Influential Article Review - Competency Management by Using Technology in the United States

Marcus Montgomery

Tomas Phelps

Clifton Pope

This paper examines management. We present insights from a highly influential paper. Here are the highlights from this paper: Despite the historic American love for privacy that has enhanced innovation and creativity throughout the country, encroachments on privacy restrain individual freedom. Noticeable, advances in technology have offered decision makers remarkable monitoring aptitudes that can be used in numerous tasks for multiple reasons. This has led scholars and practitioners to pose a significant number of questions about what is legitimate and illegitimate in the day-to-day affairs of a business. This article is composed of (a) research about electronic monitoring and privacy concerns; (b) definitions of, critiques of, and alternatives to electronic performance monitoring (EPM); (c) motives behind employee monitoring and leadership behaviors; (d) advice that makes monitoring less distressful; (e) employee monitoring policies; (f) reviewing policies and procedures; (g) the role of human resource development (HRD) in employee assessment and development; and (h) conclusion and recommendations for further studies. For our overseas readers, we then present the insights from this paper in Spanish, French, Portuguese, and German.

Keywords: employee, employer, information, monitoring, privacy, organization

SUMMARY

- According to Belcourt, Bohlander, and Snell , employee monitoring acts involve monitoring Internet links, review of emails, telephone use, video surveillance for security purposes, storage and review of computer files, video recording of employee job performance, recording and review of telephone conversations, and storage and review of voice-mail messages. Dessler noted that EPM systems are intended to allow employers access to their employees' computers and telephones to monitor the amount of time spent working on the Internet, to enhance productivity. This paradox necessitates the establishment of a security system for all data garnered by employers to thwart the theft of sensitive information, particularly to those outside the organization. Employers should articulate what they want to accomplish from a performance appraisal system to obtain the desired advantages with regard to perceptions and rights of the organization's employees.
- Comprehensively, Dessler discussed achievable and indispensable factors that might lead to developing a legally justifiable performance appraisal system, as follows: make certain what a

successful performance means, undertake a job analysis to recognize the critical requirements needed, and amalgamate these criteria into a rating tool; define job performance magnitude, write and communicate performance criteria to all employees and employers, and avoid broad terms, such as «integrity» and «hardworking,» unless you can lead by example or model the behavior you desire; use subjective supervisory ratings as only one part of the overall evaluation process, train evaluators how to use the rating instrument effectively, authorize evaluators to approach the employees they are evaluating, and conclude your evaluation on different measures for each of the job's performance criteria; have more than one evaluator and perform all evaluations independently to reduce biases and errors, employees should be given the freedom to review their appraisals and make comments before completion, and supplement your personnel decisions with documents and reasons; and whenever possible, provide supervision to aid low performers at work. Arguably, employers who justify electronic monitoring by boosting productivity in the workplace may want to exercise the following: assuage or eliminate bureaucracy, revise all systems and recognize high quality employees, overcome problems, share your vision throughout the organization, question your employees and listen to them carefully, be honest and have integrity, turn customers into strategic partners, and develop effective performance-based pay plans .

- What is more, the increasing use of e-mail and voicemail augmented every employer's risks of being legally responsible if they monitor or check employee electronic communications. As a result, the Electronic Communications Privacy Act was passed in 1986.

HIGHLY INFLUENTIAL ARTICLE

We used the following article as a basis of our evaluation:

Moussa, M. (2015). Monitoring Employee Behavior Through the Use of Technology and Issues of Employee Privacy in America. SAGE Open

.

This is the link to the publisher's website:
https://doi.org/10.1177/2158244015580168

INTRODUCTION

Research About Electronic Monitoring and Privacy Concerns

Monitoring increased concerns about employee privacy; therefore, employers must find a balance between monitoring gains and the costs of invading employee privacy (Jackson, Schuler, & Werner, 2009). However, the use of emerging technologies in monitoring employee practices is raising concerns that the privacy rights of employees are vulnerable, and it is becoming more challenging to balance employer security rights with employee privacy issues (Mathis & Jackson, 2000). Consequently, significant privacy issues are being debated in business and government, for example, (a) violation of privacy: examining and retrieving private e-mails, records, and information about employees from their access to particular Internet websites; (b) computer monitoring: continually knowing where the employee is; (c) computer matching: synthesizing information obtained from different sources to enhance your marketing services; and (d) unauthorized personnel files: gathering telephone numbers, e-mail addresses, credit card numbers, and other private information to develop customer profiles (O'Brien & Marakas, 2006). Technological advancements enabled employers to enhance employee productivity and put employee privacy under siege. Robbins and Coulter (1999) presented some perplexing questions, such as the following:

1. Is the e-mail system for business purposes only?
2. Is an employee allowed to e-mail work information to a colleague along with some personal chatting?
3. What is the acceptable use of the system?
4. Who possesses the information that is produced from the network?

Organizations regulate Internet use, or website visits by their workforce, through two regular ways: by restricting access to particular links, and by monitoring employee actions (Alampay & Hechanova, 2010). In this study, it also is revealed that monitoring policies and controlling websites vary from one country to another; for example, China, Vietnam, and Singapore not only block certain sites but also proscribe access to political and linguistic affairs. Everett, Wong, and Paynter (2006) found that a significant number of subjects related to employee and employer rights should be taken into consideration in further studies: (a) A significant issue is concerned with building trust between employers and employees in the workplace; another vital topic is linked with the establishment of pertinent legislation that manages privacy issues in workplace surveillance forthrightly; (b) a thorny factor is the growing occurrence of satellite, communal facility, and work at home, which urge employers to monitor their employees; (c) the diversification and capacities of the Internet for communication provide new topics for research; (d) the possibility to proscribe all small electronic devices in the workplace that could be used to e-mail firms' secrets to an external beneficiary; and (e) enlarging the international comparison and probing the rising position of international standards and "harmonization agreements," concerning policies developed by the European Union and the United Nations, as well as standards propagated by the International Organization for Standardization, the national defense agencies, and government branches of criminal investigation.

Everett et al. (2006) referred to certain issues potentially leading to greater employer use of the perception that such monitoring is needed. For example, government efforts to crush terrorism, assuage the proliferation of govern nuclear weapons knowledge, hinder money laundering, and limit drug traffickers, both unlawful and pharmaceutical. More recently, employers have begun tracking their employees by using global positioning system (GPS) technology, which uses an assemblage of satellites to specify the precise location of the GPS-enabled device. Therefore, Townsm and Cobb (2012) recommended realistic steps when applying GPS tracking as follows: incorporate GPS tracking with other policies; preserve the right to monitor; do not create a conclusive evidence with GPS tracking documents; limit the use of GPS technology to monitor; rigorously outline appropriate use of company cell phones, vehicles, and so on; develop a consent language; continually check GPS equipment; and consider safeguarding records.

Another study by Ciocchetti (2011) classified each of the top monitoring practices into one of the following types: (a) best practices (e.g., monitoring that presents the greatest protection and minimizes invasion of employee privacy), (b) risky practices (e.g., monitoring that offers rather low protection and minimally attacks employee privacy), (c) borderline practices (e.g., monitoring that provides high protection, yet is also highly insidious), and (d) poor practices (e.g., monitoring that provides low protection and is extremely invasive). This classification system is likely to assist lawmakers to balance both employer and employee interests when legalizing workplace technology. Ciocchetti viewed that the American legal system has been sluggish to react effectively and efficiently to the increasing invasiveness of modern monitoring technology and that all monitoring practices are disturbing and fall into the four categories just mentioned. However, Bennett and Locke (1998) stated that an effective way to avoid liability for privacy assault is to presuppose that if an employee can litigate for such a tort, the employee will.

Research showed that employees can find an inclusive source of privacy protection resulting from the common law right to privacy, which consists of three misdeeds relevant to the employment relationship: intrusion on seclusion, which arises an encroachment is an intrusion on the property of another without that person's permission; publicity given to one's private life, which exists when an individual gives publicity to an issue regarding the private life of another; and publicity placing a person in a false light, which occurs when an individual heedlessly disregards the falsity of the revealed issue and the false light in which the other person would be placed (Hames & Diersen, 1991). Alternatively, a set of reforms developed by Conlon (1997) protect individual privacy concerns in the workplace:

- No monitoring should be done in restrooms, locker rooms, and employee lounges; however, time spent outside the workplace can be monitored in less odious ways.
- Offsite monitoring should be banned; allow employees to access all information collected through monitoring methods or techniques and consider their reflection on such information; and limit the duration of monitoring each day with a suggested (maximum of 2 hr per day).

- Employees should be aware of the devices that will be used to monitor them, how the data will be used, and when exactly they will be monitored; and employees and customers should be notified when telephonic monitoring is taking place through the use of a specific tone that can be heard by both employee and customer.
- Employers should collect only information relevant to making critical decisions; and it is not enough to justify monitoring by the need to increase productivity or enhancing performance, but also, employers should be able to demonstrate how the goal was accomplished through the monitoring process.

However, the lawful foundation of the right to privacy has a theoretical underpinning for legal intellectuals that may be complex for the public to recognize or value (C. L. Swanson, 1988). Despite the different schools of thought among academics, numerous propositions have been offered for management's contemplation: formulate why, how, and when electronic monitoring is applied; gather only work-related information; gather only information for the purpose of raising employee performance; provide timely feedback to employees so that corrective actions to performance can be done; secure awards to individuals or group performance; educate employees about the behavioral and social features of electronic monitoring; accentuate qualitative characteristics of performance not accounted for by electronic monitoring; a trial period for all new applicants or new electronic systems should be provided; avoid being too quick in developing new standards or monitoring methods unless proven to be effective; and use brainstorming sessions whenever possible to enhance the electronic monitoring system in the organization (Vaught, Taylor, & Vaught, 2000). Nevertheless, too much monitoring and the publicity of a monitoring culture throughout the organization may create emotional and behavioral problems that may ultimately thrust employees into certain activities to cheat the system (Barrett, 2008).

Intriguingly, Dillon and Thomas (2006) exposed that there is a great need for universal consciousness and indulgence of accessibility, personal use, and administrative oversight issues involving e-mail and computers in the workplace; otherwise, employees are unlikely to understand privacy policies and procedures adequately. Wen, Schwieger, and Gershuny (2007) reviewed surveillance technologies and discussed the related federal and state laws along with U.S. judicial decisions and found that no U.S. federal or state law prohibits employers from monitoring their electronic workplace. Their scientific investigation also provided the following strategies that are likely to be most effective and productive for both employees and employers, and help employers prevent the negative aspects of monitoring: designating privacy policy oversight and execution should be implemented by an authority; consider a legal stand-point to legally guide the development of all policies and procedures; develop a formal policy and keep all employees informed of all modifications to the policy; notify employees of the electronic monitoring system; avoid an aggressive work environment; develop clear rules on the use of e-mail; decide which data should and should not be accessed; specify online time limits; maintain a software running in the background of every computer, such as popup blockers or spam filters; and communicate a policy that is acceptable for instant messaging, blogging, and chat room use in and out of the organization.

Haller (2002) also proposed the main ingredients of effective privacy policies: (a) notice, firms should provide stakeholders with a prominent notice vis-à-vis its information practices; (b) consumer choice, firms should give stakeholders the freedom to choose whether it may divulge personal data about them to unaffiliated third parties; (c) access and correction, firms should accept their stakeholders to make some corrections if necessary about personal data that they have gathered about them; (d) security, firms should espouse practical security measures to protect the privacy of personal information, and these measures may comprise administrative, physical, and technical security; and (e) enforcement, firms should develop a system that can enforce its privacy policy and ensure compliance with their own and external standards. Moreover, maintaining a balance between employers' propensity to productivity and compliance with legislative procedures, corporations may be most successful in practicing the following: creating unambiguous privacy boundaries, developing privacy formula and principles, and defending personal data (Townsend & Bennett, 2003).

Employers are less vulnerable regarding certain issues of invasion of privacy, if written policies are communicated effectively; however, Kovach, Jordan, Tansey, and Framinan (2000) argued that too much

monitoring generates a workplace filled with gridlock, blame, cynicism, and distrust. Practically speaking, to circumvent violations of employee privacy in the workplace, employers should never promote a culture of privacy within every quarter of an organization because it may be essential to monitor some practices when issues occur (Guffey & West, 1996). An ethical employer will monitor employees' work within the provisions of a particular policy (Cowan, 2008). Corporations must enroll if they are coping with personal information for any of the following purposes: private investigation, health administration, policing crime avoidance and trial of delinquents, legal services, debt administration, trading, public casework, education, research, administration of justice, consultancy services, or a credit reporting system (Grupe, Kuechler, & Sweeney, 2002).

Summed up briefly, Zachary (2013) acknowledged the following: Workplace encroachment to privacy is of immense concern to both employers and employees in the United States, and violation of privacy has been augmented in employment proceedings. Invasion of privacy may fall into four categories: (a) information leakage that denigrates others, (b) using someone else's name without consent, (c) inappropriate communication of private data, and (d) when a perpetrator purposefully intrudes, physically, electronically, or otherwise, on the private space of others. Courts vary according to when the illegal intrusion exists, and employers should be extremely vigilant to dissimilar types of invasion of privacy. Remarkably, disputes over privacy rights in the United States, which some view as a threat to eroding primary American values, have had an upsurge in controversy over the degree to which rights formerly untouched may be reduced because of the employer–employee relationship (Anton & Ward, 1998). In the following section, the author presents possible alternatives to electronic performance monitoring (EPM).

