ELECTRONIC MONITORING FOR EMPLOYEES: EMPLOYER RIGHTS IN THE XXI CENTURY

Elena Ofman, South Ural State University
Mikhail Sagandykov, South Ural State University

ABSTRACT

This article is devoted to the examination of legal and ethical issues related to employer implementation of electronic monitoring of employee behavior. To this end, we investigated the legislation and judicial practice of Russia and the United States of America related to the use of modern information and communication systems to assess employee compliance with labor discipline in the workplace. Some shortcomings of the Russian legal system for ensuring the safety of personal (biometric) data of employees were discovered. Attention is also drawn to the irrational and unreasonable use of electronic surveillance of employees in terms of maintaining a balance between production goals and the personal life of the employee. We propose attributing any personal data obtained by the employer as part of their electronic monitoring of employee behavior to biometric personal data. We consider it necessary to obtain employee consent to process biometric personal data, excluding exceptional cases established by law. Similar to US law, we propose to make electronic monitoring possible without prior written notice to employees only if the employer has reasonable grounds to assume that employees are engaged in illegal activities.

Keywords: Electronic Monitoring, Employer Rights, Employees.

INTRODUCTION

Business performance is enhanced by electronic communications in the workplace. However, this also leads to new problems related to the protection of a number of fundamental rights of workers, including the constitutionally protected inviolability of the privacy of communications and personal information (Moreira & Andrade, 2015).

The problem of employers exercising control over employee behavior has been considered both in the field of protecting the right to privacy and in the context of protecting one's dignity during the period of employment (Trofimova, 2017).

Recently, with the development of digital technologies, employers have widely (and sometimes thoughtlessly) implemented the methods and forms of monitoring employee behavior that interest them.

> *"The development of IT equipment used in the work process, the widespread use of social networks, the increasing level of telework and other flexible working methods-all this requires employers to introduce new methods of monitoring the work of their employees" (Gera, 2016).*

These methods of control include: monitoring telephone calls, electronic correspondence, and Internet usage; monitoring employee social network posts on various events and facts; monitoring employee activity at the computer at work; video surveillance of employees, including audio surveillance; GPRS and/or GPS monitoring; and monitoring the psychophysiological state of the employee throughout the work day.

US law includes the special term "*electronic monitoring*" which is an umbrella term for the collection of information on the activities or communications of employees on the premises of the employer by any means other than direct observation, including the use of a computer, telephone, radio, camera, or electromagnetic, photoelectronic, or photo-optical systems, but not including the collection of information (a) for the purpose of ensuring safety in the common areas of the employer's premises, or (b) which is prohibited in accordance with the law of the state or federal law (Law, 2019).

METHODOLOGY

We studied the issues of electronic monitoring of employee behavior through comparative legal and special legal research methods. The main subject of analysis for this article was the labor and information legislation in the field of protection of personal data of employees, including biometric data. We used materials from the practice of the judicial authorities of Russia and the United States of America which reflect the general and situational approach of the law enforcer to employers' use of electronic monitoring of employees at work.

RESULTS AND DISCUSSION

The peculiarity of control systems today is that computers make monitoring of employees invisible and constant (Moreira & Andrade, 2015).

U.S. privacy laws give employers leeway regarding how far they can go with their employee monitoring programs. In some cases, employers are not required to inform employees that they are being monitored, but this depends on state and local laws.

New media technologies provide employers with more "*invasive and expansive methods*" of employee control, emphasizing the vulnerability of their privacy, and the introduction of more modern technologies only exacerbates the problem. The confidentiality of personal life and the right of the employer to control the actions of the employee converge at a point that in literature and legal practice is called *"a reasonable expectation of privacy*" (Opeyemi, 2017).

In the United States, a long discussion has been held about maintaining the confidentiality of personal life, and not just in labor relations. For example, Katz v. United States examined a situation of the FBI listening to a public telephone used by a suspect, providing the FBI a recorded conversation which leads to the conviction of Mr. Katz. The US Supreme Court upheld the appeal of Mr. Katz and proclaimed the formula:

"The fourth amendment (to the US Constitution) protects people, not places (Cases, 1967)"

In other words, citizens have the right to expect privacy regardless of where they are: not only on their own property, but also in public places.

