difference of approach to the employee's right to privacy has been discussed by US scholars[7,8] and not without criticism. [9,10] Moreover, while the right to privacy, to the extent that it exists in the United States, is perceived as part of the concept of liberty; in Europe it is perceived as part of the fundamental concept of human dignity.

The first and foremost European source is the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 that has been ratified by all the European Union (EU) Member States, as well as Norway, that states in Article 8, on the right to respect for private and family life:

(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 interest 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.

---

[6] For a more in-depth discussion of the difference of these two approaches, see Wallach, 2007, at 199.

[7] For a discussion and comparison of the two legal systems, see 'Privacy and the Internet: A Study Report to the Michigan Law Revision Commission', <www.council.legislature.mi.gov/files/mlrc/2000/privacy and internet>.

[8] See J. R. Reidenberg, 'Privacy Protection and the Interdependence of Law, Technology, and Self-Regulation', 2001 <www.paris-conference-2001.org/eng/contribution/reidenberg.contri.pdf>.

[9] See S. J. Korbrin & E. Johnson, 'The Wharton School, University of Pennsylvania, May 1999', *Economics may be global but politics are local: personal privacy in the digital age,* <www.management.wharton.upenn.edu/kobrin/reaserch/privacyrevised3 PDF> that analyses the historic, political, social and economic reasons for the difference of approaches, criticizing the United States and calling for more supervision by legislation in the United States instead of self-regulation as is the case today.

[10] See M. Finkin, 'Information Technology and Workers Privacy: The United States Law', *Comparative Labour Law & Policy Journal* 23 (2002): 471; M. Finkin, 'Menschenbild: The Conception of the Employee as a Person in Western Law', *Comparative Labour Law & Policy Journal* 23 (2002): 577.

In 1970, the Council of Europe's committee of experts on human rights stated that the right to respect for private life is mainly based on a recognition of the interest that individuals have in protection from intrusion into their private lives.

In *Niemitz v. Germany*, the European Court of Human Rights in Strasbourg held that the right to respect for private life extends to professional or business activities and that it applies to the shop floor:

> Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationship with the outside world. A fact that has been underlined by the commission confirms this: it is not always possible, in someone's occupational activities, to disentangle what falls within the professional domain from what lies outside it.[11]

The Court established that as well as correspondence, respect for private life applies to telephone conversations (whether business related or private), a principle that suggests that e-mail and internet use may also be covered, as can be inferred from the right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights[12] states the following:

> it is anticipated that the concept will continue to be interpreted so as to keep pace with development in technology which may bring other methods of communication such as e-mails, within its sphere of protection.

The Charter of Fundamental Rights of the EU, signed at the European Council in Nice in December 2000,[13] essentially repeats (Article 7) the first paragraph of Article 8 of the Council of Europe Convention, stating that 'everyone has the right to respect for his private and family life, home and communications'.

It is significant that in order to apply it to new developments in technology, the term 'correspondence' in the Convention has been replaced by the all-embracing term 'communication' but the principle remains the same. In the Charter, the right to privacy was accorded the status of a Fundamental Social Right and since then has been perceived as such in Europe.[14]

The Charter is now part of the EU constitution under the Lisbon Treaty signed in December 2007, entering into force on 1 December 2009.[15] Since then it has had a legally binding status. Even before the Charter was accorded binding force, the European

---

[11] *Niemitz v. Germany*, Judgment of 16 Dec. 1992, Series A, No. 251 / B, para. 30.

[12] U. Kilkelly, 'The Right to Respect for Private and Family Life', *A Guide to the Implementation of Article 8 of the European Convention on Human Rights, Council of Europe, Human Rights Handbook,* no. 1 (2001), Strasbourg, Council of Europe.

[13] EU 0012288F.

[14] For a detailed discussion of the charter and its fundamental rights including privacy, see M. Weiss, '*The Politics of the EU Charter of Fundamental Rights*', in *Social and Labour Rights in a Global Context*, ed. B. Hepple (Cambridge: Cambridge University Press, 2002), 83.

[15] For the full text of the treaty, see <http://europa.eu/lisbontreaty/fulltext/indexen/htm>.

Court of Justice often referred to it in its rulings that are legally binding on all Member States. As the right to privacy appears as part of the Charter of Fundamental Rights, it indicates the attitude of the EU legislature to see it as a fundamental right in the EU.

Other important legal sources in the EU are, of course, the Directives concerning the issue of privacy. The first one that should be mentioned is the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[16] Another more specific one was enacted two years later: the Directive concerning the processing of personal data and protection of privacy[17] that was replaced a few years later due to developments in electronic communication and digital media with a directive concerning the processing of personal data and the protection of privacy in the electronic communication sector.[18] There is also a directive on visual display units,[19] but it does not concern privacy as it deals with health and safety.

In spite of these provisions, the EU Commission has reached the conclusion that they are not sufficient to deal with problems arising in the workplace due to the spread of digital media, and there is a proposal to enact a specific directive to deal with these issues.[20] The Directive has not yet been enacted, but there is a chance it may be in the near future.

In addition to these provisions that are binding on all EU Member States, legislation in each country deals with issues of data protection and right to privacy that are specific to each of them. However, very few countries have enacted legislation relating specifically to employment.

The Directives are binding on all twenty-seven Member States and lay down important rules and principles regarding the issue of privacy that includes the guideline that information processing should be based on the principles of legitimate purpose, proportionality, and transparency. These principles will be discussed shortly in detail, but it is worth mentioning that they are the standards applied by European courts of law, including the European Court of Justice.

2.3. International legal sources and soft law arrangements

There are a few important international sources. One is the International Labour Office (ILO) Code on Protection of Workers' Data (1996) that establishes the following guidelines:

---

[16] 95/46/EC.

[17] 97/66/EC.

[18] 2002/58/EC.

[19] 90/270/EEC.

[20] As part of the five-year social agenda adopted in February 2005, the Commission planned to propose an initiative on the protection of personal data of workers in 2005. The Directive was intended to deal with databases, medical data, drugs and genetic testing, and issues of monitoring and surveillance including e-mail and internet use. See <www.eiro.eurofound.eu.inl/2002/11/feature/euro21120gt.html>.

The five-year social agenda followed on from the social partner consultation on these issues, in August 2001 and October 2002. It passed the two required stages of consultation but was not enacted. The employee representatives were in favour of the proposal, while the employers were of the opinion that present arrangements were sufficient and there was no need for a specific directive.

For the positions of the social partners and additional information, see <www.eiro.eurofound.eu.int/2005/feature/eu0502205f.html>.

(1) If workers are monitored they should be informed in advance of the reasons for monitoring, the time schedule, the method and technique 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 or criminal activity of other serious wrongdoing.
(3) Continuous monitoring should be permitted only if required for health and safety or the protection of property.[21]

The Union Network International (UNI), an alliance of white collar unions in various countries, has published its own Code of Practice on employee use of digital and electronic media in the workplace dealing with four main topics: communication with the worker's union, non-business communication, communication monitoring, and the conditions to be applied when using electronic communication.

The driving force for drafting the code was the perception that the electronic communication and the problems that arise from its use have become a key issue in the workplace, and the lack of clear guidelines concerning use and monitoring is endangering employees' rights to privacy. In the words of Gerhard Rhode (UNI):

> In too many companies there are no fair rules and in many others the rules are just not known. We want employers to sit down with their workers and their unions to agree fair rules which give on-line rights to on-line workers – but protect employers against abuses. Used appropriately, the exploitation of electronic facilities like e-mail and the internet improve work efficiency and facilitate new ways of working.[22]

Mention should be made of the Framework Agreement on Telework[23] signed by the European social partners on 16 July 2002. Telework is defined as work carried out using electronic media and not on the premises and under the direct supervision of the employer. Article 6 of the agreement states:

> The Privacy of the teleworker must be respected by the employer. If a monitoring system is put in place it must be proportionate to the employer's objective and comply with the EU directive (90/270/EEC) on visual display units.[24]

In some European countries, and Belgium seems to be leading the way, these issues have been the subject of collective agreements, such as the use of internet and e-mail in Collective Agreement No. 81 in 2002[25] and Collective Agreement No. 68 in 1998

---

[21] For a discussion of this code and a positive appraisal by Prof. Spiros Simitis, see <www.worldii.org/journals.PLBIN/1998/21html>. See also the 1971 ILO Convention No. 135 and Recommendation No. 143.

[22] See <www.*union-network*.org>. The code will be discussed in detail below.

[23] <www.eurofound.eironline/2002/07>.

[24] On this Agreement and its implementation, see M. Weiss, 'Germany', in *European Framework Agreement and Telework. Law and Practice, A European Comparative Study*, *Bulletin of Comparative Labour Relations*, ed. R. Blanpain (The Netherlands: Kluwer Law International BV, 2007), 171 ff.

