Electronic surveillance in workplaces and their legitimate usage to provide transparency and accountability towards employees

[1]Gursimran Singh, [2]Dr. Payal Bassi
[1]Research Scholar, [2]Professor,
[1] Department of Commerce and Management
[1]Regional Institute of Management and Technology, Mandi Gobindgarh, India

Abstract: Companies used surveillance software's, CCTV cameras to watch their employees, monitoring their e-mails or the websites content they visit. Sometimes managers used surveillance to provide protection of their companies from legal acquaintances that originates against the wrong doing behavior of their employees such as download of pornography material and provoke able e-mails or messages to other individuals and to provide protection against the inappropriate exposure of exclusive or confidential information on the internet. As the reasons of employers behind these processes can be valid, there are conflicting thoughts of the usage of this technology among the employees. This paper discusses the latest surveillance measures, technologies used by the employer, lawful disputes that can arise from surveillance as well as consequences or problems originate for the management. This paper also discusses some questions about the right of usage of internet or e-mails in the corporations for the personnel motives of the employees and to what extent their can use their right. To what extent the managers or companies lawfully monitor the workplaces or employees behavior on the internet. And about the employees expectations regarding the surveillance used in order to protect their online privacy and the legal options company have provided for them. The paper expresses the ways for further research in surveillance of employees and a more detailed reasoning in improving lawful and policy-making can be analyzed further.

Index Terms **- Electronic surveillance; technology, Accessing Internet, privacy, monitoring etc.**

I. INTRODUCTION

1.1 Ethical culture and employee surveillance

Ethical culture and employee surveillance can be considered two different organizational solutions to employee norm violations. Ethical culture, defined by [1] as "the informal control system of an organization which encompasses the experiences, assumptions, and expectations of managers and employees about how the organization prevents them from behaving unethically and encourages them to behave ethically" can be considered a 'soft control' system. That is, ethical culture influences behaviors indirectly through its focus on shared organizational attitudes and norms vis-àvis workplace delinquency. Ethical culture has been found to be an important predictor of unethical behavior [2]. That is, organizations with high levels of corporate ethical virtues are less likely to have employees who behave unethically. The relation between ethical culture and unethical behaviors seems to be stronger than the more often researched relation between aspects of ethical climate [3] and dysfunctional or unethical behaviors [4] for meta-analytic reviews.

Employee surveillance can be defined as the formal control system of an organization,which encompasses the checks andmonitoring practices through which an organization attempts to prevent employees from behaving unethically. In contrast to ethical culture, employee surveillance can be considered a 'hard control' system. That is, instead of goading employees into behaving ethically through its culture, organizations using employee surveillance enforce ethical behaviors by actively monitoring deviations from organizational norms. Much less research attention has been paid to the formal (employee surveillance) control system than to the informal (ethical culture) control system. According to the Routine Activity Theory [5], lack of surveillance (or: guardianship) is one of the three factors, togetherwith motivated offenders and suitable targets, that account for the occurrence of crime. When there is surveillance, opportunities for (workplace) delinquency are curtailed. According to this perspective, opportunity makes the thief. For example, retail stores with more sophisticated surveillance systems have been found to report lower levels of theft, both by employees and shoplifters [6]. And in industries in which employees work in jobs with less strictly controlled access to goods and money, higher levels of theft have been reported than in industries in which this access is relatively restricted [7]. Based on the findings on ethical culture and employee surveillance, we expect both to be negatively related to workplace delinquency.

II. Monitoring of employees' use of the Internet by employers

If an employee's right to personal use of the Internet in the workplace is ruled out, can employers legitimately monitor the Internet behavior of employees and, if they can, to what extent, under what conditions, and with what effects? Personal use of the Internet by employees can be forbidden, regulated, or implicitly tolerated. If personal use is regulated, the employer's electronic privacy policy should clarify the related methods, conditions and limits. If there is no privacy policy, it is true that the employees do not have a right to personal use of the Internet, but conversely the employer cannot indiscriminately monitor their activities on the Net. Moreover, the employer's monitoring is twofold. On one side, employers check the utilization of the company tools, not

only internally to control the fulfillment of contractual obligations, but also externally to avoid liabilities. On the other side, employers monitor employees' use of working time. The two profiles normally overlap within one surveillance activity, but they can be separated: i.e. employees do use company property (apparatus, vehicles) outside of the normal work hours; the employees browse the Internet or send email during the working hours, but using their instruments. In these cases, the monitoring differs, under both a legal point and a technical point. Without an electronic privacy policy, the use of company instruments does not make it legitimate for the employer to monitor the Internet behaviour of the employees, but it does make the monitoring technically easy. The use by employees of their own apparatus makes the monitoring technically harder, and, at the same time, the legal framework changes. The analogy with the use of personal mobile phones for telephone calls during the working hours is substantial: wiretapping would be illegal even if included in the electronic privacy policy. The employer can object to the misuse of the working time, implicit in the extended use of a personal phone, or laptop, during the working hours: the contents of the communication are irrelevant.

The enactment of an electronic privacy policy by the employer is the key. The privacy policy is an essential requirement, a precondition, for the employer to set up a monitoring system. National legal systems, and in particular labour law, provide the employees with further rights, guarantees and protection, as Internet monitoring is strictly intertwined with issues concerning the 'distance' monitoring of the employees. While the national systems differ, as for procedures, level of protection, role of the trade unions, there is a common ground based on the principle of transparency, which is not only a specific data protection principle, but also a legal general principle and, in the end, a moral principle, as it is about correctness and fairness. Data protection directives, and their interpretation by the DPWP, offer principles, criteria and guidelines to be embedded in the labour law regulations, and co-ordinated with the specific procedures set up by the national legislations.