CONCLUSION

By monitoring, employers often argue that they are able to protect their organizations from any harm. In this sense, monitoring is perceived as a tool to maintain the security of an organization. New technologies have not only offered organizations reasons to monitor employees' behavior, but these technologies have also provided new methods and techniques to perform employee monitoring. Thus, technology must be treated with caution and discretion. Employers should realize that employees may retaliate against the organization for the perceived unfair monitoring practices. Therefore, it is essential when applying new technologies to monitor employee behavior to take into account many concerns (e.g., privacy, needs, and aspirations). Educating employees about the reasons behind monitoring them, developing a wide range of policies and procedures, and communicating them effectively will be vital to successfully implement a monitoring system.

The failure of employers to recognize employee rights can cause extensive loss, such as expensive lawsuits, damage to the organization's reputation, and impairment of employee values. Hence, employers should balance the need for productivity with regard to employee rights to privacy, safety, and security. Focusing on accomplishments rather than time spent in the workplace should be the main concern for any employer. In other words, there is no need to police a workforce because no one can work 8 hr without breaks, and a culture of disloyalty and distrust within the organization may emerge. However, employees should be aware that there are numerous software packages that could key log everything they type, search, and read on their computers.

This study offers many alternatives to EPM that are likely to satisfy an employer's objectives without violating rights of privacy. Another significant issue raised in this study is that the most effective leadership style to monitor employee performance and behavior through technology remains unidentified. From the author's point of view, there is no need to define what a moral behavior is in mature and healthy organizations, but it is crucial to shed light on how to use technologies without violating ethical protocols. Technology is a tool that can be used ethically and unethically. After reviewing a large number of studies on employee perceptions of electronic monitoring, the author found that the use of EPM has created a great deal of tension and pressure among individuals in organizations. Therefore, the author argued that employee levels of satisfaction, motivation, commitment, loyalty, and integrity in the workplace can be affected as a result of extreme levels of stress. Hence, educating employees about the monitoring system and setting fair

performance criteria, distributive justice, procedural justice, and interactional justice can make monitoring less distressful. Importantly, monitoring should be consistent with both the overall objectives of the organization and performance dilemmas; however, employers' policies should not create stress and distrust on their employees. Above and beyond, the author of this study argued that HRD efforts can be significant in monitoring employee behavior and performance in organizations. The rationale behind this school of thought is that the HRD field emphasizes crucial elements of behavioral and developmental matters in organizations.

REFERENCES

Alampay, E. A., Hechanova, R. M. (2010). Monitoring employee use of the Internet in Philippine organizations. The Electronic Journal on Information Systems in Developing Countries, 40(5), 1-20. Retrieved from http://www.ejisdc.org/Ojs2/index.php/ejisdc/article/viewFile/648/311

Anton, G., Ward, J. J. (1998). Every breath you take: Employee privacy rights in the workplace—An Orwellian prophecy come true? Labor Law Journal, 49, 897-911.

Ardichvili, A., Jondle, D. (2009). Integrative literature review: Ethical business cultures: A literature review and implications for HRD. Human Resource Development Review, 8, 223-244.

Ardichvili, A., Mitchell, J. A., Jondle, D. (2009). Characteristics of ethical business cultures. Journal of Business Ethics, 85, 445-451. Retrieved from http://files.eric.ed.gov/fulltext/ED501640.pdf

Baltzan, P., Phillips, A. (2009). Essentials of business driven information systems. Burr Ridge, IL: McGraw-Hill/Irwin.

Barrett, S. (2008). Monitoring raises privacy issues. Employee Benefits, 48-51. Retrieved from http://connection.ebscohost.com/c/articles/32800523/monitoring-raises-privacy-issues

Bartol, K. M., Martin, D. C. (1991). Management. New York, NY: McGraw-Hill.

Baye, M. R. (2009). Managerial economics and business strategy (6th ed.). New York, NY: McGraw-Hill/Irwin.

Belcourt, M., Bohlander, G., Snell, S. (2008). Managing human resources (Fifth Canadian ed.). Toronto, Ontario, Canada: Nelson.

Bennett, S. C., Locke, S. D. (1998). Privacy in the workplace: A practical primer. Labor Law Journal, 49, 781-787.

Bohlander, G., Snell, S. (2004). Managing human resources (13th ed.). Mason, OH: South-Western.

Buchner, T. W. (2007). Performance management theory: A look from the performer's perspective with implications for HRD. Human Resource Development International, 10, 59-73.

The Bureau of National Affairs. (2012). Attorneys worldwide discuss right to monitor, track workers. HR Focus, 89(11), 8-9.

Cascio, W. F., Aguinis, H. (2011). Applied psychology in human resource management (7th ed.). Harlow, UK: Pearson Education.

Certo, S. C., Certo, S. T. (2009). Modern concepts and skills management (11th ed.). Harlow, UK: Pearson Education.

Ciocchetti, C. A. (2011). The eavesdropping employer: A twenty-first century framework for employee monitoring. American Business Law Journal, 48, 285-369.

Conlon, K. J. (1997). Privacy in the workplace. Labor Law Journal, 48, 444-448.

Cowan, S. (2008). When private means private: The "do's and don'ts" of employee monitoring. Credit Management, 16. Retrieved from http://connection.ebscohost.com/c/articles/28334301/when-private-means-private-dos-donts-employee-monitoring

DeCenzo, D. A., Robbins, S. P. (2005). Fundamentals of human resource management (8th ed.). New Delhi, India: John Wiley.

Dessler, G. (2000). Human resource management (8th ed.). Upper Saddle River, NJ: Prentice Hall.

Dessler, G. (2003). Human resource management (9th ed.). Harlow, UK: Pearson Education.

Dessler, G. (2011). Human resource management (12th ed.). Harlow, UK: Pearson Education.

Dillon, T. W., Thomas, D. S. (2006). Knowledge of privacy, personal use, and administrative oversight of office computers and e-mail in the workplace. Information technology. Learning & Performance Journal, 24(2), 23-34.
Dlabay, L. R., Burrow, J. L., Eggland, S. A. (2006). Intro to business (6th ed.). Mason, OH: South-Western.
DuBrin, A. J. (2006). Essentials of management (7th ed.). Mason, OH: South-Western.
DuBrin, A. J. (2009). Essentials of management (8th ed.). Mason, OH: South-Western.
Effron, M., Gandossy, R., Goldsmith, M. (2003). Human resources in the 21st century. Hoboken, NJ: John Wiley.
Everett, A. M., Wong, Y. Y., Paynter, J. (2006). Balancing employee and employer rights: An international comparison of e-mail privacy in the workplace. Individual Employment Rights, 11, 291-310.
Ferrell, O. C., Fraedrich, J., Ferrell, L. (2009). Business ethics: Ethical decision making and cases (7th ed.). Mason, OH: South-Western.
French, W. L. (1994). Human resources management (3rd ed.). Boston, MA: Houghton Mifflin.
Garavan, T. N., McGuire, D., O'Donnell, D. (2004). Exploring human resource development: A levels of analysis approach. Human Resource Development Review, 3, 417-441. Retrieved from http://eresearch.qmu.ac.uk/270/1/270.pdf
Garavan, T. N., O'Donnell, D., McGuire, D., Watson, S. (2007). Exploring perspectives on human resource development: An introduction. Advances in Developing Human Resources, 9, 3-11. Retrieved from http://eresearch.qmu.ac.uk/262/1/262.pdf
Gomez-Mejia, L. R., Balkin, D. B., Cardy, R. L. (2004). Managing human resources (4th ed.). Harlow, UK: Pearson Education.
Griffin, R. W. (2008). Management (9th ed.). Lewiston, NY: Houghton Mifflin.
Grupe, F. H., Kuechler, W., Sweeney, S. (2002). Dealing with data privacy protection: An issue for the 21st century. Information Systems Management, 19(4), 61-70.
Guffey, C. J., West, J. F. (1996). Employee privacy: Legal implications for managers. Labor Law Journal, 47, 735-745.
Haag, S., Cummings, M. (2010). Management information systems for the information age (8th ed.). Boston, MA: McGraw-Hill.
Haller, S. C. (2002). Privacy: What every manager should know. Information Management Journal, 36, 33-40.
Hames, D. S., Diersen, N. (1991). The common law right to privacy: Another incursion into employers' rights to manage their employees? Labor Law Journal, 42, 757-765.
Hassan, A. (2006, December 2-5). Human resource development and organizational values. Proceeding of the 2006 Asian Conference of the Academy of Human Resource Development (AHRD), Putrajaya, Malaysia.
Hatcher, T. G. (2002). Ethics and HRD: A new approach to leading responsible organizations. New York, NY: Basic Books.
Jackson, S. E., Schuler, R. S., Werner, S. (2009). Managing human resources (10th ed.). Mason, OH: South-Western.
Kovach, K. A., Jordan, J., Tansey, K., Framinan, E. (2000). The balance between employee privacy and employer interests. Business and Society Review, 105, 289-298.
Kowske, B. J., Anthony, K. (2007). Towards defining leadership competence around the world: What mid-level managers need to know in twelve countries. Human Resource Development International, 10, 21-41.
Luthans, F., Doh, J. P. (2009). International management: Culture, strategy, and behavior (7th ed.). New York, NY: McGraw-Hill/Irwin.
Mathis, R. L., Jackson, J. H. (1997). Human resource management (8th ed.). Minneapolis, MN: West Publishing.
Mathis, R. L., Jackson, J. H. (2000). Human resource management (9th ed.). Mason, OH: South-Western.

McCalman, J., Paton, R. A. (1992). Change management: A guide to effective implementation. London, England: Paul Chapman.
McGuire, D., Jorgensen, K. M. (2011). Human resource development: Theory and practice. Thousand Oaks, CA: SAGE.
Megginson, D., Banfield, P., Joy-Matthews, J. (2001). Human resource development. New Delhi, India: Kogan Page.
Mello, J. A. (2006). Strategic human resource management (2nd ed.). Mason, OH: South-Western.
Mello, J. A. (2011). Strategic management of human resources (3rd ed.). Mason, OH: South-Western.
Metcalfe, B. D., Rees, C. J. (2005). Theorizing advances in international human resource development. Human Resource Development International, 8, 449-465. Retrieved from http://org8220renner.alliant.wikispaces.net/file/view/HRD+metcalf+global+theory+overview+17.pdf/32414179/HRD%20metcalf%20global%20theory%20overview%2017.pdf
Moss, G. (2006). Business secrets: Guidelines for new leader-managers. Singapore: Thomson Learning.
Nelson, D. L., Quick, J. C. (2006). Organizational behavior: Foundations, realities and challenges (5th ed.). Mason, OH: South-Western.
Noe, R. A., Hollenbeck, J. R., Gerhart, B., Wright, P. M. (2007). Fundamentals of human resource management (2nd ed.). Boston, MA: McGraw-Hill/Irwin.
Norton, P. (2006). Introduction to computers (6th ed.). New York, NY: McGraw-Hill.
Odlyzko, A. (1999). The visible problems of the invisible computer: A skeptical look at information appliances. First Monday, 4(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/688/598
O'Brien, J. A., Marakas, G. M. (2006). Management information systems (7th ed.). Boston, MA: McGraw-Hill.
Portolese-Dias, L., Shah, A. J. (2009). Introduction to business. New York, NY: McGraw-Hill.
Robbins, S. P., Coulter, M. (1999). Management (6th ed.). Upper Saddle River, NJ: Prentice Hall.
Schermerhorn, J. R. (2011). Introduction to management (11th ed.). Hoboken, NJ: John Wiley.
Short, D. C., Bing, J. W., Kehrhahn, M. T. (2003). Will human resource development survive? Human Resource Development Quarterly, 14, 239-243. Retrieved from http://media.johnwiley.com.au/product_data/excerpt/24/07879713/0787971324.pdf
Stair, R. M., Reynolds, G. W. (2008). Fundamentals of information systems: A managerial approach (4th ed.). Boston, MA; Thomson Learning.
Swanson, C. L. (1988). The constitutional foundation for privacy in the workplace. Industrial Management, 30, 6-9.
Swanson, R. A., Holton, E. F.. (2001). Foundations of human resource development. San Francisco, CA: Berrett–Koehler Publishers.
Thompson, R. L., Cats-Baril, W. L. (2003). Information technology and management (2nd ed.). Boston, MA: McGraw-Hill/Irwin.
Torraco, R. J., Swanson, R. A. (1995). The strategic roles of human resource development. Human Resource Planning, 18(4), 1-14. Retrieved from http://www.richardswanson.com/publications/Swanson(1995)TheStrategic.pdf
Townsend, A. M., Bennett, J. T. (2003). Privacy, technology, and conflict: Emerging issues and action in workplace privacy. Journal of Labor Research, 24, 195-205.
Townsm, D. M., Cobb, L. M. (2012). Notes on: GPS technology; Employee monitoring enters a new era. Labor Law Journal, 63, 203-208.
Van der Sluis, L. E. C. (2007). Umbrella for research into human resource development (HRD). Human Resource Development International, 10, 99-106.
Vaught, B. C., Taylor, R. E., Vaught, S. F. (2000). The attitudes of managers regarding the electronic monitoring of employee behavior: Procedural and ethical considerations. American Business Review, 18, 107-114.
Wen, H. J., Schwieger, D., Gershuny, P. (2007). Internet usage monitoring in the workplace: Its legal challenges and implementation strategies. Information Systems Management, 24, 185-196.

