Chapter 66
Employees' Protection:
Workplace Surveillance 3.0

Chrysi Chrysochou
Aristotle University of Thessaloniki, Greece

Ioannis Iglezakis
Aristotle University of Thessaloniki, Greece

ABSTRACT

This chapter describes the conflict between employers' legitimate rights and employees' right to privacy and data protection as a result of the shift in workplace surveillance from a non-digital to a technologically advanced one. Section 1 describes the transition from non-digital workplace surveillance to an Internet-centred one, where "smart" devices are in a dominant position. Section 2 focuses on the legal framework (supranational and national legislation and case law) of workplace surveillance. In section 3, one case study regarding wearable technology and the law is carried out to prove that national and European legislation are not adequate to deal with all issues and ambiguities arising from the use of novel surveillance technology at work. The chapter concludes by noting that the adoption of sector specific legislation for employees' protection is necessary, but it would be incomplete without a general framework adopting modern instruments of data protection.

The only realistic attitude of human beings living in such environments is to assume that any activity or inactivity is being monitored, analysed, transferred, stored and maybe used in any context in the future.[1] *(J. Cas, 2005, p. 5)*

INTRODUCTION

Surveillance in the workplace has generated increasing concern in the recent past. The shift from a non-digital to a technologically advanced work environment allowed employers to use sophisticated monitoring systems to control their employees' activity during their working hours, their breaks or in some exceptional cases even outside working hours. Although many of these practices may serve le-

DOI: 10.4018/978-1-5225-8897-9.ch066

gitimate employer rights, such as ensuring productivity and quality control, they can also carry major implications for the employees' right to privacy and data protection. The current European and national legal framework deal with certain aspects of employees' monitoring in the workplace and their right to privacy and data protection. However, it is not clear whether current laws are adequate and efficient to balance the conflicting interests of employees and employers in a modern environment where the rapid development of electronic technologies facilitates deeper and more pervasive surveillance techniques in the workplace (Lyon, 1994, p. 35).

The Context of Surveillance

The discussion on surveillance started officially in the eighteenth century with the conception of *Panopticon*[1] by J. Bentham (Boersma, 2012, p. 302) and continued in the twentieth century with Orwell's vision of a society under the watchful eye of *Big Brother (*Orwell, 1949). Since then, many scholars have defined surveillance in several ways, taking into consideration the impact that information technology had on surveillance. M. Poster (1996), for example, referred to a "*Superpanopticon*", a surveillance system that facilitates decentralized and dispersed transmission of an individual's data through computers without his (sic) knowledge. For Gary Marx (2002), surveillance is "the use of technical means to extract or create personal data. This may be taken from individuals or contexts". Marx (2007) believed that the 21st century is the era of "the new surveillance"(op. cit., p. 89), a hidden, surreptitious but ubiquitous surveillance. This "*new surveillance*" is found in everyday life; smart video surveillance cameras are found in streets and buildings; smart phones and computers are equipped with locator chips; workers are constantly monitored at work when using their corporate computers and GPS-fitted company cars or through closed circuit TV (CCTV), e-mail and phone-tapping (Coleman et al, 2011, p. 20).

In this modern computerized version of surveillance, Lyon talked about the "disappearance of the body" (Lyon, 1994, p. 35) and Van der Ploeg about the "informatisation of the body" (2007, p.47), where biometric surveillance transforms the unique characteristics of an individual's body into identification tools (fingerprints, facial recognition and iris scan). In the employment context, surveillance is expressed through monitoring, a direct or indirect observation of employees' activities and behaviour at work (Phillips, 2005, p. 40). A few examples of this monitoring include e-mail and phone-tapping, video recording and biometric surveillance. But what prompted such employee monitoring?

Reasons Why Employers Monitor

In a general context, surveillance has existed almost for as long as work itself. Traditionally, surveillance had the form of physical supervision aiming to assess work performance. Due to technological developments nowadays, employers have adopted advanced surveillance systems to monitor their employees in order to reduce the cost of human supervision. The two main types of surveillance in the workplace are 'performance surveillance' and 'behavioural surveillance' Both surveillance types exist to prevent employee misconduct, corrupted or criminal actions and to protect the employer's property rights over his undertaking.

A 2004 UK survey on employee monitoring reveals that employers might lose money for not monitoring their employees at work[2]. According to a more recent survey, 64% of the employees spent time surfing the Internet and visiting non-work-related websites, such as Facebook and LinkedIn (*cyberslacking*)[3]. As a result many employers introduced monitoring policies to avoid the loss of employees' productiv-