Do these findings relate to the workplace, which is neither the place of residence of the employee, nor a public place? An equipped workplace is the territory of the employer: in essence, his property. In addition, the above court decision had a huge impact on the scope of law enforcement interference in the private lives of citizens. But how does this apply to employee-employer relationships?

Typically, employees have little chance of privacy while on the premises or using company equipment, including company computers or vehicles said Matt C. Pinsker, Associate Professor of National Security and Criminal Justice at Virginia Commonwealth University (Rivera, 2018). The Supreme Courts of Russia hold a similar position:

> *"The labor relations that develop between the employee and the employer within the framework of the employment contract are social in nature and are not directly related to private life and personal and family secrets (Cases, 1998)"*

The corporate codes of leading companies attempt to find a balance of interests between the needs of the employee and the employer in the field of electronic control, which helps to prevent a complete rejection of the reasonable expectation of confidentiality. For example, the United Health Group Code states this:

> *"The Company will balance the privacy of employees with the need to maintain a safe and effective working environment."*

The PepsiCo Code states:

> *"Usually we do not monitor the use by employees of our information systems (Opeyemi, 2017)"*

In the corporate code of Citigroup Inc., on the contrary, there is a direct appeal to employees:

> *"Do not expect personal confidentiality when using Citi resources, whether inside or outside the workplace. To the extent permitted by laws and regulations, Citi may monitor and record the use of your equipment, systems, and services, and may intercept any information that you send or receive as a result of such use at any time (Code of Conduct, 2020)"*

This act of Citigroup Inc. contains direct recommendations on how employees should use social networks. In particular, it is proposed that employees ensure that:

> *"Personal use of social networks does not interfere with work, does not occur during working hours and meets Citi values and standards."*

It is forbidden to disclose any *"non-public, proprietary or confidential information"*, or to engage in any discriminatory or retaliatory statements (Code of Conduct, 2020).

Some Russian employers mistakenly believe that employees do not have to be informed about the establishment of various systems for employee monitoring, such as video surveillance. Because of this, such systems are often hidden from employees; they are not even aware of their presence. Employers justify their position by the fact that not only do they have the right, but also to obligation to directly or indirectly monitor the workplace, according Art. 209 of the Labor

Code of the Russian Federation In addition, employees are obliged to fulfill their work duties during working hours, which means that this time, according to employers, is not considered part of the employees' private life. Accordingly, since video surveillance is established to control work performance, and not privacy, then it is not necessary to warn employees about these systems (Kolinko, 2016).

According to Kolinko, such conclusions of the employer are erroneous, since it is impossible to completely remove privacy from working time. Employees might change clothes, take medicine, etc. during work hours (Kolinko, 2016)

When monitoring the workplace, one cannot but take into account the personal life of employees, especially considering that the same technical devices are used by employees to perform work duties and to communicate with their family members (Opeyemi, 2017).

In Russia, violations related to the implementation of electronic controls by employers are often associated with a violation of the requirements of Federal Law of July 27, 2006 No. 152-ФЗ "*On Personal Data*". The legislation of the Russian Federation describes personal data as the physiological and biological characteristics of an individual, on the basis of which it is possible to establish an identity. These are called biometric personal data, the processing of which is only possible with the prior consent of the subject of personal data. (Clause 1, Article 11 of the Federal Law "*On Personal Data*"). Supervisory authorities (Roskomnadzor, 2013) indicate that it is necessary to consider the goal pursued by operator when taking actions related to the processing of personal data. If personal data are used to establish the identity of the subject of personal data, then this processing should be carried out in strict accordance with Art. 11 of the Federal Law "*On Personal Data*" (that is, with the consent of the employee), and the physiological and biological characteristics of the employee captured by the employer during video surveillance, are considered biometric. If the processing of personal data is carried out for purposes other than "*identification*" (for example, confirmation of the performance of certain actions by a specific person), then these actions cannot be considered as the processing of biometric personal data. Therefore, article 11 of the Federal Law "*On Personal Data*" does not apply, and personal processing is carried out without the consent of the subject-holder of the specified data (employee), since it is necessary for the execution of the contract (including labor contracts) (Clause 5, Part 1, Article 6).