Wooten, L. P., James, E. H. (2008). Linking crisis management and leadership competencies: The role of human resource development. Advances in Developing Human Resources, 10, 352-379. Retrieved from http://karshenasanrasmi.ir/Editor/UploadFiles/PDF%20Articles/352.pdf
Yorks, L. (2005). Strategic human resource development. Mason, OH: South-Western.
Zachary, M. K. (2013). Invasion of privacy: The moment of intrusion. Supervision, 74, 18-22.

TRANSLATED VERSION: SPANISH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUCIDA: ESPAÑOL

A continuación se muestra una traducción aproximada de las ideas presentadas anteriormente. Esto se hizo para dar una comprensión general de las ideas presentadas en el documento. Por favor, disculpe cualquier error gramatical y no responsabilite a los autores originales de estos errores.

INTRODUCCIÓN

Investigación sobre monitoreo electrónico y preocupaciones de privacidad

Monitoreo de mayores preocupaciones sobre la privacidad de los empleados; por lo tanto, los empleadores deben encontrar un equilibrio entre el monitoreo de las ganancias y los costos de invadir la privacidad de los empleados (Jackson, Schuler, Werner, 2009). Sin embargo, el uso de tecnologías emergentes en el monitoreo de las prácticas de los empleados está planteando preocupaciones de que los derechos de privacidad de los empleados son vulnerables, y cada vez es más difícil equilibrar los derechos de seguridad de los empleadores con los problemas de privacidad de los empleados (Mathis & Jackson, 2000). En consecuencia, se están debatiendo importantes cuestiones de privacidad en las empresas y el gobierno, por ejemplo, a la violación de la privacidad: examinar y recuperar correos electrónicos privados, registros e información sobre los empleados desde su acceso a determinados sitios web de Internet; (b) monitoreo informático: saber continuamente dónde está el empleado; (c) emparejamiento informático: sintetizar información obtenida de diferentes fuentes para mejorar sus servicios de marketing; y (d) archivos de personal no autorizados: recopilación de números de teléfono, direcciones de correo electrónico, números de tarjetas de crédito y otra información privada para desarrollar perfiles de clientes (O'Brien & Marakas, 2006). Los avances tecnológicos permitieron a los empleadores mejorar la productividad de los empleados y poner bajo asedio la privacidad de los empleados. Robbins y Coulter (1999) presentaron algunas preguntas desconcertantes, como las siguientes:

1. ¿Es el sistema de correo electrónico solo para fines comerciales?
2. ¿Se permite a un empleado enviar por correo electrónico información de trabajo a un colega junto con algunas charlas personales?
3. ¿Cuál es el uso aceptable del sistema?
4. ¿Quién posee la información que se produce desde la red?

Las organizaciones regulan el uso de Internet, o las visitas al sitio web por parte de su fuerza de trabajo, a través de dos formas regulares: restringiendo el acceso a enlaces particulares y monitoreando las acciones de los empleados (Alampay & Hechanova, 2010). En este estudio, también se revela que las políticas de monitoreo y el control de sitios web varían de un país a otro; por ejemplo, China, Vietnam y Singapur no sólo bloquean ciertos sitios, sino que también proscriben el acceso a asuntos políticos y linguísticos. Everett, Wong y Paynter (2006) encontraron que un número significativo de temas relacionados con los derechos de los empleados y empleadores deberían tenerse en cuenta en estudios posteriores: a Una cuestión importante se refiere a la creación de confianza entre los empleadores y los empleados en el lugar de trabajo; otro tema vital está relacionado con el establecimiento de una legislación pertinente que gestione

directamente las cuestiones de privacidad en la vigilancia del lugar de trabajo; (b) un factor espinoso es la creciente ocurrencia de satélites, instalaciones comunitarias y trabajo en el hogar, que instan a los empleadores a vigilar a sus empleados; (c) la diversificación y las capacidades de Internet para la comunicación proporcionan nuevos temas para la investigación; (d) la posibilidad de proscribir todos los pequeños dispositivos electrónicos en el lugar de trabajo que puedan utilizarse para enviar por correo electrónico los secretos de las empresas a un beneficiario externo; y e) ampliar la comparación internacional y sondear la creciente posición de las normas internacionales y los "acuerdos de armonización", en relación con las políticas desarrolladas por la Unión Europea y las Naciones Unidas, así como las normas propagadas por la Organización Internacional de Normalización, los organismos nacionales de defensa y las ramas gubernamentales de investigación criminal.

(2006) se refirió a ciertas cuestiones que potencialmente conducen a un mayor uso del empleador de la percepción de que se necesita ese monitoreo. Por ejemplo, los esfuerzos del gobierno para aplastar el terrorismo, aducir la proliferación del conocimiento de las armas nucleares, obstaculizar el lavado de dinero y limitar a los narcotraficantes, tanto ilegales como farmacéuticos. Más recientemente, los empleadores han comenzado a rastrear a sus empleados mediante el uso de la tecnología del sistema de posicionamiento global (GPS), que utiliza un conjunto de satélites para especificar la ubicación precisa del dispositivo habilitado para GPS. Por lo tanto, Townsm y Cobb (2012) recomendaron pasos realistas al aplicar el rastreo GPS de la siguiente manera: incorporar el seguimiento GPS con otras políticas; preservar el derecho a vigilar; no crear una evidencia concluyente con documentos de seguimiento GPS; limitar el uso de la tecnología GPS para monitorear; trazar rigurosamente el uso apropiado de los teléfonos celulares de la compañía, los vehículos, etc.; desarrollar un lenguaje de consentimiento; comprobar continuamente el equipo GPS; y considerar la posibilidad de salvaguardar los registros.

Otro estudio de Ciocchetti (2011) clasificó cada una de las mejores prácticas de monitoreo en uno de los siguientes tipos: a) mejores prácticas (por ejemplo, monitoreo que presenta la mayor protección y minimiza la invasión de la privacidad de los empleados), (b) prácticas riesgosas (por ejemplo, monitoreo que ofrece una protección bastante baja y ataca mínimamente la privacidad de los empleados), (c) prácticas fronterizas (por ejemplo, monitoreo que proporciona alta protección, pero también es altamente insidiosa) , y d) malas prácticas (por ejemplo, un seguimiento que proporciona baja protección y es extremadamente invasiva). Es probable que este sistema de clasificación ayude a los legisladores a equilibrar los intereses del empleador y de los empleados al legalizar la tecnología en el lugar de trabajo. Ciocchetti consideró que el sistema legal estadounidense ha sido lento para reaccionar de manera efectiva y eficiente a la creciente invasividad de la tecnología de monitoreo moderna y que todas las prácticas de monitoreo son perturbadoras y caen en las cuatro categorías que acabamos de mencionar. Sin embargo, Bennett y Locke (1998) declararon que una manera efectiva de evitar la responsabilidad por el asalto a la privacidad es presupontar que si un empleado puede litigar por tal agravio, el empleado lo hará.

La investigación demostró que los empleados pueden encontrar una fuente inclusiva de protección de la privacidad resultante del derecho de derecho común a la privacidad, que consiste en tres fechorías relevantes para la relación laboral: la intrusión en el aislamiento, que surge una invasión es una intrusión en la propiedad de otra persona sin el permiso de esa persona; publicidad dada a la vida privada, que existe cuando un individuo da publicidad a un tema relacionado con la vida privada de otro; y la publicidad colocando a una persona en una luz falsa, que ocurre cuando un individuo descuida sin hacer caso a la falsedad de la cuestión revelada y a la luz falsa en la que se colocaría a la otra persona (Hames & Diersen, 1991). Alternativamente, un conjunto de reformas desarrolladas por Conlon (1997) protegen las preocupaciones individuales de privacidad en el lugar de trabajo:

- No se debe realizar ningún monitoreo en baños, vestuarios y salones de empleados; sin embargo, el tiempo que pasa fuera del lugar de trabajo puede ser monitoreado de maneras menos odiosas.
- Debe prohibirse la supervisión fuera del sitio; permitir a los empleados acceder a toda la información recopilada a través de métodos o técnicas de monitoreo y considerar su reflexión sobre dicha información; y limitar la duración del monitoreo cada día con un sugerido (máximo de 2 horas por día).

- Los empleados deben ser conscientes de los dispositivos que se utilizarán para supervisarlos, cómo se utilizarán los datos y cuándo exactamente se supervisarán; y los empleados y clientes deben ser notificados cuando el monitoreo de telefonía se está llevando a cabo a través del uso de un tono específico que puede ser escuchado tanto por el empleado como por el cliente.
- Los empleadores deben recopilar únicamente información relevante para tomar decisiones críticas; y no basta con justificar el seguimiento por la necesidad de aumentar la productividad o mejorar el rendimiento, sino que también los empleadores deberían ser capaces de demostrar cómo se logró el objetivo a través del proceso de monitoreo.

En cualquier caso, la base legal del derecho a la privacidad tiene un fundamento teórico para los intelectuales legales que pueden ser complejos para el público reconocer o valorar (C. L. Swanson, 1988). A pesar de las diferentes escuelas de pensamiento entre los académicos, se han ofrecido numerosas propuestas para la contemplación de la dirección: formular por qué, cómo y cuándo se aplica el monitoreo electrónico; reunir sólo información relacionada con el trabajo; reunir sólo información con el propósito de elevar el desempeño de los empleados; proporcionar retroalimentación oportuna a los empleados para que se puedan realizar acciones correctivas en el rendimiento; asegurar premios a individuos o desempeño grupal; educar a los empleados sobre las características conductuales y sociales del monitoreo electrónico; acentuar las características cualitativas del rendimiento no contabilizado por la supervisión electrónica; debe proporcionarse un período de prueba para todos los nuevos solicitantes o nuevos sistemas electrónicos; evitar ser demasiado rápido en el desarrollo de nuevas normas o métodos de monitoreo a menos que se demuestre que es eficaz; y utilizar sesiones de lluvia de ideas siempre que sea posible para mejorar el sistema de monitoreo electrónico en la organización (Vaught, Taylor, & Vaught, 2000). Sin embargo, el exceso de monitoreo y la publicidad de una cultura de monitoreo en toda la organización pueden crear problemas emocionales y conductuales que en última instancia pueden empujar a los empleados a ciertas actividades para engañar al sistema (Barrett, 2008).

Intrigantemente, Dillon y Thomas (2006) expusieron que existe una gran necesidad de conciencia universal y la indulgencia de las cuestiones de accesibilidad, uso personal y supervisión administrativa que involucran correo electrónico y computadoras en el lugar de trabajo; de lo contrario, es poco probable que los empleados entiendan adecuadamente las políticas y procedimientos de privacidad. Wen, Schwieger y Gershuny (2007) revisaron las tecnologías de vigilancia y discutieron las leyes federales y estatales relacionadas junto con las decisiones judiciales de los Estados Unidos y encontraron que ninguna ley federal o estatal de los Estados Unidos prohíbe a los empleadores monitorear su lugar de trabajo electrónico. Su investigación científica también proporcionó las siguientes estrategias que probablemente sean más eficaces y productivas tanto para los empleados como para los empleadores, y ayudar a los empleadores a prevenir los aspectos negativos de la supervisión: designar la supervisión y ejecución de la política de privacidad debe ser implementada por una autoridad; considerar un punto de vista jurídico para guiar jurídicamente el desarrollo de todas las políticas y procedimientos; desarrollar una política formal y mantener a todos los empleados informados de todas las modificaciones a la política; notificar a los empleados del sistema de monitoreo electrónico; evitar un ambiente de trabajo agresivo; desarrollar normas claras sobre el uso del correo electrónico; decidir qué datos deben y no deben ser accedidos; especificar límites de tiempo en línea; mantener un software que se ejecuta en segundo plano de cada equipo, como bloqueadores de ventanas emergentes o filtros de spam; y comunicar una política que sea aceptable para mensajería instantánea, blogs y uso de salas de chat dentro y fuera de la organización.

Haller (2002) también propuso los principales ingredientes de las políticas eficaces de privacidad: a) aviso, las empresas deben proporcionar a las partes interesadas un aviso destacado con respecto a sus prácticas de información; (b) la elección del consumidor, las empresas deben dar a las partes interesadas la libertad de elegir si pueden divulgar datos personales sobre ellos a terceros no afiliados; (c) acceso y corrección, las empresas deben aceptar a sus partes interesadas para hacer algunas correcciones si es necesario sobre los datos personales que han recopilado sobre ellos; (d) la seguridad, las empresas deben defender medidas de seguridad prácticas para proteger la privacidad de la información personal, y estas medidas pueden comprender la seguridad administrativa, física y técnica; y (e) la observancia, las empresas deben desarrollar un sistema que pueda hacer cumplir su política de privacidad y garantizar el cumplimiento

de sus propias normas y externas. Además, manteniendo un equilibrio entre la propensión de los empleadores a la productividad y el cumplimiento de los procedimientos legislativos, las corporaciones pueden tener más éxito en la práctica de lo siguiente: crear límites de privacidad inequívocos, desarrollar fórmulas y principios de privacidad, y defender los datos personales (Townsend & Bennett, 2003).

