Pîslaruc Maria
PhD student, State University of Moldova

DIGITAL FREEDOM OF EMPLOYEES

Abstract. *The digitalization of processes within companies has seen a significant increase so that employers can not give up control over the use of the Internet or devices by employees because this aspect is related to work discipline. The objective of the article is to clarify the concept of digital freedom in the context of labor relations and the legal coverage provided by national and international norms. The analysis of the criteria that legitimize the monitoring of the digital activity of the employees will allow highlighting the limits of exercising the freedom of information and good practices.*

Keywords: *employee, employer, digital freedom, private life, workplace, monitoring, internet, information.*

The notion of freedom is defined as the possibility to act according to one's own will or desire [1]. Within the legal labor relations, without disturbing the essence of the concept of freedom, the possibility of the employee to act according to his own will is configured by the work discipline and the hierarchy of the subjects, specific to the labor relations.

According to the dex, the term digital means something that is or can be represented by numbers or

by numbers or by generating, measuring, processing, or storing digital signals.

Digital freedom can be defined as uncensored access to the open internet, mobile phones, or other information technologies while respecting freedom of expression, access to information, the right to privacy, and freedom of assembly worldwide.

According to Resolution No. 38/7 of 17.07.2018 of the UN Human Rights Council, on "Promotion, protection, and enjoyment of human rights on the Internet", the signatory states stated that the same rights that people have offline must also, protected online, in particular freedom of expression, following Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and

Political Rights of 1966. That resolution recognizes and reiterates the importance of protecting human rights and the free movement of information in the field of online [2].

The same resolution states that these provisions must encourage commercial enterprises to work to enable technical solutions to secure and protect the confidentiality of digital communications, which may include encryption measures and anonymity.

The Recommendation of the Committee of Ministers of the Council of Europe to the Member States on the processing of personal data in the context of employment, adopted on 1 April 2015, prescribes respect for human dignity, privacy and the protection of personal data must be protected in the processing of personal data staff for employment purposes, in particular, to allow the free development of the employee's personality, as well as for possibilities for individual and social relationships at work [3].

Employers should minimize the processing of personal data only to the data necessary for the purpose pursued in individual cases. Employers should also develop appropriate measures to ensure that they comply in practice with the principles and obligations relating to the processing of data for employment purposes.

The acts in question enshrine the employee's right to an online environment and the protection of privacy in both dimensions, real and virtual.

Returning to the national framework, art.9 par. (2) letters a), d) of the Labor Code of the Republic of Moldova no. 154 of 28.03.2003, indicateas that the employee is obliged to conscientiously fulfill his work obligations provided by the individual employment contract and to respect the labor discipline [4].

Correlatively, the employer has the right enshrined in art. 10 par. (1) letter b) of the Labor Code of the Republic of Moldova no. 154 of 28.03.2003, to ask the employees to fulfill their work obligations and to manifest a household attitude towards its goods.

Currently, based on the general rules mentioned above, the employer has the prerogative to supervise and control the devices made available to employees, subject to certain conditions.

More recently, in 2020, the Labor Code of the Republic of Moldova was completed with chapter IX[1] which regulates remote work, is defined as the form of work organization in the fields of activity, through which the employee fulfills his duties specific to occupation, function or profession who holds it elsewhere than the one organized by the employer, including means in the field of information and communication technology.

By art.2923 par. (2) of the CM of the Republic of Moldova, the individual employment contract regarding distance work must contain, in addition to the clauses provided in art. 49, clauses regarding: a) the conditions for performing distance work; b) the program within which the employer is entitled to verify the activity of the employee and regarding the manner of performing the control; c) the manner of recording the working hours provided by the employee with remote work; d) the conditions regarding the bearing of the expenses related to the activity in the remote work regime; e) other conditions agreed by the parties.

Thus, we see that according to the cited norm, the employer must coordinate in advance with the employee a program in which he has the right to verify the employee's activity and the exact way of performing the control.

In this regard, it is worth noting that international instruments are increasingly urging states to adopt, implement, and, if necessary, reform regulations to ensure the protection of personal data and the protection of online privacy to prevent, mitigate and remedy the collection, storage, processing, use or disclosure of personal data on the Internet that may violate human rights, arbitrary or illegal.

According to a report by the Engagement Institute, the loss of labor productivity costs US companies about $ 550 billion annually. In another report by Udemy (World's Largest Education Site), internet use was at the top of the list of time-wasting activities for 78% of respondents [5].

Currently, there are various ways in which the employer can digitally monitor the employee's activity, such as internet monitoring, monitoring the use of the service phone, GPS monitoring, video surveillance of employees, input/output control system.