[25] This approach of using collective agreements to regulate this issue has been chosen by Israel, with a collective agreement signed on 25 Jun. 2008.

concerning the placing of surveillance cameras in the workplace. Another agreement between employers and unions in Belgium was reached in 2006 with regard to the searching of workers suspected of committing theft that has since been transposed into legislation. However, there are still few countries that have chosen collective bargaining as a way to regulate those matters, though it seems the most suitable approach, especially for e-mail and internet use.[26] Surprisingly, there are few court rulings on these matters in the United States, Europe and Israel by the supreme, constitutional or higher courts.

2.4. Israeli legal sources

In Israel, like other Organization for Economic Co-operation and Development (OECD) countries, there is no specific law dealing with privacy in the workplace, but there are two legal sources addressing the issue of privacy from which the Israeli courts (including labour courts) derive the legal basis for their rulings and court decisions:

The first is the Basic Law: Human Dignity and Liberty:[27]

(a) All persons have the right to privacy and to intimacy.
(b) There shall be no entry into the private premises of a person who has not consented thereto.
(c) No search shall be conducted on the private premises or body of a person, nor in the body or personal effects.
(d) There shall be no violation of the confidentiality of conversation, or of the writing or records of a person.

The second is the Protection of Privacy Act of 1981.[28] In addition we now have a specific collective agreement, signed on 25 June 2008, governing employee use of computers made available by the employer.[29] There are also some court rulings regarding monitoring and surveillance.

3. Electronic Monitoring of Employees

So far the focus has been on legal provisions in the United States, Europe and, in particular, the EU concerning employee privacy and electronic communication. The rapid spread of electronic and digital media into almost every workplace has given rise to threats to employee privacy in ways that were unknown before.

There can be many reasons for employers to monitor their employees: some may be legitimate and some may be not. We have to bear in mind that monitoring can take

[26] See Wallach, 2007, at 226. A similar opinion was expressed by M. Jeffery, 'Information Technology and Workers Privacy: The English Law', *Comparative Labour Law & Policy Journal* 24, no. 1 (2005): 301.
[27] Enacted on 17 Mar. 1992.
[28] Enacted in 1981.
[29] For an overview of the legal situation in Israel concerning privacy in the workplace, see Judge Elika Barak's report in the *XVIIth Meeting of European Labour Court Judges*, 12 Jun. 2009.

many forms, starting with the use of the computer and access to websites and e-mail, through to monitoring of surfing habits and access to private e-mails, installing surveillance cameras, security checks when employees leave the premises, and the identification of their exact whereabouts at any given moment. All this poses a threat to the privacy of employees.

Since the technology makes such monitoring available even to people with no particular technological skills, and, at least theoretically, there is always a temptation for the employer to use it, it is legislators and legal scholars who have the duty to draw clearly defined boundaries for the employer and the employee and to distinguish between what should be considered legitimate and what should not.

The responses of different legal systems on these issues are not identical and to a great extent reflect the cultural beliefs of the society in which the rulings or judgments have been handed down. The difference between the US and European perceptions is fundamental, but even among European countries there are various legislative measures and court rulings. However, all EU Member States are bound by the Council of Europe's Convention for the Protection of Human Rights and Fundamental freedoms and by the Directives.

Although the Directives leave room for interpretation in the transposition into the different national legislations of each Member State, a directive prevails over domestic law in cases referred to the European Court of Justice. We now examine monitoring more closely.

3.1. Internet and e-mails: use and access

In examining the use of internet and e-mail, we should distinguish between the use by employees of computers that an employer has put at their disposal, such as access to websites, sending and receiving e-mails, and the monitoring of these activities by the employer, even to the point of reading e-mails sent or received by the employee. It is in this latter connection that the problems and conflicts of interest may arise, as well as the potential for invasion of privacy.

In principle, as the computer system belongs to the employer, he has the prerogative to decide who should have access to it and how it should be used (only for work-related purposes or for personal use also, and if so, to what extent). This basic right of the employer is not in dispute. However, there are different approaches to the limits on use for personal purposes from country to country and even between different employers.

With regard to limitations on use, in particular the use by e-mail, there are different views. While restricting the use of some websites, such as pornographic ones, is certainly within an employer's prerogative, some take the view that this also applies to the use of private e-mails, up to an outright ban on sending e-mails that are not business related. Some take the more lenient view that e-mail should be used only for work-related purposes and that an employee should be allowed to use it for personal reasons in case of emergency such as letting their partner know that they are staying late at work.

The last two approaches are more prevalent in the United States than in Europe (and Israel), but there are also prominent European scholars like Roger Blanpain, who endorse such an approach,[30] while other employers are more liberal about the use of internet and e-mail and do not restrict it specifically. In my view, e-mail and internet use do not present special problems in relation to privacy, as it cannot be claimed that an employee has a fundamental right to read news websites or send e-mails to friends while working and as long as the employer does not deny him access to the computer in a way that prevents him from doing his job, which would amount to creating a hostile work environment that can be a ground for a lawsuit, there is no legal reason to prevent an employer from imposing such limitations on computer use.

My view in this regard is that a reasonable employer should allow such use for personal purposes as long as the employee does not abuse it, as this contributes to a more positive work environment and sometimes even proves to be cost-effective for the employer, as the employee can make personal arrangements, for instance, using an on-line bank account that will take a few minutes instead of having to take a few hours or even a day off from work.[31,32]

3.2. Monitoring of internet and e-mail

The most significant area of conflict is not in the use and access issue, which can be easily reconciled with privacy, as mentioned above, but in the monitoring of activities when the employee accesses websites or sends messages that may be of a personal or intimate nature. There are five key reasons why an employer may wish to monitor on-line communication by employees:

(1) To safeguard employee productivity. Working time could be wasted dealing with inappropriate e-mail and unwanted advertising or spam, following links to websites that are not relevant to the employee's job, shopping during working hours, downloading music or watching videos on the internet.

(2) To avoid overloading the company network. The network risks being tied up by multimedia activities such as gaming, downloading music or movies or watching sporting events. Clearly, the employer must ensure that the company's resources are available to employees for work-related purposes.

(3) To protect the company from potential lawsuits. Misuse of e-mail by workers could lead to lawsuits for a variety of reasons such as sexual harassment, bullying or racist comments, reflecting badly on the company when sent from its computers, or the unlawful downloading of materials.

---

[30] R. Blanpain & M. van Gestel, *Use and Monitoring of E-Mail, Internet and Internet Facilities at Work, Law and Practice* (The Hague/London/New York: Kluwer Law International, 2004), 31, 71, 76, 125, 395.

[31] That is the view adopted in Israel in the Collective Agreement concerning computer use in the workplace signed on 25 Jun. 2008.

[32] The Israeli Law, Information and Technology Authority (ILITA) is planning to distribute a draft code of practice on the protection of personal data in the workplace among employers, endorsing this view.

(4) To ensure the confidentiality of company information. Today most intellectual property is held in digital form. At the click of a mouse it can be sent round the world, either inadvertently or on purpose. This could obviously include customer names and addresses, pricing policies and similar confidential information.

(5) To minimize the risks resulting from exposing the network to cyber threats. Surfing dubious websites or indiscriminately sending and opening e-mails may result in viruses and spyware entering the system.

Modern information and communications technology makes such monitoring easy for any employer without the need for specialist skills. The question is not whether the employer can do so but whether he should be allowed to and if so, under what conditions and restrictions. We now look more closely at some of the answers given by various legal systems.

3.3. Legal provisions regarding internet and e-mail: the US and european approach

The way the US legal system deals with this issue is fundamentally different from the way it is perceived and dealt with in Europe. As mentioned above, the legal source from which the US courts draw their authority on the issue of privacy is the Fourth Amendment.

In *O'Connor v. Ortega*, the US Supreme Court ruled that a 'reasonable standard', a term taken from the Fourth Amendment, refers to search and seizure of public employees. In *Ortega*, the Court ruled that if an employee has a 'reasonable expectation of privacy' the reasonableness of the search has to be examined. The ruling in *Ortega* implies that private employees were not afforded protection. The case further suggests that e-mail should be considered a resource of the employer that is issued to employees for work-related communications.