Los empleadores son menos vulnerables con respecto a ciertos temas de invasión de la privacidad, si las políticas escritas se comunican eficazmente; sin embargo, Kovach, Jordan, Tansey y Framinan (2000) argumentaron que demasiado monitoreo genera un lugar de trabajo lleno de estancamiento, culpa, cinismo y desconfianza. Prácticamente hablando, para eludir las violaciones de la privacidad de los empleados en el lugar de trabajo, los empleadores nunca deben promover una cultura de privacidad dentro de cada trimestre de una organización porque puede ser esencial monitorear algunas prácticas cuando ocurren problemas (Guffey & West, 1996). Un empleador ético supervisará el trabajo de los empleados dentro de las disposiciones de una política en particular (Cowan, 2008). Las corporaciones deben inscribirse si están haciendo frente a la información personal para cualquiera de los siguientes propósitos: investigación privada, administración de salud, prevención de delitos policiales y juicio de delincuentes, servicios legales, administración de deudas, comercio, trabajo público, educación, investigación, administración de justicia, servicios de consultoría o un sistema de informes de crédito (Grupe, Kuechler, & Sweeney, 2002).

En resumen, Zachary (2013) reconoció lo siguiente: La invasión de la privacidad en el lugar de trabajo es de inmensa preocupación tanto para los empleadores como para los empleados en los Estados Unidos, y la violación de la privacidad se ha aumentado en los procedimientos de empleo. La invasión de la privacidad puede dividirse en cuatro categorías: (a) fuga de información que denigra a otros, (b) usar el nombre de otra persona sin consentimiento, (c) comunicación inapropiada de datos privados, y (d) cuando un perpetrador intrusa intencionalmente, física, electrónicamente, o de otra manera, en el espacio privado de otros. Los tribunales varían según cuando existe la intrusión ilegal, y los empleadores deben estar extremadamente atentos a los diferentes tipos de invasión de la privacidad. Sorprendentemente, las disputas sobre los derechos de privacidad en los Estados Unidos, que algunos consideran una amenaza para erosionar los valores primarios estadounidenses, han tenido un aumento en la controversia sobre el grado en que los derechos antes intactos pueden reducirse debido a la relación empleador-empleado (Anton & Ward, 1998). En la siguiente sección, el autor presenta posibles alternativas a la supervisión electrónica del rendimiento (EPM).

CONCLUSIÓN

Mediante el monitoreo, los empleadores a menudo argumentan que son capaces de proteger a sus organizaciones de cualquier daño. En este sentido, la supervisión se percibe como una herramienta para mantener la seguridad de una organización. Las nuevas tecnologías no solo han ofrecido a las organizaciones razones para monitorear el comportamiento de los empleados, sino que estas tecnologías también han proporcionado nuevos métodos y técnicas para realizar la supervisión de los empleados. Por lo tanto, la tecnología debe ser tratada con precaución y discreción. Los empleadores deben darse cuenta de que los empleados pueden tomar represalias contra la organización por las prácticas de monitoreo desleales percibidas. Por lo tanto, es esencial cuando se aplican nuevas tecnologías para monitorear el comportamiento de los empleados para tener en cuenta muchas preocupaciones (por ejemplo, privacidad, necesidades y aspiraciones). Educar a los empleados sobre las razones detrás de su supervisión, desarrollar una amplia gama de políticas y procedimientos y comunicarlos eficazmente será vital para implementar con éxito un sistema de monitoreo.

El hecho de que los empleadores no reconozcan los derechos de los empleados puede causar una pérdida extensa, como demandas costosas, daños a la reputación de la organización y deterioro de los valores de los empleados. Por lo tanto, los empleadores deben equilibrar la necesidad de productividad con respecto a los derechos de los empleados a la privacidad, la seguridad y la seguridad. Centrarse en los logros en lugar del tiempo que pasa en el lugar de trabajo debe ser la principal preocupación para cualquier empleador. En otras palabras, no hay necesidad de vigilar a una fuerza de trabajo porque nadie puede trabajar 8 horas sin descansos, y puede surgir una cultura de deslealtad y desconfianza dentro de la

organización. Sin embargo, los empleados deben tener en cuenta que hay numerosos paquetes de software que podrían registrar todo lo que escriben, buscan y leen en sus equipos.

Este estudio ofrece muchas alternativas a EPM que probablemente satisfagan los objetivos de un empleador sin violar los derechos de privacidad. Otro tema importante planteado en este estudio es que el estilo de liderazgo más eficaz para monitorear el rendimiento y el comportamiento de los empleados a través de la tecnología sigue sin identificarse. Desde el punto de vista del autor, no hay necesidad de definir lo que es un comportamiento moral en las organizaciones maduras y saludables, pero es crucial arrojar luz sobre cómo utilizar las tecnologías sin violar los protocolos éticos. La tecnología es una herramienta que se puede utilizar ética y poco éticamente. Después de revisar un gran número de estudios sobre las percepciones de los empleados de monitoreo electrónico, el autor encontró que el uso de EPM ha creado una gran cantidad de tensión y presión entre los individuos en las organizaciones. Por lo tanto, el autor argumentó que el nivel de satisfacción, motivación, compromiso, lealtad e integridad de los empleados en el lugar de trabajo puede verse afectado como resultado de niveles extremos de estrés. Por lo tanto, educar a los empleados sobre el sistema de monitoreo y establecer criterios de desempeño justos, justicia distributiva, justicia procesal y justicia de interacción puede hacer que el monitoreo sea menos angustioso. Es importante destacar que la supervisión debe ser coherente tanto con los objetivos generales de la organización como con los dilemas de rendimiento; sin embargo, las políticas de los empleadores no deben crear estrés y desconfianza en sus empleados. Más allá, el autor de este estudio argumentó que los esfuerzos de DDH pueden ser significativos en el monitoreo del comportamiento y el desempeño de los empleados en las organizaciones. La razón detrás de esta escuela de pensamiento es que el campo de los DDH enfatiza los elementos cruciales de las cuestiones de comportamiento y desarrollo en las organizaciones.

TRANSLATED VERSION: FRENCH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUITE: FRANÇAIS

Voici une traduction approximative des idées présentées ci-dessus. Cela a été fait pour donner une compréhension générale des idées présentées dans le document. Veuillez excuser toutes les erreurs grammaticales et ne pas tenir les auteurs originaux responsables de ces erreurs.

INTRODUCTION

Recherche sur la surveillance électronique et les préoccupations en matière de protection de la vie privée

Surveiller les préoccupations accrues au sujet de la protection de la vie privée des employés; par conséquent, les employeurs doivent trouver un équilibre entre la surveillance des gains et les coûts liés à l'atteinte de la vie privée des employés (Jackson, Schuler et Werner, 2009). Toutefois, l'utilisation des technologies émergentes dans la surveillance des pratiques des employés soulève des préoccupations quant à la vulnérabilité des employés en matière de protection de la vie privée et il devient de plus en plus difficile d'équilibrer les droits à la sécurité des employeurs et les questions de protection de la vie privée des employés (Mathis et Jackson, 2000). Par conséquent, d'importantes questions relatives à la protection de la vie privée font l'objet de débats au sein des entreprises et du gouvernement, par exemple a) la violation de la vie privée : examen et récupération de courriels privés, de dossiers et d'information sur les employés à partir de leur accès à des sites Web Internet particuliers; b) la surveillance informatique : savoir continuellement où se trouve l'employé; c) correspondance informatique : synthèse des informations

obtenues de différentes sources pour améliorer vos services de marketing; d) dossiers de personnel non autorisés : collecte de numéros de téléphone, d'adresses électroniques, de numéros de carte de crédit et d'autres renseignements personnels pour établir des profils de clients (O'Brien et Marakas, 2006). Les progrès technologiques ont permis aux employeurs d'accroître la productivité des employés et de mettre en état de siège la vie privée des employés. Robbins et Coulter (1999) ont posé quelques questions troublantes, comme les suivantes :

1. Le système de messagerie est-il uniquement à des fins commerciales?
2. Est-ce qu'un employé est autorisé à envoyer des renseignements sur le travail par courriel à un collègue ainsi qu'à un chat personnel?
3. Quelle est l'utilisation acceptable du système?
4. Qui possède l'information produite à partir du réseau?

Les organisations réglementent l'utilisation d'Internet ou les visites de sites Web par leur main-d'œuvre, par deux moyens réguliers : en restreignant l'accès à des liens particuliers et en surveillant les actions des employés (Alampay et Hechanova, 2010). Dans cette étude, il est également révélé que les politiques de surveillance et de contrôle des sites Web varient d'un pays à l'autre; par exemple, la Chine, le Vietnam et Singapour non seulement bloquent certains sites, mais proscrivent également l'accès aux affaires politiques et linguistiques. Everett, Wong et Paynter (2006) ont conclu qu'un nombre important de sujets liés aux droits des employés et des employeurs devraient être pris en considération dans d'autres études : a) Une question importante porte sur l'établissement de la confiance entre les employeurs et les employés en milieu de travail; un autre sujet essentiel est lié à l'établissement d'une législation pertinente qui gère les questions de protection de la vie privée dans la surveillance en milieu de travail de façon franche; b) un facteur épineux est l'apparition croissante de satellites, d'installations communautaires et de travail à la maison, qui incitent les employeurs à surveiller leurs employés; c) la diversification et les capacités d'Internet en matière de communication fournissent de nouveaux sujets de recherche; d) la possibilité d'interdire tous les petits appareils électroniques sur le lieu de travail qui pourraient être utilisés pour envoyer par courriel les secrets des entreprises à un bénéficiaire externe; e) élargir la comparaison internationale et sonder la position croissante des normes internationales et des « accords d'harmonisation », concernant les politiques élaborées par l'Union européenne et les Nations Unies, ainsi que les normes propagées par l'Organisation internationale pour la normalisation, les agences nationales de défense et les branches gouvernementales des enquêtes criminelles.

Everett et coll. (2006) ont mentionné certaines questions qui pourraient mener à une plus grande utilisation par les employeurs de la perception selon laquelle une telle surveillance est nécessaire. Par exemple, les efforts du gouvernement pour écraser le terrorisme, apaiser la prolifération des connaissances sur les armes nucléaires, entraver le blanchiment d'argent et limiter les trafiquants de drogue, à la fois illégaux et pharmaceutiques. Plus récemment, les employeurs ont commencé à suivre leurs employés en utilisant la technologie du système de positionnement global (GPS), qui utilise un assemblage de satellites pour spécifier l'emplacement précis de l'appareil GPS. Par conséquent, Townsm et Cobb (2012) ont recommandé des mesures réalistes lors de l'application du suivi GPS comme suit : intégrer le suivi GPS avec d'autres politiques; préserver le droit de surveillance; ne créez pas de preuves concluantes avec des documents de suivi GPS; limiter l'utilisation de la technologie GPS pour surveiller; décrire rigoureusement l'utilisation appropriée des téléphones cellulaires, des véhicules, et ainsi de suite; élaborer un langage de consentement; vérifier continuellement l'équipement GPS; et envisager de protéger les dossiers.

Une autre étude de Ciocchetti (2011) a classé chacune des principales pratiques de surveillance dans l'un des types suivants : a) les meilleures pratiques (p. Ex., la surveillance qui présente la plus grande protection et minimise l'atteinte à la vie privée des employés), b) les pratiques à risque (p. Ex., la surveillance qui offre une protection plutôt faible et porte le minimum sur la vie privée des employés), c) les pratiques limites (p. Ex., la surveillance qui offre une protection élevée, mais qui est également très insidieuse) , et d) les mauvaises pratiques (p. Ex., la surveillance qui offre une faible protection et est extrêmement invasive). Ce système de classification est susceptible d'aider les législateurs à équilibrer les intérêts des employeurs et des employés lorsqu'ils légalisent la technologie en milieu de travail. M. Ciocchetti a estimé que le système juridique américain a été lent à réagir efficacement et efficacement à

l'invasivité croissante de la technologie de surveillance moderne et que toutes les pratiques de surveillance sont inquiétantes et relèvent des quatre catégories que nous venons de mentionner. Toutefois, Bennett et Locke (1998) ont déclaré qu'un moyen efficace d'éviter la responsabilité pour atteinte à la vie privée consiste à présupposer que si un employé peut intenter une poursuite pour un tel délit, l'employé le fera.