Lacking an electronic privacy policy (or a different, equivalent document), employees have a reasonable expectation of privacy. If the employer has not expressly stated that Internet and email surveillance is possible, the employee can legitimately assume that no monitoring will take place. On the contrary, if the electronic privacy policy has been adopted and made public, according to national rules and procedures, the employer can monitor employees' online activities. Therefore, the electronic privacy policy is neither a 'duty', nor an 'obligation', but a 'burden', a precondition for making the monitoring licit.

2.1 Surveillance technology

Surveillance software can track employees' Internet movements and prepare reports to management. As employees surf and browse the Web, those movements are actively monitored and reports generated, including real-time, online notification to the administrator of selected 'hits'. The technology is capable of taking a picture of an employee's computer screen at periodic intervals, enabling the employer to see the sites employees are visiting or the messages they are emailing. Surveillance technologies can screen employees' email for potentially offensive or inappropriate messages by scanning for questionable keywords pre-determined by the employer. For example, an employer concerned with the theft of its trade secrets can list the names of its primary competitors as keywords. The surveillance system can also automatically email 'flagged' messages to the employer. The capabilities of surveillance technology are described in Table 1 [8] Electronic surveillance supported by increasingly sophisticated technology is here to stay, and it is a powerful tool for employers. However, how to use this tool to monitor employees' Internet access in the workplace most effectively is an open question. In the following section, the strengths of the arguments for and against electronic surveillance are discussed, in order to elucidate answers.

2.2 The arguments

Employers justify electronic surveillance of employee Internet access as promoting sound business interests [8]. Yet the practice also raises concerns from all areas of society – business organizations, employee interest groups, privacy advocates, civil

Table 1: Type of surveillances and its application

Surveillance capability	Description
Keystroke monitoring	• Maintains a record of keystrokes along with the window they are typed in and time stamp. • Tracks computer idle time. • Recreates 'deleted' documents because the keystrokes are logged and stored even if deleted.
Emails sent and received	• Monitors and logs all emails sent and received by users of all company owned computers. • Screens emails for potentially offensive or inappropriate messages. • Scans employee emails for questionable keywords pre-determined by the employer.
Events timeline logging	• Logs all events users performed and view them in an organized chronically ordered listing. • Views what the events the user performed, in the order they did them. • Logs program starts/stops, website visits, document viewings and printings.

Application usage	• Monitors and logs all applications run by users. • Logs when the application was started, stopped, and how long it was actually used. . Records application installations performed by users. • Logs software name, installation path, and time when installation is logged.
Window activity	• Records documents and files opened and viewed by users. • Logs all windows in which the user directly interacts on the desktop. • Monitors and logs all Internet sessions and all chat conversations made on the PC. . Records documents and files that are printed by users. . Logs all passwords used during monitoring sessions via its keystrokes recorder.
Remote desktop viewing	• Takes snapshots of every desktop at set intervals of time, allowing managers to visually see what is happening. • Views a listing of various system information for the remote PC, including processor type, system directory. • Views a list of the current Internet connections on the PC. • Views a list of the recent documents users have opened. • Remotely views what the user is doing in real time.

libertarians, lawyers, and professional ethicists. Each advocate advances economic, legal, and ethical rationales in support of their position. However, no argument is conclusive and each raises important managerial and moral issues.

2.3 Liability

The primary reason cited by employers for conducting electronic surveillance is to minimize legal liability arising from employee misconduct: harassing email and illegal downloading, for example [9] But surveillance is at best a two-edged sword in this regard. To the extent that surveillance and monitoring deter employee misconduct, employer liability is reduced. The same is true if surveillance accomplishes early detection and response, such that misconduct is identified and stopped before it becomes actionable. However, electronic surveillance also simply accumulates data. Many companies retain business records, including electronically stored information, for some period of time as dictated by law or in order to promote business management and planning purposes. Others automatically archive and retain data because they do not have a document retention and destruction policy in place [10] Extensive surveillance coupled with data retention increases the likelihood that evidence of employee wrongdoing via Internet access is in the company's custody or possession. If that evidence is discovered by an opposing party, the company has, because of its surveillance, increased the likelihood of being found liable for that misconduct.

2.4 Productivity

A second justification for surveillance of Internet access is to reduce non-business use of the Internet [11]. When employees surf the Internet and send personal email they are using company resources for unproductive purposes and reducing time spent doing the job, as the reasoning goes. Surveys indicate that personal or recreational Internet access is common. For example, a 2004 survey found that 85% of employees engaged in personal email while on the job [10] The Internet may have usurped gossiping in the coffee room or talking on the telephone as the leading employee diversion from work. However, there is no definite evidence that employee productivity, as a whole, has decreased because employees are forwarding email to colleagues instead of meeting them in the coffee room. Indeed, email could be quicker, reducing the amount of employee time spent on personal matters. If surveillance of employee Internet access deters personal use of the Internet – another unproven assumption – the result may be counterproductive. Employees who would book a flight on line have to leave the office to go to a travel agent. Even if surveillance deters employees' recreational use of the Internet, the fact of surveillance alone may otherwise adversely affect productivity. 'When workers begin to feel that their employer does not trust them, their mental well-being is harmfully impacted' [8] The exact effect of employee surveillance is uncertain because little research has been done on separating the effects of surveillance from job design, equipment design, lighting, machine pacing, and other potentially stressful aspects of a computer-based office worker. Early studies showed that working under surveillance provides a source of worry for workers. More recent studies indicate that employees feel electronic surveillance is beneficial, or at least necessary [12]. But an environment of surveillance may unknowingly curtail otherwise productive activity, as employees act and then think in response to the unseen observer. New, radical, unconventional ideas may be filtered out of communications if the employee is constantly worried what the observer may think. But corporations rely upon creative, new thinking in order to constantly move forward and improve. In fact, most companies work hard to form innovative and open teams to foster creative employees and improved products and services. Innovation comes only from creativity and, it is argued, is in jeopardy when that creativity is stifled with even the threat of surveillance.

