Panopticon's Electronic Resurrection: Workplace Monitoring as an Ethical Problem

Köksal Büyük*, Uğur Keskin**

Abstract: We live in a world of electronic monitoring with a view to improve the employees' efficiency. The lack of legal regulations in this area leads to shift from monitoring the employees' work lives towards their private lives. Failing to restrict such monitoring may cause losses in organizational efficiency and it negatively affects the psychology of employees. Rapid changes in technology in recent years have greatly reduced the costs of electronic monitoring systems, and as a result new electronic monitoring tools have emerged in work life. The purpose of this study is to find out the ethical ways for electronic monitoring in organizations. To this end a comprehensive literature review has been conducted and the findings have been discussed. An unnecessary monitoring system will cost financially to businesses and imply lack of trust in employees. In order to prevent violations of privacy in the workplace the boundaries of monitoring should be clearly stated to all employees in accordance with the principles set by various international organizations.

Key Words: Workplace Surveillance, Panopticon, Electronic Monitoring, Employee Privacy, Business Ethics.

Development of information technologies has significantly affected the forms of work and structure of labour. In no time in history have employees been under such close surveillance, which is one of the consequences of the transformation from industrialisation society into information society. Information technologies that were used in military and defense purposes during World War II were introduced into the business world in the 1970s and brought about radical changes in organizational structures. Information society was born as a result of such changes. The transformation into information society has accelerated since the 1980s with the

* Ph.D., is an assistant professor Management. His research interests include strategic performance management, management philosophy, and corporate governance.
Correspondence: Eskişehir Osmangazi Üniversitesi, İktisadi ve İdari Birimler Fakültesi, Eskişehir, Turkey.
§ E-mail: koksalbuyuk@gmail.com § Phone: +90 222 239 3750/1038.

** Ph.D., his research interests include human resource management, management philosophy, performance management.
Correspondence: Hava Teknik Okulları Komutanlığı, Gaziemir, İzmir, Turkey.
§ E-mail: ugurkeskin08@gmail.com § Phone: +90 232 251 1600 /4497.

transformation of information into a strategic competitive factor. Products and services of the new economy have brought to foreground the conversion of information into knowledge, knowledge management, processing, and distribution. The rapid development of information technologies has necessitated rapid changes in business processes, organizational structures, and the structure of workforce profile, products and services. This new economy indicates a change in the mind set and understanding at micro and macro levels (Söylemez, 2001). Castells (2005, p. 99) suggests that the outcome of this change is the global economy that is based on information and network organization. This transformation has also affected the organizational designs: horizontal and rigid organizational structures have been replaced with flexible organizations, mass consumption with niche consumer products, mass production with flexible production supported by information technologies, fixed and limited capabilities with versatility and the focus has shifted from strategic business units and products towards HRM skills (Erdemir, 2007, p. 74).

Extinction of Privacy in the Workplace: Organizational Surveillance

Privacy could be defined as to what extent the individual is recognized by others, he or she is physically accessible to others and is the object of others' interest and attention (Yüksel, 2009, p. 278). Organizations should fulfill some basic moral responsibilities towards their employees. The prime responsibility should be about respecting the employees' opinions, human dignity, and confidentiality of private life (Bowie & Duska, 1990, p. 86). Privacy could be identified in three different levels, the first is spatial privacy which involves the physical area surrounding the individual, the second is personal privacy which involves protection of the individual from unjustified interference and the third is information privacy which involves gathering, storage, processing and distribution of personal data (Eralp, 2013). The debate about employee privacy in work is usually grouped under three main headings; the first one is about monitoring the use of technological tools such as phone and computer; the second one is about surveillance of behaviour or performance of employees in the workplace through cameras; and the third one is the information security of companies who possess personal information about their employees (Erdemir & Çeliktaş, 2006, p. 90).