La recherche a montré que les employés peuvent trouver une source inclusive de protection de la vie privée résultant du droit à la vie privée en common law, qui se compose de trois méfaits pertinents à la relation d'emploi : l'intrusion dans l'isolement, qui découle d'un empiétement est une intrusion sur la propriété d'une autre personne sans la permission de cette personne; la publicité donnée à sa vie privée, qui existe lorsqu'un individu donne de la publicité à une question concernant la vie privée d'une autre; et la publicité plaçant une personne sous un faux jour, qui se produit lorsqu'un individu ignore sans égard la fausseté de la question révélée et la fausse lumière dans laquelle l'autre personne serait placée (Hames et Diersen, 1991). Par ailleurs, un ensemble de réformes élaborées par Conlon (1997) protègent les préoccupations individuelles en matière de protection de la vie privée en milieu de travail :

- Aucune surveillance ne doit être effectuée dans les toilettes, les vestiaires et les salons des employés; toutefois, le temps passé à l'extérieur du lieu de travail peut être surveillé de façon moins odieuse.
- La surveillance hors site devrait être interdite; permettre aux employés d'accéder à toutes les informations recueillies par le biais de méthodes ou de techniques de surveillance et d'examiner leur réflexion sur ces informations; et limiter la durée de la surveillance chaque jour avec une suggestion (maximum de 2 heures par jour).
- Les employés doivent être au courant des appareils qui seront utilisés pour les surveiller, de la façon dont les données seront utilisées et du moment exact où elles seront surveillées; et les employés et les clients doivent être avisés lorsque la surveillance téléphonique a lieu par l'utilisation d'un ton spécifique qui peut être entendu par l'employé et le client.
- Les employeurs ne devraient recueillir que des renseignements pertinents pour prendre des décisions critiques; et il ne suffit pas de justifier la surveillance par la nécessité d'accroître la productivité ou d'améliorer le rendement, mais aussi de démontrer comment l'objectif a été atteint par le biais du processus de surveillance.

Quel que soit le fondement légitime du droit à la vie privée a un fondement théorique pour les intellectuels juridiques qui peut être complexe pour le public à reconnaître ou à valoriser (C. L. Swanson, 1988). Malgré les différentes écoles de pensée parmi les universitaires, de nombreuses propositions ont été proposées pour la contemplation de la direction : formuler pourquoi, comment et quand la surveillance électronique est appliquée; recueillir uniquement des informations relatives au travail; recueillir uniquement de l'information dans le but d'accroître le rendement des employés; fournir des commentaires opportuns aux employés afin que des mesures correctives soient prises; obtenir des récompenses aux particuliers ou au rendement de groupe; sensibiliser les employés aux caractéristiques comportementales et sociales de la surveillance électronique; accentuer les caractéristiques qualitatives de la performance qui ne sont pas expliquées par la surveillance électronique; une période d'essai pour tous les nouveaux demandeurs ou nouveaux systèmes électroniques devrait être prévue; éviter d'être trop rapide dans l'élaboration de nouvelles normes ou de nouvelles méthodes de surveillance à moins qu'elles ne s'avèrent efficaces; et utiliser des séances de remue-méninges dans la mesure du possible pour améliorer le système de surveillance électronique de l'organisation (Vaught, Taylor et Vaught, 2000). Néanmoins, trop de surveillance et la publicité d'une culture de surveillance dans toute l'organisation peuvent créer des problèmes émotionnels et comportementaux qui peuvent finalement pousser les employés dans certaines activités pour tromper le système (Barrett, 2008).

Curieusement, Dillon et Thomas (2006) ont exposé qu'il y a un grand besoin de conscience universelle et d'indulgence à l'égard de l'accessibilité, de l'utilisation personnelle et des questions de surveillance administrative impliquant le courrier électronique et les ordinateurs en milieu de travail; autrement, il est peu probable que les employés comprennent adéquatement les politiques et les procédures en matière de protection de la vie privée. Wen, Schwieger et Gershuny (2007) ont examiné les technologies de surveillance et discuté des lois fédérales et étatiques connexes ainsi que des décisions judiciaires

américaines et ont conclu qu'aucune loi fédérale ou étatique des États-Unis n'interdisait aux employeurs de surveiller leur lieu de travail électronique. Leurs recherches scientifiques ont également fourni les stratégies suivantes qui sont susceptibles d'être les plus efficaces et productives tant pour les employés que pour les employeurs, et aident les employeurs à prévenir les aspects négatifs de la surveillance : la désignation de la surveillance et de l'exécution de la politique de protection de la vie privée devrait être mise en œuvre par une autorité; envisager un point de vue juridique pour guider juridiquement l'élaboration de toutes les politiques et procédures; élaborer une politique officielle et tenir tous les employés informés de toutes les modifications apportées à la politique; aviser les employés du système de surveillance électronique; éviter un environnement de travail agressif; élaborer des règles claires sur l'utilisation du courrier électronique; décider quelles données devraient et ne devraient pas être consultées; spécifier les délais en ligne; maintenir un logiciel en cours d'exécution en arrière-plan de chaque ordinateur, tels que les bloqueurs de fenêtres contextuelles ou les filtres anti-spam ; et communiquer une politique acceptable pour la messagerie instantanée, les blogs et l'utilisation des salles de chat dans et hors de l'organisation.

Haller (2002) a également proposé les principaux ingrédients de politiques efficaces en matière de protection de la vie privée : a) avis, les entreprises devraient fournir aux intervenants un avis important sur ses pratiques en matière d'information; b) le choix des consommateurs, les entreprises devraient donner aux parties prenantes la liberté de choisir si elles peuvent divulguer des données à caractère personnel à leur sujet à des tiers non affiliés; c) l'accès et la correction, les entreprises devraient accepter que leurs parties prenantes fassent des corrections si nécessaire au sujet des données à caractère personnel qu'elles ont recueillies à leur sujet; d) la sécurité, les entreprises devraient adopter des mesures de sécurité pratiques pour protéger la vie privée des renseignements personnels, et ces mesures peuvent comprendre la sécurité administrative, physique et technique; e) l'application de la loi, les entreprises devraient mettre au point un système qui puisse faire respecter sa politique de protection de la vie privée et assurer le respect de leurs propres normes et de leurs propres normes externes. De plus, en maintenant un équilibre entre la propension des employeurs à la productivité et le respect des procédures législatives, les sociétés peuvent avoir le plus de succès à pratiquer ce qui suit : créer des limites de protection de la vie privée sans ambiguïté, élaborer des formules et des principes en matière de protection de la vie privée et défendre les données à caractère personnel (Townsend et Bennett, 2003).

Les employeurs sont moins vulnérables en ce qui concerne certaines questions d'atteinte à la vie privée, si les politiques écrites sont communiquées efficacement; Cependant, Kovach, Jordan, Tansey et Framinan (2000) ont fait valoir que trop de surveillance génère un milieu de travail rempli d'impasses, de blâmes, de cynisme et de méfiance. Concrètement, pour contourner les violations de la vie privée des employés en milieu de travail, les employeurs ne devraient jamais promouvoir une culture de la vie privée au sein de chaque quart d'organisation parce qu'il peut être essentiel de surveiller certaines pratiques lorsque des problèmes se produisent (Guffey et West, 1996). Un employeur éthique surveillera le travail des employés dans le cadre des dispositions d'une politique particulière (Cowan, 2008). Les sociétés doivent s'inscrire si elles font face à des renseignements personnels à l'une des fins suivantes : enquête privée, administration de la santé, prévention policière de la criminalité et procès de délinquants, services juridiques, administration de la dette, négociation, travail public, éducation, recherche, administration de la justice, services de consultation ou système d'information sur le crédit (Grupe, Kuechler, et Sweeney, 2002).

Résumé brièvement, Zachary (2013) a reconnu ce qui suit : l'empiétement des lieux de travail à la vie privée est d'une grande préoccupation pour les employeurs et les employés aux États-Unis, et la violation de la vie privée a été augmentée dans les procédures d'emploi. L'atteinte à la vie privée peut se situer en quatre catégories : a) une fuite d'information qui dénigre les autres, b) l'utilisation du nom d'une autre personne sans consentement, c) la communication inappropriée de données privées et d) lorsqu'un auteur empiète délibérément, physiquement, électroniquement ou autrement, sur l'espace privé d'autrui. Les tribunaux varient en fonction du moment où l'intrusion illégale existe, et les employeurs devraient être extrêmement vigilants à des types différents d'atteinte à la vie privée. Fait remarquable, les différends relatifs au droit à la vie privée aux États-Unis, que certains considèrent comme une menace à l'érosion des valeurs américaines primaires, ont suscité une recrudescence de controverses quant à la mesure dans laquelle les droits autrefois intacts peuvent être réduits en raison de la relation employeur-employé (Anton

et Ward, 1998). Dans la section suivante, l'auteur présente des alternatives possibles à la surveillance électronique des performances (EPM).

CONCLUSION

En surveillant, les employeurs soutiennent souvent qu'ils sont en mesure de protéger leur organisation contre tout préjudice. En ce sens, la surveillance est perçue comme un outil pour maintenir la sécurité d'une organisation. Les nouvelles technologies ont non seulement offert aux organisations des raisons de surveiller le comportement des employés, mais ces technologies ont également fourni de nouvelles méthodes et techniques pour effectuer la surveillance des employés. Ainsi, la technologie doit être traitée avec prudence et discrétion. Les employeurs devraient se rendre compte que les employés peuvent se venger de l'organisation pour les pratiques de surveillance déloyales perçues. Par conséquent, il est essentiel, lorsqu'on applique de nouvelles technologies pour surveiller le comportement des employés, afin de tenir compte de nombreuses préoccupations (p. Ex., protection de la vie privée, besoins et aspirations). Il sera essentiel d'éduquer les employés sur les raisons qui les sous-tendent, d'élaborer un large éventail de politiques et de procédures et de les communiquer efficacement pour mettre en œuvre avec succès un système de surveillance.

Le fait que les employeurs ne reconnaissent pas les droits des employés peut entraîner des pertes importantes, comme des poursuites coûteuses, des dommages à la réputation de l'organisation et une atteinte aux valeurs des employés. Par conséquent, les employeurs devraient trouver un équilibre entre le besoin de productivité en ce qui concerne les droits des employés à la vie privée, à la sécurité et à la sécurité. Mettre l'accent sur les réalisations plutôt que sur le temps passé en milieu de travail devrait être la principale préoccupation de tout employeur. En d'autres termes, il n'est pas nécessaire de faire de la police une main-d'œuvre parce que personne ne peut travailler 8 heures sans pauses, et une culture de déloyauté et de méfiance au sein de l'organisation peut émerger. Toutefois, les employés doivent être conscients qu'il existe de nombreux logiciels qui pourraient clé enregistrer tout ce qu'ils tapent, rechercher et lire sur leurs ordinateurs.

Cette étude offre de nombreuses solutions de rechange à l'epm qui sont susceptibles de satisfaire les objectifs d'un employeur sans violer le droit à la vie privée. Une autre question importante soulevée dans cette étude est que le style de leadership le plus efficace pour surveiller le rendement et le comportement des employés grâce à la technologie reste non identifié. Du point de vue de l'auteur, il n'est pas nécessaire de définir ce qu'est un comportement moral dans les organisations matures et saines, mais il est crucial de faire la lumière sur la façon d'utiliser les technologies sans violer les protocoles éthiques. La technologie est un outil qui peut être utilisé de manière éthique et contraire à l'éthique. Après avoir examiné un grand nombre d'études sur les perceptions des employés à l'égard de la surveillance électronique, l'auteur a constaté que l'utilisation de l'epm a créé beaucoup de tensions et de pressions parmi les individus dans les organisations. Par conséquent, l'auteur a soutenu que le niveau de satisfaction, de motivation, d'engagement, de loyauté et d'intégrité des employés en milieu de travail peut être affecté en raison de niveaux extrêmes de stress. Par conséquent, l'éducation des employés au sujet du système de surveillance et l'établissement de critères de rendement équitables, de justice distributive, de justice procédurale et de justice interactionnelle peuvent rendre la surveillance moins pénible. Fait important, la surveillance devrait être conforme à la fois aux objectifs généraux de l'organisation et aux dilemmes du rendement; toutefois, les politiques des employeurs ne devraient pas créer de stress et de méfiance à l'égard de leurs employés. Au-delà, l'auteur de cette étude a soutenu que les efforts de DRH peuvent être importants dans la surveillance du comportement et du rendement des employés au cours des organisations. La raison d'être de cette école de pensée est que le domaine du DRH met l'accent sur des éléments cruciaux des questions comportementales et de développement dans les organisations.

TRANSLATED VERSION: GERMAN

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

ÜBERSETZTE VERSION: DEUTSCH

Hier ist eine ungefähre Übersetzung der oben vorgestellten Ideen. Dies wurde getan, um ein allgemeines Verständnis der in dem Dokument vorgestellten Ideen zu vermitteln. Bitte entschuldigen Sie alle grammatikalischen Fehler und machen Sie die ursprünglichen Autoren nicht für diese Fehler verantwortlich.