Without the consent of the personal data subject, the processing of biometric personal data is possible if the goal is to implement international readmission agreements, administer justice, and enforce judicial acts. It is also possible in cases stipulated by the legislation of the Russian Federation on defense, security, countering terrorism, transport security, countering corruption, operative-search activity, public service, the criminal-executive legislation of the Russian Federation, and the legislation on the exit procedure from the Russian Federation and entry into the Russian Federation (Part 2 of Article 11 of the Federal Law "*On Personal Data*").

An analysis of Russian legislation allows us to conclude that the legality of the procedure for establishing video surveillance of employees at the workplace and at the place of work is established by the employer observing a number of organizational procedures without obtaining consent from the employees to process personal data.

In the United States, the situation is quite similar: in order for video surveillance to be legal, the employer must inform employees about the surveillance; obtaining consent from employees is not required.

Each employer places a notification about the types of electronic monitoring that the employer can engage in in a conspicuous place visible to its employee. These accommodations constitute advance notice. "*Just knowing that cameras are monitoring everything that's going on may be enough to prevent employee misconduct*" (Rivera, 2018) and real monitoring may not be (D'Urso, 2006).

Electronic control, although becoming more scrupulous, since it allows for the evaluation of all actions taken by employees, may be less intrusive for the employees. Direct human control can be accompanied by an imbalance of power and subordination between the manager and the employee. With electronic (computer) control, this interaction is excluded. Electronic control is less stringent, but also more structurally deep (Elliott & Long, 2015).

Maria Falk Mikkelsen, Lotte Beg Andersen, and Christian Böcher Jacobsen quote Frey, who argues that if employees perceive external interventions as a deterrent, internal motivation is supplanted by counteracting the disciplining effect. On the contrary, if employees perceive external interventions as support from the employer, then internal motivation will be strengthened and the intervention will become effective (Mikkelsen et al., 2015).

At the same time, the practice of using electronic monitoring and observation (control) in labor relations may contradict the basic methods of personnel management, which are based on empowering employees, the active participation of employees in the labor process, and are based on trust between the employee and the employer (Holland et al., 2015).

Judicial Practice Analysis

In the USA, covert monitoring is used in some cases. For example, if (1) the employer has reasonable grounds to believe that employees are engaging in behavior that (i) violates the law, (ii) violates the legitimate rights of the employer or fellow employees, or (iii) creates a hostile work environment, and (2) electronic monitoring may indicate this misconduct, the employer may conduct monitoring without prior written notice (Law, 2018).

U.S. courts hold the position that an employer who is notified that one of his employees has used a computer in the workplace to access pornography (possibly child pornography) is required to investigate the employee's actions and take prompt and effective measures to stop unauthorized activity to prevent harm to innocent third parties. No employee's personal interests stand in the way of this obligation on the part of the employer (Cases, 2005; Cases, 2009).

A. Opeyemi provides an example of judicial practice. In Holmes v. Petrovich Development Co. in 2011, it was found that a pregnant employee had been using her company's email account to maintain conversations with her lawyer about alleged workplace discrimination during her pregnancy. She objected to her employer's access to her email. However, the court ruled that the employee unreasonably expected confidentiality of her personal data, having been informed that correspondence carried out using the company's resources could not be protected by the fourth amendment (Opeyemi, 2017).

The case file contains a very interesting comparison made by the court:

> *"…emails sent through the company's computer in the circumstances of this case were akin to a consultation made by a lawyer in the conference room of her employer in a loud voice with an open door when any reasonable person could suggest that this conversation can be heard (Cases, 2011)"*

The courts note that there is a high risk of losing legally recognized expectations of confidentiality when employees use company equipment for personal purposes. This, in turn, leads to increased monitoring of them (Opeyemi, 2017).

