COMPARATIVE LABOR LAW DOSSIER
LABOR IMPACT OF TECHNOLOGICAL DEVICES

Coordinated by Sergi Galvez Durán (PhD candidate Universitat Ramón Llull-ESADE) and Andrés Camargo Rodríguez (PhD candidate, Pompeu Fabra University).

Abstract

The Comparative Labor Law Dossier (CLLD) in this issue 2/2018 of *IUSLabor* is dedicated to the labor impact of technological devices. We have had the collaboration of internationally renowned academics and professionals from Belgium, France, Italy, Poland, Portugal, Slovenia, Spain, Argentina, Brazil, Colombia, Mexico, Dominican Republic and Uruguay

El Comparative Labor Law Dossier (CLLD) de este número 2/2018 de IUSLabor está dedicado al impacto laboral del uso de dispositivos tecnológicos. Se ha contado con la participación de académicos y profesionales de prestigio de Bélgica, Eslovenia, España, Francia, Italia, Polonia, Portugal, Argentina, Brasil, Colombia, México República Dominicana y Uruguay.

Título: Comparative Labor Law Dossier. Labor impact of technological devices.

Keywords: cameras, control, data protection, e-mail, employer, GPS, labor relation, personal data, surveillance, technological devices, worker, working time, workplace.
Palabras clave: cámaras, control, correo electrónico, dispositivos tecnológicos, empleador, jornada de trabajo, GPS, protección de datos, relación laboral, sitio de trabajo, trabajador, vigilancia.

IUSLabor 2/2018, ISSN 1699-2938, p. 4-139.
DOI. 10.31009/IUSLabor.2018.i02.02

Summary

1. **Labor impact of technological devices in Belgium by Pieter Pecinovsky**
2. **Labor impact of technological devices in France by Marie Morin and Francis Kessler**
3. **Labor impact of technological devices in Italy by Emmanuele Dagnino**
4. **Labor impact of technological devices in Poland by Michał Barański**
5. **Labor impact of technological devices in Portugal by Milena Rouxinol**
6. **Labor impact of technological devices in Slovenia by Darja Senčur Peček**
7. **Impacto laboral del uso de dispositivos tecnológicos en España por Sergi Galvez Durán**
8. **Impacto laboral del uso de dispositivos tecnológicos en Argentina por Vanessa Lamamí**
9. **Impacto laboral del uso de dispositivos tecnológicos en Brasil por Carolina Lins Mesquita.**
10. **Impacto laboral del uso de dispositivos tecnológicos en Colombia por Juliana Morad A. y Carlos Prieto M.**
11. **Impacto laboral del uso de dispositivos tecnológicos en México por José Aparicio V y Oscar Zavala G.**
12. **Impacto laboral del uso de dispositivos tecnológicos en República Dominicana por Gina María Polanco Santos.**
13. **Impacto laboral del uso de dispositivos tecnológicos en Uruguay por Leticia Iglesias Merrone**

LABOR IMPACT OF TECHNOLOGICAL DEVICES IN BELGIUM

Dr. Pieter Pecinovsky
Researcher at the Institute for Labour Law, KU Leuven

Introduction

In principle, Belgian labour law sees the regulation of the use of electronic devices by employees as a prerogative of the employer. Yet, usually a code of conduct and disciplinary sanctions connected to the abuse of the devices will be laid down in the work regulations. However, the most important exception to the prerogative of the employer is however when the use of these devices has a possible impact on the privacy of the employees. In this case the employer needs to take into account (next to the fundamental right to privacy) several privacy regulations in the Belgian legislation (as well as the relevant EU legislation) and in national collective agreements of the social partners. The monitoring of employees will only be allowed if the monitoring system meets certain conditions of legitimate aims (purpose), proportionality and information (and consultation) obligations. However, there is a continuing discussion on the use of 'illegally' obtained data or recordings in judiciary cases regarding to labour law (can the judge take the illegal evidence in consideration or not?). Lastly a recent Act of 26 March 2018 has promoted employers and worker representatives to start a discussion on the disconnection of work (and electronic devices) of employees in their free time and to set up a company policy about it.

1. Is there any regulation in your country regarding employees' use of technological devices in the company?

There is no specific regulation in Belgium on the employee's use of the technological devices in the company (to render services). Employers are free to restrict the use of the devices, they can i.a. do this in the individual labour contracts or in the work regulations. The regulation of the access and use of electronic devices is the prerogative of the employer (as made clear in article 1, §2 of Collective agreement n° 81 - see *further*). If the employees can make use of the devices for private matters or in their free time the use of the devices will be seen as part of their (wage) benefits. The Belgian labour law only interferes in the aspect of control by the employer on the use of the electronic devices by the employees as this interferes with the right to privacy of the employees. The most important regulation with regard to privacy is the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data (adapted to comply with EU Directive 95/46/EG and the GDPR), which in the context of labour law has been specified by national Collective agreement n° 81 of 26

April 2002 on the protection of the privacy of employees with regard to the monitoring of electronic online communication data and national Collective agreement n° 68 of 16 June 1998 on the protection of the privacy of workers with regard to camera surveillance at work.

The Belgian parliament is still working on the legislation in order to fully comply with the new EU legislation on privacy (Regulation 2016/679 and Directive 2016/680) which replaced the old Directive 95/46/EG. The government introduced a draft act ('projet de loi') of 18 June 2018 in the parliament (Chambre des répresentants 2017-18, n° 54-3126), which includes the adaptation of the Act of 8 December 1992. However, it is not likely that the GDPR will have a major impact on the existing collective agreements regulation the monitoring of online communication data and video surveillance at the work place.

2. Is it mandatory for the company to have a code of conduct or an internal policy regulating the use technological devices? If not, what is the procedure that the company must follow to regulate the use of technological devices?

In Belgium it is not mandatory for the company to have a code of conduct or an internal policy regulating the use technological devices. However, a smart employer should set up such rules in the work regulations. First, this is the case because the abuse of electronic devices could lead to disciplinary sanctions. Article 6, 6° of the Act of 8 April 1965 on the instalment of work regulations states that the disciplinary sanctions, the amount and the purpose of the penalties, and the infractions which the sanctions want to punish should be included in the work regulations (in a limitative way). So, without such a code of conduct in the work regulations it will be hard to take disciplinary measures against employees who abuse the electronic devices. The inclusion in the work regulations of those sanctions also follows from the individual information obligation on the monitoring of electronic communication in Collective agreement n° 81 (see question 3). Second, the employer should introduce a company code of conduct on the use of electronic devices in the work regulations because in case of a dismissal (with urgent cause), the judges will also take into account the fact that it was clearly provided in the work regulations that certain abuses of electronic devices can lead to a dismissal with urgent cause. This is an important element for a judge to consider whether the dismissal was legitimate.

The Act of 8 April 1965 includes the procedure to install work regulations. The work regulations shall be drawn up in consultation between the employer and his employees.
If a works council exists, it shall draw up the regulations and any amendments thereto. The regulations shall enter into force 15 days after the agreement in the works council.

If no agreement is reached in the works council, the chairman will report this to the inspector of the Federal Inspectorate of Social Laws, who will try to reconcile the various positions within 30 days. If that inspector fails to reconcile the positions, the dispute shall be submitted to the competent sectoral joint committee by the chairman of the works council.

In the absence of a works council, the employer shall prepare and amend the draft or amendments to the work regulations and post it on a visible place at the work place. For 15 days from this posting, the workers may make comments in a register kept at their disposal for this purpose, or they may communicate these comments directly to the inspector of the Inspectorate of Social Laws. Once this period has elapsed, the employer shall send the draft and the register to the inspector. If no comments have been made, the work rules shall enter into force on the 15th day following the day of posting.

Where observations have been made, the inspector of the Inspectorate of Social Laws shall endeavour to reconcile the divergent views within 30 days of the draft and the register being sent to him. If the inspector is unable to reconcile the different views, he shall immediately send a copy of the record of non-alignment to the chairman of the Joint Committee responsible.

It is clear that in Belgium, an employer cannot simply unilaterally install the work regulations as the strict procedure has to be followed in order for the work regulations to be valid.

3. In which cases and under what conditions is it possible to access and monitor employees' personal communications through the company's technological devices (e-mail, instant messaging, etc.)?

For the employees' personal communications through the company's technological devices the Belgian National Labour Council (national social partners) has closed the Collective Agreement n° 81 of 26 April 2002 on the protection of the privacy of employees with regard to the monitoring of electronic online communication data. This collective agreement wants to clarify the general principles of privacy for the factual situation of employers and employees, while taking into account the importance of the proper functioning of the undertaking. Collective agreement n° 81 offers protection to electronic communication data in a broad sense. It does not matter on which device the data are transmitted by the employee.

Article 4 and following of the collective agreement set out the conditions for the monitoring of online communication data. There are some principles that need to be

respected by the monitoring. These principles originate from Act of 8 December 1992 on the processing of personal data. First, the principle of purpose (‘finaliteit’/finality/legitimate aim) means that the monitoring can only be done if it has one or more of the following purposes:

1. The prevention of wrongful or defamatory acts, acts contrary to good morals or which may harm the dignity of another person.
2. The protection of the economic, commercial and financial interests of the company, which are confidential, as well as the prevention of conflicting practices (with the interests of the company).
3. The security and/or the proper technical functioning of the company's IT network systems, including the control of the costs involved and the physical protection of the company's installations.
4. To comply in good faith with the principles and rules applicable in the company for the use of online technologies.

The employer has to describe and clarify the purposes of the monitoring.

Second, there is the principle of proportionality. In principle, the control of electronic online communication data should not lead to an intrusion in the privacy of the employee.

If, however, the control does result in an intrusion of the privacy of the employee, this intrusion must be kept to a minimum. This means: only the electronic online communication data necessary for control purposes, i.e. data which, given the legitimate purpose of the control, have the least intrusive effect on the privacy of the employee. More specifically, in the first place the purpose of the monitoring should be restricted to the collection of the global data of the company.

Third, there is a condition of transparency and information. The employer who wants to install a monitoring system should inform the works council in advance. If there is no works council he should inform the Committee on the Prevention and Portection at Work, if there is no such committee he should inform the workers representatives (or the employees themselves if there are no representatives). This collective information obligation relates to:

- The control policy and the prerogatives of the employer and supervisory staff;
- The objective(s) pursued;
- Whether or not personal data are stored, the place and duration of storage;
- The permanent character of the control.

Next, the employer shall also inform (in advance) the individual workers concerned of all aspects of the control. The information must be effective, understandable and up to date. The choice of the information medium is left to the employer. This individual information obligation relates to:

- The use of devices made available to the worker for the performance of his work, including restrictions on use in the context of the job;
- The rights, obligations and obligations of employees and, where applicable, prohibitions on using the company's electronic means of communication online;
- The sanctions provided for in the work regulations for failure to comply with them.

The principle of proportionality ensures that (in a first phase) the monitoring system only controls the global data of the company. However, it is possible to individualise the monitoring and thus to see which data can be linked to specific employees. The employer can only individualise the electronic online communication data in good faith and in accordance with the objective(s) pursued by this verification (principle of purpose). Where the electronic on-line communication data collected are processed for purposes other than those for which the global check was installed, the employer must ensure that this is compatible with the original purpose and take all measures necessary to avoid any misinterpretation. Next, the employer may not individualise the electronic online communication data obtained during a check in a way incompatible with the mentioned objective(s), and only electronic on-line communication data necessary for the control objective(s) may be individualised (principle of proportionality). The data should be adequate, relevant and not excessive in relation to those objectives.

There are two forms of individualisation: direct and indirect. Direct individualisation is only allowed for the purpose of the first three purposes (1. Prevention of wrongful or defamatory acts, or contrary to good morals; 2. Protection of the interests of the company; 3. Protection of the IT-network). In this case the employer can simply link the data of the global data of the company to an individual employee. However, if the monitoring happened merely for the purpose of complying in good faith with the principles and rules applicable in the company for the use of online technologies, direct individualisation is not allowed as there should be a prior information phase. In this information phase the workers are informed in a clear and comprehensible manner of the existence of the irregularity and of the fact that the electronic online communication data will be individualised when such an irregularity is detected again.

An employee who is held responsible for an irregularity in the use of electronic means of on-line communication when applying the indirect individualisation procedure should be invited by the employer for a conversation. This interview takes place before

any decision or evaluation that may affect the employee individually. The purpose of the interview is to give the employee the opportunity to explain his objections with regard to the intended decision or evaluation and to justify the use of the electronic means of on-line communication made available to him.

Finally, the rules of the collective agreement n° 81 are not applicable if the employer accidentally stumbles upon an irregularity in the use of electronic means of on-line communication. The collective agreement also states that the individualisation procedure is not necessary if the information is without any doubt purely of a professional nature. However, this exclusion is vague and difficult to use in practice. Therefore, certain opinions in the Belgian lower case law state that the exclusion is in conflict with the privacy right in article 8 ECHR (e.g. Labour court of appeal Antwerp, 15 December 2004, *Soc. Kron* 2006, n° 3, 146).

4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?

Again, it was the Belgian National Labour Council who laid down the rules for camera surveillance at the work place in Collective agreement n° 68 of 16 June 1998. The provisions of this collective agreement are rather similar to collective agreement n° 81 as they both are specifications of the general Ac of 8 December 1992 on the processing of personal data. The valid purposes for camera surveillance are limited and the proportionality principle is also applicable. The valid purposes (which the employer needs to clarify) are:

1. Health and safety.
2. The protection of the company's assets.
3. The control of the production process. The control of the production process can concern both the machinery and the employees. Where the checks concern machinery only, they are intended to check that the machinery is working properly. Where checks concern workers, they shall cover the evaluation and improvement of the work organisation.
4. The control of the work of the employee. The pursuit of this objective must not result in decisions and assessments that are solely based by the employer on data obtained through camera surveillance.

The National Labour Council clarifies that the rules for camera surveillance are not applicable when the cameras are used for education purposes. It also states that secret/hidden video surveillance is subjected to the procedural rules and conditions of

the criminal/penal procedural code (see question 5) and that in case of the use of purpose number 4 it will not be the objective to constantly film an employee.

Collective agreement n° 68 distinguishes continuous and temporary camera surveillance. If the purpose of the surveillance is the health and safety, the protection of the company's assets or the control of the production process which only concerns the machinery, the recording can be continuous. However, if the purpose is the control of the production process concerning workers or the control of the worker's work, the camera surveillance can only be temporary, i.e. if the cameras or cameras are either temporarily or permanently installed but only function for one or more periods.

In light of the principle of proportionality, the employer may not use the camera surveillance in a way that is incompatible with the expressly defined purpose. Camera surveillance should be sufficient, relevant and not excessive for this purpose. In principle, camera surveillance should not interfere with the privacy of employees. If the camera surveillance does lead to an intrusion in the privacy of the employee, the interference must be kept to a minimum.

Next, the employer has information and consultation duties. Prior to and at the start of the camera surveillance the employer has to inform the works council (or its replacements if there is no works council) about every aspect of the surveillance. If the purpose of camera surveillance is to monitor work performance, and in particular to measure and check with a view to determining the wages or salary or has implications with regard to the rights and obligations of supervisory staff, the employer shall provide this information in the work regulations. At the start of the camera surveillance, the employer must provide information to the employees concerned. The information to be provided must include at least the following aspects of camera surveillance:

- The intended purpose;
- Whether or not the image data are retained;
- The number and position of the camera(s);
- The period(s) of operation of the camera(s) concerned.

The works council (or the Committee on the Prevention and Protection at Work) can, in case the camera surveillance seems to have an impact on the privacy of one or more employees, do an examination of the measures to be taken to minimalise the impact. If camera surveillance is introduced in order to control of the production process concerning workers or to control of the worker's work and in the absence of a works council or a committee for prevention and protection at work, the examination shall be carried out in consultation with the employer and the trade union delegation.

The employer must process the images obtained in good faith and in accordance with their purpose. If the images obtained are used for purposes other than those for which camera surveillance is carried out, the employer must ensure that this use is compatible with the original purpose and that all measures are taken to avoid misinterpretation.

5. Under what circumstances is it possible to install hidden cameras to control work activity? In particular, is its installation only possible when the company suspects that a criminal offense has been committed or also when there are signs of a breach of contract?

The use of hidden cameras to monitor employees is an infraction of Collective agreement n° 68 as the employer is obliged to inform the employees concerned about the number and the position of the camera(s) (see question 4). In addition, the National Labour Council has clarified that the use of hidden or secret cameras is subjected to the conditions set out in the criminal procedural code. In any case, the general Act of 1992 on the processing of personal data requires that employees are informed in advance about the processing of personal data during camera surveillance. There is no exception to this obligation to provide information. Moreover the ECtHR case of *López Ribalda et al. v. Spain* (cases 1874/13 and 8567/13) of 9 January 2018 made it clear that a hidden camera is an intrusion of the privacy right of the employee.

However, as the evidence of the hidden camera will be illegal, this does not necessarily mean that the evidence cannot be used in court (see question 7).

6. In what cases is it possible to install geolocation systems (GPS) to control work activity?

Although several attempts have been made, the Belgian legislator has not introduced a specific legislation concerning the use of geolocation and GPS-systems with regard to the tracing of employees. It could be argued that a geolocation system transmits online electronic communication data and that therefore the provisions of Collective agreement n° 81 (see question 3) should apply. However, in the first place, as confirmed by a case of 14 April 2017 of the labour court of appeal of Ghent, one should mainly look at the provisions of the general Act of 8 December 1992 on the processing of personal data.