EINLEITUNG

Forschung über elektronische Überwachung und Datenschutzbedenken

Überwachung erhöhter Bedenken hinsichtlich der Privatsphäre der Mitarbeiter; Daher müssen die Arbeitgeber ein Gleichgewicht zwischen der Überwachung der Gewinne und den Kosten für die Privatsphäre der Mitarbeiter finden (Jackson, Schuler, & Werner, 2009). Der Einsatz neuer Technologien bei der Überwachung von Mitarbeiterpraktiken gibt jedoch Anlass zur Sorge, dass die Datenschutzrechte der Arbeitnehmer anfällig sind, und es wird immer schwieriger, die Sicherheitsrechte der Arbeitgeber mit Fragen der Privatsphäre der Mitarbeiter in Einklang zu bringen (Mathis & Jackson, 2000). Folglich werden in derwirtschaft und Regierung wichtige Datenschutzfragen diskutiert, z. B. (a) Verletzung der Privatsphäre: Prüfung und Abruf privater E-Mails, Aufzeichnungen und Informationen über Mitarbeiter von ihrem Zugang zu bestimmten Internet-Websites; b) Computerüberwachung: ständig zu wissen, wo sich der Arbeitnehmer befindet; c) Computerabgleich: Synthese von Informationen aus verschiedenen Quellen, um Ihre Marketing-Dienstleistungen zu verbessern; und (d) nicht autorisierte Personalakten: Sammeln von Telefonnummern, E-Mail-Adressen, Kreditkartennummern und anderen privaten Informationen zur Entwicklung von Kundenprofilen (O'Brien & Marakas, 2006). Technologische Fortschritte ermöglichten es Arbeitgebern, die Produktivität der Mitarbeiter zu steigern und die Privatsphäre der Mitarbeiter zu schützen. Robbins und Coulter (1999) stellten einige verblüffende Fragen, wie z. B. Die folgenden:

1. Ist das E-Mail-System nur für geschäftliche Zwecke?
2. Darf ein Mitarbeiter Arbeitsinformationen an einen Kollegen per E-Mail versenden und persönliche Chats führen?
3. Was ist die akzeptable Nutzung des Systems?
4. Wer besitzt die Informationen, die aus dem Netzwerk stammen?

Organisationen regeln die Internetnutzung oder Website-Besuche ihrer Mitarbeiter auf zwei regelmäßige Weise: durch die Beschränkung des Zugriffs auf bestimmte Links und durch die Überwachung von Mitarbeiteraktionen (Alampay & Hechanova, 2010). In dieser Studie wird auch gezeigt, dass die Überwachungspolitik und die Kontrolle von Websites von Land zu Land unterschiedlich sind; China, Vietnam und Singapur blockieren beispielsweise nicht nur bestimmte Websites, sondern verbieten auch den Zugang zu politischen und sprachlichen Angelegenheiten. Everett, Wong und Paynter (2006) stellten fest, dass eine beträchtliche Anzahl von Themen im Zusammenhang mit Arbeitnehmer- und Arbeitgeberrechten in weiteren Studien berücksichtigt werden sollte: a) Ein wichtiges Thema ist die Vertrauensbildung zwischen Arbeitgebern und Arbeitnehmern am Arbeitsplatz; ein weiteres wichtiges Thema ist die Schaffung einschlägiger Rechtsvorschriften, die Datenschutzfragen bei der Überwachung am Arbeitsplatz offen behandeln; b) ein heikler Faktor ist das zunehmende Auftreten von Satelliten, gemeinschaftsgefährdeten Einrichtungen und arbeiten zu Hause, die arbeitgeberzur Beobachtung ihrer Arbeitnehmer drängen; c) die Diversifizierung und die Kommunikationskapazitäten des Internets neue Forschungsthemen liefern; d) die Möglichkeit, alle kleinen elektronischen Geräte am Arbeitsplatz zu verbieten, die dazu verwendet werden könnten, die Geheimnisse der Unternehmen an einen externen Begünstigten zu senden; und e) Erweiterung des internationalen Vergleichs und Sondierung der zunehmenden Position internationaler Normen und "Harmonisierungsabkommen" in Bezug auf die von der

Europäischen Union und den Vereinten Nationen entwickelte Politik sowie die von der Internationalen Organisation für Normung, den nationalen Verteidigungsbehörden und den staatlichen Untersuchungsbereichen propagierten Standards.

Everett et al. (2006) verwiesen auf bestimmte Fragen, die möglicherweise zu einer stärkeren Nutzung der Wahrnehmung durch die Arbeitgeber führen, dass eine solche Überwachung erforderlich ist. Zum Beispiel die Bemühungen der Regierung, den Terrorismus zu zerschlagen, die Verbreitung von Kernwaffenwissen zu bekämpfen, Geldwäsche zu behindern und Drogenhändler sowohl illegal als auch pharmazeutisch einzuschränken. In jüngerer Zeit haben Arbeitgeber begonnen, ihre Mitarbeiter zu verfolgen, indem sie die GPS-Technologie (Global Positioning System) verwenden, die eine Assemblage von Satelliten verwendet, um den genauen Standort des GPS-fähigen Geräts zu spezifizieren. Daher empfahltownsm und Cobb (2012) realistische Schritte bei der Anwendung von GPS-Tracking wie folgt: GPS-Tracking mit anderen Richtlinien integrieren; das Recht auf Überwachung zu wahren; keine schlüssigen Beweise mit GPS-Tracking-Dokumenten erstellen; die Nutzung der GPS-Technologie zur Überwachung zu beschränken; die angemessene Nutzung von Mobiltelefonen, Fahrzeugen usw. Des Unternehmens genau umreißen; eine Zustimmungssprache zu entwickeln; gps-Geräte kontinuierlich zu überprüfen; und erwägen, Aufzeichnungen zu schützen.

Eine weitere Studie von Ciocchetti (2011) ordnete jede der Top-Überwachungspraktiken in eine der folgenden Arten ein: (a) Best Practices (z. B. Überwachung, die den größten Schutz bietet und die Verletzung der Privatsphäre der Mitarbeiter minimiert), (b) riskante Praktiken (z. B. Überwachung, die eher geringen Schutz bietet und die Privatsphäre der Mitarbeiter minimal angreift), (c) Grenzpraktiken (z. B. Überwachung, die einen hohen Schutz bietet, aber auch sehr unerheblich ist) und (d) schlechte Praktiken (z. B. Überwachung, die einen geringen Schutz bietet und extrem invasiv ist). Dieses Klassifizierungssystem dürfte den Gesetzgebern dabei helfen, sowohl Arbeitgeber- als auch Arbeitnehmerinteressen bei der Legalisierung der Arbeitsplatztechnologie in Einklang zu bringen. Ciocchetti war der Der vertreten, dass das amerikanische Rechtssystem träge war, effektiv und effizient auf die zunehmende Invasivität der modernen Überwachungstechnologie zu reagieren, und dass alle Überwachungspraktiken beunruhigend sind und in die vier gerade genannten Kategorien fallen. Bennett und Locke (1998) erklärten jedoch, dass ein effektiver Weg, um die Haftung für Datenschutzangriffe zu vermeiden, voraussetzt, dass, wenn ein Mitarbeiter für eine solche unerlaubte Handlung klagen kann, der Mitarbeiter dies tun wird.

Untersuchungen haben gezeigt, dass Mitarbeiter eine integrative Quelle des Schutzes der Privatsphäre finden können, die sich aus dem allgemeinen Recht auf Privatsphäre ergibt, das aus drei für das Arbeitsverhältnis relevanten Missetaten besteht: Eindringen in die Abgeschiedenheit, das einen Eingriff auf das Eigentum eines anderen ohne die Erlaubnis dieser Person verursacht; Werbung für das Privatleben, die besteht, wenn eine Person ein Thema über das Privatleben eines anderen bekannt macht; und Öffentlichkeitsarbeit, die eine Person in ein falsches Licht stellt, das auftritt, wenn ein Individuum die Falschheit der aufgedeckten Frage und das falsche Licht, in das die andere Person gestellt würde, achtlos missachtet (Hames & Diersen, 1991). Alternativ werden von Conlon (1997) eine Reihe von Reformen zum Schutz der individuellen Datenschutzbedenken am Arbeitsplatz durchgeführt:

- In Toiletten, Umkleidekabinen und Mitarbeiterlounges sollte keine Überwachung durchgeführt werden; Die Außerhalb des Arbeitsplatzes verbrachte Zeit kann jedoch auf weniger abscheuliche Weise überwacht werden.
- Die Überwachung vor Ort sollte verboten werden; den Mitarbeitern den Zugang zu allen Informationen zu ermöglichen, die durch Überwachungsmethoden oder -techniken gesammelt werden, und ihre Reflexion über diese Informationen zu prüfen; und begrenzen Sie die Dauer der Überwachung jeden Tag mit einem vorgeschlagenen (maximal 2 Stunden pro Tag).
- Die Mitarbeiter sollten sich der Geräte bewusst sein, die zur Überwachung dieser Geräte verwendet werden, wie die Daten verwendet werden und wann genau sie überwacht werden; Mitarbeiter und Kunden sollten benachrichtigt werden, wenn die telefonische Überwachung durch die Verwendung eines bestimmten Tons erfolgt, der sowohl von Mitarbeitern als auch vom Kunden gehört werden kann.

- Arbeitgeber sollten nur Informationen sammeln, die für kritische Entscheidungen relevant sind; und es reicht nicht aus, die Überwachung durch die Notwendigkeit einer Steigerung der Produktivität oder Leistungssteigerung zu rechtfertigen, aber auch sollten die Arbeitgeber in der Lage sein, zu zeigen, wie das Ziel durch den Überwachungsprozess erreicht wurde.

Wie auch immer, die rechtmäßige Grundlage des Rechts auf Privatsphäre hat eine theoretische Grundlage für juristische Intellektuelle, die für die Öffentlichkeit komplex zu erkennen oder zu bewerten sein kann (C. L. Swanson, 1988). Trotz der unterschiedlichen Denkschulen unter Akademikern wurden zahlreiche Vorschläge für die Betrachtung des Managements angeboten: formulieren, warum, wie und wann elektronische Überwachung angewendet wird; nur arbeitsbezogene Informationen zu sammeln; nur Informationen zu sammeln, um die Leistung der Mitarbeiter zu steigern; den Mitarbeitern rechtzeitigfeedback zu geben, damit Korrekturmaßnahmen zur Leistung ergriffen werden können; sichere Auszeichnungen für Einzelpersonen oder Gruppenleistungen; die Mitarbeiter über die verhaltens- und sozialen Merkmale der elektronischen Überwachung aufzuklären; qualitative Leistungsmerkmale zu betonen, die nicht durch elektronische Überwachung berücksichtigt werden; für alle neuen Antragsteller oder neue elektronische Systeme sollte eine Probezeit vorgesehen werden; vermeidung, bei der Entwicklung neuer Normen oder Überwachungsmethoden zu schnell zu sein, wenn sich nicht als wirksam erweisen; und brainstorming-Sitzungen zu nutzen, wann immer möglich, um das elektronische Überwachungssystem in der Organisation zu verbessern (Vaught, Taylor, & Vaught, 2000). Dennoch kann zu viel Überwachung und die Publizität einer Überwachungskultur in der gesamten Organisation emotionale und Verhaltensprobleme verursachen, die letztlich Mitarbeiter in bestimmte Aktivitäten drängen können, um das System zu betrügen (Barrett, 2008).

Faszinierenderweise haben Dillon und Thomas (2006) aufgedeckt, dass es ein großes Bedürfnis nach universellem Bewusstsein und Nachsicht bei der Zugänglichkeit, der persönlichen Nutzung und der administrativen Aufsicht im Zusammenhang mit E-Mail und Computern am Arbeitsplatz gibt; Andernfalls ist es unwahrscheinlich, dass Mitarbeiter Datenschutzrichtlinien und -verfahren angemessen verstehen. Wen, Schwieger und Gershuny (2007) überprüften Überwachungstechnologien und diskutierten die damit verbundenen Bundes- und Landesgesetze zusammen mit US-Justizentscheidungen und stellten fest, dass kein US-Bundes- oder Landesgesetz Arbeitgebern die Überwachung ihres elektronischen Arbeitsplatzes verbietet. Ihre wissenschaftliche Untersuchung lieferte auch die folgenden Strategien, die sowohl für Arbeitnehmer als auch für Arbeitgeber am effektivsten und produktivsten sein und arbeitgebern helfen, die negativen Aspekte der Überwachung zu verhindern: Die Benennung der Aufsicht und Durchführung der Datenschutzpolitik sollte von einer Behörde umgesetzt werden; einen rechtlichen Standpunkt zu prüfen, um die Entwicklung aller Politiken und Verfahren rechtlich zu lenken; eine formelle Politik zu entwickeln und alle Arbeitnehmer über alle Änderungen der Richtlinie auf dem Laufenden zu halten; die Mitarbeiter über das elektronische Überwachungssystem zu informieren; ein aggressives Arbeitsumfeld zu vermeiden; klare Regeln für die Verwendung von E-Mails zu entwickeln; entscheiden, auf welche Daten zugegriffen werden soll und welche nicht; Online-Zeitlimits festlegen; eine Software zu verwalten, die im Hintergrund jedes Computers ausgeführt wird, z. B. Popupblocker oder Spamfilter; und kommunizieren Sie eine Richtlinie, die für Instant Messaging, Blogging und Chatroom-Nutzung in und a-out in der Organisation akzeptabel ist.