A separate but related issue arises from the fact that employers must devote resources to managing the surveillance itself. As surveillance technologies become increasingly complex, even more resources must be devoted to interpreting the data that is collected [13] The extent to which employee Internet access should be monitored in order to increase productivity should be determined to some extent by the true costs of conducting and responding appropriately to that surveillance.

2.5 Security

With a greater reliance on computer systems, information assets are seen as a vulnerable point of attack by would-be saboteurs. Corporations that do not adequately secure their systems risk unwanted dissemination, retrieval, or modification of private corporate information. Proponents argue that monitoring employees protects the safety and security of the organization and even the nation. In addition, disloyal employees are able to email trade secrets and confidential documents quickly and easily to a large audience. In fact, most security breaches come from knowledgeable insiders – not random hackers from the outside [14]. By monitoring Internet usage and content, corporations argue that they are able to detect and halt security breaches. Securing confidential and proprietary information from unauthorized access from outside, and prohibiting unauthorized and illegal disclosure by employees is inarguably a legitimate objective. Whether or not surveillance of employee Internet usage accomplishes these objectives is unclear. Certainly a company would have to update its surveillance technology in order successfully to combat a hacker or disloyal employee using the most sophisticated detection-avoidance software.

2.6 Ethical issues and fairness

Electronic surveillance offers a distinct advantage to the employee: it is objective. This is a benefit because it provides an unbiased method of monitoring employee Internet access; managers are not picking and choosing which employees to monitor. Electronic surveillance may be objective and unbiased, but it also invades employees' privacy. To what extent employees have a right to privacy in the workplace is a matter of considerable debate [15] [16]. However, most commentators would agree on certain parameters. Employers are entitled to conduct electronic surveillance of employees in order to meet the legitimate objectives discussed above [16] But if the employer's surveillance practices are seen as unduly intrusive [12] excessively controlling [12] or employed for no legitimate business objective [16] those practices may be viewed as unethical. The practical effect of surveillance practices viewed as unfair may be a loss of productivity or employee resignations.

III. CCTV in surveillance

From a general perspective, the topic of surveillance in the workplace has been debated since the early 1980s. Since then, academics in organizational behavior disciplines, organizational sociologists and occupational psychologists have investigated the effects of monitoring and surveillance but tend to write about the phenomena in different ways in their respective publication venues [17]. However, the approach taken in this article is essentially based on criminological and legalistic perspectives, although some managerial and ethical considerations are also made. Certainly, the complexity of the real issue calls for an interdisciplinary and integrated approach, but, in getting closer to the issue, one or another focus should be taken as predominant. Therefore, the intended approach seeks to find a balanced and practical analysis by merging overall legal (normative) and criminological (empirical) considerations.

Looking back at the recent changes in the field, the diffusion of CCTV in society and particularly in the workplace has increased dramatically [18] CCTV has become a major weapon and common prevention strategy in the fight against crime and its use appears to be expanding [19]. However, from a critical perspective, it could be argued that the use of CCTV in the workplace is not so much about deterring crime as it is about enhancing control over workers and increasing organizational efficiency and productivity. In fact, although the growth of CCTV surveillance in the private sector can largely be accounted for by the increased recognition of the impact of business victimization (e.g. internal and external threats), CCTV use unexpectedly proved to be more valuable in checking whether staff were meeting company requirements (e.g. compliance with till procedures; [18]

In the workplace context, CCTV provides useful tools for a series of legitimate purposes, such as the monitoring of employees' productivity, the maximization of the productive use of apparatus, the investigation of complaints of employees' misconduct or the preparation of the employer's defense in lawsuits or administrative complaints such as those brought by employees related to discrimination, harassment, discipline or termination of employment [20]. However, this paper only addresses a special case among a vast range of monitoring goals, that is, the use of covert CCTV based on a crime occurrence, and it is based on the crucial distinction between ordinary and exceptional monitoring cases.

In terms of privacy concerns, as Kristie Ball has synthesized, in recent years a combination of available technologies and a management culture that emphasizes individual measurement and management has resulted in an extension and intensification of individual monitoring. The implication is that surveillance at work is, first, a necessity, and second, a normal, taken-for-granted element of working life. Among the various monitoring practices, which may focus on measuring employees' performance, their behavior or their personal characteristics, surveillance in the workplace is developing in three directions the increased use of personal data, biometrics and of covert surveillance [17].

[21] have analyzed from a comparative perspective privacy case law and surveillance practices and perceptions relating to CCTV in the workplace in 11 countries, but they did not focus specifically on covert surveillance, despite the fact that it is not an infrequent practice as the number of cases analyzed in the present paper reveals.