The control of the employee's internet traffic is a frequent way of monitoring,

which can be achieved by: a complete ban on the internet within the entity; banning access to some particular web pages (for example Facebook, Instagram, youtube, odnoklassniki, etc.); use of various IT tools to monitor the entire digital activity of employees (keyloggers, video loggers); monitoring the time used by the Internet by employees and/or accessing applications (method used eg by Apple, Verizon);

What is certain is that the Internet is a distraction at work, at the same time it is an essential element for business processes, most modern companies being based on online activities. Given such a considerable dependence on the Internet, banning it altogether may be a disproportionate measure, depending on the specifics of the work [6].

The reality is that there is a multitude of sites that the employee could access for entertainment. However, by blocking the most used social networks, the employer aims to focus the employee's attention on work tasks. At the same time, it is not uncommon for the employee to need to use such websites for work-related purposes, such as the case of a social media marketing agency. In this case, social networks can be seen as an integral part of the employee's work operations and not as entertainment during working hours.

If the employee uses his personal computer for work, restricting access to certain websites may involve more severe restrictions on the employee's privacy and freedom of information.

Currently, there are various tools through which the employee's digital activity can be monitored. For example, keyloggers offer the ability to track keystrokes pressed by an employee on a computer. Video loggers are software that records or takes screenshots of an employee's computer screen while working. Such intrusive monitoring of the person's privacy must be duly justified by the employer.

Monitoring internet usage time allows the employer to view information about websites and applications that have been used by each employee and how long they have used them. If the employee is paid by the hour, the method in question allows us to find out if someone spends hours off as hours worked.

Particular monitoring of certain activities (service email, intranet, specialized software)

The employer only needs to monitor what is related to the work and what he

has made available to the employee. However, even if the employer strictly monitors the information related to work, the employee even in these conditions benefits from the protection of privacy, and if the employer does not comply with certain conditions, this monitoring can be classified as a violation.

As jobs become more technological, the protection of employees from the risks and damage that can be caused by the use of intrusive technologies becomes relevant.

There are conditions that both sides of the legal employment relationship must take into account to capitalize on their digital rights and to balance the power asymmetry that results from the use of surveillance information technologies.

In this sense, any freedom, including the digital freedom of employees, is correlated with other rights and freedoms, both of employers and other employees, which must comply with several conditions for a monitoring measure to be legitimate.

– Clear and prior information on the nature of the monitoring.

The information can be communicated to staff in various ways, depending on the specific circumstances of each case. The European Court of Human Rights considers that the measures can be considered following the requirements of art. 8 of the European Convention on Human Rights, if the information is clear as to the nature of the monitoring and before its implementation. If the employer has a well-argued legitimate aim, the employee's consent will not be an essential element, provided that he has been informed sufficiently clearly in advance. Denial of consent is not absolute. The condition of consent arises if subsequently there are purposes other than those directly related to the execution of the CIM, which were not discussed in the negotiation of the employment contract and which the employee does not reasonably expect (e.g. posting the picture on the site). In these cases, consent must be sought in addition. The described condition is guided by the principle of transparency and predictability. A particularly clear and complete description of the categories of personal data that may be collected by ICTs, including video surveillance and their possible use, should be provided where appropriate [7].

– Evaluating and establishing the extent of monitoring;

In this respect, a distinction must be made between monitoring the flow of communications and that of their content. In addition, it must be considered whether all or only part of the communications were monitored and whether or not the monitoring was limited in time, as well as the number of people who had access to its results. The same is true for the spatial limits of monitoring [8].

– Existence of legitimate reasons for monitoring;

Monitoring employees and in particular monitoring, the content of communications is, by its nature, a much more invasive method, requiring more serious justifications (risks to the employer's property, other types of crime). For example, the employer may justify the need for monitoring by the fact that the employee's actions could harm the company's computer systems and possibly generate liability for the company in case of illegal activity in the virtual space, as well as to avoid revealing its trade secrets. However, in order not to be categorized only as theoretical indications, the risks in question must be real and specific to the field in which the employee carries out his activity [9].

– Evaluate the opportunity to set up a less intrusive monitoring system;

In this respect, it is necessary to assess, depending on the specific circumstances of each case, whether the purpose pursued by the employer could be achieved without the employer having direct and full access to the content of the employee's communications [10].

– Assessing the consequences of monitoring for employees;

The stated condition requires an analysis of how the employer used the results of the monitoring measure, in particular, those results were used to achieve the stated purpose of the measure [11].

Existence of sufficient guarantees for the protection of legitimate rights and interests.

These guarantees must, in particular, make it possible to prevent the employer's access to the actual content of the communications in question where the employee has not been informed in advance of such a possibility. In this context, the European Court of Human Rights states that to thrive, labor relations must be based on trust between people [12].

Finally, employees whose digital activity has been monitored must be able to benefit from an appeal before a judicial body that has the power to rule, at least in essence, on compliance with the criteria mentioned above. above, as well as on the legality of the disputed measures [13].

In the context of this topic, the recent judgment of the European Court of Human Rights in June 2021 in the case of Melike v. Turkey is of interest. The applicant, being an employee of the national authority for education, was dismissed without the right to compensation, because she "liked" certain posts on Facebook.