Haller (2002) schlug auch die Wichtigsten Bestandteile wirksamer Datenschutzrichtlinien vor: a) Bekanntmachung, Unternehmen sollten den Interessenträgern eine prominente Mitteilung gegenüber ihren Informationspraktiken geben; b) die Entscheidung der Verbraucher, dass die Unternehmen den Interessenträgern die Freiheit einräumen sollten, zu entscheiden, ob sie personenbezogene Daten über sie an nicht verbundene Dritte weitergeben können; c) Zugang und Berichtigung sollten die Unternehmen von ihren Interessenträgern akzeptieren, erforderlichenfalls Korrekturen zu personenbezogenen Daten vorzunehmen, die sie über sie gesammelt haben; d) Sicherheit sollten Unternehmen praktische Sicherheitsmaßnahmen zum Schutz der Privatsphäre personenbezogener Daten ergreifen, und diese Maßnahmen können administrative, physische und technische Sicherheit umfassen; und (e) Durchsetzung sollten Unternehmen ein System entwickeln, das ihre Datenschutzrichtlinien durchsetzen und die Einhaltung ihrer eigenen und externen Standards sicherstellen kann. Darüber hinaus können Unternehmen,

die ein Gleichgewicht zwischen der Neigung der Arbeitgeber zur Produktivität und der Einhaltung gesetzlicher Verfahren wahren, am erfolgreichsten sein, wenn es darum geht, Folgendes zu praktizieren: Schaffung eindeutiger Datenschutzgrenzen, Entwicklung von Datenschutzformeln und -prinzipien und Verteidigung personenbezogener Daten (Townsend & Bennett, 2003).

Arbeitgeber sind in Bezug auf bestimmte Fragen der Verletzung der Privatsphäre weniger anfällig, wenn schriftliche Richtlinien wirksam kommuniziert werden; Kovach, Jordan, Tansey und Framinan (2000) argumentierten jedoch, dass zu viel Überwachung einen Arbeitsplatz mit Stillstand, Schuld, Zynismus und Misstrauen erzeugt. In der Praxis sollten Arbeitgeber niemals in jedem Quartal einer Organisation eine Kultur der Privatsphäre fördern, um Verletzungen der Privatsphäre der Arbeitnehmer am Arbeitsplatz zu umgehen, da es möglicherweise wichtig ist, einige Praktiken zu überwachen, wenn Probleme auftreten (Guffey & West, 1996). Ein ethischer Arbeitgeber überwacht die Arbeit der Arbeitnehmer im Rahmen einer bestimmten Politik (Cowan, 2008). Unternehmen müssen sich einschreiben, wenn sie mit personenbezogenen Daten für einen der folgenden Zwecke fertig werden: private Ermittlungen, Gesundheitsverwaltung, polizeiliche Verbrechensvermeidung und Prozess gegen Straftäter, Juristische Dienstleistungen, Schuldenverwaltung, Handel, öffentliche Fallarbeit, Bildung, Forschung, Justizverwaltung, Beratungsdienste oder ein Kreditberichterstattungssystem (Grupe, Kuechler, & Sweeney, 2002).

Kurz zusammengefasst, räumte Zachary (2013) Folgendes ein: Der Eingriff in die Privatsphäre am Arbeitsplatz ist sowohl für Arbeitgeber als auch für Arbeitnehmer in den Vereinigten Staaten von immenser Bedeutung, und die Verletzung der Privatsphäre wurde in Arbeitsverfahren verstärkt. Die Verletzung der Privatsphäre kann in vier Kategorien unterteilt werden: (a) Informationslecks, die andere verunglimpft, (b) die Verwendung des Namens einer anderen Person ohne Zustimmung, (c) unangemessene Übermittlung privater Daten und (d) wenn ein Täter absichtlich, physisch, elektronisch oder anderweitig, in den privaten Raum anderer eindringt. Die Gerichte variieren je nachdem, wann das illegale Eindringen existiert, und Arbeitgeber sollten äußerst wachsam sein, um unterschiedliche Arten von Eingriffen in die Privatsphäre zu bekämpfen. Bemerkenswerterweise haben Streitigkeiten über die Privatsphäre in den Vereinigten Staaten, die einige als Bedrohung für die Aushöhlung der primären amerikanischen Werte ansehen, einen Anstieg der Kontroverse darüber ausgelöst, inwieweit Rechte, die früher unberührt geblieben sind, aufgrund der Arbeitgeber-Arbeitnehmer-Beziehung eingeschränkt werden können (Anton & Ward, 1998). Im folgenden Abschnitt stellt der Autor mögliche Alternativen zur elektronischen Leistungsüberwachung (EPM) vor.

SCHLUSSFOLGERUNG

Durch die Überwachung argumentieren Arbeitgeber oft, dass sie in der Lage sind, ihre Organisationen vor jeglichem Schaden zu schützen. In diesem Sinne wird die Überwachung als ein Werkzeug zur Aufrechterhaltung der Sicherheit einer Organisation wahrgenommen. Neue Technologien haben Organisationen nicht nur Gründe geboten, das Verhalten ihrer Mitarbeiter zu überwachen, sondern diese Technologien haben auch neue Methoden und Techniken zur Überwachung von Mitarbeitern bereitgestellt. Daher muss Technologie mit Vorsicht und Diskretion behandelt werden. Die Arbeitgeber sollten erkennen, dass Arbeitnehmer Vergeltungsmaßnahmen gegen die Organisation wegen der als unlauter empfundenen Überwachungspraktiken ergreifen können. Daher ist es bei der Anwendung neuer Technologien zur Überwachung des Mitarbeiterverhaltens unerlässlich, um viele Bedenken (z. B. Privatsphäre, Bedürfnisse und Bestrebungen) zu berücksichtigen. Die Schulung der Mitarbeiter über die Gründe für ihre Überwachung, die Entwicklung einer breiten Palette von Richtlinien und Verfahren und ihre wirksame Kommunikation werden für die erfolgreiche Implementierung eines Überwachungssystems von entscheidender Bedeutung sein.

Das Versäumnis der Arbeitgeber, Arbeitnehmerrechte anzuerkennen, kann zu erheblichen Verlusten führen, wie z. B. Kostspielige Klagen, Einen Schaden für den Ruf der Organisation und eine Beeinträchtigung der Mitarbeiterwerte. Daher sollten Arbeitgeber die Notwendigkeit der Produktivität in Bezug auf die Rechte der Arbeitnehmer auf Privatsphäre, Sicherheit und Sicherheit in Einklang bringen. Die Konzentration auf Leistungen und nicht auf die am Arbeitsplatz verbrachte Zeit sollte das Hauptanliegen eines jeden Arbeitgebers sein. Mit anderen Worten, es besteht keine Notwendigkeit, eine

Belegschaft zu bestätigen, weil niemand 8 Stunden ohne Pausen arbeiten kann, und eine Kultur der Illoyalität und des Misstrauens innerhalb der Organisation kann entstehen. Mitarbeiter sollten sich jedoch bewusst sein, dass es zahlreiche Softwarepakete gibt, die alles, was sie eingeben, suchen und auf ihren Computern lesen, als Schlüssel protokollieren können.

Diese Studie bietet viele Alternativen zu EPM, die wahrscheinlich die Ziele eines Arbeitgebers erfüllen, ohne die Rechte auf Privatsphäre zu verletzen. Ein weiteres wichtiges Thema, das in dieser Studie angesprochen wird, ist, dass der effektivste Führungsstil zur Überwachung der Leistung und des Verhaltens der Mitarbeiter durch Technologie nicht identifiziert wird. Aus der Sicht des Autors besteht keine Notwendigkeit, zu definieren, was ein moralisches Verhalten in reifen und gesunden Organisationen ist, aber es ist entscheidend, Licht in die Art und Weise zu bringen, wie Technologien verwendet werden, ohne ethische Protokolle zu verletzen. Technologie ist ein Werkzeug, das ethisch und unethisch eingesetzt werden kann. Nach einer Vielzahl von Studien über die Wahrnehmung elektronischer Überwachung durch Mitarbeiter stellte der Autor fest, dass der Einsatz von EPM eine große Spannung und einen hohen Druck zwischen Einzelpersonen in Organisationen erzeugt hat. Daher argumentierte der Autor, dass das Niveau der Zufriedenheit, Motivation, des Engagements, der Loyalität und der Integrität der Mitarbeiter am Arbeitsplatz durch extreme Belastungen beeinträchtigt werden kann. Daher kann die Aufklärung der Mitarbeiter über das Überwachungssystem und die Festlegung fairer Leistungskriterien, Verteilungsgerechtigkeit, Verfahrensgerechtigkeit und Interaktionsgerechtigkeit die Überwachung weniger belastend machen. Wichtig ist, dass die Überwachung sowohl mit den allgemeinen Zielen der Organisation als auch mit den Leistungsdilemmas im Einklang stehen sollte; Die Politik der Arbeitgeber sollte jedoch keine Belastungen und Misstrauen gegenüber ihren Arbeitnehmern erzeugen. Darüber hinaus argumentierte der Autor dieser Studie, dass HRD-Bemühungen bei der Überwachung des Mitarbeiterverhaltens und der Leistung in Organisationen von Bedeutung sein können. Der Grund für diese Denkschule ist, dass HRD-Bereich entscheidende Elemente von Verhaltens- und Entwicklungsfragen in Organisationen betont.

TRANSLATED VERSION: PORTUGUESE

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSÃO TRADUZIDA: PORTUGUÊS

Aqui está uma tradução aproximada das ideias acima apresentadas. Isto foi feito para dar uma compreensão geral das ideias apresentadas no documento. Por favor, desculpe todos os erros gramaticais e não responsacule os autores originais responsáveis por estes erros.

INTRODUÇÃO

Investigação sobre monitorização electrónica e preocupações de privacidade

Monitorização de preocupações acrescidas sobre a privacidade dos colaboradores; por conseguinte, os empregadores devem encontrar um equilíbrio entre os ganhos de monitorização e os custos de invasão da privacidade dos trabalhadores (Jackson, Schuler, & Werner, 2009). No entanto, o uso de tecnologias emergentes na monitorização das práticas dos colaboradores está a suscitar preocupações de que os direitos de privacidade dos colaboradores sejam vulneráveis, e está a tornar-se cada vez mais desafiante equilibrar os direitos de segurança do empregador com questões de privacidade dos empregados (Mathis & Jackson, 2000). Consequentemente, estão a ser debatidas questões de privacidade significativas nas empresas e no

governo, por exemplo, (a) violação da privacidade: examinar e recuperar e-mails privados, registos e informações sobre funcionários a partir do seu acesso a determinados websites da Internet; b Controlo informático: saber continuamente onde está o trabalhador; c Correspondência informática: informações sintetizadas obtidas de diferentes fontes para melhorar os seus serviços de marketing; e (d) ficheiros de pessoal não autorizados: recolha de números de telefone, endereços de e-mail, números de cartões de crédito e outras informações privadas para desenvolver perfis de clientes (O'Brien & Marakas, 2006). Os avanços tecnológicos permitiram que os empregadores aumentassem a produtividade dos colaboradores e colocassem a privacidade dos colaboradores sob cerco. Robbins e Coulter (1999) apresentaram algumas questões perplexas, tais como:

1. O sistema de e-mail é apenas para fins comerciais?
2. Um empregado pode enviar informações de trabalho por e-mail a um colega, juntamente com algumas conversas pessoais?
3. Qual é a utilização aceitável do sistema?
4. Quem possui a informação que é produzida a partir da rede?

As organizações regulam o uso da Internet, ou visitas ao site pela sua força de trabalho, através de duas formas regulares: restringindo o acesso a determinados links, e monitorizando as ações dos colaboradores (Alampay & Hechanova, 2010). Neste estudo, é também revelado que as políticas de monitorização e controlo dos websites variam de um país para outro; por exemplo, a China, o Vietname e Singapura não só bloqueiam determinados sítios, mas também proscrevem o acesso a assuntos políticos e linguísticos. Everett, Wong e Paynter (2006) consideraram que um número significativo de sujeitos relacionados com os direitos dos trabalhadores e dos empregadores deve ser tomado em consideração em estudos posteriores: a Uma questão significativa está relacionada com a construção da confiança entre empregadores e trabalhadores no local de trabalho; outro tema vital está relacionado com o estabelecimento de legislação pertinente que gere as questões de privacidade na vigilância do local de trabalho de forma direta; b Um fator espinhoso é a ocorrência crescente de satélites, instalações comunitárias e trabalho em casa, que instam os empregadores a controlar os seus empregados; c A diversificação e as capacidades da Internet para a comunicação fornecem novos tópicos para a investigação; d A possibilidade de proscrever todos os pequenos dispositivos eletrónicos no local de trabalho que possam ser utilizados para os segredos das empresas de correio eletrónico a um beneficiário externo; e alargar a comparação internacional e sondar a posição crescente das normas internacionais e dos "acordos de harmonização", relativamente às políticas desenvolvidas pela União Europeia e pelas Nações Unidas, bem como às normas propagadas pela Organização Internacional para a Normalização, pelas agências nacionais de defesa e pelos ramos governamentais de investigação criminal.

Everett et al. (2006) referiu-se a determinadas questões que podem levar a uma maior utilização do empregador da perceção de que esse controlo é necessário. Por exemplo, os esforços do governo para esmagar o terrorismo, aliviar a proliferação do conhecimento das armas nucleares, dificultar o branqueamento de capitais e limitar os traficantes de droga, tanto ilegais como farmacêuticos. Mais recentemente, os empregadores começaram a rastrear os seus empregados utilizando a tecnologia global de sistema de posicionamento (GPS), que utiliza uma montagem de satélites para especificar a localização exata do dispositivo ativado por GPS. Por isso, a Townsm e a Cobb (2012) recomendaram medidas realistas ao aplicar o rastreio de GPS da seguinte forma: incorporar o rastreio de GPS com outras políticas; preservar o direito de controlo; não criar provas conclusivas com documentos de rastreio gps; limitar a utilização da tecnologia GPS para monitorizar; Delinear rigorosamente a utilização adequada dos telemóveis, dos veículos da empresa, assim por diante; desenvolver uma linguagem de consentimento; verifique continuamente o equipamento GPS; e considerar a salvaguarda de registos.