The most important conditions are set out in article 4 of the Act of 8 December 1992. These conditions were/are/will not be influenced by the GDPR. It states that personal data must be provided:

1. To be processed fairly and lawfully.

2. To be obtained for specified, explicit and legitimate purposes and not to be further processed in a way that is incompatible with those purposes, taking into account all relevant factors, in particular the reasonable expectations of the data subject and the applicable legal and regulatory provisions.
3. To be adequate, relevant and not excessive in relation to the purposes for which they are obtained or for which they are further processed.
4. To be accurate and, if necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
5. In a form which makes it possible to identify the data subjects, to be kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

In addition, article 5 states that personal data may only be processed in one of the following cases:

a. Where the data subject has given his or her unambiguous consent.
b. Processing is necessary for the performance of a contract to which the data subject is party or for the taking of measures prior to the conclusion of such a contract which were taken at the request of the data subject.
c. Processing is necessary for compliance with an obligation to which the controller is subject by or pursuant to a law, regulation or ordinance.
d. Processing is necessary in order to safeguard the vital interests of the data subject.
e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority and has been entrusted to the controller or to a third party to whom the data are disclosed.
f. Processing is necessary for the purposes of the legitimate interest of the controller or of the third party to whom the data are disclosed, provided that the interest or the fundamental rights and freedoms of the data subject claiming protection under this Act are not overridden.

Next, the Act of 8 December 1992 provides a duty of information to the controller about all the aspects of the processing of data (which data, where is the data kept, for how long, by who, who has access to the data…) and it gives some other rights to the subject of the processing, e.g. to correct the data.

In the case of 17 April 2017 before the labour court of appeal of Ghent (mentioned above) the condition of proportionality was not met, as the employer did not limit the

tracing of the employee to the work hours, but in fact also controlled the location of the employee in her free time. This resulted in the intrusion of the right to privacy.

7. In the event that the company fires an employee in breach of the conditions regarding control communications by e-mail or installation of video surveillance systems, what would be the qualification of the dismissal and what administrative sanctions could be derived?

Usually, an employer would use the obtained data (or recording) to dismiss an employee with urgent cause. This means that the employer can dismiss an employee immediately without any compensation or notice period. If the 'illegally' obtained data is the only evidence on which the dismissal is based, this would form a major problem for the case of the employer. According to article 35 of Act of 3 July 1978 on labour contracts, the employer has to prove that the cause of the dismissal was of such a severe nature that every future cooperation between the employer and employee would be impossible. In theory the employer cannot demonstrate this with illegally obtained evidence as the judge will not take this evidence into consideration (in theory, see further) and therefore the 'urgent cause' will not be proved and the dismissal will be unjust. In this case the employer will have to pay the normal dismissal compensation plus certain damages. There are no additional administrative sanctions as the sanction is the illegality of the information itself.

However, it is not because data or evidence is obtained illegally or in conflict with the legal provisions, which it in practice automatically cannot be taken into consideration by the judge. The case law in Belgium is in a longstanding evolving discussion about this issue. The Cour de Cassation (Highest Court) has developed the so-called Antigoon-doctrine (Cass. 14 October 2003) which states that illegal evidence can be used nonetheless, if three conditions are met:

1. The provision that was ignored by the employer is not prescribed under penalty of nullity.
2. The unlawfulness does not affect the right to a fair trial.
3. The unlawfulness does not affect the reliability of the evidence.

It is important to know that the provisions of the Act of 8 December 1992, Collective agreement n° 68 and Collective agreement n°81 are not prescribed by nullity. Some are of the opinion that therefore the collective agreement are merely theoretical rules with almost no enforceability. However, it is still not certain whether the Antigoon-doctrine can be applied in purely private labour law cases. The Cour de Cassation has so far applied the doctrine in criminal cases (including in labour cases in which by example

the employee was dismissed because he had stolen something of the employer, Cass. 2 March 2005, *Le Chocolatier Manon*) and social security cases (in which the state is a party). But the Cour de Cassation has not yet applied it in purely private labour cases between employers and employees (two private actors). The majority of the lower case law started to apply the Antigoon-doctrine in labour cases after the application of the Cour de Cassation in a social security case on 10 March 2008. But some courts, like the Labour court of appeal of Brussels on 7 February 2013, have refused the application in labour cases. In the meanwhile, the ECtHR has approved the use of the Antigoon-doctrine in the case of *Lee Davis v. Belgium* of 28 July 2008, with regard to the right to privacy in article 8 ECHR. On one hand, article 8 ECHR is also applicable in labour law cases, on the other hand the *Lee Davis* case was also a purely criminal case and the ECtHR did not specifically mention the application of the Antigoon-doctrine in labour law cases. Therefore, the discussion will only be settled when such a purely private labour case will appear before the Cour de Cassation (or the ECtHR) or if new legislation is introduced.

Unlike the collective agreements, the Act of 8 December 1992 on the processing of personal data seems to deliver the means to override the Antigoon-doctrine. According to article 14 of this Act, a person who was subjected to the processing of his personal data can demand the correction or the deletion of the data or the prohibition to use the data in case the data where obtained in breach of the provisions of the Act. It will be the President of the (general) tribunal of first instance who will need to handle this claim. If the claim is granted it is logical that the obtained data cannot be used in a later case, e.g. a dismissal case at the labour tribunal. In this case, Antigoon cannot be applied.

8. What personal data can be collected and processed in the framework of the employment relationship? In particular, is employees' consent necessary? In what cases is it not necessary?

If one looks at article 5 of the Act of 8 December 1992 on the processing of personal data it is clear that the employees consent is not necessary if other purposes for the processing of the data are used. This i.a. could be the case when the processing is necessary for the performance of a contract to which the data subject is party (which is a similar provision as article 6.1 b of the GDPR) or when the processing is necessary for the purposes of the legitimate interest of the controller (the employer). In general, consent of employees will not be necessary (and no provision demands a written consent). Nonetheless, as seen, there are certain information obligations of the employer towards the employees. Most important is the proportionality principle (to be found in all the Belgian provisions on privacy) which means that the data have to be adequate, relevant and not excessive in relation to the purposes for which they are obtained or for

which they are further processed. The employer therefore will have to take care that he is not collecting irrelevant data. Furthermore, in the case of online electronic communication the employer has to take into account the specifics of Collective agreement n° 81.

Finally, it is important to notice that the Act of 8 December 1992 also in principle prohibits the collection of certain specific information. First, this is the case for personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, and the processing of personal data concerning sex life. However, the collection of this data is i.a. accepted if the employee/subjected person gives consent or where the processing is necessary for the purposes of carrying out the specific obligations and rights of the controller in relation to labour law (i.e. only when it is really relevant to comply with labour law). This prohibition is of course in force to prevent discrimination. Second, there is also a prohibition (with similar exceptions) for the collection of data regarding the health of a person. An employer can only collect health data of an employee when the health and safety regulations demand this (and even if so, the medical information will be handled by a professional (prevention advisor/company doctor) who has to regard his professional/medical secrecy.

9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?

As seen, Collective agreement n° 68 on camera surveillance not only obliges the employer to inform (in advance) the works council (or workers representatives) on the instalment of a system of camera surveillance, but the works council (or workers representatives) also should be consulted on the taking of necessary measures if this camera surveillance appears to have an impact on the privacy of employees. Furthermore, the works council or the committee for prevention and protection at work must also regularly evaluate the monitoring systems used and make proposals for revision in the light of technological developments.

Also, Collective agreement n° 81 foresees an information obligation for the employer to the works council (or Committee for Prevention and Protection at Work or the workers representatives) when he wants to install a system of electronic online communication data (about all aspects of the system). In addition, the control systems put in place are regularly evaluated, as appropriate in the Works Council, the Committee for Prevention and Protection at Work or with the trade union delegation, with a view to proposing ways of adapting them to technological developments.

The Act of 8 December 1992 does not foresee in similar collective information obligations.

10. Is there a right to disconnect from technological devices outside working time? In this case, should the company define the extension and limits of this right jointly with the workers' representatives or can it do so through an internal policy?

The Belgian legislator has introduced a sort of 'right to disconnect' in the Act of 26 March 2018 on strengthening economic growth and social cohesion. However, the legal provisions are merely supporting the start of a debate between the employer and worker representatives and do not contain any real rights or obligations. Articles 15 to 17 of this Act provide that the employer will organise a consultation on disconnection of work and the use of digital means of communication in the Committee for Prevention and Protection at Work. This concerns in particular the company policy on the accessibility of employees (applicable only to the private sector) outside their normal working hours by means of, for example, mobile phones, smartphones or computers. The purpose of the consultation is to ensure respect for workers' rest periods, annual leave and other leave entitlements and to safeguard the work-life balance. Consultation must take place at regular intervals and whenever requested by the employees' representatives in the Committee. On the basis of this consultation, the committee can formulate proposals and issue opinions to the employer. The agreements arising from this can be included in the work regulations or included in a collective agreement.

LABOR IMPACT OF TECHNOLOGICAL DEVICES IN FRANCE

Marie Morin
Student, master 2 DPSE, University Paris 1
Trainee, Gide Loyrette Nouel, Paris

Francis Kessler
Prof. Sorbonne Law School, University Paris 1
Attorney, Senior counsel, Gide Loyrette Nouel, Paris

Introduction

Computers, smartphones, CCTV cameras, GPS systems, and biometric devices: Technology is omnipresent in the workplace. As technology continues to develop, employees' personal data is more regularly collected and potential threats to their privacy become more commonplace. Four different aspects of the implications of technological changes for work and employment can be differentiated: tasks and occupations, conditions of work, conditions of employment and industrial relations[1].

The control of the employees' activity, which results from the employer's management powers and the employees' subordination, increased with the digital revolution and the use of technological devices at work. Indeed, since 1990, technological devices and their use at work constantly increased. In 2013, 71,1% of the employees used hardware or a network for professional purposes[2]. The emergence of these technological devices changed the scope of the employer's control. Today, the employer doest not only control physically his employees' activity but he can control their activity through all these technological devices such as computers or geolocation systems.

As software allow invisible control on computers, the employer can collect many personal datas on employees, which is likely to violate their fundamental rights and freedoms such as privacy and the secrecy of communication. The Court of cassation ensures these fundamental rights, considering that "*the employee has the right, even at the time and place of work, to the respect of his privacy, which implies in particular the secrecy of communication*"[3].

[1] FERNANDEZ-MACIAS E., Automation, digitalisation and platforms: Implications for work and employment, *Eurofound*, 24 May 2018.
[2] DARES analysis, June 2018, n° 029.
[3] Labour Division of the Court of cassation, 2 October 2001, n° 99-42.942.

The use of mobile technological devices such as a mobile phone and a profesional messaging is also related to an important workload which is likely to impinge on privacy[4]. To remedy this impingement, law n°2016-1088 of 8 August 2016 introduced into the French labour code the right to disconnect from technological devices outside working time in the French legal system, in order to ensure the employees the respect of their rest times, leaves and personal and family life[5].

The impact of the use of social media in the workplace has regularly given rise to controversies and debates as how this subject is to be handled by a company's management. The current state of employment law is still not entirely settled in this respect.

1. Is there any regulation in your country regarding employees' use of technological devices in the company?

In the French legal system, there is no specific regulation on employees' use of the technological devices put at their disposal to render services.

As the employer has management powers, he can control his employees' activities during working time. Unlike the employees' use of technological devices in the company, the employer's control is regulated by the French legal system and case law.

The implementation of technological devices to control the employees' activity must respect the following conditions to be lawful:

- Employees must be informed individually[6].
- The workers representatives the Social and Economic Committee must be informed and consulted[7].
- The device must be declared to the National Commission for Data Processing and Liberties.

On top of that, French case law applies the general principle of article L. 1121-1 of the French Labour Code which states that "[n]*o one can limit the people's rights and the individual and collective freedoms in a way which would not be justified by the nature of the task to perform and proportionate to the intended aim*" to the control of the use of technological devices in the company.

[4] DARES analysis, June 2018, n° 029.
[5] Law n°2016-1088, 8 August 2016, article 55.
[6] French Labour Code, article L. 1222-4.
[7] French Labour Code, article L. 2312-38.

French case law takes into account fundamental rights such as privacy[8] and secrecy of communication[9] to determine wheter or not the monitoring of employee's use of technological devices in the company is lawful.

2. Is it mandatory for the company to have a code of conduct or an internal policy regulating the use technological devices? If not, what is the procedure that the company must follow to regulate the use of technological devices?

In France, as we have seen, there is no specific regulation on the use by employees of technological devices in the company and, therefore, the French Labor Law does not include a legal obligation to have a code of conduct or an internal policy on the use of these devices.

However, the employer can limit or forbid the use of the technological devices in the company in the rules of procedure, a memorandum or in an IT charter.

In companies employing at least 20 employees, the implementation of a rules of procedure is compulsory[10]. In this case, the employer can provide the conditions of the use of the technological devices in it.

In companies employing less than 20 employees, the employer can transmit the rules related to the use of the technological devices in the company in a memorandum.

Some companies settle these rules in an IT charter or a code of conduct. The IT charter allows the employer to oversee and secure the use of technological devices in the company and to inform the employees of their rights and obligations as users of these technological devices.

In companies employing at least 20 employees, the IT charter is considered as a rules of procedure's appendix when it provides some obligations, prohibitions and disciplinary sanctions[11]. The IT charter is enfoceable against employees when it is established after the information and consultation of the staff representatives, attached to the rules of procedure and when employees are informed of it[12].

The IT charter can:

[8] Labour Division of the Court of cassation, 2 October 2001, n° 99-42.942.
[9] Labour Division of the Court of cassation, 26 January 2016, n°14-15.360.
[10] French Labour Code, article L. 1311-2.
[11] Court of appeal of Versailles, 24 January 2008, n°07-1659.
[12] Court of appeal of Besançon, 21 September 2004, n°03-1807.

- Ensure the company's computer network security (such as the prohibition to download software or to tell other employees their username and password);
- Prevent the employees' abusive use of the technological devices (such as the limitation of the use of the personal messaging and social networks);
- Prevent behaviours which do not respect law or ethic (no offensive and discriminatory messages, no messages damaging the company's image);
- Provide the modalities of the use of the intranet and the company's messaging for the staff representatives and union representatives.

The National Commission for Data Processing and Liberties advises that the IT charter provides a reminder of the rules related to data protection, the scope of application of the charter, the modalities of the use of technological devices, the responsabilities and the sanctions in case of disrespect of the charter[13].

The National Commission for Data Processing and Liberties discourages the total prohibition of the use of the technological devices for personal reasons, considering that this prohibition is not reasonnable in a society based on information and communication[14].

The employer can authorize the reasonnable use of the technological devices for personal reasons. This reasonable use is not clearly defined by the French case law. The repeated or systematic use, time spent on technological devices instead of working and the fact that the employer already warned the employee are the most important criteria to define the abusive use. For example, using the technological devices 41 hours per month for personal reasons is considered as a gross misconduct[15].
In the absence of a rules of procedure, memorandum or IT charter on the use of technological devices, the French case law considers that the employees must use them in a reasonable way. If the use is abusive, the dismissal of the employee can be based on a gross misconduct[16].

[13] Guide of the National Commission for Data Processing and Liberties on personal data security, 2018, p. 7.
[14] National Commission for Data Processing and Liberties's report, 28 March 2001.
[15] Labour Division of the Court of cassation, 18 March 2009, n°07-44.247.
[16] Labour Division of the Court of cassation, 16 May 2007, n°05-43.455.

3. In which cases and under what conditions is it possible to access and monitor employees' personal communications through the company's technological devices (e-mail, instant messaging, etc.)?

The French Court of cassation established conditions that the employer must respect to access and monitor employees' personal communications through the company's technological devices such as e-mail and instant messaging.

Documents on the company's technological devices are presumed to be professional, except if the employee identifies them as personal. If it is not the case, the employer can open the documents when the employee is not present[17].

The following documents are presumed professional :

- Files with the employee's initials[18];
- The file entitled "my documents"[19]
- The employee's USB stick connected to the company's computer[20];
- Text messages sent or received on the company's mobile phone, except if the employee identifies them as personal[21].

The employer can open these documents but he cannot use them in court or to sanction the employee if they are part of the employee's private life[22].

Concerning the contents identified as personal, the Court of cassation used to consider that the employer could not open them. Indeed, "*the employee has the right, even at the time and place of work, to the respect of his privacy, which implies in particular the secrecy of communication*"[23]. The employer cannot open the personal messages that the employee sent and received on the company's technological devices, even if he forbids the personal use of these technological devices. However, the Court of cassation limited this case law. France's highest court ("Cour de cassation") ruled 26 June 2012 in *Monsieur X v. YBC Helpevia* that a company's internal rules may limit an employer's access to employee emails.

[17] Labour Division of the Court of cassation, 21 October 2009, n°07-43.877.
[18] Labour Division of the Court of cassation, 21 October 2009, n°07-43.877.
[19] Labour Division of the Court of cassation, 10 May 2012, n°11-13.884.
[20] Labour Division of the Court of cassation, 12 February 2013, n°11-28.649.
[21] Commercial Division of the Court of cassation, 10 February 2015, n°13-14.779.
[22] Labour Division of the Court of cassation, 5 July 2011, n°10-17.284; Labour Division of the Court of cassation, 18 October 2011, n°10-25.706.
[23] Labour Division of the Court of cassation, 2 October 2001, n° 99-42.942.

French case-law has traditionally held that employees have a right to privacy at their workplace and that an employer cannot search an employee's personal files stored on a work computer without breaching the employee's right to privacy (*Nikon France v. Onof*). As a result, case-law allows a French employer to search an employee's professional messages, but prohibits any access to his/her personal files and messages that are specifically identified and marked "personal". The current decision has, however, narrowed the employer's ability to search an employee's professional files if the internal rules of the company place restrictions on the search.