It can also be inferred from the ruling that e-mail has been taken outside the scope of protection of privacy and that the right of privacy as a whole enjoys less protection in the workplace then at home.[33,34] Subsequent decisions in the United States such as *Schowengerdt v. General Dynamics Corp.* followed *Ortega,* further weakening the employee's right to privacy in the computerized workplace to the point of virtually eliminating it.[35,36]

In *United States v. Simmons*, an employee of the Central Intelligence Agency (CIA) was found by his manager, who was checking for improper usage of the system, to be accessing child pornography websites. Simmons claimed the searches whereby the graphic files were intercepted had been conducted in violation of his Fourth Amendment rights and that all evidence should therefore be suppressed. The Court rejected this claim and

---

[33] *O'Connor v. Ortega*, US Supreme Court 480 45, 709 (1987).
[34] L. L. Ride, '*Rights of Privacy in the Information Age*', 2003, <www.publaw.com>.
[35] *Schowengerdt v. General Dynamics Corp*. 823F 2d. 1328 (9th Cir. 1987).
[36] For in-depth discussion of the United States regarding this issue, see Finkin, 2009, Ch. 5, at 297–481.

held that he did not have a legitimate expectation of privacy with regard to the records of his internet use, in light of the employer's policy that clearly stated that they would 'audit, inspect and/or monitor' the employee's use of the internet including all file transfers, websites visited and e-mails.[37] The Court held that, as such notice had been given to the employees, Simmons could not have a reasonable expectation of privacy.

We can conclude from the above that, as a rule in the United States, there is no real protection of employee privacy and no restriction to speak of imposed on an employer wishing to monitor an employee, including reading his mails. In the EU, by contrast, although there is still no specific directive on privacy in the workplace,[38] the prevalent position is that the existing Directive (95/46/EC) refers to monitoring internet use and e-mails. This can be clearly seen from the view of the Data Protection Working Group in their Opinion 8/2001:

> There should no longer be any doubt that data protection requirements apply to the monitoring and surveillance of workers whether in terms of e-mail use, internet access video cameras or location data.[39]

Although Europe and, in particular, the EU have the most extensive provisions on the protection of personal data,[40] there is a realization that they are still not sufficient and as mentioned before; there is a proposal for a specific directive to deal with these issues.[41]

The most important ruling so far in Europe on these issues was given in France by the *Cour de Cassation* in *Nikon* on 2 October 2001. The employee, Mr O., had been fired by Nikon in June 1992, when it was discovered that he had made use of e-mail contrary to company policy. He claimed that his dismissal was not justified in the circumstances. During the trial, it was revealed that Nikon had intercepted his e-mails in order to verify their private nature. The *Cour de Cassation* found that the right of privacy of correspondence, already recognized for paper communications under French law, extends to e-mail and that an employee has a right to privacy even in the workplace:

> Employees have the right, even during working hours and in the workplace, to respect for the privacy of their private lives. This entails the secrecy of correspondence in particular: the employer therefore cannot, without violating this fundamental freedom, examine the contents of personal messages sent and received by employees using computer equipment made available to them for their work, even in cases where an employer has forbidden non-business use of the computer.[42]

In my view, this ruling is well founded, though other courts in Europe have reached different conclusions. On similar facts to *Nikon*, in Spain the *Tribunal Superior de Justicia*

---

[37] 206 F. 3ed 392 (4th cir. 2000).

[38] That Directive will deal with issues of monitoring and surveillance including e-mail and internet use. See <www.eiro-eurofound.eu.uni/2002/feature/eu06/21120gt.html>.

[39] Article 29 Data Protection Working Group, opinion 8/2001 on the processing of Personal Data in the Employment Context EU Doc. 5062/CI/WP48 (13 Sep. 2001). See also the Working Documentation on the Surveillance of Electronic Communications in the Workplace, EU Doc. 5402/01/WP55 (29 May 2002).

[40] For a comparison of EU Member State provisions, see <www.eiro.eurofound.en-int/2003/07/study/in 030710/s.html>.

[41] See *supra* n. 38.

[42] <www.courdecassation.fr> (in French). See also <www.out-law.com>, 2052 (in English).

de Catalune[43] ruled that employers have the right to read the information stored on their employees' computers, as did an Italian Court in Milan in 2002. However, a Supreme Court ruling in Austria in 2002 and in the Netherlands in 1998 reached the same conclusion as *Nikon*.[44] There is no uniformity of opinion on these issues even in European case law.

The UNI, which brings together white collar and private sector unions from around the world, including the information technology sector, has been active in the area of the on-line rights of employees for a number of years. UNI warned in October 2002 that electronic communications are a 'time bomb' for industrial relations, as employees can easily fall foul of written and unwritten rules governing the use of the internet and e-mail at work. In order to provide greater clarity, UNI has issued a code of practice on on-line rights at work.

The code covers four main issues:

- trade union communication;
- non-business communication;
- monitoring and surveillance of communication;
- conditions for the use of electronic facilities.

The code states that works councils and/or trade unions and their representatives should have the right to access enterprise electronic facilities for works council/trade union purposes, both internally and externally, and to send relevant information to all employees. It also states that employees should have the right to use company facilities to communicate with their representatives. UNI states that this part of the code extends to electronic means of communication contained in the 1971 International Labour Organization (ILO) Convention No. 135 and Recommendation No. 143. In addition, it notes that the nature of communication has now changed, with employee representatives in different branches of a multinational company needing to be able to cooperate and coordinate work across international borders. Moreover, an increasing number of employees are now working from home, from telecottages, or on the move.

The code states that employees should be permitted to use enterprise electronic facilities for non-business purposes, both internally and externally, provided this is not detrimental to their work. It also says that the employer should be obliged to undertake not to subject employee use of the enterprise's electronic facilities to covert surveillance and monitoring, and that communication should be subject to surveillance and monitoring only if:

- it is permitted by collective agreement;
- the employer is under a legal obligation;
- the employer has reason to believe that an employee has committed a criminal or serious disciplinary offence.

---

[43] Case AS/3452 of 2000. Cited in M. Jeffery, '*Information Technology and Workers Privacy: Introduction*', *Comparative Labour Law & Policy Journal* 23 (2003): 251, 264.

[44] *Supra* n. 40, where these cases are cited.

Moreover, access to surveillance and monitoring records relating to individual employees should take place only in the presence of a trade union representative or other representative selected by the employee. The code lists a number of conditions to which the right of the employee to use enterprise electronic facilities should be subject:

- communication must be lawful and not include defamatory or libellous statements;
- company facilities may not be used as a means of sexually harassing other members of staff or making offensive comments based on an individual's gender, age, sexuality, race, disability, or appearance, or knowingly to visit websites promoting pornography, racism or intolerance;
- the employer can require a disclaimer when employees communicate internally and externally, making clear that the views expressed are those of the author alone and not those of the enterprise.[45]

Although this code, like the ILO Code of Practice, is not legally binding, the importance of such codes should not be underestimated, as they can inspire hard law legislation or soft law arrangements such as collective agreements, guidelines or codes of practice among employers and employees worldwide.

Another approach is by collective agreement. This option has been chosen in Belgium, where the first collective agreement on internet and e-mail use in the workplace was signed in April 2002.[46] The collective agreement strives to protect the employee's right of privacy in the workplace in electronic communication on a computer provided by the employer.[47] The same path has recently been taken by Israel, which has decided to deal with this issue by means of a Collective Agreement, the second of its kind in the world,[48] to be discussed below.

However, while some countries have legislation governing privacy in general that is interpreted as dealing with the issue of monitoring at work, seeking thereby to protect the employee's privacy rights, some other countries have legislation that allegedly (and I shall explain shortly why I am using this term) gives the employer a free hand to use monitoring and surveillance of employees at the expense of their privacy while using e-mail, internet and other forms of electronic communication (including phones). These measures in favour of employers have been enacted as a result of strong lobbying and pressure by employers' organizations in the countries concerned.

In the United Kingdom, the Regulation of Investigatory Powers Act 2000 was enacted to regulate and enable interception of communication together with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations

---

[45] <www.eurofound.europa.eu/eiro/2002/10/feature/eu0210205.sf.htm>.

[46] BED 28302 signed 26 Apr. 2002 – National Collective Agreement No. 81 *on the protection of employees personal privacy with respect to the monitoring of electronic on-line communication data*. It was signed as a Royal Decree on 12 Jun. 2002, thus making it binding on the whole country.

[47] For the full text of the agreement, analysis and criticism, see Blanpain & van Gestel, 106–173, 189, 247. A total of thirty Codes of Practice were collected and examined in this book, and many examples are to be found there.

[48] Signed on 25 Jun. 2008 and officially registered a month later.