Monitoring refers to information that is collected in relation to the workplace and employees in an automated manner, regardless of purpose, while the concept surveillance has a narrower scope in that it refers to the relationship between an authority and the person that is under control (Yılmaz, 2005, p. 3). Monitoring involves examining the performance of employees through a variety of software and electronic equipment and reporting it (Alder & Ambrose, 2005). Monitoring involves continuously and regularly recording information related to working life and business, irrespective of the purpose (Botan, 1996, p. 294). There is a close relationship between monitoring and technology. The main components of this relationship could be listed as how much technology makes employees visible, how much it makes the surveillance authority invisible, how regularly and detailed records it keeps and, and how it contributes to data analysis (Yılmaz, 2005, p. 3).

E-surveillance technology focuses on three different areas: the focus on employee performance measures employees' computer or phone use, the focus on employee behaviour measures resource utilization and tracks employees' location, and the focus on employee characteristics provides information on topics such as health status and employee reliability (Al-Rjoub et al., 2008, p. 190). Employers want to keep their employees under electronic surveillance with an urge for higher profitability. However, this situation leads to negative consequences for employees' privacy. Thanks to the electronic monitoring equipment in today's workplaces, everything can be monitored through cameras, e-mails can be kept under control, documents and visited sites on the hard disk are traceable. Employers are in contact with their employees on a regular basis via smart mobile phones and computers, even at home. A survey that has been done in the United States revealed that 48% of employers are uncomfortable being monitored by mobile phones (Esen, 2005, p. 23). In addition, as supported by the results of some other studies, monitoring that takes place outside the working hours is not welcomed and perceived as interference with private life (Pearce & Kuhn, 2003, p. 372).

Recent research demonstrates that surveillance of employees is increasing with every passing day. A study conducted by the American Management Association has identified that the number of companies monitoring employees' phones, e-mails, voice mails, and computer use rose from 37% to 43% within a year (Lyon, 2006, p. 84). Another study conducted in

the USA has revealed 45% of the businesses monitor their employees' all kinds of electronic communications. Internet monitoring software records each and every word in e-mail messages and employees' search histories (Watson, 2001, p. 82).

Technical facilities provided by the internet, cameras, and listening devices have made surveillance more widespread than ever, both in communal and personal areas. For example, more than 4 million closed-circuit cameras are recording in the UK every day and when compared to the total population, there is a surveillance camera for every 15 people (Dolgun, 2008, p. 253).

Those who are under surveillance are unfortunately not aware whether it is their e-mails, web pages, or hard drives that are being monitored. In addition, it is not known whether the surveillance is continuous, random or as needed (National Work Rights Institute, n.d., p. 3-4). It is important that the employees be informed of the framework for recording activities. The board in Jean Monnet Building of the European Commission in Luxembourg which is easily visible by everyone, says "the personal data recorded by the cameras in the building will be processed in accordance with the European Commission's statute numbered 2001/45 and will not be used otherwise. The data will be stored for a period of 30 days only, and if necessary will be forwarded to the judicial authorities to be used in the investigation and prosecution of offenses when necessary". Thus, the individuals are assured that the data obtained from the records will not be used for purposes other than those mentioned (Civelek, 2011, p. 42).

Most employers think they are entitled to monitor their employees because they use company resource. Employees, on the other hand, feel humiliated and belittled as a result of monitoring (Ariss, 2002, p. 555). Electronic monitoring is said to cause extreme stress, a decline in job satisfaction and the quality of performance in workplaces (Watson, 2001, p. 82). Employees think of monitoring as an intervention in their private lives, also as an unethical and illegitimate practice (Lease & Gordon, 2005, p. 4).

According to a survey carried out by Massachusetts Coalition on New Office Technology with the participation of 49 enterprises and 700 employees, 81% of respondents stated that being monitored makes their work more stressful. A similar result was obtained by The National Institute for Occupational Safety and Health in America NIOSH, which confirms that employees who are exposed to more monitoring than their peers have been identified to experience a higher degree of depression, tension and frustration (Yılmaz, 2005, p. 33).

The use of computers and the internet is rapidly increasing in our country. According to TÜİK (2012a) Household ICT Usage Survey results, 47.2% of households in Turkey have internet access at home. As of January 2012, 92.5% of enterprises with 10 and more employees are reported to have internet access. Internet access rate is 99.6% for enterprises with 250 or more employees, 98.1% for enterprises with 50-249 employees, and 91.2% for enterprises with 10-49 employees (TÜİK, 2012b).