Russian courts note that:

> *"Video recording of workflow is not a disclosure of personal data. The employer's use of video surveillance tools... is for purposes related to the employee's work and not to investigate his private life or personal and family secrets (Cases, 2016; Cases, 2017)"*

> *"The establishment of a video surveillance system is connected with ensuring security on the territory of the employer... and copying a video of a work process is not a disclosure of personal data (since in this case there is no goal being pursued by the operator to establish the identity of the subject of personal data) and does not violate the law (Cases, 2016)"*

> *"The employee's labor activity is public... The office is not an environment that is inviolable... No additional information regarding the identity of the plaintiff is known to the employer (Cases, 2012)"*

In another decision, it was established that *"the office in the school is a public place*", in connection with which the employee's demands to dismantle the CCTV system in an office were denied (Cases, 2011).

Monitoring employee behavior should be reasonable. For example, surveillance in bathrooms, in rooms intended for the health or personal comfort of employees, for the protection of their property, or in locker rooms, is strictly prohibited. West Virginia Code prohibits employers from using video and other electronic means of monitoring employee activities in rooms intended for the health or personal comfort of employees or for protecting their property (e.g. lounges, showers, changing rooms) (Law, 2019). However, the installation of CCTV cameras in public places (for example, in the corridor) is legal. One of the decisions of the Russian courts determined that:

> *"The court finds the installation of video surveillance cameras in the corridors of an educational institution legal, since the video surveillance system was installed to ensure the safety of students and employees, as well as to prevent accidents with students during their stay in an organization providing educational activities, and employees were made aware of this (Cases, 2016)"*

Particular attention in US law is paid to wiretapping (interception) of telephone calls. US law provides sufficient detail on the rules for monitoring telephone calls:

1. Interception of the contents of telephone conversations without judicial authorization by any person (except as otherwise expressly provided in the chapter) is prohibited (Law, 1968);
2. This prohibition shall not be applied if the person, company, or corporation notifies employees that monitoring may take place at any time during the performance of work duties (Law, 2018). Employees may be informed at different intervals (Law, 2018);
3. Monitoring of a telephone conversation or other oral message is not illegal if one of the parties to the message has given prior consent to such monitoring;
4. Both business calls and personal calls may be monitored. Moreover, to determine the nature of the call (personal or business); it is necessary to determine the main (signal) topic of the conversation, the nature of the conversation.

> *"A personal call can be intercepted during the usual business activities of the employer to determine its nature, but not its content... Therefore, the employer (his representative) should stop listening as soon as he determines that the call was personal, regardless of the content of the conversation heard (Cases, 1983)".*

In the United States, state laws are supplemented by specific obligations on the part of employers. For example, employers must provide employees with personal telephones that are not subject to monitoring or control (Law, 2019).

American courts adhere to the rule that employers may (and in some cases must) record personal conversations of employees if there is suspicion that employees are using the phones for illegal purposes, in an unauthorized way, or to trick the employer. But there are limits to the exercise of this right. In Deal v. Spears (Cases, 1991 & 1992) the court found that the employer White Oak Package Store, wanting to expose an employee's intention to steal, eavesdropped on conversations without authorization, thereby violating Section III of the Combined Crime and Safe Streets Act of 1968 (Law, 1968), because during monitoring, conversations of an intimate nature between Sibbie Deal with a third party (Calvin Lucas) were exposed. The employee did not give consent to monitoring, but in conversation the employer had warned her that long personal conversations during working hours were not allowed. The court found that *"the extent of the interception in this case goes beyond the ordinary conduct of business"* (ordinary business), as it was about listening to personal conversations, and the disclosure of these conversations did not pursue from any business purpose (Larry, 1995).

CONCLUSIONS

In the United States, the right to privacy must meet certain standards: individuals must have the right to expect confidentiality, these expectations must be reasonable, and the employee must prove that invasions of privacy by the employer are "*serious*" in nature, scope, and potential impact, "*unreasonable*", and "*offensive*".