The Court of cassation now considers that the employer can open the personal documents of the employee if the employee is here or duly summoned[24].

A particular risk or event such as unfair competition can also justify the opening of a personal document as a mail[25]. In this case, the employer can ask the judge to pronounce some investigation measures in order to maintain or establish, before trial, the evidence of the facts that may be necessary to the solution of a future dispute[26]. This procedure can be claimed if there exist a legitimate reason and that the measures are necessary to the protection of the rights of the party who asks them[27].

The Court of cassation considered that the message, sent by the employee at workplace and during work time, related to his professional activity, is not personal and can be used in a disciplinary procedure[28]. Mails between two employees related to their professional activities are not personal and can also be used in a disciplinary procedure[29].

However, mails from the personnal messaging of the employee, separate from the professional messagining, cannot be used in court as they violate the secrecy of communication[30].

4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?

The installation of permanent video surveillance systems to control work activity in a public place (banks, cinemas, shops) must be authorized beforehand by the prefecture.

[24] Labour Division of the Court of cassation, 17 May 2005, n°03-40.017.
[25] Labour Division of the Court of cassation, 17 June 2009, n°07-20.740.
[26] French Civil Procedure Code, article 145.
[27] Labour Division of the Court of cassation, 23 May 2007, n° 05-17.818.
[28] Labour Division of the Court of cassation, 2 February 2011, n°09-72.313.
[29] Labour Division of the Court of cassation, 2 February 2011, n°09-72.449.
[30] Labour Division of the Court of cassation, 26 January 2016, n°14-15.360.

If the video surveillance is installed in a private place, the device must be declared to the National Commission for Data Processing and Liberties if the images are registered. However, the device must be authorized by the National Commission for Data Processing and Liberties if the video surveillance also provides a face recognition, as it is a biometric procedure.

The employees' video surveillance must respect the proportionnality principle[31]. The aim of this device cannot only be the control of one particular employee or group of employees. To determine whether or not the device is proportionnate, the Court of cassation takes into consideration the number, the place, the direction and the nature of the tasks of the employees. If the video surveillance also records the sound, the National Commission for Data Processing and Liberties considers that the device is disproportionnate[32].

Every employee must be informed individually of the installation of video surveillance and its purpose[33] and the Social and Economic Committee must be informed and consulted on the implementation of the video surveillance[34].

Only entitled people can watch the images (such as the security manager)[35].

The installation of a video surveillance in order to control a place in which employees do not work such as a warehouse does not have to respect the previous conditions. If an employee goes in this place, the employer can use the video surveillance images to prove the facts reproached to the employee (theft or damage to property)[36].

5. Under what circumstances is it possible to install hidden cameras to control work activity? In particular, is its installation only possible when the company suspects that a criminal offense has been committed or also when there are signs of a breach of contract?

The employee must be individually informed of the installation of a video surveillance[37]. If the employee is not informed, the device is not legitimate and the

[31] Council of State, 18 November 2015, n°371196.

[32] National Commission for Data Processing and Liberties Guide for employers and employees, 2010.

[33] French Labour Code, article L. 1222-4; Labour D**i**vision of the Court of cassation, 20 November 1991, n°88-43.120.

[34] French Labour Code, article L. 2312-38.

[35] National Commission for Data Processing and Liberties Guide for employers and employees, 2010.

[36] Labour Division of the Court of cassation, 31 January 2001, n°98-44.290 ; Labour Division of the Court of cassation, 19 April 2005, n°02-46. 295.

[37] French Labour Code, article L. 1222-4.

evidence is inadmissible in court. Judges cannot take into account the recording of images or sounds made by hidden cameras[38]. The French Court of cassation, as the European Court of Human Rights (ECHR), considers that hidden video surveillance violates the employees' privacy[39].

6. In what cases is it possible to install geolocation systems (GPS) to control work activity?

Under French legal system, a geolocation system (GPS) can be installed to control work activity after the individual information of the employees[40], the information and consultation of the Social and Economic Committee[41] and after the declaration to the National Commission for Data Processing and Liberties.

Datas resulting from gelocation systems must have the following purposes:

- The respect of a legal obligation needing the use of a geolocation system because of the kind of transport or the nature of the goods transported;
- The tracking and the invoicing of people or goods transport and the justification of the service to a client;
- The safety and security of the employee, goods or vehicles, in particular to prevent the theft of the vehicle;
- A better allocation of ressources for the services to perform in different places, in particular for urgent interventions;
- The control of the respect of the using rules of the vehicles.

A geolocation system must be used for the purposes declared to the National Commission for Data Processing and Liberties[42].

The geolocation system can control working time when this controle is not posible by another mean[43]. This control of the working time is not justified when the employee is free to organize his work[44].

The data manager can collect[45] :

- The employee identification (name, surname, professional adresss, license plate);

[38] Labour Division of the Court of cassation, 20 November 1991, n°88-43.120.
[39] ECHR, 9 January 2018, n°1874/13.
[40] French Labour Code, article L. 1222-4.
[41] French Labour Code, article L. 2312-38.
[42] Labour Division of the Court of cassation, 3 November 2011, n°10-18.036.
[43] Council of State, 15 December 2017, n°403776.
[44] Labour Division of the Court of cassation, 17 December 2014, n°13-23.645.
[45] National Commission for Data Processing and Liberties, 4 June 2015, n°2015-165, article 3.

- Datas related to the employees' travels;
- Complementary datas related to the use of the vehicle (speed, number of kilometers, number of stops);
- Dates and hours of the use of the geolocation system during working time.

The employees must have the possibility to turn off the geolocation system, in particular after working hours or during break times[46].

In principle, datas collected cannot be saved during more tan two months. However, they can be saved during one year when they are used in order to prove the interventions, if the evidence cannot be obtained in another way. When working time cannot be controlled in another way, datas can be saved during five years[47].

7. In the event that the company fires an employee in breach of the conditions regarding control communications by e-mail or installation of video surveillance systems, what would be the qualification of the dismissal and what administrative sanctions could be derived?

In France, if the employer breaches the conditions regarding control communications by e-mail or installation of video surveillance systems, the evidence collected is inadmissible in court. Indeed, article 9 of the French Civil Procedure Code states that "*each party must prove, in accordance with law, the facts necessary to the success of the claim*".

As the evidence is not admissible in court, the dismissal pronounced on this base does not rely on a real and serious ground if the employer does not have other evidence.

Indeed, the Court of cassation considered that information collected before the declaration to the National Commission for Data Processing and Liberties were unlawful means of evidence, inadmisible in court[48]. The dismissal of an employee did not rely on a real and serious ground when she was dismissed because of her abusive use of her profesional messaging for personal reasons and that the modalities of the control were not declared to the National Commission for Data Processing and Liberties.

In another case, the Court of cassation considered that "*if the employer has the right to control the activity of his staff during hours of work, he cannot* (…) *implement a control*

[46] National Commission for Data Processing and Liberties, 4 June 2015, n°2015-165, article 5.
[47] National Commission for Data Processing and Liberties, 4 June 2015, n°2015-165, article 5.
[48] Labour Division of the Court of cassation, 8 October 2014, n°13-14.991.

without informing the employees beforehand"[49]. In this case, the employer asked to a surveillance company to control the use of beverage and food dispensers by the employees, who were not informed of this control. The employer dismissed several employees on the basis of a gross misconduct. As their dismissal was only based on the surveillance company's report, the dismissals did not rely on a real and serious ground.

Furthermore, the employee's refusal to use a technological device such as an electronic badge does not justify a dismissal when this control was declared to the National Commission for Data Processing and Liberties only two years after his dismissal. The dismissal does not rely on a real and serious ground[50].

Since Ordinance n°2017-1387 of 22 September 2017, when the dismissal does not rely on a real and serious ground, the employee is entitled to a compensation according to a scale depending of his seniority[51].

A control device which does not respect the conditions required by the law (employees' individual information, information and consultation of the Social and Economic Committee, declaration to the National Commission for Data Processing and Liberties) can constitute a manifestly unlawful disturbance justifying its suspension by the judge[52].

Several administrative sanctions can be pronounced if the employer fires an employee in breach of the conditions of the control. First, the National Commission for Data Processing and Liberties can suspend a video surveillance system which use was disproportionate and violated the employees' right to privacy regardless several reminders[53].

Then, the National Commission for Data Processing and Liberties can pronounce a financial penalty of 20 million euros or 4% of the annual sales revenue of the company in case of disrespect of the conditions of the employees' control[54].

The employer who disrespects the conditions of the employees' control can also be condamned on a penal basis, in particular in case of violation of privacy[55] or secrecy of communications[56].

---

[49] Labour Division of the Court of cassation, 15 May 2001, n°99-42.219.
[50] Labour Division of the Court of cassation, 6 April 2004, n°07-35.227.
[51] French Labour Code, article L. 1235-3.
[52] Labour Division of the Court of cassation, 10 April 2008, n°06-45.741.
[53] Law n°76-17, 6 January 1978, article 45; National Commission for Data Processing and Liberties, n°2010-112, 22 April 2010.
[54] Law n°76-17, 6 January 1978, article 45.
[55] French Penal Code, article 226-1.

8. What personal data can be collected and processed in the framework of the employment relationship? In particular, is employees' consent necessary? In what cases is it not necessary?

Through the technological devices, the employer have access to his employees' personal datas such as their name, surname, date of birth, social security number, adress, mobile phone number, pictures and videos.

According to law n°78-17 of 6 January 1978 modified by the entry into force of the General Data Protection Regulation 2016/679 of 27 April 2016, personal datas can be collected if :

- They are collected in a loyal and lawful way for determined, explicit and legitimate purposes;
- They must be adequate, relevant and not abusive regarding these purposes;
- They must be exact, comprehensive and updated[57].

In the context of the workplace, the treatment will be legitimate when it is "*necessary for the performance of a contract to which the data subject is party*", or because it is necessary for "*compliance with the legal obligation to which the controller is subject*"[58].

The consent will be necessary when there is no other legal basis that legitimizes the collection or processing of data. Consecuently, the space for employees' consent is limited in the scope of the employment relationship. For example, in those cases in which data collection responds to organizational issues or accessory services, such as the recording of the employee's image for commercial purposes or the subscription of health insurance.

As an example Employees are being assessed, evaluated, and profiled throughout their careers. Whether it be to evaluate the skills of a candidate or to assess the performance of an employee, companies are drawn towards sophisticated programs that provide valuable information in support of their decisions. In so doing, companies must make sure that they comply with the above mentoned legal principles.

---

[56] French Penal Code, article 226-15.

[57] Law n°78-17 of 6 January 1978, article 6 ; General Data Protection Regulation 2016/679, 27 April 2016, article 5.

[58] Law n°78-17 of 6 January 1978, article 7 ; General Data Protection Regulation 2016/679, 27 April 2016, article 6.

9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?

The General Data Protection Regulation does not foresee the obligation to inform workers' representatives about the collection and processing of personal data of the company's employees.

The French legal system only provides that the Social and Economic Committee must be informed and consulted on the devices controlling the employees' activity before their implementation in the company[59]. The Social and Economic Committee is also informed and consulted on the implementation of new technologies and all important organization which modifies the health, security and work conditions[60].

10. Is there a right to disconnect from technological devices outside working time? In this case, should the company define the extension and limits of this right jointly with the workers' representatives or can it do so through an internal policy?

Law n°2016-1088 of 8 August 2016 introduced the right to disconnect in the French legal system, after the recommendations of the Mettling report of 15 September 2015 which considered that this right should also be "*an obligation*" "*encouraged by the companies*" and that this right is *"likely to reconcile work and family life*"[61].

Since 1st January 2017, companies must settle the modalities of the right to disconnect from technological devices outside working time in order to ensure the employees the respect of their rest times, leaves and personal and family life[62]. The modalities are implemented in the context of the annual collective negotiation on professional equality between women and men and quality of work life with the union representatives[63].

There is no legal definition of what is exactly the right to disconnect to be given.

The right is generally described as a right for the employee to not be connected to a digital professional tool (email, smartphone…) during off-duty and vacation time. However, it is not easy to impose the right to disconnect in a professional environment in which the "BYOD" concept has experienced a takeoff without precedent and which

[59] French Labour Code, article L. 2312-38.
[60] French Labour Code, article L. 2312-8.
[61] http://travail-emploi.gouv.fr/IMG/pdf/rapport_mettling_-transformation_numerique_vie_au_travail.pdf.
[62] Law n°2016-1088, 8 August 2016, article 55.
[63] French Labour Code, article L. 2242-8, 7°.

therefore has the consequence of dimming a little more the barrier between professional and private life.

The right to disconnect is not uniform and can materialize itself in several ways:

- By a reinforced information of the employees on the use of digital tools (*e.g.* avoiding to reply to all recipients or to send emails during the week-end or holidays).
- By the implementation of training actions or sensitization to new technologies (*e.g.* reminding the employees that they should not send emails after 9.00 pm or the absence of obligation of the recipient to answer emails outside of regular hours).
- More radically, by automatically redirecting the emails of the employees who are out of the office to an appropriate available employee or the interruption of the professional mailbox during evenings and weekends, or even during holidays.

In the absence of a collective bargaining agreement on this subject with the union representatives, the employer has to implement a charter on the right to disconnect after the Social and Economic Committee's opinion. In this case, the employer is the only decision-maker as the staff representative's opinion does not impose to him. The charter must provide some vocational training and awareness measures for a reasonable use of the technological devices to the employees and managers[64].

If the employer does not negotiate a collective bargaining agreement, one year of imprisonment and a 3.750 EUR fine can be prounounced[65]. However, there is no sanction if the employer does not establish a charter.

The national and interprofessional collective bargaining agreement of 19 June 2013 on quality of work life establishes four guidelines for the bargaining of the right to disconnect:

- Establish a prior diagnosis.
- Define the particular indicators to the company.
- Provide help to managers.
- Promote a smart use of the technological devices in the company respecting the employees' private life.

Companies can provide the obligation to justify an emergency to use the professional messaging or the professional mobile phone outside the working time. Employees who do not disconnect can receive some alerts reminding them to disconnect.

[64] French Labour Code, article L. 2242-8.
[65] French Labour Code, article L. 2242-8.

Concerning employees whose working time is counted by days, the collective bargaining agreement must determine the modalities of the right to disconnect[66]. In the absence of such provisions, the modalities are defined by the employer and transmitted to the employees[67]. In companies employing more than 50 employees, the modalities must respect the charter mentionned by article L. 2242-8, 7° of the French Labour Code.

On 27 September 2016, telecommunications group Orange signed an agreement on measures to accompany its digital transformation. The agreement stipulates that 'respect for private life and the right to switch off are considered to be fundamental rights at Orange'. It is a matter of protecting employees from 'intrusive practices' (such as email, SMS, or instant messaging services) 'at any time of the day or night, over the weekend, during days off or during training courses' originating from managers, but also from their colleagues or themselves. In a previous agreement concluded on 5 March 2010, Orange's social partners explained that employees had no obligation to reply to such messages and recommended that employees made use of the 'send later' function.

This recommendation is upheld in the new agreement; it stipulates automatic mechanisms, such as the stopping of servers, to protect employees' private lives. To prevent employees being exposed to psycho-social risks or facing a paradoxical situation, Orange advises staff not to use their email service or other communication tools during rest periods, or on days off. It says its management has a duty to set an example in its use of digital tools and 'must ensure that this right is respected', while employees must realise that their own use of the digital tools may be inappropriate and they must show respect for their colleagues in their use of digital technologies. The handling of individual switching on and off of digital tools in the professional context 'must be reflected collectively, by taking the activity and service needs into account'. To avoid bombarding staff with emails, managers will also organise periods when employees will be encouraged to talk to each other. Employees are also invited to set aside periods when they will not use the electronic messaging service during the working day, for example during meetings or to facilitate concentration.

11. Other relevant aspects regarding the labor influence of the technological devices in the workplace

For several years, since the appearance of the GPS devices, the employers are able to track their employees in vehicles. Employers frequently install geolocation devices in company-owned vehicles in order to locate them. While such devices are extremely convenient, they also pose a threat for employees if used unlawfully to track their every

[66] French Labour Code, article L. 3121-64.
[67] French Labour Code, article L. 3121-65.

movement. Therefore, employers must find a fair balance between locating a vehicle and tracking the employees who use that vehicle.

The CNIL recommends using Global Positioning Systems (GPS) in company vehicles for the following purposes:[68]

- To optimise productivity (*e.g.*, to dispatch the closest vehicle in case of an emergency).
- To guarantee the safety of the individuals or merchandise in the vehicle.
- To monitor an employee's working hours (although only if this cannot be measured otherwise[69]).
- To organise transportation services (*e.g.*, ambulance services) and send out invoices.
- To comply with a legal requirement regarding the use of a geolocation device, for example, due to the type of transportation or the nature of the goods being transported (*e.g.*, public transportation, transportation of dangerous materials).

The employer must follow a three-step procedure in order to monitor its employees with devices. First, the employer must consult with the employee's representative (social and economic council) prior to implementing any sort of geolocalisation device. Then the employer must file a declaration to the data protection authority. Finally, the employer must inform the employee about the installation of such devices, the data that will be collected and ask for his/her consent.

The French Court of Cassation upheld a decision[70] against a company that unlawfully used a geolocation device to track the company vehicle used by one of its salesmen. Furthermore, geolocation devices should not be used after working hours. Finally, geolocation devices can collect large quantities of information and, for that reason, must only collect data that is relevant and non-excessive. In particular, geolocation should not be used to monitor a vehicle's speed or to record broken speed limits. Finally, pursuant

[68] See Délibération n° 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en ceuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public, available at: http://www.cnil.fr/documentation/deliberations/deliberation/delib/97/.