According to a study carried out in Turkey, the majority of employees tend to think the management has the right to monitor the workplace and it will bring positive results such as an increase in employee productivity and reduction of workplace incidents such as theft and abuse. However, the results also indicate that workplace monitoring may harm employees' privacy, demoralise and demotivate the employees and disturb the peaceful working environment (Erdemir & Koç, 2006, pp. 559-560). In another study analysing the current situation in Turkey, it has been found out that monitoring the internet, telephone, computer, and instant messaging programs is quite frequent. However, checking desks and offices, taking employee fingerprints, retinal scan, scanning e-mails and mobile camera phones were found to be the least encountered methods (Erdemir, 2008).

The Source of Legitimacy for Monitoring Employees: Productivity and Efficiency

Sennett (1992, p. 57) suggests that each person in society needs an authority. Flexible work forms of information society leads to "authority without power". Employers are in fear of losing their authority over workers and tend to think that home office employees would abuse this freedom. For this reason, they wish to establish a strict control mechanism for people who are not in the company premises. This control mechanism is operated through asking employees to contact the enterprise by phone on a regular basis or inspecting their e-mails over an intranet (Sennett, 2002, pp. 48-61).

Organizations derive their authority from such functions as deterrence, conditioning and rewarding. According to Berle and Means (1991) the reason why organizations are so powerful in information-based society is because the authority has shifted from property owners to executives. These two scientists studied why U.S. company executives who have only some small shares of the company capital have such great decision-making powers (Galbraith,

2004). Modern corporate executives are today's powerful classes. Russell (1990, p. 45) asserts that with the development of large organizations, a new, powerful individual who possess "executive powers" has emerged

Along with the development of information technologies, there has been a widespread use of electronic monitoring systems allowing for increased control over information. During this period, which is also known as post-industrial society, information and knowledge has become an integral part of power, and also "the main force of production" (Lyotard, 1990, pp. 11-12). One of the most important goals of modernism is progress, and in this respect all the elements within the organization should be mobilized in accordance with pre-determined objectives (Erdemir, 2007, p. 82). Monitoring systems that are set up for controlling employee productivity are mainly used to ensure that information technologies, electronic e-mail or the internet are used appropriately and in a work related manner, to detect psychological mobbing, violence, theft and harassment incidents, to prevent leakage of trade secrets and proprietary information and to prevent malicious people from entering the employer's computer system, to prevent overloading in the computer network, to provide evidence for any legal cases that have gone to court, and to monitor customer satisfaction standards (Grey-Noble, 2008, p. 3; Lasprogata, King, & Pillay , 2004, pp. 2-3).

In the new capitalist period, on the one hand individuals are regarded as the "the most precious capital", on the other hand they are converted into robots or cyborgs being integrated into the same system as inanimate minds of machines, and turned into capital, goods and labour and eventually they have become a manufacturing tool as a whole. Moreover, in case the individual rejects being a part of this production process, he or she is inevitably isolated, excluded and mistreated (Gorz, 2001, p. 16). Foucault (2007) theorizes that the effectiveness of surveillance came about due to the rise of division of labour. With each person's task becoming more and more exact and differentiated from that of his or her co-workers, each person becomes more specialized and therefore individualized. This in fact allows individuals to be more easily documented, separated, and controlled in case of lethargy, resistance or threatening the capitalist system.

Foxconn factories which manufacture iPhones that have made Apple the world's most valuable company have recently shaken with riots and suicides. G. Crothall, a journalist in China Labour Bulletin analyses the situation as "workers are revolting against injustice and want their rights but they are under pressure for incessant production" ("Foxconn kilidi vurdu",

2012). This analysis reveals how performance pressure affects the employees. As Maier (2006, p. 31) puts forward, companies are the real actors of this big game in the business world, whereas employees act only as a pawn in such a system.