2000, which came into force in October 2000, establishing the circumstances under which an employer is allowed to monitor the employees' electronic communications such as websites and e-mail and even record them without getting the consent of the employee or the other party, though employers are required under this Act and Regulations to take reasonable steps to notify employees of the possibility of interception of their personal communications in the workplace.[49] This Act and its Regulations were the result of strong lobbying by the biggest employers' organization, the The Confederation of British Industry (CBI) (www.cbi.org.uk). [50]

A measure enacted recently as a result of pressure by employer organizations, this time in Finland, the Act on the Protection of Privacy in Electronic Communications, is known informally as the Lex Nokia, because of the alleged intense interest and involvement of Nokia (though the company flatly denied any such involvement). This establishes similar guidelines to the Act in the United Kingdom and gives extensive prerogatives to employers to monitor and intercept the on-line communications of their employees.[51]

On the face of it, we see here legislation that may restrict, or even severely infringe, employee privacy in on-line communication at work, using equipment that the employer has put at their disposal. However, as argued by Mark Jeffery in his analysis of the Act and Regulations in the United Kingdom mentioned above, that is also relevant to the case of Lex Nokia, as both countries are EU Member States (though in principle, they may still enact Acts and Regulations), in the EU legal hierarchy, EU directives (95/46/EC and 97/66/EC) take precedence, and so does Article 8 of the European Convention on Human Rights. In case of conflict between domestic legislation and EU fundamental Rights enshrined in an EU Directive, Treaty or Convention, it is the latter that prevails.

In light of this, in case this issue is brought before either the European Court of Justice or the European Court of Human Rights, it seems likely that such domestic legislation will be found to be incompatible with EU rules and principles, and the employee's right to privacy will be upheld. It also appears likely that if the issue of internet and e-mail use is referred to the European Court of Justice, it will deliver a similar ruling to the *Cour de Cassation* in *Nikon*.[52] As there is a feeling that current legislation in the EU still does not respond sufficiently to the issues of privacy in the workplace, there is an ongoing initiative to regulate it, including all forms of monitoring and surveillance.[53]

3.4. Internet and e-mail: the case of israel

In Israel there were two sources that enshrined the right to privacy (Basic Law: Human Dignity and Liberty, Article 7, and the Protection of Privacy Act of 1981). Although, as

[49] On these Regulations and the Trades Union Congress (TUC) critique, see <www.eurofound.europa.eu/eiro/2000/12/inbrief/UK0012103n.htm>.

[50] For a discussion of English Law on workers' privacy and electronic communication, see M. Jeffery, 'Information Technology and Workers Privacy: The English Law', *Comparative Labour Law & Policy Journal* 23, no. 2 (2005): 301.

[51] For more information about this legislation and the reactions it provoked, see <www.eurofound.europa.eu/eiro/2009/03/articles/fi0903029i.htm>.

[52] See *supra* n. 42.

[53] See *supra* n. 38.

in other OECD countries, there is no specific legislation addressing privacy in the workplace, the Israeli courts, including the labour courts, find their authority in these acts.

Recently there has been added a new legal source, more specific this time: the Collective Agreement dealing with employees' use of computers made available by the employer. This is only the second of its kind in the world (after Collective Agreement No. 81 in Belgium mentioned earlier)[54] and will be discussed below.

3.4.1. *The Collective Agreement on Employees' Use of Computers in the Workplace*

The parties to this Agreement, signed on 25 June 2008,[55] are the New General Labour Federation (the Histadrut), which is the most representative Labour Union in Israel, and the Federation of the Israeli Economic Organization, a federation representing the majority of employers' organizations, who also signed it on behalf of the major employers' associations specified at the end of the Agreement.[56] The purpose of this Collective Agreement is to set clear norms for employers and employees regarding their mutual rights and boundaries concerning employee use of computers made available by the employer.

The agreement aims to strike a balance between the employer's legitimate property rights and managerial prerogatives on the one hand, and on the other hand the employee's right to privacy, which modern technology makes it easy to invade if no clear norms prevent it. This is evident from the opening declarations, stating that the aim is to strike a fair balance between the employer's rights to property and the employee's right to privacy. Both rights, as stated therein, are enshrined in the Basic Law: Human Dignity and Liberty.

In Article 2, titled Agreed Principles, the parties acknowledge the employer's property rights and managerial prerogative and that the use of the computer by the employee shall be: 'for work-related purposes, fairly, reasonably and in good faith according to the law and this Agreement', but subsection D stresses that: 'an individual's private life is no one else's affair and his dignity and privacy in the workplace shall be preserved and respected'.

Article 3 deals with Rules of Conduct. Subsection B makes it clear that, although the use of the computer is for work-related purposes, the employee may 'to a proportional degree and for a reasonable length of time' make use of it also for personal and private purposes that are not work related. Subsection C states that the activities by the employer in section A (dealing with maintenance and software) shall be carried out in 'good faith, reasonably observing transparency and for a legitimate purpose' and shall

---

[54] See *supra* nn. 30, 46, and 47.

[55] See *supra* n. 48 (the agreement is in Hebrew but as I have translated it into English, readers may find it in an appendix to Finkin's book cited in n. 4 or contact me directly).

[56] It should be noted that, unlike Belgium, where the agreement has been made binding on the whole country by Royal Decree, in Israel it is at present binding on the parties to the agreement who are in the private sector, although the possibility of an extension clause is built into the agreement in Art. 6, but not yet implemented. Art. 7 of the agreement makes it possible for other employers or employers' organizations to join this agreement.

make 'no use of personal data of the employee in a harmful way that effects his dignity and private life'. The most important subsection is D:

> In circumstances in which a reasonable employer would have cause to assume in good faith that an employee is making an illegal use of the computer or such use that could expose the employer to a legal suit by a third party such as to harm the enterprise, the employer shall be entitled to take actions to check the employee's computer, internet and / or e-mail, but it shall be done in a reasonable and proportional way, for a reasonable length of time and for the above mentioned purposes.
>
> Any entry into a personal mail box bearing only the employee's mail address and his personal files requires an explicit consent by the employee, and shall be done in his presence if he so wishes.

The key words appear to be 'in circumstances in which a reasonable employer would have a cause to assume in good faith', meaning that this right of the employer to actively monitor or check the employee's computer, internet or e-mail should not be used arbitrarily or out of pure unfounded suspicion but has to be grounded on reasonable cause and in good faith. The Agreement does not apply when the computer (and the mailbox therein) is owned by the employee.

It may be assumed that in the future, when disputes concerning the implementation of this Collective Agreement are brought before the labour courts, this will be the article or subsection they will be asked to consider, and it is to be hoped that it will be interpreted in a way that gives as much protection to the employee's right to privacy as is evident in the spirit of this Agreement.[57]

Such an agreement as this one in Israel, which is hard law but retains some of the features of soft law due to the relative ease with which it can be amended by the parties, thus lending it greater flexibility than typical hard law,[58] may be a suitable way to set clearer guidelines for employers and employees to deal with the issues arising from computer use in a spirit of cooperation between the parties.

3.4.2. *Case Law in Israel Concerning Monitoring Employees' E-Mail*

In Israel there is hardly any case law on e-mail monitoring and the rights of the employer to intercept and read e-mails. In this regard, Israel is no different from other countries, as this issue has not been brought before the courts very often: in the United States, the leading case is *Ortega,*[59] in Europe *Nikon*.[60]

---

[57] In Israel, unlike some other countries in which collective agreements are an instrument of soft law, collective agreements are subject to a specific law (Collective Agreements Act 1957) and once such an agreement has been registered by the Registrar of Collective Agreement, it becomes hard law. In the Israeli Collective Agreement, there is a mechanism that allows for amendments to the Agreement, should the need arise in the future (Art. 5 subs. D) as well as a mechanism of conflict resolution that reflects both the spirit of cooperation between the parties and an added dimension of flexibility, both typical of soft law.

[58] See *supra* n. 57.

[59] See *supra* n. 33.

[60] See *supra* n. 42.

While these rulings have been handed down by the highest courts, the Supreme Court in *Ortega* and the *Cour de Cassation* in *Nikon*, in Israel the two leading rulings have been handed down by regional labour courts, with conflicting outcomes. In the more famous (and controversial) case *Isakov-Inbar,*[61] the e-mail intercepted by the employer was a curriculum vitae that the plaintiff – the employee – had sent by e-mail to potential employers from her current employer's computer. Although, in principle, the Court acknowledged an employee's right to a degree of privacy in the workplace even when making use of the employer's property including phone calls, internet and e-mails for personal and private use as long as it is done in a reasonable manner, the Court reached the conclusion at the end of a lengthy analysis that the employee – the plaintiff – should be seen as consenting to the company's interception of her e-mails.

Two main reasons leading the Court to this conclusion can be inferred from the Court ruling: first, an implementation of the US reasonable expectation of privacy that leaves the employee with little, if any, right to privacy and is tilted heavily in favour of the employer (whereas normally in Israel the issue of privacy is regarded by the Courts as a matter of human dignity); second, a discussion of the consent allegedly given by the plaintiff. The Court inferred such consent as having been given because the plaintiff was aware that the computer system, including the mailbox, was regularly subject to antivirus checks.