[69] The Cour de cassation said that using a GPS to check the working hours of an employee is only permissible if such a check cannot be done by other means. In this case it was held that the use of a GPS to monitor the employee's working time was not justifiable when the employee's employment contract permitted the employee to freely organise his work schedule (Cass. Soc. 3 November 2011 No. 10-18.036 Société Moreau Incendies contre Decaen, RJS 1/12).

[70] Court of Cassation, labour chamber, 3 Novembre 2011, pourvoi n° 10-18036, available at: http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000024761408&fastReqId=
1128855373&fastPos=1.

to article 39, Data Protection Act employers must grant employees access to any personal data that is stored on a geolocation device.

LABOR IMPACT OF TECHNOLOGICAL DEVICES IN ITALY

Emanuele Dagnino
Temporary Research Fellow, Università di Modena e Reggio Emilia

Introduction

The first regulation directly regarding the impact of technological devices on labour relations dates back to 1970 with the introduction of the article 4 of the Workers' Statute (l. n. 300/1970). The aim of this regulation is to protect the dignity and the privacy of the workers from pervasive monitoring and controls over their activities through the use of technology. Until its reform in the context of the so-called Jobs Act (in 2015), article 4 of the Workers' Statute provided a clear prohibition of the use of technologies for the monitoring of workers' activities, with the exception of those technological equipments or tools which only indirectly allow the remote monitoring of workers, if used for organizational, productive or safety purposes and only after the stipulation of an agreement with workers' representatives in the company or, lacking the agreement, after an administrative authorization. The information produced by these equipments and tools, as a result of a prohibited remote monitoring, could not be used for decisions regarding the workers.

Following the 2015 reform, even though it is still prohibited to monitor workers' activities by means of technological tools and equipments, important changes have been introduced. While the use of technological equipments which only indirectly allow the remote monitoring of workers is still bound to specific needs (beyond the organizative, productive and safety purposes, also reasons concerning the protection of employeers' goods in the new version) and to the stipulation of an agreement with workers' representatives (or, lacking the agreement, the administrative authorization)[71], these requirements do not apply for the use of working tools and systems for registering the access and presence at work. Moreover, after the reform, the employer can use information produced by tools and equipments "for any aims related to the labour relations" (promotion, training but also sanctions, including dismissal) if the usage of the tools and the practice of monitoring of such data are adequately communicated to the employee and if the processing of such information is legitimate according to data protection regulations.

[71] After the reform, in case the company has establishments in different provinces or regions the agreement can be stipulated with comparatively more representative unions at national level. In a similar manner, lacking the agreement, the autohorization can be asked to the head office of the Labour Inspectorate, instead of the office competent for the different territories.

Beyond the regulation of the remote monitoring, few other provisions address the impact of technologies on the labour relations. Apart from those directly related to the safety of the tools assigned to the workers' (contained in the occupational health and safety regulation, Legislative Decree n. 81/2008) and the few provisions regarding teleworking[72], the most relevant innovation in the field has been the regulation of the right to disconnect introduced for employees involved in *lavoro agile* (smart working) practices according to article 19 of the Law n. 81/2017.

2. Is there any regulation in your country regarding employees' use of technological devices in the company?

The Italian legal system does not provide a specific regulation concerning the use of technological devices provided by the company for the work performance. General regulations on employees' conduct are relevant for the use of technological devices as well, notably those related to the duties of good faith and care.

Except for these general principles, the regulation of the use by the employee of technological devices is left to the companies, which increasingly decide to provide a specific policy regulating the use of technological devices. As said, the introduction in the companies of new technological devices and applications must conform with article 4 of the Workers' Statute when these technologies entail the possibility of a remote monitoring of workers' activities.

2. Is it mandatory for the company to have a code of conduct or an internal policy regulating the use technological devices? If not, what is the procedure that the company must follow to regulate the use of technological devices?

As said, lacking a specific regulation in the law regarding the use of technological devices, while the codes of conduct and internal policies are not mandatory in general terms, employers use them to regulate the matter of the use of such devices. Thus internal policies and codes of conduct regarding the use of technological devices are growing in importance.

Fistly, as we have seen, the employer can use information provided by technological devices only upon adequate communication of the use of such tools and devices given to the employee (article 4, paragraph 3 of the Workers' Statute).

[72] With regards to teleworking see Dagnino E., Teleworking and Labor Conditions in Italy, IUS LABOR, 2017, vol. 2, 24 ff.

Secondly, lacking a clear regulation concerning the use of technological devices by the employees, it could be difficult for the employer to prove that the behaviour of the employee was in breach of his/her duties, for example in the case of personal/private use of the devices provided by the company.

Finally, the internal policies are useful instruments for the employer to demonstrate the compliance with regulations relevant outside the labour relations, such as the one regarding the corporate administrative and criminal liability (Legislative Decree n. 231/2001), and those regarding data protection (GDPR and Legislative Decree n. 196/2003).

3. In which cases and under what conditions is it possible to access and monitor employees' personal communications through the company's technological devices (e-mail, instant messaging, etc.)?

The legitimacy of the access to and monitoring of employee's personal communication through company's devices (e-mail and instant messaging) must be evaluated from an integrating perspective taking into account both labour law (article 4 and 8 of the Workers' Statute) and the data protection regulation (GDPR and Legislative Decree n. 196/2003), whithout overlooking the constitutional right of secrecy of the correspondence, which has an important criminal corollary.

As far as labour law is concerned, the first problem is if e-mail could be considered as working tools, thus not falling under the application of article 4, paragraph 1 of the Workers' Statute (requiring the above-mentioned procedure with workers' representatives or Labour Inspectorate and the use bound to specific reasons). With reference to the e-mail itself, this seems to be the right interpratetion; differently, once the e-mail are collected and monitored through a specific software, the use of this software must conform to article 4, paragraph 1.

The Privacy Authority as well as case law has confirmed that a costant collection and monitoring of e-mail entails a monitoring of the worker's activity forbidden by article 4 and it also violates data protection regulation.

In order to provide some guidance for a legitimate management of company e-mail addresses, the Privacy Authority has issued the Guidelines Applying to the Use of E-Mails and the Internet in the Employment Context - 1 March 2007[73].
In some cases, the access to the content of communications is allowed according to the case law doctrine of *controlli difensivi* (see *infra*, § 5), thus not requiring the respect of

[73] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1408680

article 4 of the Workers' Statute. In the other cases, the information collected through the access could be used by the employer in the context of the employment relationship only if the employee has been informed in terms of tools, their usage and the ways of monitoring and if the following processing complies with data protection regulation.

Since the access to private communications can provide information regarding non-work related aspects of employee's life, it can also imply the violation of article 8 of Workers' Statute, which forbids the investigation by the employer on information regarding opinions, beliefs and any other aspect of the employee's life that are not relevant for the evaluation of employee's attitude to the work.

4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?

According to article 4 of the Workers' Statute, workers' activities (including work performance and other behaviours put in place by the workers while at work) can not be (directly) controlled by the employer by means of technological monitoring. Video surveillance systems can be used only for the aims above-mentioned (organizational and productive reasons or regarding workers' safety or the protection of employers' goods) and can be installed only after the stipulation of an agreement with workers' representatives or, lacking the agreement, after the authorization of the Labour Inspectorate.

Their use should also comply with data protecton regulations, with reference, *inter alia*, to the principles regarding data processing, the right to be informed and the legal basis of the processing.

When the above-mentioned conditions are respected, information provided by video surveillance can be used by the employer in the context of the employment relationship (also for dismissal purposes) only if the employee has been informed about the way the control is put in place and if the following processing comply with data protection regulations (article 4, paragraph 3 of the Workers' Statute).

5. Under what circumstances is it possible to install hidden cameras to control work activity? In particular, is its installation only possible when the company suspects that a criminal offense has been committed or also when there are signs of a breach of contract?

Before the reform regarding article 4 passed in 2015, Courts have considered as legitimate the use of hidden cameras (thus falling outside the application of article 4 and

its limits and procedure) if used not for the monitoring and control of the work performance but for the investigation regarding misbehaviour by the employees (so-called *controlli difensivi*, defensive controls). After a first decision (Cass. n. 4746/2002) stating that the use of monitoring technologies aimed to ascertain employees' misbehaviour falls always outside the application of article 4 of the Workers' Statute, case law has been consolidated in the interpretation of the exception from the application of article 4 only when the monitoring through technological tools was aimed to ascertain employees' misbehaviour not related to the work performance, but impacting on employers' goods.

After the reform, scholars debated the survival of this case law, since the new version of article 4 of the Workers' Statute clearly states that the technologies (including cameras) used for the protection of employers' goods fall within the application of the article, so that can be installed and used only after the stipulation of an agreement with workers' representatives or, lacking the agreement, after the authorization by the Labour Inspectorate.

The first decisions of the lower courts[74] –decisions from the Corte di Cassazione are still awaited– regarding hidden remote monitoring seem to confirm the possibility to use hidden cameras but only for ascertaing misbehaviour that are not related to the work performance. Notwithstanding, the nature and extent of this specific category of monitoring activities (*controlli difensivi*) is still debated and we have to wait the consolidation of case law by the Corte di Cassazione in next years.

6. In what cases is it possible to install geolocation systems (GPS) to control work activity?

As previously said, according to article 4 technological devices and tools can not be used for direct monitoring of the workers' activities, but information produced by such tools, if their use is not aimed to workers' monitoring, can be used in the context of the employment relationships under the condition outlined above. Geolocation systems (GPS) are widely used nowadays: under the regulation of article 4 of the Workers' Statute, it is important to distinguish between their usage for monitoring of workers' activities (forbidden), for the reasons outlined above (thus requiring an agreement with unions or the authorization before their installation) or if they can be considered

[74] See, for example, Trib. La Spezia 25 novembre 2016 cited in SITZIA A., "Videosorveglianza occulta, privacy e diritto di proprietà: la Corte Edu sul criterio del bilanciamento", *Argomenti di Diritto del Lavoro*, nº 2, 2018, note 23 and Trib. Roma ord. 24 marzo 2017, commented by GRAMANO E., "La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi", *Diritto delle Relazioni Industriali*, nº 1, 2018, p. 265.

working tools. While there are not particular difficulties in distinguishing when GPS are installed for the control of the workers' activities, many doubts raised around the qualification as tools used by the employer for reasons related to the organization, the production, the workers' safety or the protection of employers' good or, otherwise, as working tools.

While a settled case law is not yet available about this matter, a circular[75] issued by the Labour Inspectorate clearly states that geolocation systems are not normally used by the employee directly in the performance of his/her work. For example, if they are installed on company vehicules, they aim to protect an employer's good; if they are installed in workers' equipment they are used for safety reasons or, in some cases, to a better management of the work performance. It follows that the installation of such tools on a device must be preceeded by the stipulation of an agreement with the workers' representatives or, lacking the agreement, by the authorization provided by the Labour Inspectorate.

In the few cases where the GPS are used as working tools or as systems for registering access and presence at work, they can be used without the need of any agreement or authorization, but in compliance with data protection regulations.

7. In the event that the company fires an employee in breach of the conditions regarding control communications by e-mail or installation of video surveillance systems, what would be the qualification of the dismissal and what administrative sanctions could be derived?

In case of dismissal of the employee in breach of the requirements regarding technological monitoring of the workers' activities, the dismissal will be deemed unjustified, if the misbehaviour alleged to the dismissal of the worker is not proven through other means of proof obtained lawfully. In this event, the consequence depends on the protection regime applied to the employement relationship according to the number of employees employed by the company and the date of stipulation of the contract: the sanction ranges from the payment of an indemnity to the reinstatement of the employee.

Beyond the consequences related to the dismissal, it is worth mentioning that a complex system of sanctions is provided by the different regulations applied to remote monitoring of the employees in administrative, civil and criminal field. Apart from the

[75] Circolare INL n. 2/2016. http://www.lavoro.gov.it/documenti-e-norme/normative/Documents/2016/Circolare%20INL%20n.2%20indicazioni%20operative%20%20utilizzazione%20%20impianti%20GPS-signed.pdf

sanctions provided by the GDPR regarding the breach of data protection regulations (article 83), it must be highlighted that the violation of article 8 and article 4 – if a direct monitoring of the workers' activities is put in place or when equipments and tools requiring the agreement with the workers' representatives or the authorization are used in lack of them – entails the application of criminal sanctions. Criminal sanctions are applied also in cases of violation of the secrecy of the correspondence.

8. What personal data can be collected and processed in the framework of the employment relationship? In particular, is employees' consent necessary? In what cases is it not necessary?

Italy has not yet adapted its internal regulation (Legislative Decree n. 196/2003) to the content of the GDPR, creating some problems of coordinations between the two regulations.
Since the European Regulation prevails on the internal regulation, we will focus on the first one.

The processing of personal data regarding the employee – as well as for any other data subject – shall conform to the principles of: lawfulnes, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability (article 5 of the GDPR). The employee must also be informed by the employer regarding the existence, the nature and the features of the processing.

In general terms, the processing of employee's personal data is legitimate –without the need of express consent by the employee– when it is necessary for the performance of a contract or for complying with legal obligation regarding the controller. In the other cases, the legal basis for the processing should usually be the explicit consent by the employee.

For specific processing, such as those implying automated decision making (section 4 of the GDPR), including profiling, or those "*likely to result in a high risk to the rights and freedoms of natural persons*" (see article 35 regarding data protection impact assessment), other protections apply.

9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?

Except for the obligation to negotiate an agreement (not to stipulate it, since it is possible, lacking the agreement, to ask for an authorization to the Labour Inspectorate)

for the installation of technological equipments and tools when they entail the possibility for an indirect control of the workers' activities, no specific regulation establishes a duty to inform workers' representatives about data treatments. Nor does the GDPR provide any specific obligation in this field[76].

10. Is there a right to disconnect from technological devices outside working time? In this case, should the company define the extension and limits of this right jointly with the workers' representatives or can it do so through an internal policy?

A specific mention to the disconnection from technological devices is contained in the Law n. 81/2017 which is applied to the so-called *smart workers* or *lavoratori agili*. *Lavoro agile* is a particular way of working characterized by flexibility regarding the place and time of work[77]. Italian regulator decided to require the stipulation of a specific individual agreement between employer and employee to access that specific form of work. The law provides some mandatory contents of this agreement between employer and employee: one of them is the definition of organizational and technical measures to guarantee the disconnection of the employee from technological devices used to work. It is still debated among the scholars, if this provision establishes a specific right to disconnect, but it is clear that not defining adequate measures can lead to responsibility for the employer in case a work-related illness affecting a *smart worker*. The law does not establish the specific measures, since the measures should be adapted to the organization of work of the company and, also, to the specific features of the way of working adopted by the employee (*lavoro agile* could be tailored).

While there is a duty of specification in the individual agreement of *lavoro agile*, no role is spefically assigned to the unions. Notwithstanding, it is worth saying that the stipulation of individual agreements of *lavoro agile* is often preceeded by a company-level collective agreement introducing a framework regulation of *lavoro agile* in the company. Collective agreements are now starting to provide some general regulation regarding the right to disconnect, even if unions in Italy seem not to be ready to regulate this right of new generation as a comparison with the content of French collective agreement on the issue makes clear[78].

---

[76] The only reference to representatives of the data subjects is contained in article 35 paragraph 9 which states that in the context of a Data Protection Impact Assessment, "*where appropriate*", the controller must "*seek the views of data subjects or their representatives*". No specification is given regarding who should be considered a legitimate representative of the data subject and, in any case, the obligation seems to be weak.

[77] See, again, DAGNINO E., "Teleworking and Labor Conditions in Italy", *Teleworking and labor conditions. Comparative Labor Law Dossier*, *IUSLabor* nº 2, 2017, p. 26-27.

[78] A comparison between the contents of collective agreements regarding the right to disconnect in Italy and France is offered in DAGNINO E., "The Right to Disconnect in the Prism of Work-life Balance. The

11. Other relevant aspects regarding the labor influence of the technological devices in the workplace

New regulations impacting on the introduction and the use of technologies in the company –such as GDPR, new version of the article 4 of the Workers' Statute; the regulation regarding the right to disconnect– as well as the application of traditional regulation to the technological context of the new workplace, are feeding debate among Courts and scholars with different positions. As a consequence, some interpretations provided in the article according to decisions by Courts and administrative bodies can be subverted in the future.

Role of Collective Bargaining: A Comparison between Italy and France", paper accepted for presentation at the XXII ISLSSL World Congress Torino 2018.

LABOR IMPACT OF TECHNOLOGICAL DEVICES IN POLAND

Michał Barański
Doctor of Juridical Sciences
Assistant Professor at the Faculty of Law and Administration
University of Silesia in Katowice, Poland

Introduction

At present, also in Poland, there is a continuous and rapid increase in the importance of information and related processes. This development, in connection with technological development, causes the transformation of the labour market. It is noticeable the evolution in Poland of legal provisions regarding the effects of technological devices on labour relations. Initially, these provisions focused on safe and hygienic working conditions. Since 2004, specific regulations regarding the processing of personal data in employment came into force. In 2007, provisions on teleworking were introduced. Recently, important regulations are related to the applicable (also in Poland) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[79]. In this matter, there is an increasing impact of the so-called autonomous sources of labour law. However, conflict between the employee's right to privacy and the employer's right to inspect the employee is still a serious challenge for the Polish legislator.

1. Is there any regulation in your country regarding employees' use of technological devices in the company?

According to article 94 point 2 of the Polish Labour Code "*the employer is obliged to organise work in a manner ensuring the effective use of working time, as well as achieving high efficiency and appropriate quality of work through using the employees' abilities and qualifictions*"[80], which in particular means that the employer should provide the employee with appropriate materials and work tools (e.g. technological devices). An employee also has certain obligations that may apply to the use of these

[79] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, referred to as Regulation 2016/679.