Regarding the interest of the research topic, it is worth noting that much of the recent literature on surveillance in the workplace focuses on improving worker performance and electronic monitoring, rather than on crime prevention or reaction and CCTV systems. Looking to fill this gap, it is important to remark to exclude from focus what is probably the primary aim in using CCTV, namely, that businesses are keen to maintain productivity. In doing so, assuming that covert CCTV follows a rationale completely different from what we refer to as ''ordinary monitoring''. As by examining, only in ''exceptional monitoring'' cases, within which covert surveillance fits, can companies not inform workers of the extent to which they are being watched. Because of that exceptional nature, covert CCTV systems are rarely justified. On the contrary, ordinary monitoring focused on labor performance has to be transparent and, based on its transparency, allows a much greater extent of pervasiveness.Moreover, as one important practical insight, in recognizing important changes in surveillance practices, law and crime prevention, it is analyzed

how the use of CCTV surveillance systems in the workplace means that issues relating to trust, transparency and proportionality need to be revisited. For the purposes of this of surveillance of employees, three previous clarifications are needed in relation to three main concepts, i.e. ‘‘CCTV’’, ‘‘crime prevention and crime reaction’’, and the ‘‘workplace’’.

3.1 Concept of CCTV

In line with the UK doctrine [22]; [23] it has opted to use the term ‘‘CCTV’’ as generic term to cover any video-surveillance system irrespective of the technology used, that is, whether it is a closed television system relying on analogue technology or a network IP video system that runs on a local area network. Nevertheless, it is important to stress the fact that CCTV systems may differ considerably in their technological components and capabilities, and such differences have important implications, especially on legal and ethical grounds [24]; [23].

3.2 CCTV as crime prevention and crime reaction tool

In controlling crime, CCTV may help to prevent potential offenses and may also help in the reaction to actual crimes once they have occurred, in order to provide evidence. From situational crime prevention strategies, CCTV allegedly demotivates potential offenders, who seek to target a place without any kind of surveillance. Within such logic, ‘‘opportunity makes the thief’’ [25] However, a given situation only creates an opportunity for crime if there is a lack of capable guardians or managers around. Thus, lacking other human resources, cameras may foster rational choice considerations by increasing perceptions of the probabilities of being caught [26]. Nevertheless, implementing CCTV systems is only one measure within a vast range of alternatives in preventing crime, and their effectiveness is not clear among scholars. CCTV works best in small, well-defined sites, and in combating property crimes rather than violence or disorder [27] All in all, for some scholars the small number of evaluations can be a limiting Innovation: The European Journal factor in arriving at conclusions about an intervention’s effectiveness, as well as being able to generalize results [28]

On the other hand, CCTV may be an effective tool in reacting to crime that has occurred within a company in order to detect the wrongdoers and eradicate the problem if it persists. In fact, prevention and reaction may be seen as a continuum and, hence, by having the power to react, a preventative function becomes more effective. However, crime reaction operates upon a given fact, while prevention operates only upon suspicion. As we will see, such a difference becomes relevant in terms of legitimating privacy limitations.

Based on prevention and reaction differences, the present paper is not going to analyze CCTV as a crime prevention tool in the workplace. Neither is it going to deal with a general approach to employee crime prevention strategies or the CCTV’s alleged effectiveness. Certainly, in the framework of employee or corporate crime and in organizational settings, there are some duties of surveillance and control by the employer that may trigger different kinds and degrees of liability for those crimes committed by others within the organization [29] Such duties and responsibilities are much more related to general preventative surveillance measures. In contrast, we will analyze the use of hidden cameras upon the understanding that it is an exceptional form of monitoring and it is only legitimate when addressed under certain and restrictive circumstances (i) to protect corporate interests from employees’ wrongdoings and (ii) to protect the company from legal liabilities.

3.3 Extended concept of workplace

An important point related to CCTV in operation at a workplace is the concept of ‘‘workplace’’ itself. In this regard, as our concern focuses on crime reaction in the workplace, both internal and external threats should be included within the ‘‘workplace’’, as they both may lead to damage to company assets. Such kinds of crime may occur at different places depending on the type of services a company is providing. Moreover, given the technological revolution and its implications for labor relationships, the traditional physical boundaries are no longer the limits of many workplaces. The head-cams worn by police officers or CCTV systems in operation on buses may be examples of CCTV uses that should not be excluded from our concerns. However, some places within the physical boundaries of the workplace, inasmuch as they can affect intimacy expectations, will exceed boundaries for covert cameras’ purposes (e.g. changing rooms or toilets).

IV. Existed work in digital surveilance

In 2000, Jeffrey M. Stanton et al demonstrate a strategy for understanding workers’ fairness reactions to performance monitoring. They collected data on whether traditional or electronic monitoring techniques were used, workers’ reports about how these techniques were deployed, and workers’ feelings about the fairness about their work situation. Regression analyses showed two general results. First, after controlling for organization, job type, and the EPM techniques in use, monitoring consistency, knowledge of performance from monitoring, control over the time and place of monitoring, and justifications for monitoring all predicted at least one of the three fairness outcomes. Second, organizations and job types differ on the levels of these predictors, and two of the predictors, control over the time and place of monitoring and justifications for monitoring, covary with the particular EPM techniques in use [30]. Then in 2005, Filiz Tabak et al explored the relationship between employee privacy rights, development of trust between management and employees, and electronic monitoring in the workplace. A framework was forwarded in which both the managers’ and the employees’ experiences at the current and past organizations as well as their disposition to trust as a personality factor were argued to impact how they make sense out of the current organizational environment and how this sense-making process leads to categorizing one another as either trustworthy or non-trustworthy. Such cognitive framing was presented as an antecedent to organizational and individual outcomes of implementation of electronic monitoring and employee turnover and commitment. Secret electronic monitoring may lead to perceptions of the procedure being unfair and of management as non-trustworthy. In addition, they proposed a positive relationship between individual disposition to trust and cognitive categorization of employees and management as trustworthy. Trustworthiness was discussed as the label of a group of traits that subsequently leads to lower levels of turnover, increased organizational commitment, and lower levels of