In Russia, the incorrect formulation of biometric personal data and, most likely, the incorrect interpretation of this concept by Roskomnadzor led to the fact that employers process personal data which allows them to identify individual employees without the prior consent of the employee. It turns out that in order to recognize personal data as biometric, it is necessary to establish and comply with the purpose of data processing and not to determine the volume of data collected. This approach seems fundamentally incorrect. It seems that the main, basic feature of biometric personal data is that they characterize the physiological and biological characteristics of a person, regardless of the purpose for which the employer processes them. In addition, with the help of audio and video monitoring, the employer can establish the identity of the employee violating workplace rules. Accordingly, indirectly, the characteristic of biometric personal data which includes "*establishing the identity of the subject of personal* data" may occur when the employer exercises control in the form of video surveillance of the employee's performance of work duties. Therefore, we can state that:

1. Personal data that has become known to the employer as part of video surveillance of the employee's behavior at work should be considered biometric personal data;
2. These biometric personal data should be processed with the consent of the subject of personal data (employee), with the exception of cases established by federal laws (in particular, Part 2 of Art. 11 of the

Federal Law "*On Personal Data*": in connection with the implementation of international readmission agreements, the administration of justice, or the enforcement of judicial acts; as well as in cases provided for by the legislation of the Russian Federation on defense, security, countering terrorism, transport security, anti-corruption, operational-search activities, public service, criminal-executive legislation of the Russian Federation, and legislation of the Russian Federation on the procedure for entering or exiting the Russian).

In Russia, the public and covert (secret) receipt of information is made possible by direct instruction of the law and is exclusively to be exercised by bodies authorized to solve the problems of intelligence operations; the employer is not authorized to carry out covert activities to monitor the employee using technical means. But since hidden audio and video monitoring of the behavior of workers in Russia is nevertheless carried out, it is advisable to adhere to a rule similar to the United States: if the employer has reasonable grounds to assume that employees are engaged in illegal activities, then electronic monitoring without prior written notice of their behavior is admissible.

REFERENCES

Cases. (1967). *Case of Katz v. United States (389 US 347*). Retrieved from https://legaldictionary.net/katz-v-united-states/

Cases. (1983). *Case of Carmie Watkins v. L.m. Berry&Company, 704 F.2d 577.* Retrieved from https://law.justia.com/cases/federal/appellate-courts/F2/704/577/107387/

Cases. (1991). *Case of Deal v. Spears, 780 F. Supp. 618.* Retrieved from https://law.justia.com/cases/federal/district-courts/FSupp/780/618/1445275/

Cases. (1992). *Case of Deal v. Spears, 980 F.2d 1153.* Retrieved from https://casetext.com/case/deal-v-spears-2/?phone_number_group=p&new_case_page=n

Cases. (1998). *Decision of the constitutional court of the Russian Federation of November 20, no. 157-O*. Retrieved from http://www.consultant.ru/online/

Cases. (2005). *Case of Jane Doe individually et al. v. XYC Corporation (no 1:19-cv-01542).* Retrieved from https://law.justia.com/cases/new-jersey/appellate-division-published/2005/a2909-04-opn.html

Cases. (2009). *Case of Abigail Hernandez et al. v. Hillsides, Inc. et al. Supreme Court of California (no. S147552).* Retrieved from https://www.law.berkeley.edu/files/House_-_03-Hernandez-v-Hillsides.pdf

Cases. (2011). *Decision of the Klinskiy city court of the Moscow region dated November 23, (no 2-2191/2011).* Retrieved from https://sudact.ru/

Cases. (2011). *Gina M. Holmes, Plaintiff and Appellant, v. Petrovich development company, LLC (No. C059133).* Retrieved from https://caselaw.findlaw.com/ca-court-of-appeal/1552780.html

Cases. (2012). *Decision of the Sengileevsky district court of the Ulyanovsk region dated October 25, 2012 (no 2-363/2012).* Retrieved from https://sudact.ru/

Cases. (2016). *Appeal decision of the Sverdlovsk regional court of 25 March 2016 (no 33-5427/2016).* Retrieved from http://www.consultant.ru/online/