[80] The Act of 26 June 1974 Labour Code (unified text: Journal of Laws of 2018, item 917 with amendments), referred to as KP; translated by A. JAMROŻY: The Labour Code. Kodeks pracy, Warsaw 2010, p. 101.

devices (an employee is obliged in particular to respect the interest of the work establishment and protect its poperty).

In Poland fundamentally there is no general and explicit regulations of generally applicable law on the use by employees of technological devices in the company. The only exception is the regulations regarding telework, personal data protection, health and safety as well as monitoring employees.

The Polish Labour Code regulate in detail employment in the form of telework (articles 67^5-67^{17} KP). In the field of teleworking "*work may be performed away from the premises of an employer, on a regular basis, by means of information and communications technologies (ICT's) in the meaning of the provisions on rendering services by electronic means*" (article 67^5 § 1 KP)[81]. A teleworker is any person carrying out telework under the conditions specified in article 67^5 § 2 KP and "*presenting the effects of work to an employer, in particular by means of information and communications technologies (ICT's)*" (article 67^5 § 2 KP)[82].

Another aspect of employee`s use of technological devices in the company is the issues of monitoring employees and processing their personal data in connection with work. These issues were described in detail further in this dossier.

2. Is it mandatory for the company to have a code of conduct or an internal policy regulating the use technological devices? If not, what is the procedure that the company must follow to regulate the use of technological devices?

The Polish Labour Law does not include a legal obligation to have a general code of conduct or an internal policy on the use of technological devices.

Appropriate specific regulations in this area should be included in the so-called autonomous sources of Labour Law (e.g. provisions of collective labour agreements, regulations based on the law and determining the rights and duties of the parties to an employment relationship). For example, according to article 67^6 § 1-4 KP the conditions of an employer applying telework must be defined in an agreement between employer and enterprise trade unions or in the workplace regulations. The objectives, scope and method of monitoring employees (e.g. monitoring of the employee's e-mail, video monitoring) are "*set in the collective labour agreement or in the workplace regulations or in the notice, if the employer is not covered by a collective labour agreement or is*

[81] Translated by A. JAMROŻY: The Labour Code.., p. 67.
[82] Translated by A. JAMROŻY: The Labour Code..., p. 67.

not obliged to determine the workplace regulations" (article 22^2 § 6 KP in relation to article 22^3 § 3-4 KP)[83].

3. In which cases and under what conditions is it possible to access and monitor employees' personal communications through the company's technological devices (e-mail, instant messaging, etc.)?

The Polish legal system establish criteria for monitoring of employees' personal communications through technological devices in the company.

According to article 22^3 § 1 KP "*if it is necessary to ensure the organization of work enabling full use of working time and proper use of work tools made available to the employee, the employer may introduce a control of the employee's e-mail (monitoring of e-mail)*"[84]. It should be remembered that "*monitoring of e-mail can not violate the secrecy of correspondence and other personal rights of an employee*" (article 22^3 § 2 KP)[85]. For monitoring of e-mail, the regulations regarding video monitoring (articles 22^2 § 6-10 KP) are applied accordingly (article 22^3 § 3 KP)[86].

Moreover, the provisions of articles 22^3 § 1-3 KP shall apply accordingly to other forms of monitoring if their use is necessary to achieve the objectives set out above (article 22^3 § 4 KP).

Issues of monitoring in the workplace have been repeatedly the subject of the case law of the European Court of Human Rights (ECHR). The judgment of the ECHR in the case "Lynette Copland v. the United Kingdom" (application no. 62617/00) on April 3, 2007, analyzes a case in which the superior supervised the telephone, e-mail and internet connections of the employee, while monitoring the use of the Internet took the form of an analysis of visited websites, dates and times of visits and their duration[87]. The ECHR stated that "t*he applicant in the present case had been given no warning that her calls would be liable to monitoring, therefore she had a reasonable expectation as to the privacy of calls made from her work telephone* (…). *The same expectation should apply in relation to the applicant's e-mail and internet usage*". In the case there has therefore been an interference with the rights guaranteed by article 8 section 1 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, according to which "*everyone has the right to respect for his private and family life, his*

[83] Translated by the author.
[84] Translated by the author.
[85] Translated by the author.
[86] These provisions will be quoted later in this dossier.
[87] See Case of Copland v. The United Kingdom, Application no. 62617/00 (3 April 2007) ECHR.

home and his correspondence"[88]. The employee must be aware of the possibility of monitoring his activities, and this requires the creation of appropriate procedures and familiarize the employee to the procedure.

Monitoring employees' personal communications through the company's technological devices must respect the principles related to the treatment of data foreseen in Regulation (EU) 2016/679, which is directly applicable without the need for transposition.

4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?

According to article 22^2 § 1 KP "*if it is necessary to ensure the safety of employees or to protect property or to control production or keep secret information whose disclosure could expose an employer to a damage, the employer may introduce specific supervision over the workplace or the area around the workplace in the form of technical means enabling image registration (monitoring)*"[89]. However, "*the monitoring does not include sanitary rooms, cloakrooms, canteens and smoking rooms or premises made available to the trade union organization, unless the use of monitoring in these rooms is necessary to achieve the purpose specified in § 1 and does not violate the dignity and other personal rights of the employee, as well as the principles of freedom and independence of trade unions, in particular through the use of techniques that prevent recognition of persons staying in these rooms*"[90] (article 22^2 § 2 KP).

Should be noted that "*the video recordings are processed by the employer only for the purposes for which they were collected and stored for a period not exceeding 3 months from the date of recording*"[91] (article 22^2 § 3 KP). After this period, video recordings obtained as a result of monitoring, containing personal data, as a rule are destroyed, unless separate provisions provide otherwise (article 22^2 § 5 KP)[92].

[88] European Convention for the Protection of Human Rights and Fundamental Freedoms signed at Rome on 4 November 1950, subsequently amended by Protocols No. 3, 5 and 8 and supplemented by Protocol No. 2 (Journal of Laws of 1993 No. 61, item 284 with amendments).

[89] Translated by the author.

[90] Translated by the author.

[91] Translated by the author.

[92] According to article 22^2 § 4 KP "*in the case where the image recordings are evidence in law-based proceedings or the employer has received a message that they may be evidence in the proceedings, the time limit specified in § 3 is extended until the final conclusion of the proceedings*". After this period, video recordings obtained as a result of monitoring, containing personal data, fundamentally are destroyed, unless separate provisions provide otherwise.

In Poland, as previously indicated, the objectives, scope and method, among others, of this form of monitoring are "*set in the collective labour agreement or in the workplace regulations or in the notice, if the employer is not covered by a collective labour agreement or is not obliged to determine the workplace regulations*" (article 22^2 § 6 KP). Moreover, according to article 22^2 § 7 KP "*the employer informs employees about the insertion of monitoring, in a manner accepted by a particular employer, no later than two weeks before its launch*"[93]. Employees should receive written information about video monitoring before they are allowed to work (article 22^2 § 8 KP). Furthermore, in the case of video monitoring, "*the employer means monitored premises and areas in a visible and legible manner, by means of appropriate signs or sound notices, not later than one day before its launch*"[94] (article 22^2 § 9 KP).

Workplace video monitoring must respect the principles related to the treatment of data foreseen in Regulation (EU) 2016/679. In particular, according to article 22^2 § 10 KP the provision of article 22^2 § 9 KP does not violate the provisions of articles 12 and 13 of Regulation (EU) 2016/679.

5. Under what circumstances is it possible to install hidden cameras to control work activity? In particular, is its installation only possible when the company suspects that a criminal offense has been committed or also when there are signs of a breach of contract?

Due to the above-mentioned articles 22^2 § 1-10 KP and Regulation (EU) 2016/679, in Poland it is not currently possible to install hidden cameras to control work activity.

6. In what cases is it possible to install geolocation systems (GPS) to control work activity?

As already indicated, the provisions of articles 22^3 § 1-3 KP (therefore, also articles 22^2 § 6-10 KP) shall apply accordingly to other forms of monitoring if their use is necessary to achieve the objectives set out in article 22^3 § 1 KP (i.e. if it is necessary to ensure the organization of work enabling full use of working time and proper use of work tools made available to the employee). Among these other forms of monitoring should be mentioned monitoring of employees' work by processing their geolocation data.

Employee geolocation data should therefore be treated as personal data under the legal regime of Regulation (EU) 2016/679.

[93] Translated by the author.
[94] Translated by the author.

7. In the event that the company fires an employee in breach of the conditions regarding control communications by e-mail or installation of video surveillance systems, what would be the qualification of the dismissal and what administrative sanctions could be derived?

First of all, it should be pointed out that the Polish Labor Code regulates rights of the employee in the case of an unjustified or unlawful termination of the employment contract with notice by the employer (articles 44-51 KP) and rights of the employee in the case of an unlawful termination of the employment contract without notice by the employer (articles 56-61 KP). Depending on the circumstances, these provisions may apply to this matter.

Such a situation may also be considered through the prism of abuse of subjective right (article 8 KP) and provisions on the protection of personal rights (e.g. the right to privacy).

Apart from the above, Regulation (EU) 2016/679 typifies the infractions, whose would be punishable regardless of the qualification of the dismissal.

8. What personal data can be collected and processed in the framework of the employment relationship? In particular, is employees' consent necessary? In what cases is it not necessary?

The Polish Labour Law directly regulates disclosure of personal data to an employer. According to article 22^1 § 1 KP "*an employer may demand a person applying for employment to provide the following personal data, including:*

- *name(s) and surname,*
- *names of parents,*
- *date of birth,*
- *residential address (address for correspondence),*
- *education,*
- *employment history*"[95].

Moreover, according to article 22^1 § 2 KP an employer may also demand an employee to present, regardless of the personal data referred to in article 22^1 § 1 KP:

- "*other personal data of the employee, as well as names, surnames and dates of birth of the children of the employee, if it is necessary for an employee to exercise special rights provided for by the labour law,*

[95] Translated by A. JAMROŻY: The Labour Code..., p. 27.

- *the PESEL number of the employee issued by the Government Information Centre of the Common Electronic System for the Registration of Population (Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności – RCI PESEL)*"[96].

It should be emphasized that due to the amendment of the Polish Labour Code provisions regarding the procedure for paying remuneration, from January 1, 2019, the above personal data catalog (article 22^1 § 2 KP) will be extended by the payment account number if the employee has not applied for the payment of remuneration to his own hands[97].
Personal data are provided to an employer "*in the form of a statement by the person whom the personal data concern*" (however, the employer has the right to demand the certification of the personal data of the persons referred to in article 22^1 § 1-2 KP) (article 22^1 § 3 KP).

According to article 22^1 § 4 KP an employer may demand personal data other than those referred to in article 22^1 § 1-2 KP, "*provided the duty to present them results from separate provisions*"[98] (e.g. personal data collected in the National Criminal Register). To the extent not regulated in article 22^1 § 1-4 KP, "*the provisions on the protection of personal data apply to the personal data referred to in the provisions therein*"[99] (article 22^1 § 5 KP).

Of course Regulation (EU) 2016/679 is the applicable norm in terms of collection and processing employees personal data.

In Poland, serious doubts are raised by the issue of the possibility of obtaining consent from an employee (a person applying for employment) to the processing of personal data by the employer. Generally, the consent will be necessary when there is no other legal basis that legitimizes the collection or processing of data. However, The Supreme Administrative Court in Warsaw in the justification of the judgment of December 1, 2009 indicated that the employee's written consent to obtain and process his biometric data violates the employee's rights and freedom of expression of will. Due to employee subordination, an employee is a weaker party to the employment relationship (there is no balance in the employer-employee relationship). Recognition of the fact of consent

[96] Translated by A. JAMROŻY: The Labour Code..., p. 28.
[97] The Act of 10 January 2018 on amending certain acts in connection with shortening the period of storage of employee files and their electronicisation (Journal of Laws of 2018, item 357).
[98] Translated by A. Jamroży: The Labour Code..., p. 28. Separate provisions within the meaning of art. 22^1 § 4 KP there are only generally applicable laws (excluding autonomous sources of Labour Law).
[99] Translated by A. JAMROŻY: The Labour Code..., p. 28.

by the employee for the circumstance of legalizing collecting from the employee other data than indicated in article 22^1 § 1-2 KP would constitute a violation of this provision[100].

Currently in Poland, legislative work is underway on a new act amending certain acts in connection with ensuring the application of Regulation 2016/679, which will, inter alia, significantly change the The Polish Labour Code in the field of personal data protection in employment. At the moment, the project provides for the possibility of the employee's consent to the processing of his personal data in employment, or specifies in detail the processing of biometric data of the employee[101].

9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?

The Polish Labour Law directly does not foresee the obligation to inform workers' representatives about the collection and processing of personal data of the employees. However, according to article 8 of the Act of May 23, 1991 on trade unions, "*the employer is obliged to provide, at the request of the trade union, information necessary to conduct trade union activities, in particular information on working conditions and rules of remuneration*"[102].

10. Is there a right to disconnect from technological devices outside working time? In this case, should the company define the extension and limits of this right jointly with the workers' representatives or can it do so through an internal policy?

The Polish legal system does not recognize a specific right of employees to disconnect from technological devices outside working time (e.g. an employer may oblige an employee to remain on call outside of regular working hours). On the other hand, an employee is entitled to some periods of rest specified in the Polish Labour Law.

At the same time, due to the right to privacy, the employer may not process employees' geolocation data outside of their working hours (any equipment provided to the

[100] See judgment of the Supreme Administrative Court in Warsaw of 1 December 2009, I OSK 249/09, LEX No. 785755.

[101] See Draft Act amending certain acts in connection with ensuring the application of Regulation 2016/679, https://legislacja.rcl.gov.pl/projekt/12302951, as of July 10, 2018.

[102] the Act of May 23, 1991 on trade unions (unified text: Journal of Laws of 2015, item 1881 with amendments); translated by the author.

employee should have a system that allows the employee to disable location functionality)[103].

[103] It should be noted, however, that "the collection of geolocation data for these devices may also serve the purpose of protecting the property itself, for example, from theft. A possible ban on processing of geolocation data outside the employee's working hours should take into account the above circumstances. However, given the risk of fraud, the processing of such data should be entrusted to a third party, such as a service provider". See M. BARAŃSKI, M. and GIERMAK, "Protection of employees' geolocation data in EU law", in M. JANKOWSKA, M. PAWEŁCZYK, S. AUGUSTYN, M. KULAWIAK (red.): *Earth Observation & Navigation. Law and Technology*, Warsaw 2017, p. 203.

LABOR IMPACT OF TECHNOLOGICAL DEVICES IN PORTUGAL

Milena Rouxinol
Assistant professor, Portuguese Catholic University – Oporto School

Introduction

The main regulatory source regarding the issues arising from the use of technological devices on labour relations is the Portuguese Labour Code, which includes a chapter [articles 14-22] dedicated to personal rights, namely those put in danger due to the use of such technological tools. As for collective agreements, these issues are not a typical subject therein regulated.

1. Is there any regulation in your country regarding employees' use of technological devices in the company?

The Portuguese Labour Code dedicating some dispositions to personal rights implicated in labour relationships, its article 22 concerns, in particular, employees' personal communications and information, namely those sent, received or consulted by means of electronic devices, as electronic mail systems. Article 22 provides that employers can define rules to be accomplished in the company in what concerns the use of communication tools, namely the email (22-2), but also that employees have the right of keeping their personal communications and information not disclosed (22-1). Portuguese case law has been stressing that even if the electronic devices belong to the employer and even if the email account is provided by him, he is not allowed to access personal electronic contents in any circumstances.

2. Is it mandatory for the company to have a code of conduct or an internal policy regulating the use technological devices? If not, what is the procedure that the company must follow to regulate the use of technological devices?

According to the Portuguese Labour Code, the employer is entitled to define rules concerning the use of technological devices. For example, employers may establish that a professional email account shall not be used for personal effects or that some electronic sites shall not be visited during working time. However, this is not mandatory. If the company defines such rules, employers have the right to verify their accomplishment, as far as they do not access personal contents.

As the establishment of conduct patterns is not mandatory, if employers decide to define rules, they may use the means of their choice and convenience. The creation of an

internal rules of procedure document is one the employers' prerogatives and this document may contain the regulation of the use of electronic devices.

3. In which cases and under what conditions is it possible to access and monitor employees' personal communications through the company's technological devices (e-mail, instant messaging, etc.)?

According to article 22-1 of the Portuguese Labour Code, employers are not allowed, in any case, to access the content of employees' personal communications. If employers need to assess the compliance of employees' behaviour with rules previously defined, they may verify external elements, such as messages' recipients and subject matters, but not contents. According to case law, even when the employer accesses an email account for professional purposes, if he detects any personal content while reading, he shall immediately stop reading, which means, at least, that information unlawfully accessed may not be used as evidence against the employee for punishment purposes. This position is upheld by Comissão Nacional de Proteção de Dados (National Committee for Data Protection) (see Deliberation no. 1638/2013).

4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?

The Portuguese Labour Code answers to this question in articles 20 and 21. According to article 20-1, there is a general prohibition for employers to install permanent video surveillance systems in companies aiming to control work activity. In contrast, the use of such equipment is allowed for people and property safety purposes, and – which is exceptional – when the nature of the activity requires that sort of surveillance (20-2).

In any case, employers have to be given an administrative authorization. For that, if interested in installing such equipment, they shall make a requirement to Comissão Nacional de Proteção de Dados (National Committee for Data Protection), which analyses the reasonableness of the interest, and decides if such systems may be used, to what extent and in which terms (21-1). This assessment shall be made in compliance with the principle of proportionality (21-2) and it may take into account the opinion of the workers' committee, that shall be previously required by employers (21-4).