electronic monitoring [31]. Afterthat, Yael Brender-Ilan et al explored differences in the perceptions of fairness between two employee evaluation methods: one based on data collected using the mystery customer method and the other based on supervisor judgment. Fifty eight female sales clerks filled out a questionnaire which assessed their perceptions with respect to the fairness of the two evaluation methods and their job satisfaction. Given apparent differences in the evaluating agent, the extent of process consistency, the breadth of behaviors evaluated, and the extent of employees' awareness of the evaluation process, they hypothesize and find that evaluation procedures conducted by supervisors are perceived as more fair both procedurally and distributively than those conducted by means of the mystery customer method. The expected relationship between perception of fairness and job satisfaction was, however, found only in the correlations with supervisor evaluations and not in the correlations with the mystery customer evaluation method [32]. Moreover in 2007, Cynthia F. Cohen et al examined the changing legal landscape of the right of the employer to control and monitor employee behavior. Two distinct areas are defined: behavioral monitoring and behavioral restrictions. Relevant statutory laws and the developing common law are discussed. They also examine potential employee reactions to such policies by evaluating the reactions of graduate students to six employer policies including weight restrictions, grooming requirements, use of GPS locators, drug testing, ban on off-duty smoking, and email and internet monitoring. Students responded to these policies by determining the reasonable interest of the employer in the behaviors being monitored or controlled and the manner in which policies were implemented [33]. Furthermore, H. Joseph Wen et al reviewed surveillance technologies and discuss the related federal and state laws along with U.S. judicial decisions. Implementation strategies to help employers defuse or avoid the negative aspects of monitoring are provided [34]. Then in 2008, G. Stoney Alder et al demonstrated that employee reactions to monitoring systems depend on both the characteristics of the monitoring system and how it is implemented. However, little is known about the role individual differences may play in this process. This study proposes that individuals have generalized attitudes toward organizational control and monitoring activities. They examined this argument by assessing the relationship between employee's baseline attitudes toward a set of monitoring and control techniques that span the employment relationship [35]. And in 2010, Marian K. Riedy et al reviewed surveillance technologies, discusses arguments for utilizing electronic surveillance, and concludes with legal issues arising from surveillance and implications for management [36]. Then in 2011, Laurel A. McNall et al employed a 2 (purpose) × 2 (control) factorial design using 208 college students. Study hypotheses were tested using hierarchical regression. They explored reactions to location sensing technologies (LSTs) which enable organizations to track the location and movements of employees, even off-site. In particular, they examined the relationships among two monitoring characteristics (i.e., purpose and control), perceptions of privacy invasion, and monitoring fairness [37]. In 2014, Bernadine Van Gramberg et al presented the misuse of electronic communication in the workplace through the international literature and also recent court and tribunal cases in Australia. In particular, they consider the impact of new communication technologies in blurring of the boundaries between home and work and the way in which this is being dealt with by HR managers. They draw out the challenge of balancing the interests of employees and organisations, and outline the tension between HR as a strategic partner and employee champion [38]. Afterthat in 2015, Reinout E. de Vries et al provides evidence for the importance of Honesty–Humility, Conscientiousness, ethical culture, and employee surveillance in the prediction of workplace delinquency. Especially in companies in which workplace delinquency carries large costs, employers may be advised to select on Honesty–Humility and Conscientiousness, to create an ethical culture which is clear, congruent, and feasible, and which is openly supported, discussed, and enforced by its members, and to make sure that proper surveillance mechanisms are in place for employees who have access to valuable material and financial organizational means [39]. Then in 2016, Rebecca M. Chory et al examine these employee concerns through an empirical study of full-time working adults' beliefs about their computer-mediated workplace communication privacy and their evaluations of organizational justice, trust in upper management, and commitment to the organization. The results suggest that employees who perceive less computer-mediated workplace communication privacy tend to view their organization's policies as less fair, trust upper management less, and demonstrate less commitment to their organizations. Furthermore, results indicate that procedural justice mediated the relationship between privacy and organizational commitment and moderated the relationship between privacy and organizational trust [40]. In 2017, Krista Jaakson et al presented that employees outside capital cities are more sensitive to negative signals in their work environment, especially in the case of perceived injustice. When this scenario was given to the respondents the projection of all dishonest behaviours increased more outside capital cities, and significantly so in six behaviours out of nine. They can only hypothesise that the reason for this is stronger identification with the employer – again, due to high unemployment in these regions – and possibly respondents' higher negative affectivity [41]. Moreover, Lorenzo Bizzi et al presented the importance of building a stronger bridge between research in social media and HRM to tackle a key dilemma that HR managers face. The literature has not sufficiently explored the positive and negative implications of social media on employees. The evidence shows the divergent effects of blogging on employee motivation and behavior. HR managers could intervene in job design to reinforce the association between social media use and blogging with coworkers, empowering the benefits of social media [42]. Furthermore, Emma S. Nordback et al demonstrates how the effect of structure in the form of flexibility policy produced differing flows of communication in membership negotiation, reflexive selfstructuring, and activity coordination. In the organization with the more flexible policy, communication flows centered on reflexive self-structuring and activity coordination, and shaped organizational membership that was inherently focused on organizational members. In the organization with a more rigid policy, organization communication flows maintained the policy and membership equated to presence at the office, which altered and constrained members from negotiating this aspect of their membership [43]. Afterthat, Bard Kuvaas et al explore the predictive validity of these theories of intrinsic and extrinsic motivation in work settings; they tested how both intrinsic and extrinsic motivation affected supervisor-rated work performance, affective and continuance commitment, turnover intention, burnout, and work–family conflict. In the course of three studies (two cross-sectional and one cross-lagged) across different industries, they found that intrinsic motivation was associated with positive outcomes and that extrinsic motivation was negatively related or unrelated to positive outcomes. In addition, intrinsic motivation and extrinsic motivation were moderately negatively correlated in all three studies [44]. Then in 2018, Chase E. Thiel et al propose nine practitioner-oriented principles for monitoring program administration rooted in ethical leadership theory. Fair and ethical treatment of employees, coupled with a carefully designed monitoring system that also preserves fairness and ethical treatment, should alleviate concerns related to monitoring [45]. Consequently, Yaniv Kanat-Maymon et al tested and found support for a model in which perceived supervisor legitimacy mediates the association between the supervisor autonomy-supportive motivating style and important employee work-related