Whalen and Gates (2010, pp. 14-22), underline the positive aspects of voluntary monitoring in a qualitative study they conducted in America by interviewing eight IT employees who were monitored both before and during the hiring process. The study has suggested four benefits of employee monitoring, such as personal safety, identifying errors easily, facilitating collaboration, and ease of recording. In addition, increased job satisfaction and career identification have been suggested as secondary benefits. Farlee's (2010, pp. 204-206) model for disclosure and concealment of information obtained during monitoring employees shows that concealment of information may contribute to risk-sharing whereas disclosure may help in decision-making. In this study, it is found out that the information disclosed is related to the production system rather than the monitoring system, and if the disclosed information does not have a direct influence on the relationship between employee activities and outputs, the information may be disclosed. Smith and Tabak (2009, p. 46) express the organizational environment, technology, structure, and cultural factors should be taken into account in designing e-mail monitoring systems. According to the authors "trust" is at the heart of high-performance work environment, and confidentiality is a necessary component to build relationships that are based on trust.

All monitoring activities are in conflict with approaches such as empowering the employees, delegation, teamwork, or promoting information sharing (Taft, Mithas, & Krishnan, 2007). Al-Rjoub et al. (2008, p. 194) carried out a survey in private and public universities and banks in Jordan about the use of electronic monitoring. This survey has identified that employee behaviour improves when they are electronically monitored. However, the employees mentioned they would not like to be monitored.

However, various research has also revealed that employees copy corporate software for home use, use internet services provided by the company for personal or recreational purposes, access files that they are unauthorised to see, visit pornographic sites, use corporate tools and facilities outside organizational purposes, damage corporate and co-workers' data, hide some employees' faults and blame others for such faults, extend the standard processing time for a task or coffee breaks (Erdemir & Çeliktaş, 2006, p. 91; TÜGİAD, 1992, p. 48).

Panopticon's Electronic Resurrection

Communication surveillance to provide intelligence is taking place in the international arena. There is even a conspiracy theory about the intelligence agencies of five states (U.S., UK, Canada, Australia and New Zealand) jointly establishing a surveillance system known as ECHELON (Big Ear). According to allegations, this system is capable of content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission, public switched telephone networks and microwave links (Beceni, 2004, p. 14). Such theories confirm Foucault's approach which regards authority as a reflection of power relations. According to this approach, authority is a mechanism which basically controls individuals, groups, and classes, puts pressure on them and does not leave room for manoeuvre (Foucault, 2004, p. 31). However, for Foucault (2004, p. 47) analysing power requires analysing the tools that produce, disseminate, distribute and record knowledge rather than analysing the ideology of power. According to Foucault, examining the source of power will only lead us to endless discussions, instead we should focus on ways the power influences us (Foucault, 2000, p. 308). Power is everywhere and 'comes from everywhere' so in this sense is neither an agency nor a structure. Power is not about who manages and who is managed, but it is about historical institutions such as prison, school and hospital. Relating the power to monarchy would be a simplistic approach, monarchy would not be able to intervene in the private lives of people. The essential thing to focus on is not the visibility or monitoring activities of power, it is how it makes its targets visible and traceable (Rouse, 1994, p. 95). From this perspective, electronic monitoring systems indeed continuously make their targets visible and traceable. In the information society, governments cannot confine people indoors, but virtual space makes people always visible and monitored. G. Morgan (1998, p. 383), uses metaphors to explain the administrative processes. According to him, even though organizations are social realities, they have turned into entities that enable a certain extent of monitoring on those who have established them.

Allen, Coopman, Hart, and Walker (2007, p. 174) suggest that many authors have used the metaphor of the Panopticon to express the secretive character of organizational monitoring. Bentham (1995, p. 34) devised an architectural device he called the *Panopticon*. The Panopticon was a universal institution based on the design for a Russian factory that minimised the

number of supervisors required, and proposed by Bentham for the design of prisons, workhouses, mental asylums and schools. The underlying principle of Panopticon order is the total and constant surveillance of inmates, workers, patients or pupils. But Bentham believed this approach could be successfully adopted in any environment which involved some level of supervision.

For Foucault, Bentham's Panopticon is a symbol for the modern disciplinary society. The Panopticon creates a consciousness of permanent visibility as a form of power, where no bars, chains, and heavy locks are necessary for domination any more. Foucault proposes that not only prisons but all hierarchical structures like the army, schools, hospitals and factories have evolved through history to resemble Bentham's Panopticon. This is the trick played by authority, and the authority actually covers much more than all the places and things in an insidious manner (Aktas, 2012, pp. 62-63). According to Bakunin those who represent authority invent such systems for their own benefit (2000, p. 114).