On the other hand, if they install a video surveillance system in the company, employers are obliged to give notice to employees, namely by posting an advice on the wall, close to the camera (20-3).

Data shall be conserved for the period required by the purposes therein implied and destroyed after that and in case of contract termination or transfer of the employee for another place (21-3).

5. Under what circumstances is it possible to install hidden cameras to control work activity? In particular, is its installation only possible when the company suspects that a criminal offense has been committed or also when there are signs of a breach of contract?

According to the Portuguese Labour Code, installing hidden cameras is not allowed in any circumstances. In fact, article 20-3 prescribes that employers shall give notice to employees on the existence and purposes of the surveillance systems used.

6. In what cases is it possible to install geolocation systems (GPS) to control work activity?

In Portugal, the legal framework of geolocation systems as tools used by employers to control working activity is not clear, which is an important problem, given the fact that employers are interested in the use of those systems in many cases. The reason for such uncertainty is that it is doubtful if that sort of equipment shall be considered means of remote surveillance, for the effects of articles 20 and 21, applicable, v. g., to video cameras. Despite some discussion in the legal literature and especially in case law, most of the judicial rulings consider that GPS shall not be included in the concept of remote surveillance systems, because it is not possible to capture images of the employees and to locate them in real-time. However, there is an important deliberation of the Comissão Nacional de Proteção de Dados (National Committee for Data Protection), deliberation no. 7680/2014, stating, in contrast, that geolocation systems shall be considered means of remote surveillance, namely for the effects of articles 20 and 21 of the Labour Code. This Committee underlines the large variety of GPS models and their potentialities, which have been increasing and becoming more and more intrusive. Despite what has been stated above, it is observable that, currently, case law begins to follow this position.

If these systems are included in the regime defined in articles 20 and 21 of the Labour Code, the conditions to be observed are clear (see question 4). If they are not, one has to recognize, anyway, that their use may put in danger employees' privacy and, in that sense, the principles regarding privacy protection, mainly the principle of proportionality, have to be accomplished.

7. In the event that the company fires an employee in breach of the conditions regarding control communications by e-mail or installation of video surveillance systems, what would be the qualification of the dismissal and what administrative sanctions could be derived?

In the Portuguese system, the consequence of a dismissal made in breach of legal conditions is, in general, its nullity, the consequence being the obligation of reinstating the employee, unless he/she prefers being given an economic indemnity. There is only an exceptional case in which the dismissal is unfair but not devoid of the effect of terminating the contract –when the employer does not perform the mandatory probationary proceedings. Furthermore, it is important to underline that, even when the dismissal is null, there are two special situations in which the employer is entitled to refuse the reinstatement: if the company employs less than 10 employees; or if the dismissed employee had a management position. Even in those cases, however, the employer is not allowed to deny the reinstatement if the dismissal is considered discriminatory.

According to this framework, if the company fires an employee in breach of the conditions regarding control communications by e-mail or installation of video surveillance systems, the consequence will be, in principle, the nullity of the contract termination and the employee will be reinstated, unless he/she choses to be economically compensated. In this later case, the amount of the indemnity is calculated considering the seriousness of the dismissal illegality.

In any case, the employee shall be compensated for the losses caused by the unlawful dismissal; in the situation herein taken into consideration, he/she must prove, in particular, damages arising from the breach of the legal rules concerning his/her privacy (articles 389-392 of the Labour Code).

Furthermore, there are administrative consequences, which are linked to the violation of such legal rules, regardless of the question if that violation leads to a dismissal or not.

Finally, the employer may incur criminal liability in case of unlawful access to private communications (article 194 of the Criminal Code).

8. What personal data can be collected and processed in the framework of the employment relationship? In particular, is employees' consent necessary? In what cases is it not necessary?

In the Portuguese system, the data that can be collected and processed within the framework of the employment relationship is that which extends to the point that it is adequate and necessary for the compliance and performance of the employment contract, which is in line with the principle of the minimization of the data, set forth in article 5-1-c) of the GDPR.

Considering that the employment relationship is, very often, unbalanced, the employee being in a lower position, the Portuguese labour law does not give relevance to employees' consent as an autonomous ground to make the collection and processing of data lawful. However, this does not mean that such consent is not necessary: in fact, data cannot be accessed, in any case, without this consent.

According to article 17, personal information only can be required when the compliance and performance of the contract impose that the employer is aware of that information. The company shall provide a written justification. As for information concerning health status and pregnancy, it shall be given to a doctor, who shall communicate to the company nothing more than the ability or inability of the employee to accomplish the contract.

As for medical exams (article 19), also a written justification must be given and, again, the doctor only communicates if the employee is able or not.

Regarding biometric data, the company shall respect the principle of proportionality and it cannot manage that information without communicating that to the Comissão Nacional de Proteção de Dados (National Committee for Data Protection) (article 18).

9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?

According to article 18 of the Labour Code, the collection and processing of biometric data are not allowed if the Comissão Nacional de Proteção de Dados (National Committee for Data Protection) is not informed. This communication shall be filed with a written opinion of the company employees' committee attached (or evidence of the requirement of this opinion).

As already stated, the utilisation of remote surveillance tools shall be authorised by the National Committee for Data Protection and the requirement of this authorisation shall also be filed with a written opinion given by the employees' committee in attachment.

10. Is there a right to disconnect from technological devices outside working time? In this case, should the company define the extension and limits of this right jointly with the workers' representatives or can it do so through an internal policy?

The Portuguese legal system does not recognize a specific right of employees to disconnect from technological devices outside working time. However, despite the absence of such rule, one cannot say that employees are obliged to be connected outside working time. The periods of working time are those in which the employee is performing the activity, or available to work, that is, available to respond to employer's requirements (article 197 of the Labour Code).

As for this latter situation, the majority of the case law argue that if the employee is not obliged to remain in the working place, that period shall not be considered working time, even if he/she is obliged to be connected and available to be called to work. This is in line with some rulings of the Court of Justice (of the European Union), such as those of the cases SIMAP (C-303/98; 3/10/2000; Pfeiffer (C-397/01 e C-403/01; 5/10/2004), Jaeger (C-151/02; 9/09/2003), Dellas (C-14/04, 1/12/2005) and Vorel (C-437/05, 11/01/2007). However, that does not appear to be the most immediate literal meaning of the article 197, which is wider than the Directive 2003/88/CE, as far as the concept of working time is concerned.

Furthermore, that position is not in compliance with the decision adopted by the European Committee of the Social Rights (of the Council of Europe), responding to the complaint no. 55/2009 (against France). According to this decision, if the employee is obliged to be available to respond to employer's requirements and may be called to work, this period shall not be considered rest time. In conclusion, due to the company's obligation to respect the regulations on working time, and also to grant safety and health conditions, it is not correct to say that employees are obliged to stay connected outside working time, even in the absence of a legal or conventional rule recognizing the right to disconnection.

LABOR IMPACT OF TECHNOLOGICAL DEVICES IN SLOVENIA

Darja Senčur Peček
Professor
University of Maribor, Slovenia

1. Is there any regulation in your country regarding employees' use of technological devices in the company?

Slovenian legislation does not specifically regulate the impact of technological devices on employment relationships and it is also not included in the collective agreements yet.

Concerning permissibility of employer's monitoring of the use of these devices, general regulation regarding privacy protection of the employee applies. Even the Constitution of the Republic of Slovenia includes protection of the right to privacy and personality rights (in article 35), protection of the privacy of correspondence and other means of communication (article 37) and protection of personal data (article 38) among human rights and fundamental freedoms. Employment Relationship Act (ZDR-1) determines a general obligation of the employer to guard and respect the employee's personality and to protect the employee's privacy (article 46) and it also establishes an obligation to protect the employee's personal data (article 48). In this regard, the employer must also consider the Personal Data Protection Act (ZVOP-1), which has entered into force prior to GDPR (the new legislation is now in the drafting phase). The execution of ZVOP-1 is monitored by a special state authority –Information Commissioner, who is also a misdemeanor authority. Nonbinding legal opinions and guidelines–clarifications about issues in the field of data protection, adopted and published by the Information Commissioner at his website, are also important.

2. Is it mandatory for the company to have a code of conduct or an internal policy regulating the use technological devices? If not, what is the procedure that the company must follow to regulate the use of technological devices?

Slovenian legislation does not provide an obligatory adoption of codes of conduct or rules regarding the use of technological devices.

The employer can adopt a code of conduct to regulate this matter. A code of conduct (this applies to all codes of conduct) must be sent to trade unions at the employer to express their opinion prior to its adoption. If the trade unions forward their opinion in 8 days, the employer must consider it before adopting the code of conduct and also state its position about the opinion.

There are no specific rules regarding permitted monitoring by the employer neither in Slovenian legislation nor in its case law. The Information Commissioner refers to the case law of European Court of Human Rights (Halford v. United Kingdom, Copland v. United Kingdom, Bärbulescu v. Romania) in its guidelines "Protection of personal data in employment relationships" (20. December 2016) and emphasizes that the employees reasonably expect privacy at working place. For the monitoring of the use of technological devices to be permitted, the employees must first be precisely notified about how the monitoring is carried out and by who. All these issues can be regulated in a code of conduct. However, the sole regulation of the monitoring in a code of conduct does not already mean that such monitoring is also permitted. It is only permitted, if it is in accordance with constitutional provisions regarding protection of privacy of the employees and protection of personal data.

3. In which cases and under what conditions is it possible to access and monitor employees' personal communications through the company's technological devices (e-mail, instant messaging, etc.)?

The Constitution of the Republic of Slovenia ensures privacy of correspondence and other means of communication in article 37, which also applies to phone communication, e-mail etc. Not only the content of the communication is protected (the content of a phone conversation, e-mail), but also the data connected to it (for example the information about who sent an e-mail or to who this individual has sent it; the subject of the e-mail etc.). These also count as personal data and can therefore be collected and processed only in line with article 38 of the Constitution (which determines a right protection of personal data) and ZVOP-1 (in case of employees also in line with ZDR-1). About this see answer to question no. 8.

As mentioned, specific rules regarding if and under what conditions an employer can monitor employee's communication through company's technological devices, are not included in legislation. Considering constitutional theory, this is about a collision between two constitutional rights, the right to property and the right to privacy. An employer has the right to control his means and by extension, the right to monitoring and the employee justifiably expects a certain level of privacy even at work. Considering principle of proportionality, only such interference into a constitutional right is allowed, which will not grant absolute protection to the other right, but will only mean its limitation, proportional to the protection of the first right. The criteria in this regard have not been developed by case law yet, since these kinds of judicial cases are rare.

The position of Information Commissioner (evident from guidelines from 20 December 2016) is that insight to an employee's e-mail box or his computer (and reading his e-mails) is not allowed –unless in exceptional cases (for example death or a longer unavailability of an employee), when this is absolutely necessary to prevent a larger business damage, which could occur to the employer or to enable completing his legal obligations (finishing a business transaction, following obligations towards other employees, fulfilling the request of police or court…) and only if such possibility is provided in an employer's code of conduct, with which the employee was previously acquainted with and which determines appropriate measures (so called commission insight or just securing evidence).

4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?

Slovenian ZVOP-1 regulates general requirements for introduction of video surveillance and specifically determines the requirements for video surveillance of acces into official office or business premises and the video surveillance within work areas.

Video surveillance of access to official office or business premises can only be carried out if this is required to ensure safety of people or property, to ensure monitoring of entry or exit into and out of office or business premises or if due to the nature of work there could be a threat to employees. The decision of surveillance is made by an authorized head or the director of the company, and the written notice must include specified reasons for the implementation of video surveillance (specifically for each installed video camera). The Information Commissioner's cases show that such video surveillance is not permitted solely for the reason of monitoring the use of working time, since the employer has many other less invasive methods to carry out such monitoring.

The requirements to carry out video surveillance of working premises are even stricter. The video surveillance inside working premises can only be carried out in extraordinary cases, when this is necessary for safety of people or property or the protection of undisclosed data or business secrets, and this cannot be insured by other less invasive measures. The employer must in any case find out whether there is a milder measure, which would allow the employees to not be subject to video recording, so the employer must establish whether video surveillance is indeed the most proportional measure. Video surveillance can only be carried out in those parts of premises where earlier stated interests must be protected and is forbidden by law in working spaces outside of the working place, especially in changing rooms, elevators and in sanitary facilities.

Information Commissioner's cases explain, video surveillance is normally permitted for example in stores, warehouses, in places of the production where there is a higher risk of alienation of objects or causing greater damage, at bank counters, over cashiers in catering establishments, at working places dealing with cash transactions, working places where secret, sensitive or other classified personal data is stored (where video cameras must be pointed to carriers of such data and not to employees), etc. Video surveillance is not permitted for example in dining rooms, kitchens and regular offices where employees work.

Before introducing video surveillance of work premises, the employer must consult with the representative trade unions about the necessity of introduction of such video surveillance (if such trade union exists at the employer). In any case the employer must notify the employees in writing of the intended video surveillance beforehand.

5. Under what circumstances is it possible to install hidden cameras to control work activity? In particular, is its installation only possible when the company suspects that a criminal offense has been committed or also when there are signs of a breach of contract?

ZVOP-1 specifically determines requirement to introduce video surveillance (among which there is also prior notice too employees). In its Guidelines on exercising video surveillance (17. March 2015), Information Commissioner takes the view that a retraction from legally specified obligation to notify employees of video surveillance is only possible in case there is a valid reason. In this regard it refers to European Court on Human Rights in case KÖPKE v. Germany (no. 420/07 from 5 October 2010), which explains that such monitoring can only be legal if there is a founded suspicion of commitment of a criminal offense by employee and this suspicion cannot be confirmed any other way, at least not without greater costs, effort or time consumption, and if the monitoring is properly limited by time, space and in regard to exposed individuals and if the collected recordings are used exclusively for the purpose of dealing with the stated criminal offense (in a disciplinary procedure, probable judicial procedure that could follow).

In short, the purpose of hidden monitoring must only be in the investigation of a specific and serious incident, for example of long lasting evident theft by employees. Employer must consider other possibilities for investigation of the case before taking this step. It is also advised to entrust a private investigator or an outside security service with performance of such video surveillance.

6. In what cases is it possible to install geolocation systems (GPS) to control work activity?

Neither ZVOP-1 nor any other legislation does not specifically cover the use of GPS for monitoring employees. Since the use of GPS causes a formation of a personal data collection, ZVOP-1 and ZDR-1 rules must be followed in regard to permissibility of collecting and processing personal data of employees. ZDR-1 states in article 48 that personal data of employees can be collected and processed only if this is specified by law or if it necessary to exercise rights and obligations in an employment relationship or in regard to and employment relationship. Since there is not legal ground for running a register formed by the use of GPS devices, the employer must specifically determine which data he needs and for what purpose. If he does not prove this is necessary for the exercise of rights and obligations from an employment relationship or in relation to an employment relationship, he cannot obtain such data from employees. Besides this the employer must also judge the suitability and proportionality of GPS implementation –if he could reach the same purpose to his satisfaction by implementing measures that are less invasive to privacy, freedom of movement and dignity of employees.

Information Commissioner takes a view in his opinion no. 0712-2/2010/462 from 23 March 2010 that implementation of GPS devices is only permitted in cases when this is necessary for protection of people or property. Processing of personal data with the help of tracking devices is excessive, when the employer can organize work in a manner that enables the use of other means and methods for reaching these purposes.

Moreover, the employer must specify the use of GPS devices in its codes of conducts beforehand. All employees must be acquainted with content of such codes, especially the ones to whom these provisions apply (for example employees who use company vehicles, into which a GPS device is installed). Before implementing such monitoring, the employees must also be acquainted with a manner in which this device is used, functioning and purpose of installation by the employer and also with cases in which the collected data will be used. All these issues must be regulated in an employer's code of conduct.

7. In the event that the company fires an employee in breach of the conditions regarding control communications by e-mail or installation of video surveillance systems, what would be the qualification of the dismissal and what administrative sanctions could be derived?

Slovenian legislation stipulates that in case when an employee judicially exercises the wrongfulness of dismissal, the employer must prove there was a legal reason. In doing

so, he can use all available means to prove these facts and the court takes them into account in line with the principle of free assessment of evidence. The court normally cannot use evidence obtained by breaching constitutionally provided human rights and fundamental freedoms (see judgment of Supreme Court of the Republic of Slovenia in cases no. VIII Ips 120/2014; VIII Ips 156/2016, VIII Ips 2/2018). Constitutional Court's judgment no. Up-472/02 states that a consideration of evidence, obtained by a breach of the right to privacy is only exceptionally permitted in litigation, if there are specific justified circumstances (consideration of such evidence must have a special meaning for exercising constitutionally protected right and the court must take into account principle of proportionality and carefully judge which right should have an advantage).

If the court does not consider the evidence, obtained by a breach of human right and the employer does not manage to prove existence of a dismissal reason, the court establishes the wrongfulness of employment contract termination. In this case, an employer must take the employee back to work (reintegration) and acknowledge the time of service for the mean time and pay him all cash benefits (difference in salary etc.). On employee's or employer's initiative, the court can (when it establishes the wrongfulness of dismissal) establish that in regard of the circumstances and contractual parties' interests, the continuation of employment relationship is not possible anymore, therefore terminates the employment relationship with the judgment and acknowledges the employee a monetary compensation (instead of reintegration).

An employer who breaches his obligations in regard to video surveillance and also in regard to protection of personal data in general, is punished by a penalty in the amount from 4.170,00 to 12.510,00 EUR and the responsible person at the employer with the penalty from 1.250,00 to 2.080,00 EUR. Offenses and penalties are specified in ZVOP-1 and are imposed by Information Commissioner.