outcomes. By integrating SDT with RMA, our work highlights that deference to authority is a unique motivational force that may impact important organizational outcomes above and beyond types of task motivation. Finally, it shows how managerial practices (i.e., autonomy support) have the potential to enhance deference [46]. What's more, Eva Nechanska et al developed a multi-layered and multi-level conceptual framework that HR audiences can use to better understand employee voice, and more importantly silence. OB voice and silence research has utility, but could be integrated with an IR-LP fusion, which connects actors, processes, and institutions, while embedding micro workplace relationships with macro and meso socio-political contexts of change and continuity. Our framework contributes understanding to both voice and silence as a dynamic interface combining the formal/informal, direct/indirect and structure/agency within a context of structural power imbalances and diverse interests [47]. In addition to this, Alexander McLeod et al investigated the effects of independent and interdependent self-construal on three newly developed dimensions of employee privacy concern related to organizational use of biometric technology. These dimensions include perceived accountability, perceived vulnerability, and perceived distrust toward the organization. They test the predictive power of our model using data from an organization deploying a new biometric system designed to track employee work assignments under the auspices of improving personnel safety [48]. Moreover, Lotem Perry-Hazan et al explored the surveillance of Israeli teachers by CCTV systems (CCTVs), based on interviews with teachers who reported being monitored by CCTVs in their schools and with school principals using CCTVs to monitor teachers. The findings present and analyze forms of teachers' CCTV surveillance, its impact on teachers' behavior, their feelings, and their normative perceptions. They find that teachers' surveillance by CCTVs includes spatial and temporal dimensions that differ from other forms of teachers' monitoring. The findings show how surveillance demoralizes teachers, induces resistance, and produces social categorizations that exacerbate teachers' low social status [49]. After that, May Fen Gan et al examined the change in work processes as well as employee perceptions following PETs implementation and found that the technology exerted different effects on employees' workload, the time required to complete a task and the communication loads depending on their work nature. It also found that PETs introduced more systematic and secured work processes in protecting personal data while recognizing the need for effective mechanisms to govern human factors and vendor threats. With increasing digital footprints, the amount of personal data collected by organizations will increase. To protect the interest of their clients, organizations have the responsibility to secure these data by ensuring the sustainability of their PETs systems, implementing effective mechanisms to manage vendor access to clients' personal data, and raising employee awareness in data protection and compliance. Governments and policy makers should also formulate effective monitoring plans to ensure organizational compliance with data protection regulations so as to protect the privacy of their citizens [50]. Then, Christopher Blodgett et al examined the prevalence and consequences of intimate partner violence (IPV) in the workplace. Surveys were completed by 1,390 employees in 32 different companies representing different organization types. Over half of the women and almost a quarter of the males reported that they had been an IPV victim at some point in their lives with 16% reporting victimization in the previous 12 months. Younger workers and workers who witnessed IPV frequently as a child were more likely to be current IPV victims [51]. Additionally, Lara Khansa et al developed a model to study cyberloafing and technological intervention and tested the model using a combination of field surveys utilizing a set of scenarios. Our results reveal that, within the context of cyberloafing prevention, past cyberloafing, context, and organizational commitment are three important considerations that should be accounted for to accurately assess interactional justice, negative affective reactions, and perceived fairness; they found these factors to determine behavioral outcomes. What is important, and contrary to common belief, is that organizational measures that engender unfairness perceptions in employees are surprisingly capable of effectively curtailing cyberloafing, albeit at the expense of employee loyalty [52]. At last, David L. Tomczak et al offered five recommendations for maximizing the positive effects and minimizing the negative effects of EPM: (1) Be transparent with employees about EPM use, (2) be aware of all potential employee reactions to being monitored, (3) use EPM for learning and development rather than deterrence, (4) restrict EPM to only work-related behaviors, and (5) consider organizational makeup when implementing an EPM system [53].