Bentham's Panopticon plan is an expression of asymmetrical surveillance. Each individual, in his place, is securely confined to a cell from which he is seen from the front by the supervisor; but the side walls prevent him from coming into contact with his companions. He is seen, but he does not see; he is the object of information, never a subject in communication. The panoptic mechanism arranges spatial unities that make it possible to see constantly and to recognize immediately. It reverses the principle of the dungeon; or rather of its three functions -to enclose, to deprive of light and to hide- it preserves only the first and eliminates the other two. Full lighting and the eye of a supervisor capture better than darkness, which ultimately protected. Visibility is a trap (Foucault, 2005, p. 251). Electronic monitoring systems are a kind of virtual simulation of the Panopticon. All video recordings, electronic monitors, GPS signals, sound recordings create a prison environment in our daily lives by not allowing a single dark spot. An illusionary freedom has surrounded us, because the new system keeps a record of everything you did, which gives you the chance to re-watch that moment that happened even months or years ago. Sennett (2011, p. 38) asserts that ICT facilitates panoptic surveillance by digitizing the highlights of real-time maps.

Tight control and monitoring manifested itself for the first time in the Fordist period with Taylor's scientific management principles. Fayol also

emphasized the efficiency of close monitoring and surveillance. Taylorism and Fordism are two prominent strategies for controlling the labour process (Munck, 1995, p. 218), and the organizational design in Classical theory resembles a prison where inmates are monitored. Functional foreperson system creates a structure that follows the personnel everywhere.

E-monitoring emerged in the 1960's in America, Canada and the UK to be used in prisons, then began to be used in business environment (Al-Rjoub et al., 2008, p. 190). In capitalist production forms, the efficiency of the worker has been replaced by the efficiency of management. Now management carried out all the functions of production, thus eliminating labour from the process of production (Braverman, 2008, pp. 175-176).

Conclusion

One of the major repression tools in today's business environment is organizational surveillance, which is an outcome of flexible working conditions. As Sennett (2002) expresses, with flexible working hours, the organizations seem to give the time as an award to employees but then expose them to strict surveillance tools in fear of losing their authority.

The Council of Europe emphasizes some basic principles to be complied with for a fair surveillance. These principles are: necessity, certainty, proportionality, transparency and security (Mitrou & Karyda, 2006, p. 170). International Labour Organization has also adopted some principles regarding the protection of privacy, according to which, employees and representatives must be informed of the conditions of the data gathering process and their rights within this process. Also utmost care should be taken to protect the privacy of the employees and records of personal information must be kept to a minimum. Regular training should be provided for data recording and analysis officials to increase their awareness of the seriousness of the work they are doing. Employers, employees and their representatives should cooperate for the confidentiality of personal information and this information should not give rise to any discrimination. Employers should not gather any data about employee's sex life, political, religious and other beliefs and should not test employees' tendency for crime. The information collected should be accessed by authorized personnel only and this information should not be shared with third parties without the employee's knowledge and consent (Kaplan, 1997, p. 383).

Mitrou and Karyda (2006, p. 176) suggests a list of fundamental principles that should be complied with for a lawful monitoring to balance employers' security and employees' privacy. The purpose of the monitoring policy should be explained to the employees, the company e-mail, Internet, and telephone usage policies must be dynamic policies that are under constant review and posted in the workplace, on computer sign-on screens, and mentioned at weekly staff meetings, employees should be encouraged to submit ideas and become an integral component of the policy creation process. This would certainly help with compliance and could also improve employee morale since the employees would be invested in the process.

The location information obtained from GPS systems, and tablet devices to keep track of employees should be limited to work hours. Recording information about the location of employees 24 hours a day is a violation of privacy. The employer is not a guardian following every movement of prisoners. Grey-Noble (2008, p. 6-7) states that inappropriate monitoring in the workplace will cause insecurity between employees and managers, which will reduce the motivation of the work environment and negatively influence the organizational culture.