8. What personal data can be collected and processed in the framework of the employment relationship? In particular, is employees' consent necessary? In what cases is it not necessary?

ZVOP-1 generally stipulates that personal data can be processed either if the law allows it or if the individual allows it. By processing personal data in employment relationship, employer must oblige both ZVOP-1 and article 48 of ZDR-1, which states that the employer can collect, process, uses and forwards the personal data in cases, specified by ZDR-1 or and other law and if this is necessary to exercise rights and obligations from an employment relationship or in relation to an employment relationship.

Most collections of personal data and their contents are specified by Labour and Social Security Registers Act (ZEPDSV). As it derives from Article 12 of ZEPDSV, the employers can run a register of employees, a register of work expenses, a register of use of working time and a register of forms of solving collective work disputes at the employer. In the register of employees, the employers can collect the following personal data about an individual employee: name, date of birth, if the person does not have a personal identification number, place of birth, state of birth, if the state of birth is abroad, personal identification number, tax ID number, citizenship, permanent address, temporary address, education, information whether the employee is disabled, category of disability, whether the emlployee is partially retired, whether the employee carries out complementary work at other employer, the name of the other employer (and registration number) by which the employee carries out complementary work. Employer can collect and process these data (in line with general rules in ZVOP-1), without obtaining the consent from employee.

Other personal data can only be collected and processed by an employer in case this is necessary to exercise rights and obligations from an employment relationship or in relation to an employment relationship. If the employer proves such intention, he can collect the data without obtaining the consent from employee.

Although ZVOP-1 generally allows collection of personal data also when having a consent of the individual, the Information Commissioner took a view in guidelines (from 20 December 2016), that personal data of an employee can only be collected based on his personal consent in exceptional cases. It is permitted only under the condition that rejection of a consent does not have consequences on employment relationship or the employee's legal status (for example collection of personal data only for the purpose of organizing a trip, which can also be joined by employee's family members). The consent should normally be written (for the purpose of easier proof).

9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?

ZDR-1 stipulates and obligation of the employer in Article 10 to send the drafts of codes of conduct by which he regulates obligations of the employees to representative trade unions beforehand. If the trade union(s) gives its opinion in 8 days, the employer is obliged to consider this opinion and express its own position towards it before adopting the code of conduct. This obligation of an employer is also applicable to codes of conduct, with which an employer regulates the use of technological devices by employees.

Furthermore, ZVOP-1 provides an obligation of an employer in article 77 to consult representative trade unions by an employer before implementing video surveillance of work areas.

10. Is there a right to disconnect from technological devices outside working time? In this case, should the company define the extension and limits of this right jointly with the workers' representatives or can it do so through an internal policy?

Slovenian legal system does not specifically regulate the right of the employees to disconnect.

Employer is only bound by general rules regarding providing safety and health at work, which includes the prohibition of delegating work over specified time frames (full working time, under certain conditions overtime work). Employer must also ensure the employee minimal daily and weekly rest.

If the employee only works from home, he can distribute the time on his own, but even then the employer must ensure safe and healthy work.

With employees, who work at the employer's premises and occasionally from home by using technological devices (outside working hours), general rules should be applied and such work should count as overtime work that should be paid extra.

Monitoring in regard to respecting working time and ensuring safety and health at work, is carried out by labour inspection, which in case of employees, working at the employer's premises, is carried out only at the employer's premises (and not at employee's home).

IMPACTO LABORAL DEL USO DE DISPOSITIVOS TECNOLÓGICOS EN ESPAÑA

Sergi Gálvez Duran
Abogado laboralista, Cuatrecasas
Doctorando en Derecho, Universitat Ramón Llull-ESADE

Introducción

En España, la normativa laboral no contiene una previsión específica que establezca los derechos y deberes de los trabajadores en el ámbito del uso de las nuevas tecnologías en la empresa. Como consecuencia de la falta de regulación en el ámbito laboral y de las escasas previsiones de los convenios colectivos en materia de nuevas tecnologías, son los acuerdos e instrucciones a nivel de empresa, recogidos en forma de códigos de conducta o políticas internas, donde encontramos las regulaciones más precisas al respecto.

Mientras tanto, son las decisiones de los tribunales laborales, en la mayor parte basadas directamente en los preceptos constitucionales dedicados a los derechos fundamentales, las que están estableciendo la extensión y los limites sobre el uso de los dispositivos tecnológicos por los trabajadores, habiéndose construido en los últimos años principios doctrinales muy significativos con respecto a determinadas tecnologías –ordenador, e-mail, cámaras de videovigilancia–, que habrá que evaluar si son también aplicables a las denominadas tecnologías disruptivas –redes sociales, robótica, Internet of Things, Inteligencia Artificial, etc.–, que están llamadas a alterar sustancialmente aspectos esenciales de las relaciones laborales.

En ese contexto de desarrollo exponencial de las tecnologías en la empresa, el trabajador y su actividad laboral se convierten en una fuente constante y regular de datos, cuya calificación jurídica como "datos personales" hace entrar plenamente la relación laboral dentro de la normativa de protección de datos, que se ha visto reforzada con el Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPD), que supone un salto cualitativo respecto al nivel de exigencia al empresario y que, en los últimos años, ha tenido una trascendencia progresiva en las relaciones laborales y que se manifiesta en la continuidad de la litigiosidad en los tribunales laborales sobre su extensión y límites.

Por último, no es casualidad que, junto al tema de protección de datos, el otro centro de atención sea el de conseguir un equilibrio jurídico entre el uso intensivo de dispositivos tecnológicos en la empresa y la conciliación de la vida familiar y personal. En este sentido, al margen de alguna iniciativa parlamentaria, no se ha desarrollado a día de hoy

una regulación que establezca las bases de un derecho a la desconexión digital del trabajador fuera de la jornada de trabajo.

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa?

En España, no existe una regulación específica sobre el uso por los trabajadores de los dispositivos tecnológicos que la empresa pone a su disposición para el desarrollo de la actividad profesional. Por este motivo, los preceptos constitucionales y, en particular, los derechos fundamentales a la intimidad (artículo 18.1 Constitución Española (CE)), al secreto de las comunicaciones (artículo 18.3 CE) y a la autodeterminación informática (artículo 18.4 CE) son los parámetros delimitadores de los derechos de empresarios y de trabajadores en la aplicación de los dispositivos tecnológicos.

A pesar de esta ausencia de normativa laboral estatal en la ordenación específica de la incidencia de las nuevas tecnologías en las relaciones laborales, no es posible deducir que se haya dado un mayor protagonismo a la negociación colectiva que pueda haber colmado este relativo vacío. En efecto, debemos partir de una realidad estadística y es que la negociación colectiva en España sólo se ha introducido marginalmente en las nuevas tecnologías, a pesar de la recomendación de los Acuerdos Interprofesionales sobre Negociación Colectiva (2015-2017) en favor de ello: menos de un 15% de los convenios colectivos, entre un 10-15% en los últimos tres años, tratan de una forma relevante e identificativa la relación entre organización del trabajo y las nuevas tecnologías[104].

Por este motivo, son los tribunales los que están teniendo el protagonismo ordenador en materia de los efectos de la utilización de dispositivos tecnológicos en las relaciones laborales, ponderando los derechos fundamentales a la intimidad, al secreto de las comunicaciones y a la autodeterminación informática con el derecho empresarial al control de la prestación de trabajo.

2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o de una política interna sobre el uso de estos dispositivos? En caso contrario, ¿cómo se regula el uso de los dispositivos tecnológicos en la empresa?

En España, como hemos visto, no existe una regulación específica sobre el uso por los trabajadores de los dispositivos tecnológicos que la empresa pone a disposición de los

[104] Avance del Anuario de Estadísticas Laborales para el año 2016 sobre Convenios Colectivos (los datos para el año 2017 no están disponibles a fecha de cierre del presente artículo) (anuario disponible en: http://www.empleo.gob.es/es/estadisticas/anuarios/2016/index.htm).

trabajadores y, por tanto, el ordenamiento jurídico-laboral no contempla una obligación legal de disponer de un código de conducta telemático o una política interna sobre el uso de estos dispositivos.

Ahora bien, la sentencia del Tribunal Supremo de 26.9.2007[105] –reiterada por las sentencias de 8.3.2011 y 6.10.2011[106]– consideró que, como consecuencia de la creación de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores, existe una expectativa general de confidencialidad que, de acuerdo con las exigencias de buena fe, impone el deber de la empresa a establecer previamente las reglas de uso de esos medios e informar a los trabajadores de que va a existir control, así como de los medios y medidas que han de aplicarse en orden a comprobar la corrección de los usos, sin perjuicio de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

En virtud de lo anterior, la sentencia concluye que el empresario puede controlar el uso del ordenador –con base en el artículo 20.3 del Estatuto de los Trabajadores (ET)–, pero para que ese control sea lícito ha de establecer las reglas del uso del ordenador.

En virtud de esta jurisprudencia del Tribunal Supremo, con la prohibición empresarial del uso personal desaparecería la expectativa de confidencialidad del trabajador, por lo que no habría lesión del derecho a la intimidad ni del derecho al secreto de las comunicaciones.

Ahora bien, la sentencia del Tribunal Europeo de Derechos Humanos (TEDH) de 5.9.2017 (caso Barbulescu v. Rumanía), que resulta de aplicación directa en el ordenamiento español, estableció, entre los criterios que los estados miembros de la Unión Europea deben considerar como relevantes cuando sus tribunales enjuicien casos en los que esté en juego el respeto de la vida privada en el marco de las relaciones laborales, la necesidad de verificar si el empresario ha notificado de forma "*previa, explicita, precisa y clara*" a los trabajadores afectados sobre la posibilidad de control y su naturaleza. Así, a diferencia de la jurisprudencia española, el TEDH señala que, a los efectos de que la advertencia de no utilizar los recursos de la empresa para fines personales sea válida no es suficiente la mera prohibición de uso no profesional, de manera que para destruir la expectativa de confidencialidad es necesario, además de la

[105] Rec. núm. 966/2006.
[106] Rec. núm. 826/2010 y Rec. núm. 4053/2010.

prohibición, la advertencia previa de que la empresa se reserva la posibilidad de control[107].

Hay que entender, por tanto, que ya no basta con la prohibición de uso personal para superar la expectativa de confidencialidad, sino que, además, resulta necesario una advertencia clara y previa de control. Sin embargo, el TEDH no precisa el contenido de la información que debe proporcionarse al trabajador, por lo que podría tratarse de una advertencia genérica sobre la existencia de control o una información específica sobre los medios de control a aplicar y sobre la extensión de éste.

En España, la sentencia del Tribunal Supremo de 8.2.2018[108] declara ajustado a derecho el acceso de la empresa a los correos electrónicos del trabajador, por entender que en la empresa existía una política de uso estrictamente profesional de los medios de la empresa, que impedía una expectativa razonable de privacidad. El tribunal considera suficiente el hecho de que los empleados, cada vez que accedían con su ordenador a los sistemas informáticos de la compañía, y de forma previa a dicho acceso, debían aceptar las directrices en Política de Seguridad de la Información, en la que se indicaba que el acceso lo era para fines estrictamente profesionales, reservándose la empresa el derecho de adoptar las medidas de vigilancia y control necesarias.

3. ¿En qué supuestos y en qué condiciones es posible el acceso y la monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos propiedad de la empresa (e-mail, mensajería instantánea, etc.)?

El ordenamiento jurídico español no establece los criterios para la monitorización de las comunicaciones personales de los trabajadores mediante dispositivos tecnológicos en la empresa.

Ahora bien, la sentencia del Tribunal Supremo de 8.2.2018[109], aplicando la doctrina del TEDH contenida en la sentencia de 5.9.2017 (caso Barbulescu v. Rumanía), entiende que para validar el acceso a las comunicaciones personales es necesario realizar una ponderación de los intereses en juego (por un lado, la vida privada y correspondencia del trabajador y, por otro, el poder de dirección del empresario), lo cual exige una valoración de los siguientes parámetros:

[107] Aurelio DESDENTADO BONETE y Elena DESDENTADO DAROCA, "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", nº 1, *Revista de Información Laboral*, 2018, p. 10.
[108] Rec. núm. 1121/2015.
[109] Rec. núm. 1121/2015.

1. Grado de intromisión del empresario en las comunicaciones personales.
2. Concurrencia de una razón legítima de la empresa para la monitorización.
3. Existencia (o no) de otros medios menos intrusivos.
4. Destino dado por la empresa al resultado del control.
5. La previsión de garantías para el trabajador.

Según establece el Tribunal Supremo, los citados requisitos se reconducen al triple juicio de proporcionalidad aplicado para la ponderación de derechos fundamentales o derechos constitucionalmente garantizados fijado por el Tribunal Constitucional[110], por lo que resulta necesario constatar si la medida de control de las comunicaciones cumple los tres requisitos siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en el sentido estricto).

4. ¿En qué circunstancias es posible instalar sistemas de videovigilancia de carácter permanente para controlar la actividad laboral?

La eventual instalación de cámaras de videovigilancia en el centro de trabajo estaría incluida dentro de las potestades ordinarias de vigilancia del empresario, facultadas por el artículo 20.3 ET[111], por lo que la empresa se encontraría legitimada para tratar imágenes de los trabajadores sin necesidad de obtener el consentimiento de los trabajadores.

Ahora bien, la legitimación en la instalación y uso de tales cámaras no es absoluta, sino que se encuentra sometida a las exigencias generales del ordenamiento jurídico laboral, así como a la normativa referente a la protección de datos de carácter personal, en tanto que a través de estos sistemas de control se captan imágenes de personas identificadas o identificables.

En este sentido, la normativa de protección de datos establece la obligación del responsable del tratamiento de datos (la empresa) de informar al interesado (los trabajadores) sobre la recogida y el tratamiento de sus datos personales, de conformidad

[110] Sentencia 66/1995, de 8 de mayo.

[111] El artículo 20.3 ET establece que el empresario "*podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso*".

con lo previsto en el artículo 13 RGPD. A los efectos de cumplir con este deber, es necesario diferenciar si la instalación de la cámara en el centro de trabajo es como medida de seguridad para proteger la instalación y sus empleados, o si es una medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

En el primer caso, es decir cuando la finalidad es la seguridad y protección de las instalaciones y personal de la empresa, con carácter previo a la instalación de los dispositivos de videovigilancia, la empresa deberá colocar en las zonas videovigiladas un distintivo informativo con el siguiente contenido:

- La existencia del tratamiento (videovigilancia).
- La identidad del responsable del tratamiento o del sistema de videovigilancia, y la dirección del mismo.
- La posibilidad de ejercitar los derechos reconocidos en los artículos 15 a 22 RGPD.
- Dónde obtener más información sobre el tratamiento de los datos personales.
- También se pondrá a disposición de los interesados el resto de la información que debe facilitarse a los afectados en cumplimiento del derecho de información regulado en el RGPD.

En el segundo supuesto, es decir cuando el objetivo principal de la instalación de las cámaras va dirigido al control del cumplimiento por los trabajadores de sus deberes laborales, la empresa –además de cumplir con los requisitos señalados en el apartado anterior– tiene la obligación de informar expresamente a los trabajadores del tratamiento de datos con este fin, indicando el alcance específico que se va a dar las imágenes para el control laboral, conforme a lo previsto en la normativa de protección de datos[112].

Habida cuenta de la vinculación existente entre la empresa y el trabajador, dicha información podría ser facilitada a través del correspondiente contrato de trabajo (en la cláusula en materia de protección de datos de carácter personal que se incluya) o en las políticas que se adopten a nivel interno, siempre que estas últimas gocen de difusión suficiente.

Adicionalmente, con carácter previo a la adopción de la medida, la empresa debe informar a la representación legal de los trabajadores de la intención de instalar un sistema de cámaras de videovigilancia en sus instalaciones, en la medida en que la

[112] Así lo establecen las resoluciones de la Agencia Española de Protección de Datos (AEPD) E/03676/2016 y E/05488/2016.

decisión indicada constituiría la adopción de un nuevo sistema de control del trabajo a los efectos del artículo 64.5.f) ET.

En dicha comunicación, deberán detallarse la ubicación[113] de las cámaras y los motivos para la instalación de la misma, esto es, si tiene por objetivo garantizar la seguridad en las instalaciones, controlar el cumplimiento por parte de los empleados de sus obligaciones laborales, o ambas finalidades.

Al mismo tiempo, los representantes tienen derecho a emitir, con carácter previo a la ejecución de la decisión, un informe acerca de la idoneidad de la medida relativa a la implantación del sistema de videovigilancia. En este sentido, cabe destacar que el Tribunal Supremo ha declarado que la implantación en la empresa de un sistema de organización y control del trabajo exige únicamente la emisión de informe previo por parte de la representación social, pero no la consulta del empresario[114].

5. ¿En qué circunstancias es posible instalar sistemas de videovigilancia ocultos para controlar la actividad laboral? En particular, ¿su instalación sólo es posible cuando la empresa sospecha que se ha cometido un ilícito penal o también cuando existen indicios de un incumplimiento laboral?

En lo que se refiere a las cámaras ocultas, entendiendo como tales aquellas instaladas de forma no visible y, por tanto, sin previa advertencia a los trabajadores, el Tribunal Constitucional español ha venido admitiendo en las últimas resoluciones dictadas sobre esta cuestión (sentencias 29/2013 –caso Universidad de Sevilla– y 39/2016 –Caso Bershka–) su instalación temporal cuando existan indicios razonables de irregularidades y dicha instalación sea el medio idóneo para detectarlas, de forma que si se informase sobre la existencia de cámaras se frustraría esta finalidad.