V. Conclusion

The employees, provided with computers, online access and email addresses by the employer, have no rights to personal use of the Internet. It can happen, (i) if it is expressly allowed, (ii) implicitly tolerated, or (iii) simply done, in violation of an explicit prohibition. The consequences are clear, at least theoretically, in the first and in the third case. In the second case, even though the existence of a right cannot be asserted, the absence of a clear discipline rules out both the legitimacy of employer's surveillance and, consequently, the use of the outcomes of the monitoring regardless how it is carried out: personal use is not allowed, but it is also not punishable.The employer can monitor the employees' use of the Internet and email only if an electronic privacy policy has provided advance notice of the surveillance, stating related modalities, conditions, limits and consequences. Beyond labour law discipline, if the employers had the chance to define and publicize the content of the Internet and email monitoring in advance, and they had not, the monitoring is precluded. Consequently, any legal use of the outcomes of an illicit monitoring is equally precluded.The employees' right to 'electronic' privacy in the workplace is not absolute, being subject to the organisational power of the employer. In fact, the employees' reasonable privacy expectations depend on the employer's electronic privacy policy. The content of such policy should include at least the range of employees' personal online activities allowed (if any) and, in accordance with the legislation in force, the employer's intended surveillance level. As a final note, it can be observed that it is not possible to single out pre-packed solutions appropriate for any organizations, considering the numerous variables potentially involved (such as, working activity, organisational complexity, tasks differentiation and public or private employment). It follows that general principles, such as transparency, fairness, responsibility and reasonableness, and specific data protection principles, such as necessity, finality, legitimacy, proportionality, accuracy and security, play a key role in facing the challenge of regulating the use of the Internet in the workplace.

References:

[1] Kaptein, M. (2009). Ethics programs and ethical culture: A next step in unraveling their multi-faceted relationship. Journal of Business Ethics, 89(2), 261–281.

[2] Kaptein, M. (2010). The ethics of organizations: A longitudinal study of the US working population. Journal of Business Ethics, 92(4), 601–618.

[3] Victor, B., & Cullen, J. B. (1988). The organizational bases of ethical work climates. Administrative Science Quarterly, 101–125.

[4] Kish-Gephart, J. J., Harrison, D. A., & Treviño, L. K. (2010). Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work. Journal of Applied Psychology, 95(1), 1–31.

[5] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608.

[6] Hollinger, R. C., & Adams, A. (2014). 2012 National Retail Security Survey final report. Gainesville, FL: University of Florida.

[7] Hollinger, R. C., & Davis, J. L. (2006). Employee theft and staff dishonesty. In M. Gill (Ed.), The handbook of security (pp. 203–228). London: Palgrave Macmillan Ltd

[8] Wen, J., Schwieger, D., & Gershuny, P. (2007). Internet usage monitoring in the workplace: Its legal challenges and implementation strategies. Information Systems Management, 24, 185–196.

[9] Porter, W., & Griffaton, M. (2003). Between the devil and the deep blue sea: Monitoring the electronic workplace. Defense Counsel Journal, 70(1), 65–78.

[10] ePolicy Institute. (2004). 2004 workplace e-mail and instant messaging survey.

[11] Turri, M., Mariam, B., & Hynes, G. (2008). Are they watching? Corporate surveillance of employees' technology use. The Business Review, Cambridge, 11(2), 126–131.

[12] Allen, M., Coopman, S., Hart, J., & Walker, K. (2007). Workplace surveillance and managing privacy boundaries. Management Communication Quarterly: McQ, 21(2), 172–201.

[13] Brien, M. (2008). Law, privacy, and information technology: A sleepwalk through the surveillance society? Information & Communications Technology Law, 17, 25–35.

[14] Wakefield, R. (2004). Computer monitoring and surveillance. The CPA Journal, 74(7), 52–59.

[15] Lasprogata, G., King, N., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. Stanford Technology Law Review, 4, 1–76.

[16] Persson, A., & Hansson, S. (2003). Privacy at work – ethical criteria. Journal of Business Ethics, 42, 59–70.

[17] K. 2010. ''Workplace Surveillance: An overview.'' Labor History 51 (1): 87106.

[18] M., and C. Norris. (1999). Watching the Workers: Crime, CCTV and the Workplace. In Invisible Crimes. Their Victims and their Regulation, edited by P. Davis, P. Francis and V. R. Jupp, 208231. London: Palgrave Macmillan

[19] M. Gill (2006). CCTV: Is it Effective?'' In The Handbook of Security, 438 461. London: Palgrave Macmillan.

[20] Lasprogata, G., N. King, and S. Pillay. (2004). ''Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada.'' Stanford Technology Law Review 4: 146

[21] Nouwt, S., B. de Vries, and C. Prins. (2005). Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy. The Netherlands: Universiteit van Tilburg.

[22] Norris, C. 2009. A Review of the Increased Use of CCTV and Video Surveillance for Crime Prevention Purposes in Europe. Study P.E. 419.588.

[23] von Silva-Tarouca, L. B. (2011). Setting the Watch. Privacy and the Ethics of CCTV Surveillance. Oxford: Hart.

[24] von Hirsch, A. (2000).The Ethics of Public Television Surveillance and CCTV.'' In Ethical and Social Perspectives on Situational Crime Prevention, edited by A. von Hirsch, D. Garland and A. Wakefield, 5976. London: Hart.

[25] Felson, M., and R. Clarke. (1998) Opportunity Makes the Thief. Practical Theory for Crime Prevention. Police Research Series, Paper 98, edited by Barry Webb, 136. London: Home Office, Policing and Reducing Crime Unit Research, Development and Statistics Directorate

[26] Clarke, R. V. (1995). Situational Crime Prevention. Crime and Justice 9: 91150.

[27] Ratcliffe, J. 2006. Video Surveillance of Public Places. Problem-Oriented Guides for Police Response Guides, Series Guide No. 4. US Department of Justice, Office of Community Oriented Policing Services.

[28] J. Berleur, 109120. Boston, MA: Kluwer. Welsh, B. C., D. P. Farrington, and S. J. O'Dell. 2010. Effectiveness of Public Area Surveillance for Crime Prevention: Security Guards, Place Managers and Defensible Space. Stockholm, Sweden: Swedish National Council for Crime Prevention, Information and Publications.