In order to protect the privacy of personal information, computer technologies such as privacy-enhancing technologies (PET) can be used. The purpose of these technologies is to assist in the implementation of ethical principles by controlling the spread of personal data online. Report published by the OECD in 1997 supports technologies and policies which provide protection to personal data. In 1998, the OECD Ministerial Conference held in Ottawa expressed they approve of the use of PET (OECD, 1997).

Petronio (2004, p. 174), introduces CPM: Communication Privacy Management theory to solve the everyday life problems in a practical way. According to CPM, organizational monitoring must be mentioned as a written rule of business ethics. According to a study that is conducted on 1900 companies operating in the United States, Canada, Mexico and Europe in 1992, 84% of the companies in the United States and 58% of the companies in the rest have written business ethics rules. 25% of these companies mentioned to have given training to their employees, assigned ethics committees or identified ombudsmen in the last three years (Kidder, 1995, pp. 84-85).

Organizational monitoring is on the agenda with negative thoughts such as doubt, disobedience and insecurity. Any employee who feels he or she is being monitored will be disturbed by this situation thinking that there is a

lack of confidence towards him or her. On the other hand, managerial practices such as personnel empowerment and teamwork will create an environment of trust and will boost institutional commitment. Here are two different situations that represent a paradox regarding employer and employee relations. It is not easy to tell right from wrong and manager also may fall into the trap of rationalizing unethical behaviour, because organizational surveillance is a grey area that cannot simply be solved with a yes or a no.

References/Kaynakça

Aktaş, Ü. (2012). *Anarşizm.* İstanbul: Metamorfoz Yayıncılık.

Alder, G. S., & Ambrose, M. L. (2005). Towards understanding fairness judgments associated with computer task-specific monitoring: An integration of the feedback, justice, and monitoring research. *Human Resource Management Review*, *15*, 43-67.

Allen, M. W., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly, 21* (2), 172-200.

Al-Rjoub, H., Zabian, A., & Qawasmeh, S. (2008). Electronic monitoring: The employees point of view. *Journal of Social Sciences*, *4* (3), 189-195.

Ariss, S. S. (2002). Computer monitoring: Benefits and pitfalls facing management. *Information and Management*, *39*, 553-558.

Bakunin, M. (2000). *Tanrı ve devlet* (çev. S. Ergün). Ankara: Öteki Yayınevi.

Beceni, Y. (2004). *Siber uzayda mahremiyet*. İstanbul: II. Türkiye Bilişim Şurası Hukuk Çalışma Grubu.

Bentham, J. (1995). *The panopticon writings* (Ed. M. Bozovic). London: Verso.

Berle, A., & Means, G. C. (1991). *The modern corporation and private property.* New Brunswick, N.J.: Transaction Publishers.

Botan, C. (1996). Communication work and electronic surveillance: A model for predicting panoptic effects. *Communication Monographs*, *63* (4), 293-313.

Bowie, N., & Duska, E. R. F. (1990). *Business ethics*. Englewood Cliffs, N.J.: Prentice Hall.

Braverman, H. (2008). *Emek ve tekelci sermaye: Yirminci yüzyılda çalışmanın değersizleşmesi*. İstanbul: Kalkedon Yayınları.

Castells, M. (2005). *Enformasyon çağı: Ekonomi, toplum ve kültür. Ağ toplumunun yükselişi* (çev. E. Kılıç). İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Civelek, D. (2011). *Kişisel verilerin korunması ve bir kurumsal yapılanma önerisi*. Yayımlanmamış uzmanlık tezi, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı, Ankara.

Dolgun, U. (2008). *Şeffaf hapishane yahut gözetim toplumu.* İstanbul: Ötüken Neşriyat.

Eralp, Ö. (2013). *KPS (Kimlik Paylaşım Sistemi), AKS (Adres Kayıt Sistemi) uygulamaları ışığında bireysel mahremiyet*. http://www.ozgureralp.av.tr/makaleler/tckimliktbd.htm adresinden 12.03.2013 tarihinde edinilmiştir.