Um outro estudo da Ciocchetti (2011) classificou cada uma das principais práticas de monitorização num dos seguintes tipos: a As melhores práticas (por exemplo,) monitorização que apresenta a maior proteção e minimiza a invasão da privacidade dos funcionários), (b) práticas de risco (por exemplo, monitorização que oferece uma proteção bastante baixa e que ataca minimamente a privacidade dos funcionários), (c) práticas de fronteira (por exemplo, monitorização que proporciona alta proteção, mas também é altamente insidiosa) , e (d) más práticas (por exemplo, monitorização que proporciona baixa

proteção e é extremamente invasiva). Este sistema de classificação é suscetível de ajudar os legisladores a equilibrar os interesses dos empregadores e dos trabalhadores na legalização da tecnologia no local de trabalho. Ciocchetti considerou que o sistema jurídico americano tem sido lento a reagir de forma eficaz e eficaz à crescente invasividade da tecnologia moderna de monitorização e que todas as práticas de monitorização são perturbadoras e enquadram-se nas quatro categorias acabadas de ser mencionadas. No entanto, Bennett e Locke (1998) declararam que uma forma eficaz de evitar a responsabilidade por agressão de privacidade é pressupor que se um empregado pode litigar por tal delito, o empregado irá.

A investigação demonstrou que os colaboradores podem encontrar uma fonte inclusiva de proteção da privacidade resultante do direito comum à privacidade, que consiste em três erros relevantes para a relação de trabalho: a intrusão no isolamento, que surge de uma invasão, é uma intrusão na propriedade de outra pessoa sem a permissão dessa pessoa; publicidade dada à vida privada, que existe quando um indivíduo dá publicidade a uma questão sobre a vida privada de outro; e publicidade colocando uma pessoa em falsa luz, o que ocorre quando um indivíduo ignora sem atenção a falsidade da questão revelada e a falsa luz em que a outra pessoa seria colocada (Hames & Diersen, 1991). Em alternativa, um conjunto de reformas desenvolvidas pela Conlon (1997) protegem as preocupações individuais de privacidade no local de trabalho:

- Não deve ser feita qualquer monitorização nas casas de banho, balneários e salas de estar dos funcionários; no entanto, o tempo passado fora do local de trabalho pode ser monitorizado de formas menos odiosas.
- O controlo fora do local deve ser proibido; Permitir que os colaboradores acedam a todas as informações recolhidas através de métodos ou técnicas de monitorização e considerem a sua reflexão sobre essas informações; e limitar a duração da monitorização diária com uma sugestão (máximo de 2 horas por dia).
- Os colaboradores devem estar atentos aos dispositivos que serão utilizados para os monitorizar, como os dados serão utilizados e quando serão monitorizados exatamente; e os colaboradores e clientes devem ser notificados quando a monitorização telefônica está a ocorrer através da utilização de um tom específico que pode ser ouvido tanto pelo empregado como pelo cliente.
- Os empregadores só devem recolher informações relevantes para tomar decisões críticas; e não basta justificar o acompanhamento pela necessidade de aumentar a produtividade ou melhorar o desempenho, mas também, os empregadores devem ser capazes de demonstrar como o objetivo foi alcançado através do processo de monitorização.

Seja como for, a base legal do direito à privacidade tem um fundamento teórico para intelectuais legais que podem ser complexos para o público reconhecer ou valorizar (C. L. Swanson, 1988). Apesar das diferentes escolas de pensamento entre os académicos, foram apresentadas inúmeras propostas para a contemplação da gestão: formular porquê, como e quando é aplicada a monitorização electrónica; recolher apenas informações relacionadas com o trabalho; recolher apenas informações com o objetivo de aumentar o desempenho dos colaboradores; fornecer feedback oportuno aos colaboradores para que possam ser feitas ações corretivas ao desempenho; garantir prémios a indivíduos ou desempenho em grupo; educar os colaboradores sobre as características comportamentais e sociais da monitorização electrónica; acentuar as características qualitativas do desempenho não contabilizadas pela monitorização electrónica; Deve ser previsto um período experimental para todos os novos candidatos ou novos sistemas eletrónicos; Evitar ser demasiado rápido no desenvolvimento de novas normas ou métodos de controlo, a menos que se prove que é eficaz; e use sessões de brainstorming sempre que possível para melhorar o sistema de monitorização electrónica na organização (Vaught, Taylor, & Vaught, 2000). No entanto, demasiada monitorização e publicidade de uma cultura de monitorização em toda a organização podem criar problemas emocionais e comportamentais que podem, em última análise, empurrar os colaboradores para certas atividades para enganar o sistema (Barrett, 2008).

Intrigantemente, Dillon e Thomas (2006) expuseram que existe uma grande necessidade de consciência universal e indulgência de questões de acessibilidade, uso pessoal e supervisão administrativa envolvendo e-mails e computadores no local de trabalho; caso contrário, é pouco provável que os colaboradores compreendam adequadamente as políticas e procedimentos de privacidade. Wen, Schwieger e Gershuny

(2007) analisaram as tecnologias de vigilância e discutiram as leis federais e estatais relacionadas, juntamente com as decisões judiciais dos EUA, e consideraram que nenhuma lei federal ou estatal dos EUA proíbe os empregadores de monitorizarem o seu local de trabalho eletrónico. A sua investigação científica forneceu igualmente as seguintes estratégias suscetíveis de serem mais eficazes e produtivas tanto para os empregadores como para os empregadores, e ajudar os empregadores a prevenir os aspetos negativos do controlo: a designação da supervisão e execução da política de privacidade deve ser implementada por uma autoridade; considerar um ponto de vista jurídico para orientar juridicamente o desenvolvimento de todas as políticas e procedimentos; desenvolver uma política formal e manter todos os colaboradores informados de todas as alterações à política; Notificar os trabalhadores do sistema de monitorização electrónica; evitar um ambiente de trabalho agressivo; desenvolver regras claras sobre a utilização de e-mails; decidir quais os dados que devem e não devem ser acedidos; especificar os prazos em linha; manter um software em execução em segundo plano de cada computador, como bloqueadores de pop-up ou filtros de spam; e comunicar uma política que é aceitável para mensagens instantâneas, blogs e chat room usar dentro e fora da organização.

Haller (2002) propôs igualmente os principais ingredientes de políticas de privacidade eficazes: a Aviso, as empresas devem fornecer às partes interessadas um aviso proeminente em relação às suas práticas de informação; b Escolha do consumidor, as empresas devem dar às partes interessadas a liberdade de escolher se podem divulgar dados pessoais sobre eles a terceiros não filiados; c Acesso e correção, as empresas devem aceitar que as suas partes interessadas escamem, se necessário, com algumas correções sobre os dados pessoais que recolheram sobre os mesmos; d Segurança, as empresas devem espoar medidas práticas de segurança para proteger a privacidade das informações pessoais, e essas medidas podem incluir segurança administrativa, física e técnica; e a aplicação da lei, as empresas devem desenvolver um sistema que possa impor a sua política de privacidade e garantir o cumprimento das suas normas próprias e externas. Além disso, mantendo um equilíbrio entre a propensão dos empregadores à produtividade e o cumprimento dos procedimentos legislativos, as empresas podem ter mais sucesso na prática do seguinte: criar limites de privacidade inequívocos, desenvolver fórmulas e princípios de privacidade, e defender dados pessoais (Townsend & Bennett, 2003).

Os empregadores são menos vulneráveis em relação a determinadas questões de invasão de privacidade, se as políticas escritas forem comunicadas eficazmente; no entanto, Kovach, Jordan, Tansey e Framinan (2000) argumentaram que demasiada monitorização gera um local de trabalho cheio de impasse, culpa, cinismo e desconfiança. Na prática, para contornar as violações da privacidade dos trabalhadores no local de trabalho, os empregadores nunca devem promover uma cultura de privacidade dentro de cada trimestre de uma organização, porque pode ser essencial monitorizar algumas práticas quando ocorrem questões (Guffey & West, 1996). Um empregador ético acompanhará o trabalho dos trabalhadores dentro das disposições de uma determinada política (Cowan, 2008). As empresas devem inscrever-se se estiverem a lidar com informações pessoais para qualquer um dos seguintes fins: investigação privada, administração de saúde, prevenção de crimes e julgamento de delinquentes, serviços jurídicos, administração de dívidas, comércio, casos públicos, educação, investigação, administração de justiça, serviços de consultoria ou um sistema de reporte de crédito (Grupe, Kuechler, & Sweeney, 2002).

Resumidamente, Zachary (2013) reconheceu o seguinte: A invasão do local de trabalho à privacidade é de enorme preocupação tanto para os empregadores como para os empregados nos Estados Unidos, e a violação da privacidade foi aumentada nos processos de emprego. A invasão da privacidade pode recair em quatro categorias: a Fugas de informação que denegre outras pessoas, (b) utilizando o nome de outra pessoa sem consentimento, (c) comunicação inadequada de dados privados, e (d) quando um agressor intromete-se propositadamente, fisicamente, eletronicamente, ou de outra forma, no espaço privado de outros. Os tribunais variam de acordo com o momento em que a intrusão ilegal existe, e os empregadores devem estar extremamente atentos a tipos diferentes de invasão de privacidade. Notavelmente, as disputas pelos direitos de privacidade nos Estados Unidos, que alguns vêem como uma ameaça à erosão dos valores primários americanos, tiveram um aumento de controvérsia sobre o grau de redução dos direitos anteriormente intocáveis devido à relação empregador-empregado (Anton & Ward, 1998). Na secção seguinte, o autor apresenta possíveis alternativas à monitorização electrónica do desempenho (EPM).

CONCLUSÃO

Através da monitorização, os empregadores argumentam frequentemente que são capazes de proteger as suas organizações de qualquer dano. Neste sentido, a monitorização é entendida como uma ferramenta para manter a segurança de uma organização. As novas tecnologias não só ofereceram às organizações razões para monitorizar o comportamento dos colaboradores, como também forneceram novos métodos e técnicas para realizar a monitorização dos colaboradores. Assim, a tecnologia deve ser tratada com cautela e discrição. Os empregadores devem perceber que os trabalhadores podem retaliar contra a organização pelas práticas de monitorização desleais percebidas. Por isso, é essencial que a aplicação de novas tecnologias monitorize o comportamento dos colaboradores tenha em conta muitas preocupações (por exemplo, privacidade, necessidades e aspirações). Educar os colaboradores sobre as razões subjacentes à sua monitorização, desenvolver um vasto leque de políticas e procedimentos e comunicá-los eficazmente será vital para implementar com sucesso um sistema de monitorização.

A incapacidade dos empregadores em reconhecer os direitos dos trabalhadores pode causar perdas avultadas, tais como processos dispendiosos, danos à reputação da organização e deterioração dos valores dos trabalhadores. Por conseguinte, os empregadores devem equilibrar a necessidade de produtividade no que respeita aos direitos dos trabalhadores à privacidade, segurança e segurança. Concentrar-se nas realizações e não no tempo gasto no local de trabalho deve ser a principal preocupação para qualquer empregador. Por outras palavras, não há necessidade de policiar uma força de trabalho porque ninguém pode trabalhar 8 horas sem pausas, e uma cultura de deslealdade e desconfiança dentro da organização pode emergir. No entanto, os colaboradores devem estar cientes de que existem inúmeros pacotes de software que podem fazer o registo de tudo o que escrevem, pesquisam e lêem nos seus computadores.

Este estudo oferece muitas alternativas ao EPM que são suscetíveis de satisfazer os objetivos de um empregador sem violar os direitos de privacidade. Outra questão significativa levantada neste estudo é que o estilo de liderança mais eficaz para monitorizar o desempenho e o comportamento dos colaboradores através da tecnologia permanece não identificado. Do ponto de vista do autor, não há necessidade de definir o que é um comportamento moral em organizações maduras e saudáveis, mas é crucial esclarecer como usar tecnologias sem violar protocolos éticos. A tecnologia é uma ferramenta que pode ser usada eticamente e de forma não ética. Depois de analisar um grande número de estudos sobre a perceção dos colaboradores da monitorização electrónica, o autor descobriu que o uso do EPM criou uma grande tensão e pressão entre indivíduos nas organizações. Por isso, o autor argumentou que o nível de satisfação, motivação, compromisso, lealdade e integridade do trabalhador no local de trabalho pode ser afetado em resultado de níveis extremos de stress. Assim, educar os colaboradores sobre o sistema de monitorização e estabelecer critérios de desempenho justos, justiça distributiva, justiça processual e justiça interativa pode tornar o acompanhamento menos angustiante. É importante que o controlo seja coerente com os objetivos globais da organização e com os dilemas de desempenho; no entanto, as políticas dos empregadores não devem criar stress e desconfiança sobre os seus empregados. Para além disso, o autor deste estudo argumentou que os esforços da HRD podem ser significativos na monitorização do comportamento e do desempenho dos colaboradores nas organizações. A lógica por trás desta escola de pensamento é que o campo de HRD enfatiza elementos cruciais de questões comportamentais e de desenvolvimento nas organizações.