[29] Agustina, J. R. (2010). Risks in Preventing Crime by Limiting Employees' Privacy: Analysing Employers' Duties and Faculties Versus Privacy Interests in Controlling E-mails at the Workplace. International Journal of Private Law 3 (4): 333357.

[30] Jeffrey M. Stanton (2000).Traditional and Electronic Monitoring from an Organizational Justice Perspective. Journal of Business and Psychology September, Volume 15, Issue 1, pp 129–147

[31] Filiz Tabak, William P. Smith. (2005). Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development", Employee Responsibilities and Rights Journal September, Volume 17, Issue 3, pp 173–189

[32] Yael Brender-Ilan, Tamar Shultz. (2005). Perceived Fairness of the Mystery Customer Method: Comparing Two Employee Evaluation Practices", in Employee Responsibilities and Rights Journal December, Volume 17, Issue 4, pp 231–243

[33] Cynthia F. Cohen, Murray E. Cohen (2007). On-duty and Off-duty: Employee Right to Privacy and Employer's Right to Control in the Private Sector", Employee Responsibilities and Rights Journal December, Volume 19, Issue 4, pp 235–246

[34] H. Joseph Wen , Dana Schwieger & Pam Gershuny (2007) Internet Usage Monitoring in the Workplace: Its Legal Challenges and Implementation Strategies, Information Systems Management, 24:2, 185-196

[35] G. Stoney Alder, Marshall Schminke, Terry W. Noel, Maribeth Kuenzi (2008). Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation", in Journal of Business Ethics July, 80:481

[36] Marian K. Riedy & Joseph H. Wen (2010) Electronic surveillance of Internet access in the American workplace: implications for management, Information & Communications Technology Law, 19:1, 87-99

[37] Laurel A. McNall, Jeffrey M. Stanton (2011). Private Eyes Are Watching You: Reactions to Location Sensing Technologies", Journal of Business and Psychology September, Volume 26, Issue 3, pp 299–309

[38] Bernadine Van Gramberga, Julian Teicherb and Anne O'Rourke (2014). Managing electronic communications: a new challenge for human resource managers", The International Journal of Human Resource Management Volume 25, Issue 16

[39] Reinout E. de Vries, Jean-Louis van Gelder (2015).Explaining workplace delinquency: The role of Honesty–Humility, ethical culture, and employee surveillance, Personality and Individual Differences, Volume 86, Pages 112-116

[40] Rebecca M. Chory, Lori E. Vela, Theodore A. Avtgis (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses", Employee Responsibilities and Rights Journal March, Volume 28, Issue 1, pp 23–43

[41] Krista Jaakson, Maaja Vadi, Ilona Baumane-Vitolina, Erika Sumilo (2017).Virtue in small business in small places: Organisational factors associated with employee dishonest behaviour in the retail sector, Journal of Retailing and Consumer Services, Volume 34, Pages 168-176

[42] Lorenzo Bizzi (2017): Should HR managers allow employees to use social media at work? Behavioral and motivational outcomes of employee blogging, The International Journal of Human Resource Management

[43] Emma S. Nordback, Karen K. Myers & Robert D. McPhee (2017) Workplace flexibility and communication flows: a structurational view, Journal of Applied Communication Research, 45:4, 397-412

[44] Bard Kuvaas, Robert Buch, Antoinette Weibel, Anders Dysvik, Christina G.L. Nerstad (2017). Do intrinsic and extrinsic motivation relate differently to employee outcomes?, Journal of Economic Psychology, Volume 61, Pages 244-258

[45] Chase E. Thiel, Alexandra E. MacDougall, Zhanna Bagdasarov (2018). Big (Benevolent) Brother: Overcoming the drawbacks of employee monitoring through ethical administration",Organizational Dynamics,

[46] Yaniv Kanat-Maymon, Erez Yaakobi, Guy Roth (2018).Motivating deference: Employees' perception of authority legitimacy as a mediator of supervisor motivating styles and employee work-related outcomes, European Management Journal, Volume 36, Issue 6, Pages 769-783

[47] Eva Nechanska, Emma Hughes, Tony Dundon (2018).Towards an integration of employee voice and silence. Human Resource Management Review

[48] Darrell Carpenter, Alexander McLeod, Chelsea Hicks, Michele Maasberg (2018).Privacy and biometrics: An empirical examination of employee concern. Information Systems Frontiers February, Volume 20, Issue 1, pp 91–110

[49] Lotem Perry-Hazan, Michael Birnhack (2019). Caught on camera: Teachers' surveillance in schools. Teaching and Teacher Education Volume 78, Pages 193-204

[50] May Fen Gan, Hui Na Chua, Siew Fan Wong (2019). Privacy Enhancing Technologies implementation: An investigation of its impact on work processes and employee perception, Telematics and Informatics, Volume 38, Pages 13-29

[51] Christopher Blodgett & Jane D. Lanigan (2018). The Prevalence and Consequences of Intimate Partner Violence Intrusion in the Workplace, Journal of Aggression, Maltreatment & Trauma, 27:1, 15-34

[52] Lara Khansa, Reza Barkhi, Soumya Ray, Zachary Davis (2018). Cyberloafing in the workplace: mitigation tactics and their impact on individuals' behavior", Information Technology and Management. December Volume 19, Issue 4, pp 197–215

[53] David L. Tomczak, Lauren A. Lanzo, Herman Aguinis, (2018). Evidence-based recommendations for employee performance monitoring. Business Horizons, Volume 61, Issue 2, Pages 251-259