Erdemir, E. (2007). Adayış mı kaçış mı? Yönetsel kontrol karşısında postmodern dönüşüm söylemi. *Yönetim Araştırmaları Dergisi*, *7* (1-2), 67-96.

Erdemir, E. (2008). Bilgi toplumunda çalışma ilişkilerinin yeni boyutu: İşyeri ve çalışanlara yönelik izleme faaliyetleri ve Türkiye'deki durum. *Sakarya Üniversitesi I. Ulusal Çalışma İlişkileri Kongresi bildiriler kitabı* içinde (s. 40-52). Sakarya.

Erdemir, E. ve Çeliktaş, İ. (2006). Örgütsel ve hukuki açıdan işyeri izleme: Karşılaştırmalı bir inceleme. *Kazancı Hukuk Dergisi*, *19-20*, 87-102.

Erdemir, E. ve Koç, U. (2006). İşyeri izleme faaliyetlerinin çalışanlar tarafından algılanışı: Eskişehir örneği. *14. Ulusal Yönetim ve Organizasyon Kongresi bildiriler kitabı* içinde (s. 555-562). Erzurum: Atatürk Üniversitesi Yayınları.

Esen, E. (2005). Workplace privacy poll finding. *Society for Human Resource Management*, 1-47. Retrieved March 12, 2013, from http://www.shrm.org/research/surveyfindings/documents/workplace%20privacy%20poll%20findings%20-%20a%20study%20by%20shrm%20and%20careerjournal.com.pdf.

Farlee, M. A. (2010) Disclosure and secrecy in employee monitoring. *Journal of Management Accounting Research*, *22* (1), 187-208.

Foucault, M. (2000). *Hapishanenin doğuşu* (çev. M. A. Kılıçbay, 2. basım). Ankara: İmge Kitapevi Yayınları.

Foucault, M. (2004). *Toplumu savunmak gerekir* (çev. Ş. Aktaş, 3. basım). İstanbul: Yapı Kredi Yayınları.

Foucault, M. (2005). *Büyük kapatılma. Seçme yapıtlar: 3* (çev. F. Keskin ve I. Ergüden). İstanbul: Ayrıntı Yayınları.

Foucault, M. (2007). *İktidarın gözü seçme yazılar 4* (çev. I. Ergüden). İstanbul: Ayrıntı Yayınları.

Foxconn kilidi vurdu. (2012). *Radikal Gazetesi*. http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1101561&CategoryID=80 adresinden 25/03/2013 tarihinde edinilmiştir.

Galbraith, J. K. (2004). *İktidarın anatomisi* (çev. R. Dikmen). Ankara: Hece Yayınları.

Gorz, A. (2001).*Yaşadığımız sefalet, kurtuluş çareleri* (çev. N. Tutal). İstanbul: İletişim Yayınları.

Grey-Noble, B. (2008). *Workplace monitoring and the management of staff privacy: Issues and solutions*. Library 504- Individual Paper (pp. 1-11). University of British Columbia.

Kaplan, E. T. (1997). İş hukuku'nda kişilik haklarının özellikle bilgisayarda toplanan bilgilere karşı korunması. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* [Prof. Dr. Cemal Mıhçıoğlu'na Armağan], *52* (1-4), 383-386.

Kidder, R. M. (1995). *How good people make though choices.* New York: William Marrow Inc.

Lasprogata, G., King, N. J., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review*, *4*, 1-46.

Lease, D. R., & Gordon, J. (2005). *Balancing productivity and privacy: Electronic monitoring of employees*. Retrieved December 11, 2012, from http://www.drdavidlease.com/uploads/Balancing_Productivity_and_Privacy_David_Lease.pdf.

Lyon, D. (2006). *Gözetlenen toplum: Günlük hayatı kontrol etmek* (çev. G. Soykan). İstanbul: Kalkedon Yayınları.

Lyotard, J. F. (1990). *Postmodern durum* (çev. A. Çiğdem). İstanbul: Ara Yayıncılık.

Maier, C. (2006), *Merhaba tembellik: İşyerinde olabildiğince az çalışmanın yolları ve gerekliliği* (çev. R. Akman). İstanbul: Merkez Kitapçılık.