This ruling gives rise to two problems. First, there is no reason why on such a sensitive issue as employee privacy the Court should adopt the US approach that is so restrictive of the right to privacy, while in general courts in Israel are much closer to the European approach of human dignity as can be seen from the Basic Law: Human Dignity and Liberty. Secondly, inferring an employee's consent for intercepting and reading e-mails from the fact that she knows that the system is checked for viruses seems to be far fetched.[62] The consent required should at least be informed consent,[63] making clear to the employee all possible potential forms of monitoring in the workplace.

An opposite result was reached by the Regional Labour Court in Nazareth in *Afikey Maim v. Rani Fisher.*[64] At the employee's request, the Court had suppressed as evidence e-mails that the employer has intercepted from the employee's mailbox, and the Court held that it was not enough to infer an employee's consent in order to infringe his privacy, and explicit consent was required. Both cases went on appeal to the National

---

[61] Tel Aviv Regional Labour Court Case 10121/06 *Taly Isakov-Inbar v. The Commissioner of Women's labour and others*, 15 Jul. 2007.

[62] It is possible that the court in that particular case was influenced by the fact that the document involved – a curriculum vitae – was not of an intimate nature. However, this does not detract from the fact that such a ruling if applied in another case, in which more intimate or personal correspondence might be involved, may pose a risk to the concept and right of protection of privacy in the workplace.

[63] The Protection of Privacy Law was amended on 26 Jun. 2007, and informed consent is now required. The Collective Agreement requires explicit consent in Art. 3.

[64] Regional Labour Court of Nazareth *Afikey Maim v. Rany Fisher* Case 1158/06 given on 9 Apr. 2008.

Labour Court, and the appeal is still pending. It will be interesting to see which approach is upheld by the National Labour Court.[65,66]

My view is that strict conditions should be laid down regarding the consent required, not only the informed consent that is now mandatory following the recent amendment to the protection of privacy law, but explicit consent as in the EU Directives. An employee's e-mails can be of a personal nature and allowing the employer to read them constitutes a severe infringement of the right to privacy and private life. In any case, the employer should never be allowed to do so of his own accord and should be required to get a writ or court order first, after convincing the Court that such disclosure falls within the scope of legitimate purpose, proportionality and transparency and is necessary in the circumstances

4. Principles and Guidelines: When Can an Employer Monitor or Intercept an Employee's Electronic Communication?

Clearly, there are different solutions and legal provisions on these issues in legal systems in the United States and Europe, and even in Europe and other OECD countries there are various approaches and outcomes. However, we can identify three principles:

(1) *Legitimate Purpose*: It is not sufficient for the employer to have an interest, legitimate in itself, to monitor an employee's on-line activities. There should be real justification for such monitoring to take place. This could be the proper function of the company, preventing unlawful or defamatory acts that are contrary to good moral conduct or that may violate another person's dignity (that is, hate mail or harassment), protecting the company's economic, commercial and financial interests, security and/or efficient technical operation of the company network system. Some scholars, like Roger Blanpain, call this the Finality Principle.[67]

(2) *Proportionality*: This rule means as much monitoring as necessary but no more. The monitoring of on-line communication may not, as a general principle, entail intrusion into the employee's privacy, and when it does, this intrusion must be kept to a minimum.

(3) *Transparency*: When a system for monitoring on-line communication data is installed, the employee (and works council, where one exists) must be informed by the employer of the fact, and all aspects of the monitoring. Clandestine monitoring or surveillance of employees is considered inappropriate

[65] After this article was submitted for publication, the National Labour Court gave rulings upholding the employee's right to privacy, in appeal case 90/08 *Taly Isakov-Inbar v. The commissioner of women's labour and others*, and appeal case no. 312/08 *Afikey Maim v. Rani Fisher* handed down on 8 Feb. 2011. Afikey Maim has filed an appeal against this ruling before the Supreme Court sitting as a Court of Justice, and this appeal is still pending

[66] The Collective Agreement has not yet been extended, as the government was awaiting the court's decision. Now it has upheld the employee's right to privacy, it is almost certain that an extension order will be issued, making it binding on all workplaces in the country, as in Belgium.

[67] See *supra* n. 30.

even in countries that, as a rule, endorse the employer's prerogative for monitoring, such as the United States, and in some countries, like Germany, it is prohibited.

While these principles are relevant in dealing with the legal systems in Europe (and Israel), in the United States the prevailing rule is 'the reasonable expectation to privacy', which can be interpreted in a way that leaves the employee with hardly any right to privacy in the workplace.

5. Employee's Consent: What Kind of Consent Should Be Required and What Is the Meaning of Such Consent

The issue of an employee's consent is not simple, as it always raises the question as to what extent it is true consent, freely given, even when given explicitly and in writing. The employee usually has no choice but to agree to the employer's request and conditions, particularly in the case of employees who are not in senior positions.

Even if we examine the term consent, the question is: what kind of consent are we dealing with? Is inferred consent enough, or should it be an informed or even explicit consent? Or maybe it is sufficient for the employer to give notice to the employee of the existence of monitoring or the possibility that such monitoring will take place.

In the United States, as far as this issue is concerned, there is no need for explicit or informed consent, and as a rule, it is sufficient for the employer to give notice to the employee that monitoring takes place or that it might. The notice given and the agreement of the employee to work (or continue to work if already an employee) in the workplace is regarded as consent on the part of the employee.[68] This is the lowest level of consent.

In Europe and particularly the EU Member States, it is certainly not enough to give notice that monitoring/surveillance might take place, and there is a requirement for explicit not inferred consent. The Directive uses the term 'explicit consent', and in all national legislation, there is a requirement of informed consent at least. It is also mandatory to make the employee aware of existing or potential monitoring or surveillance and also the works council or union representatives, when they exist, as to all the aspects of the monitoring. It is not sufficient to give a general unspecified notification regarding its existence or the intention to install it.

It should be stressed that in many European countries, such as Germany,[69] clandestine monitoring/surveillance is prohibited by law (except in specific circumstances like

[68] See M. Finkin, n. 4, and his following articles, n. 10.

[69] For an overview of the German law on these issues of employee's right to privacy in the digital age, including monitoring and surveillance of all aspects, see A. Koelandt, 'A Comparative Study of the Impact of Electronic Technology on Workplace Disputes: National Report on Germany', *Comparative Labour Law & Policy Journal* 24, no. 1 (2002), and H.-J. Reinhard, 'Information Technology and Workers Privacy: The German Law', *Comparative Labour Law & Policy Journal* 23, no. 2 (2005). German Law sets great store on the employee's right to privacy and the first ever legislation on this issue was in Germany, in the State of Hessen.

the real probability of an offence being committed or civil wrong by the employee: mere suspicion is not enough). Even in the United States, such conduct is frowned upon, as it is considered to be unfair.

In Israel, notice is not enough, and while previously the consent required by the protection of privacy law could also have been inferred consent, it has been recently amended so that now the consent required is 'informed consent',[70] a higher level. The meaning of this consent is:

> That the person who agrees that his privacy shall be infringed shall have the information reasonably required in order to make up his mind whether he should agree or not, and that the information shall be given in a clear and understandable way.[71]

This amendment is an important step in the protection of privacy. The issue of consent – a controversial topic when considered in the context of the employment relationship – is still an important factor that we should be aware of when looking at privacy in all its aspects.[72]

6. The Right to Privacy and the Use of Phones and Mobile Phones

In any discussion of privacy regarding phones and mobile phones, we are talking, as with regard to computer use, only about phones (or phone lines) provided by the employer basically for work-related purposes. Although telephones have for many years been an inseparable part of the modern workplace, and there is a growing use of mobile phones (and similar devices) by employees whose everyday work is performed on a regular basis outside the employer's premises, it may be surprising to discover that there is little case law regarding such use.

The European sources mentioned above that refer to privacy of communication also apply to these channels of communication, and clearly under European law, they fall within the scope of privacy protection.

According to the European perception, as can be seen time and again from legislation and case law, in the modern world of work, it is difficult to draw a clear demarcation line between work and private life. Employees spend a great deal of their lives in the workplace and it is there that many of their most important relationships and communication with other human beings takes place, often using electronic devices.

One of the few court cases dealing with this issue was given by the European Court of Human Rights in Strasbourg, *Copland v. the United Kingdom*.[73] In this case the plaintiff – the employee – claimed that her employer had infringed her right to privacy by monitoring her phone calls to another employee with whom she went on a business trip (the employer, who suspected them of having an affair, wanted to verify his suspicions).

---

[70] Article 2(2) of the protection of privacy Law (Amendment No. 9) 2007, in force since 19 Jun. 2007.

[71] Proposal of Protection of Privacy Law Amendment No. 5 2005, 232.

[72] For a discussion of the issue of employee consent, see R. Fragale Filho & M. Jeffery, 'Information Technology and Worker's Privacy: Notice and Consent', *Comparative Labour Law & Policy Journal* 23, no. 2 (2005).