Cases. (2016). *Appeal decision of the Sverdlovsk regional court of November 16, 2016 (no. 1. 33-20507/2016).* Retrieved from http://www.consultant.ru/online/

Cases. (2016). *Decision of the Michurinsk city court of the Tambov region of July 15 (no 2-947/2016*). Retrieved from https://sudact.ru/

Cases. (2017). *Decision of the Samara district court of Samara of 26 July 2017 (no. 2-1676/2017*). Retrieved from https://sudact.ru/

Code of Conduct. (2020). A Citi of leaders: Enabling growth and progress. *Citigroup Inc.* Retrieved from https://www.citigroup.com/citi/investor/data/codeconduct_en.pdf

D'Urso, S. (2006). Who's watching us at work? *Communication Theory, 16*(1), 281–303.

Elliott, C.S., & Long, G. (2015). Manufacturing rate busters: Computer control and social relations in the labor process. *Work, Employment and Society, 30*(1), 135–151.

Gera, G (2016). *Balancing the right to employer control with employee privacy concerns*. Retrieved from https://www.internationallawoffice.com/Newsletters/Employment-Benefits/Hungary/Schoenherr-Rechtsanwlte/Balancing-the-right-to-employer-control-with-employee-privacy-concerns

Holland, P.J., Cooper, B., & Hecker, R. (2015). Electronic monitoring and surveillance in the workplace. *Personnel Review, 44(1),* 161–175.

Kolinko, A. (2016). Seeing the eye of the employer. *Newspaper Ej-YUrist.*

Larry O. (1995). An affront to human dignity: Electronic mail monitoring in the private sector workplace. *Harvard Journal of Law & Technology, 8*(2), 345-425.

Law. (1968). *Omnibus crime control and safe streets act.* Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/ statutes/1284

Law. (2018). *19 DE code § 705.* Retrieved from https://law.justia.com/codes/delaware/2018/title-19/chapter-7/subchapter-i/section-705/

Law. (2018). *CT Gen Stat § 31-48d.* Retrieved from https://law.justia.com/codes/connecticut/2018/title-31/chapter-557/section-31-48d/

Law. (2018). *VA Code § 18.2-167.1*. Retrieved from https://law.justia.com/codes/virginia/2018/title-18.2/chapter-5/section-18.2-167.1/

Law. (2019). *CT Gen Stat § 31-48d*. Retrieved from https://law.justia.com/codes/connecticut/2019/title-31/chapter-557/section-31-48d/

Law. (2019). *WV Code § 21-3-20.* Retrieved from https://law.justia.com/codes/west-virginia/2019/chapter-21/article-3/section-21-3-20/

Law. (2019). *WV Code § 61-3-24c.* Retrieved from https://law.justia.com/codes/west-virginia/2019/chapter-61/article-3/section-61-3-24c/

Mikkelsen, M.F., Jacobsen, C.B., & Andersen, L.B. (2015). Managing employee motivation: Exploring the connections between managers' enforcement actions, employee perceptions, and employee intrinsic motivation. *International Public Management Journal, 20(2),* 183–205.

Moreira, T.C., & Andrade, F. (2015). Electronic control in labour relations. *Vestnik of Lobachevsky University of Nizhni Novgorod, 3*(1), 158–172.

Opeyemi, A. (2017). New media, work boundaries, and privacy. *International Journal of Communication, 11*(1), 4769–4782.

Rivera, A. (2018). Spying on your employees? Better understand the law first. *Business New Daily*. Retrieved from https://www.businessnewsdaily.com/6685-employee-monitoring-privacy.html

Roskomnadzor. (2013). *On the issues of attributing photo and video images, fingerprint data and other information to biometric personal data and peculiarities of their processing.* Retrieved from http://25.rsoc.ru

Trofimova, G.A. (2017). The principles of destruction in the regulation of labor relations. *Citizen and Law, 3*(1), 64–70.

This article was originally published in Special Issue, entitled: "**Law, Politics, Economics and Human Rights: Global and National Perspectives",** Edited by **Dr. Ashgar Ali Bin Ali Mohamed**