Mitrou, L., & Karyda, M. (2006). Employees privacy vs. employers security: Can they be balanced? *Telematics and Informatics*, *23*, 164-178.

Morgan, G. (1998). *Örgüt ve yönetim teorilerinde metafor* (çev. G. Bulut). İstanbul: MESS Yayınları.

Munck, R. (1995). *Uluslararası emek araştırmaları.* Ankara: Öteki Yayınları.

National Workrights Institute. (n.d.). *Privacy under siege: Electronic monitoring in the workplace*. Retrieved December 12, 2012 from http://epic.org/privacy/workplace/e-monitoring.pdf.

The Organisation for Economic Co-operation and Development (OECD). (1997). *Implementing the OECD privacy guidelines in the electronic environment*, *focus on the Internet*. Retrieved January, 2, 2013, from http://www.oecd.org/redirect/dataoecd/33/43/2096272.pdf.

Pearce, J. A., & Kuhn, D. R. (2003). The legal limits of employees off- duty privacy rights. *Organizational Dynamics*, *32* (4), 372-383.

Petronio, S. (2004). Road to developing communication privacy management theory: Narrative in progress, please stand by. *Journal of Family Communication*, *4*, 193-208.

Rouse, J. (1994). *Power/knowledge.* In G. Gutting (Ed.), *The Cambridge companion to Foucault* (pp. 92-114). Cambridge: Cambridge University Press.

Russell, B. (1990). *İktidar* (çev. M. Ergin). İstanbul: Cem Yayınevi.

Sennett, R. (1992). *Otorite* (çev. K. Durand). İstanbul: Ayrıntı Yayınları.

Sennett, R. (2002). *Karakter aşınması: Yeni kapitalizmde işin kişilik üzerindeki etkileri* (çev. B. Yıldırım). İstanbul: Ayrıntı Yay.

Sennett, R. (2011). *Yeni kapitalizmin kültürü* (çev. A. Onocak, 2. baskı). İstanbul: Ayrıntı Yayınları.

Smith, W. P., & Tabak, F. (2009). Monitoring employee emails: Is there any room for privacy? *Academy of Management Perspectives*, *23* (4), 33-48.

Söylemez, S. A. (2001). Yeni ekonomi, rekabet ve rekabet politikaları. *Ekonomik Yaklaşım Dergisi*, *12* (40), 1-27.

Şaylan, G. (2002). *Postmodernizm.* Ankara: İmge Kitabevi.

Tafti, A., Mithas, S., & Krishnan, M. S. (2007). Information technology and autonomy-control duality: Toward a theory. *Information Technology and Management*, *8* (2), 147-166.

Türkiye Genç İş Adamları Derneği (TÜGİAD). (1992). *İş ahlakı ve Türkiye'de iş ahlakına yönelik tutumlar.* İstanbul: Yazar.

Türkiye İstatistik Kurumu (TÜİK). (2012a). Hanehalkı bilişim teknolojileri kullanım araştırması. *Haber Bülteni,* sayı: 10880. http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10880 adresinden 16/01/2013 tarihinde edinilmiştir.

Türkiye İstatistik Kurumu (TÜİK). (2012b). Girişimlerde bilişim teknolojileri kullanım anketi. *Haber Bülteni*, sayı: 10939. http://www.tuik.gov.tr/PreHaberBultenleri.do?id=10939 adresinden 16/01/2013 tarihinde edinilmiştir.

Watson, N. (2001). The private workplace and the proposed notice of electronic monitoring act: Is notice enough? *Federal Communications Law Journal*, *54*, 79-102.

Whalen, T., & Gates, C. (2010). Watching the watchers: "Voluntary monitoring" of infosec employees. *Information Management & Computer Security*, *18* (1), 14-25.

Yılmaz, G. (2005). Elektronik performans izleme sistemlerinin çalışanlar ve işletmeler üzerindeki etkileri. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, *4* (7), 1-19.

Yüksel, M. (2009). Mahremiyet hakkına ve bireysel özgürlüklere felsefi yaklaşımlar. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi* (AÜSBFD), *LXIV* (1), 275-298.