[73] *Copland v. the United Kingdom*, European Court of Human Rights, Application No. 62617/00.

The Court remarked that at that time there was no right to privacy in the law of the United Kingdom. Meanwhile the Regulations of Investigatory Power Act 2000 and the Telecommunications (Lawful Business Practice) Regulation 2000 have been enacted,[74] making possible, in certain circumstances, for an employer to monitor and even intercept an employee's electronic communications, even without consent. However, the employer is obliged to alert the employee to the possibility of such monitoring and/or interception.

The Court ruled in favour of the employee, based on Article 8 of the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms, and held that regardless of whether the employer actually made use of the information, the mere fact that he collected and stored such data regarding private phone calls without the knowledge of the employee was a violation of her right to private life and communication and awarded her monetary indemnity.

It is important to point out that the information discussed in that case was the duration of the phone calls and to whom they were made and not the contents of the conversations, as listening in to a conversation by a third party is prohibited by law in the United Kingdom, unless both parties to the conversation are aware of it and give their consent.

We might assume that the Court's decision would not have been any different had the case of *Copland* been brought before it after the Regulations of Investigatory Power Act 2000 and the Telecommunications (Lawful Business Practice) Regulation 2000 were enacted, as arguably the Convention for the Protection of Human Rights takes precedent over domestic legislation[75] that conflicts with it.

Another important ruling by the European Court of Human Right was given in *Halford v. United Kingdom*.[76] In that case, Ms Halford filed a claim of sexual harassment against her employer – the police. As a senior police officer, she was entitled to use two phone lines in her office, one for work-related purposes and the other for personal use. However, she had discovered that her employer had monitored the conversations made through on the private line and used its contents against her in the court proceedings (for sexual harassment). She appealed to the European Court of Human Rights, claiming that her privacy had been violated.

The Court found the employer's conduct to be a gross violation of the European Convention on Human Rights and condemned the lack of individual protection of privacy in such circumstances. This ruling gave the United Kingdom an incentive to enact the legislation mentioned above, as the Convention states that interception of communication can be made only in accordance with the law, and in the absence of such a law during the Halford case, that basic condition was non-existent under law in the United Kingdom.

---

[74] See *supra* nn. 49 and 50; see also the guidelines published by the UK Commissioner of Data, the Employment Practices Data Protection Code 2003.

[75] See n. 50, at 330–332, 305–308.

[76] *Halford v. U.K.* 24 Eur. Court of Human Rights 523 (1997).

It can be argued that even when such a law does exist, as it now does, it will not always stand up to the scrutiny of the European Courts and it will still have to meet the standards laid down by the Convention and the EU Directive.[77]

Although these examples concern cases in the United Kingdom, they are relevant to other European countries. The rulings of the European Court of Human Rights appear to be well founded and justified.[78] My view is that no employer should be entitled, at his discretion to monitor, and certainly not intercept, an employee's telephone conversations. Whenever he wishes to do so and in so far as this information might be relevant for a legitimate purpose, such as court proceedings in which these conversations are of crucial importance as evidence, he should apply first for a court order and persuade the Court that this disclosure of information is necessary in the circumstances.

The principles that apply to the use and monitoring of internet and e-mail (legitimate purpose, proportionality and transparency) should be the criteria for courts of law regarding this aspect of monitoring and should be the guidelines for employers.

As for SMS messages sent or received via mobile phones, they should be regarded exactly like e-mails. They are the sort of communication that should enjoy the protection of privacy, as, like e-mails, they may contain messages of an intimate and personal nature pertaining to the employee's private life.

However, I find it necessary to add that unlike the issue of monitoring and interception of phone conversations and SMSs that touch directly on the issue of privacy, as with the internet and e-mail, we should distinguish between the issue of use and that of monitoring, and only monitoring gives rise to problems of employee privacy.

7. Surveillance Cameras and CCTV

This is the most intrusive form of monitoring, as it invades the employee's personal space. There can be a number of reasons on the employer's part for such monitoring:

- *Security*: If set up in an efficient manner, a video surveillance network/CCTV can significantly improve workplace safety and security.
- *Promotion of Good Behaviour*: Surveillance might reduce the probability of workers failing to act in according with corporate standards, but it may also be argued that it is likely to decrease morale in the workplace by creating a feeling among workers that the company does not trust them.
- *Prevention of Theft (or other criminal activities):* Proper use of video surveillance systems prevents larceny and has enabled organizations to save a lot of money on stolen goods.
- *Providing a Record of Criminal Activity:* If crime has occurred in a company, it may be easier to see and prove what took place using video recordings.

---

[77] See *supra* nn. 50 and 75.

[78] Once again, the US approach is different. See M. Finkin, *Privacy in Employment* Law, 3rd edn (BNA Books, 2009), 344.

The technology that enables the employer to carry out electronic surveillance is becoming ever more sophisticated, so it can be done without the employee being aware of it. The question is, should the employer be allowed to do so and if so, under what conditions and circumstances? Once again, the US and European systems take two entirely different views.

It can be generally said that in the United States, laws are biased towards the needs of the employers. The company's space is understood to be the property of the company where the worker is employed, and employees should not have expectations of privacy at work. As a rule, employers are allowed to monitor any of their facilities with cameras and monitoring rights are extensive. The only restrictions are on recording in bathrooms, changing facilities or bedrooms (and in some states, places that are meant for the employee's rest and comfort). In many cases where the question of the legality of surveillance camera has arisen, the Courts have ruled that employee monitoring is legal provided employees are given notice. It should be noted that covert surveillance even in the United States is usually illegal and may be grounds for a lawsuit by the employee.[79] The extent to which employers in the United States can use video surveillance to monitor employees depends on the state and the type of business they engage in.

One of the most famous cases in the Supreme Court of California is *Hernandez v. Hillsides, Inc.*[80] In this case the employer installed motion-triggered hidden video cameras to catch those suspected of accessing pornography by computer. One camera was placed in an office used by two employees who were not suspected of misconduct, a place where they (the plaintiffs) stayed after office hours and sometimes changed clothing before leaving for after-work exercise. After setting the standards for privacy violations under state common law and constitutional law, the Court held that although the plaintiffs' privacy in a shared office was not absolute, they had a reasonable expectation of privacy and the employer could not install video equipment to monitor and record their activities, personal and work related, behind closed doors without their knowledge and consent.

In contrast, European law is much more oriented toward protecting the privacy of employees than US law. Many EU Member States require written individual consent for any form of monitoring that includes camera surveillance. For instance, several countries like France and the Netherlands require filing with labour authorities before monitoring can take place, and others such as France, Germany, Italy and the Netherlands require employers to consult or at least notify trade unions or works councils before using any form of surveillance.[81] In Italy, remote surveillance is forbidden by law. In Germany, the works councils have earned a reputation as fierce protectors of employee privacy rights.

---

[79] On the US position on camera surveillance, see M. Finkin, n. 78, at 310–322.

[80] *Hernandez v. Hillside Inc.*, 47cal. 4th 272 (2009). See also *Bruzinski v. Amoco Petrolium Additives Co.* 6F. 3d 1176 (7th Cir. 1993).

[81] Recently, the *XVII Meeting of European Labour Court Judges* organized by Prof. Alan Neal convened in Slovenia in 12 Jun. 2009 to discuss the issue of privacy in the workplace and Judges submitted country reports on this issue from Belgium, Finland, Germany, Hungary, Ireland, Israel, Slovenia, Spain and Sweden responding to a questionnaire prepared by Prof. Alan Neal with the aim of learning from each other.

Their opposition to the infringement of employee privacy invokes the rights and protections afforded German employees pursuant to the EU Data Protection Directives[82] as well as German federal and state data protection laws.[83] Covert surveillance and monitoring is forbidden under German law.

The Federal Labour Court in Germany has ruled that surveillance is permitted only in so far as it is subject to the proportionality principle and that the restriction of the right to privacy (conceptualized in Germany as the personality right) must be proportionate to the legitimate need of surveillance under specific circumstances.

However, even in a country like Germany, there are some aberrations, as the *Lidl* case demonstrates.[84] *Lidl* had an extensive system of video and acoustic surveillance (even in the toilets) and surveillance by detectives aimed at collecting information on the causes of diseases, reasons for sick leave, possible irregularities, how often and how long the cashiers went to the toilet, what they talked about, and whether they had plans to have children by natural or assisted fertilization. The works councils (as far as they exist, because *Lidl* is fairly successful in preventing them from being set up, which is unusual in Germany) were not informed and the company did not set up co-determination either. Moreover, they did not appoint a data protection officer as required under German Law. When the situation came to light the state's data protection officer intervened, and *Lidl* was fined EUR 1.5 million.