The domestic courts found that the content which the applicant 'liked' could not be covered by freedom of expression and could disturb the peace of the workplace, especially in schools belonging to the Ministry of Education, because the material might be considered offensive. for teachers and could cause concern for parents and students.

Therefore, the European Court of Human Rights has ruled that the national courts have not carried out a sufficiently detailed examination of the content of the contested publications or the context in which they were posted. The content consisted of virulent political criticism of alleged repressive practices by the authorities, calls, and encouragement to protest against these practices, expressions of indignation at the assassination of the president of a bar, allegations of alleged abuse of students in controlled units by the authorities, and a sharp reaction to a statement, perceived as sexist, made by a well-known religious personality.

The Court also ruled that a key moment in the field in which the employee works, so that a civil servant has a special bond of trust and loyalty to the institutional hierarchy, while the obligation of loyalty, reserve, and discretion that he owes employees in private employment relationships to their employer could not be as strong.

The use of "likes" on social networks, as a way for people to show interest and approval of the content, can be considered a form of exercising freedom of expression online.

In the case of Melike v. Turkey, the employee was not the person who created

and published the contested content on the social network in question, but her action was limited to pressing the "Like" button below that content. Adding a "Like" to the content could not be considered to have the same weight as sharing the content on social networks, in the sense that a "Like" expressed the only sympathy for the published content and not an active desire to disseminate his. Moreover, the authorities did not claim that the content in question reached a very large audience on the social networks in question [14].

Given the nature of her job, the applicant could not have been particularly well known and had only a limited representative status at work, and her activities on social networks could not have had a significant impact on students, parents, teachers, and other employees.

The European Court of Human Rights has established a violation of Article 10 of the European Convention on Human Rights, taking into account the fact that national authorities have not tried to assess the potential of these appreciation actions in the media to provoke an adverse reaction at work, given the content of the material to which they referred, the professional and social context in which they were made and their potential impact, which was insufficient to justify the dismissal of the employee from work.

At the same time, depending on the nature of the position held by the employee, opinions expressed at work, including online, may lead to disciplinary action to the extent that they are likely to disrupt order in the workplace.

In conclusion, although the employer has the right to establish monitoring policies or to restrict access to certain sources of information to limit the theft of employees during working hours, this does not in any way mean the annihilation of the person's right to privacy during working hours.

The employee's digital freedom is a side of the concept of privacy, essentially constituting controlled freedom under the employment relationship of a subordinate nature. The instructions of an employer cannot reduce to zero the exercise of the right to social privacy at work.

The task of the regulatory framework is to outline some limits or criteria on how intrusive employee monitoring software can be because it is natural to

understand that employees are not just productivity machines, but social beings with the right to privacy. basic, separate personal work-life and dignity in professional life, including a level of respect and trust on the part of the employer.

References:

1. https://dexonline.ro/definitie/libertate
2. Resolution of Human Rights Council, UN. ,, The promotion, protection and enjoyment of human rights on the Internet", nr.38/7 on 17.07.2018;
3. Recommendation CM/Rec (2015) on the processing of personal data in the context of employment, adopted by The Committee of Ministers on 01.02.2015;
4. Labour Code of the Republic of Moldova. Nr. 154-XV din 28.02.2003. In: Monitorul Oficial al Republicii Moldova, 29.07.2003, nr. 159-162/648;
5. https://www.hrdive.com/news/study-disengaged-employees-can-cost-companies-up-to-550b-a-year/437606/
6. https://www.timedoctor.com/blog/how-to-successfully-monitor-your-employees-internet-usage/
7. https://www.constcourt.md/libview.php?l=ro&id=1685&idc=179&t=/Rezumate-CEDO/2019/strongLopez-Ribalda-i-altii-v-Spania-MCstrong-Supravegherea-video-ascunsa-de-catre-angajator-a-casierilor-i-a-asistentilor-de-vanzari-din-supermarketuri-Nicio-incalcare/?l=ro&id=1685&idc=179&t=/Rezumate-CEDO/2019/strongLopez-Ribalda-i-altii-v-Spania-MCstrong-Supravegherea-video-ascunsa-de-catre-angajator-a-casierilor-i-a-asistentilor-de-vanzari-din-supermarketuri-Nicio-incalcare/
8. Case Ozpinar v. Turkey (2018). https://hudoc.echr.coe.int/eng#{%22 languageisocode %22:[%22RUM%22],%22appno%22:[%2220999/04%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-123481%22]}
9. Case Centre for Democracy and the Rule of Law v. Ukraina (2020). https://hudoc.echr.coe.int/eng#%20
10. Case Barbulescu v. Romania (2016). https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]}
11. Case Kopke v. Germany (2007). https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22kopke%22],%22itemid%22:[%22001-101536%22]}
12. https://digitalfreedomfund.org/empowering-workers-through-digital-rights/
13. https://www.worktime.com/12-most-asked-questions-on-us-employee-monitoring-laws#C1
14. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210417%22]}