In all European countries and in Israel, the legal provisions are more or less the same,[85] although as yet there is no specific legislation in any of them concerning privacy in the workplace, and the Courts draw their authority from constitutions (when they exist) or legislation on the protection of privacy in general and in EU Member States also from the Directives. A specific directive is still under consideration, as noted earlier.[86] The position of the Courts tends to be the same across most European countries and in Israel. The following examples are taken from Israel.

In *Eisner v. Richmond Knitting Company Ltd*[87] an employee was fired after she discovered that her employer had installed video surveillance cameras in the store without her knowledge and ripped them off the wall in a rage. The Labour Court held that, although employers are entitled to run the business at their discretion, the installation of surveillance camera without informing the employee of their existence and filming her was a unilateral alteration of the employment contract and a violation of her privacy.

See also S. Nouwt, B. R. de Vries & Corien Prins (eds), *Reasonable Expectation of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* (Netherlands: T.M.C. Aspen Press, 2005).

[82] See *supra* nn. 16, 17 and 18.

[83] <www.bfdi.bund.de/cln007/nn946430/EN/DataProtectionActs/Artikel/BundesdatenschutzgesetzeFederalDataProtectionAct.pdf>. Every German state has its own data protection law in addition to the Federal one.

[84] This case, as well as the scandals concerning Deutsche Bahn AG and Deutsche Telekom, was described in the German Report by Judge Annelie Mauquardt in the *XII Meeting of European Labour Court Judges*. See n. 81. Following such cases in Germany, there is now a debate on an initiative to enact specific legislation on privacy in the workplace in addition to existing legislation on privacy in general.

[85] See country reports, *supra* n. 81. The Israeli report was given by Judge Elisheva (Elika) Barak.

[86] See *supra* n. 20.

[87] *Eisner v. Richmond Knitting Company Ltd*, Case 2734/00, Tel Aviv Regional Labour Court given in 2001.

In *Olga Mochi and others v. Mishan Centre,* surveillance cameras were installed when the employer had reasonable and well founded suspicions of larceny committed by the plaintiffs (which they afterwards admitted), and their claim that their privacy had been violated was rejected by the Court, as the place where the cameras were located was an open working area and they could have no expectation of privacy there, and even if there was an infringement of privacy, the Court added, it would have been reasonable and proportional under the circumstances and the defendant could claim the legal defences of Article 18 of the protection of privacy law.[88] However, in *Hanan Adaki v. Mishan Centre*, the plaintiff, a security supervisor, was dismissed when the new CEO found out that he had installed surveillance cameras without permission, filming a secretary throughout her working hours without her knowledge and with no suspicion of any wrongdoing on her part. The Labour Court found the dismissal justified under the circumstances and stated that the secretary's right to privacy had been violated without cause.[89]

Apart from national legislation, it is worth mentioning that the UNI Code of Practice on on-line monitoring at work also deals with the issue of surveillance cameras, and although it is not legally binding, this code can be an inspiration for codes of practice or guidelines for employers and employees in the workplace around the world.

In Belgium video surveillance in the workplace is governed by Collective Agreement No. 68, 16 June 1998,[90] inspired by the ILO Code of Good Practice on Workers Privacy and the Belgian law of 8 December 1982 on the protection of private life. Employer and worker representatives on the National Labour Council wanted to define specific safeguards with respect to surveillance at work, and they agreed to introduce mandatory consultation and information disclosure on video surveillance. The agreement covers all video surveillance systems, whether or not the recordings are destroyed, and specifies four purposes for which they may be used:

- health and safety;
- protection of the firm's property;
- monitoring the impact of machinery or workers on production;
- monitoring worker output.

The agreement specifies that surveillance 'should be appropriate and not excessive with respect to the objective' (Article 7) and that it should not intrude into private life (Article 8). The agreement also imposes an obligation to inform workplace and/or union representatives on the introduction of video surveillance and matters relating to their installation and operation, as well as an obligation to consult the same bodies if it appears that video surveillance might have an impact on the workers' private lives, in which case employers are required to reduce intrusion to a minimum.

---

[88] *Olga Mochi and others v. Mishan Center*, Case 2673/04 Haifa Regional Labour Court, 2008. The same ruling was given in similar circumstances in the case of *Sergei Rivan v. Negrinka Maxim*, Case 2887/03 Haifa Regional Labour Court, 2006.

[89] *Hanan Adaki v. Mishan Centre*, Case 4270/07 Tel Aviv Regional Labour Court, 2007.

[90] <www.eurofound.europa.eu/eiro/1998/inbrief/be9807150n.htm>. The agreement was concluded on 16 Jun. 1998 by the bipartite National Labour Council (Conseil National du Travail/National Arbeidsraad).

However, even though this agreement reflects the spirit of cooperation between the social partners, workers do not like surveillance cameras, and in 2005 there was a strike in Belgium resulting from a dispute over installation of workplace cameras in a metal-working company.[91] This dispute serves to demonstrate the sensitivity of workers to the installation and operation of surveillance cameras, when the employee is made the object of surveillance or directly exposed to it.

Even when there is a valid reason for installing cameras, it should always be done in compliance with legitimate purpose and proportionality principles and in good faith, and employers should do their best to keep intrusion of employee privacy to a minimum. For instance, when a surveillance video camera is installed in the safe-deposit boxes area of a bank, undoubtedly a legitimate purpose, it should be directed, if possible, at the entrance or the safe-deposit boxes and not at the worker.

The installation and existence of such cameras should be made known to the employee, as covert surveillance brings to mind associations of autocratic regimes and has no place in a democratic workplace (except in special cases such as reasonable suspicion that an employee is committing an offence, with the camera installed for a limited span of time).

The knowledge that a surveillance camera is present and a person is subject to the constant, ever staring electronic eye, that unlike the human eye never blinks and never tires, even for an honest person, has a stressful psychological effect, hence the 'Medusa stare' as the title of this article. Clearly, an atmosphere of suspicion does not contribute to a pleasant work environment.

I leave as an open question whether such surveillance should take place on a regular basis in the case of employees taking care of older persons, small children or people with a disability.[92] My personal opinion is that workers should not be subject to such surveillance solely because they are employed as carers. However, when there is a reasonable suspicion about their conduct and behaviour towards the person they are caring for (of neglect or actual abuse), it is justified to put such surveillance systems in place even without their knowledge at least for a limited time in order to verify or rule out those suspicions. This kind of work often takes place in the home behind closed doors and those taken care of are often not in a position to defend themselves or even tell others of the abuse, and a camera might be the only way to verify what is going on.

8. Theft Prevention Checks

Another area of potential conflict of interest between employer and employee regarding the issue of privacy is theft prevention checks. Again Belgium led the way by choosing

[91] See the dispute in the company Strong Trailers at Your Service, at <www.eurofound.europa.eu/eiro/2006/10/articles/be0610069I/htm>.

[92] A few cases have come to the attention of the media in Israel, in which carers of such defenceless people were discovered abusing the person they were supposed to look after. These cases usually happened at home and could only be proven by installing hidden cameras: this is no doubt the case in other countries as well.

to deal with this sensitive issue by engaging the social partners, and since 30 January 2007, Belgian employers have been entitled to screen people for theft on leaving the company premises. This followed the consensus between the social partners on 18 October 2006 when a Collective Agreement was concluded: Collective Agreement No. 89 on theft prevention checks on workers exiting the enterprise or workplace,[93] subsequently transposed into law.

On the basis of this agreement, as of 1 January 2007 dedicated company security agents, who are not employees of the company, are allowed to perform random controls of theft on anybody leaving the premises, including employees and anyone else who has entered the company's premises, such as self-employed persons, sub-contractors, service personnel and suppliers. Security agents are only allowed to carry out checks with the prior consent of the individual. Besides these random checks, they are permitted to check an individual worker on the basis of a serious suspicion of theft.

These procedures are bound by the following rules and conditions. Body searches are not allowed (only a police officer may perform them); employers have to clearly outline what they define as theft; checks are only permitted to prevent theft or catch someone in the act of stealing but not for work performance or attendance; systematic checks are only allowed when using an electronic detection system; checks must form part of an overall theft prevention plan; checks have to be reasonable and transparent, keeping intrusion to the employee's privacy to a minimum; a company employee suspected of theft has to give their consent before being screened by private security agents; in the event of actual theft, the procedures must always be conducted with discretion and a written report must be sent to the employer, with a copy to the employee.

Moreover, checks can only take place after the employer has informed and consulted the employee representatives, either the works councils or trade union delegation, about the intended system, and this system has to be explained and described to them. In small enterprises with no such representatives, it has to be explained to the workers themselves.

Security checks that are performed without the proper information requirement are defined by the collective agreement as a non-legal act in accordance with the revised Act on Private Security and can be treated as a criminal offence.

It seems that the new theft control measures adopted in Belgium represent a precarious balance between the potential need for such controls on the part of the employer and the employee's right to privacy. However, it is likely that the mere adoption of such checks on a regular basis may generate an atmosphere of distrust, which is not a positive factor in the workplace. Therefore, it can be argued that such measures should not be adopted in the ordinary course of business but rather resorted to when in a workplace there is reasonable and well founded suspicions of theft or other criminal activities

[93] See <www.eurofound.europa.eu/2006/12/articles/be0612029i/htm> and the Collective Agreement at <www.portalecnet.it/CES/ceslink.nsf> in the French and Flemish versions.

committed by a worker or group of workers.[94] It should be stressed that in Israel and in most EU countries an employer is forbidden by law to conduct a body search on an employee.[95]

9. Miscellaneous

To complete this overview of the issue of privacy with regard to monitoring and surveillance, I would like to mention some other contexts in which this issue may arise.

9.1. Location data

In the modern workplace, many workers work away from the employer's premises. The use of location data might be the only way to verify that workers were actually at the location where they were supposed to be, as the employer has no other means of supervision, and indeed, in a case in which this issue arose in Israel, that was the position taken by the Court.[96] In Europe as well it is allowed for an employer to monitor the activities of an employee performing work away from the employer's premises as can be inferred from the Framework Agreement on Telework, Article 6, that deals with monitoring.

I do not regard the use of location data by itself as an intrusion into employee privacy, but I argue that two conditions should be applied: the first is that the employee should be made aware that such location data is in place and may be used to trace his whereabouts. Second, unlike the actual location of the worker, which the employer is certainly entitled to ascertain in order to be sure he is at work, the employer should not look into the employee's private life more than is needed, unless this is also relevant under the circumstances.

For example: it is relevant information for the employer of a sales representative who suspects him of delivering goods to a business competitor to know where he has been, at what time and for what purpose, but if it was discovered that instead of being at work at certain delivery points he was having an affair with a married woman and was at her house or a hotel, it is enough that the employer knows he was not at the places he was supposed to be in but at another location, and he should not ask more information as to the woman's name and other intimate details that relate to the employee's personal life. However, if the location data points to a competitor's place of business, he may be entitled to more details.

---

[94] This balance between control and privacy was also the subject of a recent collective dispute in Belgium over the installation of security cameras in the metalworking company Strong Trailers at Your Service. See n. 91.

[95] From the judges' reports in the *European Labour Judges Meeting*, see n. 81. Only three countries, under specific conditions, allow an employer or someone on his behalf to do so: Ireland, Hungary and Spain. In all other countries, body searches can be conducted by a police officer only.

[96] *New Histadrut v. Tashan Oil and Energy Industries Ltd*, Case 1026/06 given by the Beer Sheva Regional Labour Court, 2006.

9.2. Call centres

It is common knowledge that companies running customer care centres or call centres routinely record the conversations between the customer and the call centre. In Israel and elsewhere, both sides to the conversation are notified by means of a recorded message that in order to improve service the conversation may be taped.

In my view, this situation does not give rise to concerns about privacy strictly speaking. The recorded message before the conversation alerts both sides to the possibility of the conversation being recorded and such conversations by their nature tend not to be intimate but business/service related. The purpose of the recording is to give the employer an indication of the efficiency or attitude of the customer service worker, clearly a legitimate purpose, and it can also be argued that this recording may also offer protection for the employee by deterring customers from harassment or threatening behaviour. As these conversations are not of a personal or private nature, they measure up to the criterion of legitimate purpose, proportionality and transparency, and as such are not an intrusion on the employee's privacy.

However, my response would change if it turned out that such recording takes place on phone lines not specifically reserved for customer service, without the customer service worker being aware of it, while he can reasonably assume that he is engaged in a private conversation.

In Europe, in May 2004, the EU social partners in the telecommunication sector, the European Telecommunication Network Operators Association (ETNO) for the employers and UNI-Europa Telecom for the trade unions, announced an agreement on joint guidelines to cover customer centres or call centres across the EU. The guidelines, which take the form of a Charter for call centres, were concluded within the framework of European sectoral social dialogue.[97]

In addition to listing the key principles, the Charter lays down guidelines on the monitoring of employees and their rights to privacy. It states that monitoring may only be allowed when the purpose is 'known and acceptable' and that any data collected may be used only for that purpose. The employees must know that they are or may be monitored and any listening in may take place only 'incidentally', not continuously. Employees must be allowed access to registered data and be able to correct inaccuracies. Finally, the recordings must be destroyed after a certain period.

10. Conclusion

The growing use of electronic media and the spread of sophisticated technology in this modern digital age has many advantages but at the same time poses potential threats to our privacy in the information society as individuals and in particular as employees.

[97] <www.eurofound.europa.eu/eiro/2004/05/feature/eu0405204f.htm>.

The issue of employee monitoring and surveillance is complex, as it involves conflicting rights and interests. On the one hand, the employer has a right to property and managerial prerogatives, as well as a reasonable expectation that the employee will be available for work in the workplace. On the other hand, the employee has a right to privacy and private life that does not stop and should not be set aside at work.

I have tried to examine the issue of monitoring and surveillance in all its aspects and to refer as far as possible to legislation and other hard law and soft law arrangements, showing that there are various approaches to these issues by various legal systems, in particular the US and European perspectives. Even in Europe the responses and solutions are not always the same, even if there is greater homogeneity at least with regard to general principles.[98]

The starting point for examining these issues should be that any monitoring that accompanies intrusion of privacy, even for a legitimate purpose, causes discomfort for the employee. Reasonable employers are not overly suspicious, and reasonable employees come to work to perform the job and not to steal or otherwise engage in dishonest or criminal activities against the employer. As far as possible, these issues and interests should be defined and agreed upon in a spirit of mutual respect and cooperation by the parties to the employment relationship while attempting to strike a balance between their interests, as in the Collective Agreements in Israel and Belgium, and other kinds of agreements and guidelines that seem to be an appropriate way to reach joint and acceptable solutions to the problems and conflicts arising from those issues, observing the principles of legitimate purpose, proportionality, transparency and good faith while drawing clear and explicit boundaries for the parties[99] in order to maintain a fair and pleasant atmosphere in the workplace that serves the interests of both sides.

[98] That is why it is important to learn from each other on these issues, and this was the purpose of the European Labour Court Judges' reports, see n. 81, and the unified questionnaire prepared by Prof. Alan Neal, who designed it to obtain each country's report on the same questions and issues.

[99] We cannot dispense with hard law on these issues, which is important for laying down the legal norms and principles, but soft law or quasi-soft law solutions add the flexibility and the spirit of mutual cooperation that in my view serves to cope more adequately with the challenges of electronic media.

For subscription enquiries:
Kluwer Law International:
c/o Turpin Distribution Services Ltd., Stratton Business Park, Pegasus Drive, Biggleswade, Bedfordshire SG18 8TQ, United Kingdom,
E-mail: sales@kluwerlaw.com.

The subscription prices for 2011(volume 27, 4 issues) are
Print subscription prices: EUR 296/USD 395/GBP 218
Online subscription prices: EUR 274/USD 366/GBP 202(covers two concurrent users). This journal is also available online. Online and individual subscription price available upon request. Please contact our sales department for further information at +31 172 641562 or at sales@kluwerlaw.com.

International Co-operation
The International Journal of Comparative Labour Law and Industrial Relations is a founding member of the the International Association of Labour Law Journals established for the purpose of making collaborative arrangements for the advancement of research in the fields of labour law and industrial relations and for the exchange and publication of material.
The other members of the group are: Arbeit und Recht, Australian Journal of Labour Law, Comparative Labor Law and Policy Journal, Industrial Law Journal (UK), Japan Labor Bulletin, Lavoro e Diritto, Relaciones Laborales, Análisis Laboral, Bulletin of Comparative Labour Relations, Industrial Law Journal (South Africa).

Citation
The International Journal of Comparative Labour Law and Industrial Relations may be cited as follows: (2011)(1) *IJCLLIR*.

Refereeing process
Articles for publication in the IJCLLIR are subject to peer review under the supervision

ISSN 0952-617x

The International Journal of Comparative Labour Law and Industrial Relations is published quarterly by Kluwer Law International BV, P.O. Box 316, 2400 AH Alphen aan den Rijn, The Netherlands.
Periodicals Postage Paid at Rahway N.J., USPS No. 013–141.

U.S. Mailing Agent: Mercury Airfreight International Ltd.,
365 Blair Road, Avenel, NJ 07001, U.S.A.

Postmaster:
Send address changes to: Mercury Airfreight Int.'l Ltd. 365 Blair Road,
Avenel NJ 07001, U.S.A.