En todo caso, la instalación de las cámaras estará sometida al triple juicio de proporcionalidad, por lo que resulta necesario constatar si esta medida empresarial cumple los tres requisitos siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que

[113] En cuanto a la ubicación de las cámaras de videovigilancia, éstas deben colocarse de la forma que sea menos gravosa y menos invasiva del derecho a la intimidad de los trabajadores, para satisfacer su finalidad, lo que implica que solo deberán captarse imágenes de aquellos espacios (áreas de trabajo) que sean indispensables. Sobre este particular, el Tribunal Constitucional (sentencias 186/2000, de 10 de julio y 39/2016, de 3 de marzo) ha declarado que las grabaciones deberían realizarse únicamente en el ámbito físico estrictamente imprescindible "*para el correcto y ordenado respeto de los derechos fundamentales del trabajador y, muy especialmente, del derecho a la intimidad personal que protege el artículo 18.1 CE, teniendo siempre presente el principio de proporcionalidad*".

[114] Sentencia de 13.9.2016 (rec. núm. 206/2015).

no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en el sentido estricto).

En el caso concreto de la instalación de cámaras de videovigilancia ocultas, ello significa que habrá de valorarse, en primer lugar, si el empresario tiene un interés suficiente y objetivo para ello, en este caso, tener conocimiento del comportamiento del trabajador cuando se han detectado irregularidades en la empresa, con prohibición estricta de aquellas medidas que supongan un control arbitrario.

En segundo lugar, dado que estos dispositivos permiten un control especialmente incisivo, debe justificarse que la grabación de las imágenes resulta imprescindible para asegurar el patrimonio empresarial. De modo que si existen otras medidas menos afectantes y que permiten alcanzar el mismo resultado habrá que utilizar estas últimas. En conexión con lo anterior, dado que la utilización de las cámaras de videovigilancia debe ponerse en relación con la finalidad objetiva que justifica su instalación, su ubicación debe ser estrictamente imprescindible para satisfacer las necesidades de la empresa (sentencia del Tribunal Constitucional 186/2000, de 10 de julio).

Asimismo, y lo que es más importante en estos casos, la grabación sólo debe realizarse y mantenerse durante un tiempo estrictamente necesario para satisfacer los fines que la justifican. De un parte, el control tiene que estar sujeto a unos límites temporales definidos en función de la finalidad que justifica su adopción. Mientras que por razones de seguridad la empresa puede instalar cámaras para filmar determinadas dependencias del centro de trabajo con carácter permanente, en supuestos de investigación de irregularidades cometidas en la empresa sólo resulta lícito una vigilancia limitada en el tiempo. Además, la restricción temporal del control de los trabajadores comprende también la conservación de las imágenes captadas, que sólo podrán almacenarse aquellas que sean imprescindibles y por el tiempo estrictamente necesario para satisfacer la finalidad objetiva que justifica la grabación, de conformidad con el artículo 5.1.e) RGPD.

En mi opinión, la sentencia dictada por el TEDH en el caso "López Ribalda y otros" contra España (asuntos 1874/13 y 8567/13) el 9 de enero de 2018, ratifica la doctrina constitucional señalada arriba, exigiendo que, en la instalación de cámaras fijas, deba cumplirse con la obligación de información expuesta. En concreto, la sentencia –que analiza el supuesto de hecho de una cadena de supermercados donde se comprueba que existieron irregularidades entre las existencias y las ventas reales– declara que la

instalación de cámaras ocultas supone la vulneración de los artículos 6 y 8 de la Convención Europea de Derechos Humanos (CEDH), por los siguientes motivos:

- La Ley Orgánica de Protección de Datos española establece claramente la obligación de informar de forma previa, explícita, clara y precisa de la existencia de medios de recepción y tratamiento de datos, incluyendo la grabación (artículo 5 LOPD).

- El Tribunal, a diferencia de otro supuesto que fue igualmente analizado por el TEDH (caso Köpke v. Germany 420/07, de 5.10.2010), considera que las cámaras ocultas grabaron a todo el personal (no exclusivamente a los que pudieran resultar sospechosos), durante semanas, sin límite de tiempo y durante todo el tiempo de trabajo.

Por tanto, la instalación de sistemas de videovigilancia ocultos para controlar la actividad laboral exige el cumplimiento de los tres requisitos o condiciones siguientes: (i) que se realice sobre la base de una sospecha previa; (ii) únicamente respecto de los trabajadores sobre los que existe tal sospecha; y (iii) de forma temporal.

En España, es posible que la actual Ley Orgánica de Protección de Datos sufra una profunda modificación, a través del Proyecto de nueva Ley Orgánica de Protección de Datos que se está tramitando actualmente en las Cortes Generales, a raíz de la aprobación del RGPD. A este respecto, debe destacarse que la actual redacción del Proyecto de Ley contiene un artículo específico sobre videovigilancia. Entre otras cuestiones, recoge específicamente el deber de los empleadores de informar a los trabajadores acerca de la instalación de sistemas de cámaras para el ejercicio de funciones de control.

Además, establece de manera taxativa que, en el supuesto de que las imágenes captaran la comisión flagrante de un hecho delictivo, la ausencia de la información a los trabajadores no privará de valor probatorio a las imágenes, sin perjuicio –puntualiza– de las responsabilidades que pudieran derivarse de dicha ausencia. Por tanto, según esta previsión, la utilización de cámaras ocultas sin información a los trabajadores solamente sería posible ante sospechas de un ilícito penal, pero nunca laboral.

6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?

Con carácter general, los tribunales españoles han indicado que el empresario debe informar a los trabajadores de la instalación del sistema de geolocalización y de la

finalidad que se persigue, y han declarado la vulneración del derecho a la protección de datos del empleado (artículo 18.4 CE) en supuestos en los que la empresa únicamente informó al trabajador de la instalación del GPS mediante una condición general de un contrato de compromiso de confidencialidad, por considerar que no existió una adecuada información (tanto de la existencia del dispositivo, como de su concreto alcance y utilización) en los términos de claridad y suficiencia que son exigibles a los efectos de evitar actuaciones sorpresivas[115].

De modo más específico, el uso de un sistema de GPS presenta particularidades en función del uso que se pretenda destinar al mismo. Cuando se trata del uso de estos medios en los vehículos de la empresa, cuya función principal consiste en verificar que se realiza un uso de ellos acorde con los estándares de la buena fe, el uso del GPS en vehículos de empresa estaría justificado para dar cumplimiento a las siguientes finalidades:

- Como medida de seguridad del propio empleado o de las mercancías que tiene a su cargo. En este tipo de casos y en otros similares, estaría justificada la medida basada en lo que concierne a la seguridad de los trabajadores en virtud de la legislación sobre Prevención de Riesgos Laborales. Podría incluso aceptarse el uso de un sistema de geolocalización en objetos que portase constantemente el propio trabajador, como por ejemplo un teléfono móvil.

- Para una mejor asignación de los medios que permita cumplir las prestaciones que deben realizarse en lugares dispersos. Por ejemplo, en empresas de transporte de mercancías o personas.
- Para el seguimiento y la facturación de una prestación.

- Para el seguimiento del tiempo de trabajo, cuando este seguimiento no pueda ser realizado por otros medios menos gravosos e igualmente eficientes.

El otro gran grupo de casos lo constituye aquél en el que el dispositivo geolocalizador se inserta en el dispositivo móvil o smartphone facilitado por la empresa al trabajador. En particular, su función cobra sentido en aquellos puestos de trabajo que implican una cierta movilidad del empleado (por ejemplo, comerciales). En este sentido, la doctrina judicial[116] ha declarado que la instalación de un sistema de localización permanente del vehículo o del teléfono móvil del trabajador debe superar el triple juicio de proporcionalidad. En relación con ello, se ha considerado que la instalación de un

[115] STSJ de Castilla-La Mancha, de 17.6.2014 (Rec. núm. 1162/2013).

[116] Entre otras, la sentencia del Tribunal Superior de Justicia de Galicia de 17.1.2014 (rec. núm. 3483/2013).

sistema de geolocalización constituye un medio de vigilancia adecuado y proporcional cuando la empresa tiene un claro interés en tener localizados sus vehículos, por la necesidad de realizar el trabajo fuera de las dependencias de la empresa.

7. En el caso de que la empresa haya realizado un despido incumpliendo los requisitos de control de comunicaciones por e-mail o de instalación de sistemas de videovigilancia, ¿cuál sería la calificación del despido y qué sanciones administrativas se podrían derivar?

En el ordenamiento jurídico-laboral español, la consecuencia jurídica en caso de proceder al despido del trabajador con incumplimiento de los requisitos antes citados en materia de control de las comunicaciones y de instalación de cámaras de videovigilancia puede ser:

- La nulidad del despido, por vulneración del derecho fundamental que esté en juego en cada caso –secreto de las comunicaciones, intimidad o protección de datos–, en virtud del artículo 55.5 ET.

- La procedencia o improcedencia del despido, según haya quedado o no probado el incumplimiento contractual alegado en la carta de despido, una vez eliminados los hechos acreditados mediante pruebas que se hayan obtenido vulnerando derechos fundamentales, según lo previsto en el artículo 90.2 de la Ley Reguladora de la Jurisdicción Social (LRJS).

Se trata de una cuestión sobre la que no existe jurisprudencia consolidada. Por un lado, existen sentencias[117] que han rechazado la calificación de nulidad del despido, por considerar que la calificación de nulidad tiene su fundamento cuando el despido en sí mismo responde a una causa vulneradora de un derecho fundamental, pero no cuando la empresa ha vulnerado los derechos de los trabajadores para obtener la prueba de la existencia de la causa alegada para justificar el despido. En ese caso, esta parte de la doctrina judicial entiende que procede la nulidad de la prueba obtenida con vulneración de derechos fundamentales, pero que esa nulidad no puede extenderse a la calificación del despido, que podrá ser improcedente o procedente si, una vez eliminados los hechos acreditados mediante la prueba ilícita, aún resulta probado un incumplimiento grave y culpable del trabajador.

Por otro lado, sentencias dictadas en sede de suplicación consideran que la ilicitud en la obtención de la prueba utilizada por la empresa para acreditar el incumplimiento del

[117] Entre otras, la sentencia del Tribunal Superior de Justicia de Castilla-La Mancha de 12.1.2018 (rec. núm. 1416/2017).

trabajador supone la nulidad del despido, por entender que el artículo 55.5 ET acoge, no sólo los supuestos en los que el despido se produce como consecuencia del ejercicio legítimo de un derecho fundamental, sino también aquellos casos en que los hechos que sustentan el despido han sido conocidos por el empresario mediante métodos que vulneran los derechos fundamentales del trabajador[118].

Al margen de lo anterior, en lo que afecta a empresas como responsables o encargados del tratamiento, el artículo 83 RGPD tipifica las siguientes infracciones, cuya comisión sería sancionable con independencia de la calificación del despido:

- Infracciones de las obligaciones de responsables y encargados contenidas en los artículos 8, 11, 25-39, 42 y 43 RGPD.

- Infracciones de los artículos 5-9 (principios básicos para el tratamiento, incluidas las condiciones para el consentimiento), de los artículos 12-22 (derechos de los interesados), de los artículos 44-49 (transferencias internacionales), y las obligaciones adoptadas para tratamientos específicos por los estados miembros con arreglo al capítulo IX (que prevé la posibilidad de establecer normas en el ámbito laboral).

- Incumplimiento de una resolución, una limitación temporal o definitiva del tratamiento, o una suspensión de flujos de datos dictada por la autoridad de control, así como de la obligación facilitar el acceso a todos los datos, información, locales, equipos y medios de tratamiento de datos a la autoridad de control cuando ejerce sus poderes de investigación.

En caso de incumplimiento, las multas previstas en el RGPD pueden alcanzar los 20 millones de euros o el 4% de los ingresos brutos del grupo empresarial al que pertenezca la compañía. El organismo responsable de velar por el cumplimiento en España será la Agencia Española de Protección de Datos (AEPD).

8. ¿Qué datos personales pueden ser recogidos y tratados en el marco de la relación laboral? En particular, ¿es necesario el consentimiento del trabajador? ¿En qué casos no es necesario?

Dado que, por el momento, España no ha adaptado el contenido del RGPD a las particularidades del ordenamiento jurídico español, el Reglamento europeo –que resulta

[118] Entre otras, la sentencia del Tribunal Superior de Justicia de País Vasco de 10.5.2011 (rec. núm. 644/2011).

directamente aplicable sin necesidad de transposición– es la norma en materia de recogida y tratamiento de datos personales de los trabajadores.

Los datos que pueden recogerse y tratarse a partir de ahora en el marco de la relación laboral se limitan a aquellos que sean adecuados, pertinentes y necesarios para el cumplimiento y la ejecución del contrato de trabajo, en atención al principio de minimización de datos que introduce el Reglamento europeo (artículo 5 RGPD). En el ámbito laboral, el tratamiento será legítimo cuando resulte "*necesario para la ejecución de un contrato en el que el interesado es parte*" (artículo 6.1 b) RGPD), o bien por ser necesario para "*el cumplimiento de una obligación legal aplicable al responsable del tratamiento*" (artículo 6.1 c) RGPD).

En este sentido, es importante subrayar que el consentimiento será necesario cuando no concurra otra base jurídica que legitime la recogida o el tratamiento de datos, siendo este espacio muy reducido en el ámbito de la relación laboral. Por ejemplo, en aquellos casos en que la recogida de datos responda a cuestiones organizativas o prestaciones accesorias, tales como la grabación de la imagen del trabajador para fines comerciales, la contratación de un seguro de salud, o proporcionar la cuenta de correo electrónico personal.

En cualquier caso, y tratándose de trabajadores por cuenta ajena, la situación de dependencia respecto de la empresa hace que partamos de un "consentimiento débil" del trabajador, tal y como ha reconocido el Tribunal Supremo en su sentencia de 21 de septiembre de 2015[119]. Por esta razón, y de conformidad con lo previsto en el artículo 32 RGPD, será necesario articular las garantías necesarias para asegurar que el consentimiento del trabajador es libre, especifico, informado e inequívoco[120].

Además, debe tenerse en cuenta que el RGPD, como novedad y a diferencia de la normativa española, no admite la posibilidad de obtener el consentimiento tácito de los interesados, sino que el consentimiento debe darse "*mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen,*

[119] Rec. núm. 259/2014.

[120] Sobre este particular, el denominado "Grupo de Trabajo del artículo 29" (de la Directiva) ha afirmado lo siguiente: "[c]*uando se requiera el consentimiento de un trabajador y exista un perjuicio potencial o real relevante derivado de la falta de consentimiento, se considerará que el consentimiento no cumple lo establecido en el artículo 7 o en el artículo 8 si no es otorgado libremente. Si no es posible para el trabajador denegarlo, no se considerará consentimiento.* […] *Un ámbito conflictivo se presenta cuando otorgar el consentimiento es una condición para el empleo. En teoría, el trabajador puede denegar su consentimiento, pero la consecuencia podría ser la pérdida de una oportunidad de empleo. En tales circunstancias el consentimiento no se otorga libremente y por tanto no es válido*".

como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal" (considerando 32).[121]

Ahora bien, la gran pregunta gira en torno a la validez del consentimiento en el contrato de trabajo. Para algunos autores, "*el consentimiento para tratamientos de datos con finalidades distintas al mantenimiento o cumplimiento de la relación laboral, debería entenderse no válido por situarse en el contrato de trabajo*",[122] apoyándose para ello en la STS de 21 septiembre 2015[123], que declaró abusiva y contraria a la Ley Orgánica de Protección de Datos una cláusula tipo introducida por la empresa en todos sus contratos de trabajo por ser genérica y tras poner en duda la voluntariedad del trabajador manifestada en el contrato.[124]

La Audiencia Nacional se ha pronunciado en el mismo sentido en la reciente sentencia de 15 de junio de 2017[125] que analiza el supuesto de una empresa de telemarketing que hizo constar en el contrato de trabajo una cláusula-tipo por la que el trabajador prestaba su consentimiento para la cesión de su imagen. La Sala de lo Social entiende que la cesión de la imagen a la empresa requiere el consentimiento de los trabajadores, en tanto que el servicio de video llamada con clientes es sólo "*una de las múltiples funcionalidades del telemarketing, que es absolutamente minoritaria en la empresa, como demuestra que, a día de hoy, la desempeñan quince trabajadores en un colectivo de 6000*" y, por consiguiente, "*no es absolutamente imprescindible para el cumplimiento del objeto del contrato*".[126]

En cuanto a la forma en la que debe prestarse ese consentimiento, la Audiencia Nacional, en línea con la interpretación del Tribunal Supremo, entiende que es inadmisible "*la utilización de cláusulas tipo de contenido genérico, que no vayan asociadas a servicios concretos, requeridos por contratos específicos*", por considerar que dicha generalización "*deja sin contenido real el derecho a la propia imagen de los*

[121] Jennifer BEL ANTAKI y Sergi GÁLVEZ DURAN, "Claves sobre la recogida de datos personales del trabajador en el marco de la relación laboral (a la luz del nuevo Reglamento UE 679/2016)", LA 2017 - I International Congress Labour 2030 - "rethinking the future of work", *publicación en curso*, p. 17.

[122] Carlos PRECIADO DOMÈNECH, *El derecho a la protección de datos en el contrato de trabajo (adaptado al nuevo Reglamento 679/2016, de 27 de abril,* Aranzadi, Pamplona, 2017, p. 10.

[123] Rec. núm. 259/2014.

[124] Jennifer BEL ANTAKI y Sergi GÁLVEZ DURAN, "Claves sobre la recogida de datos personales del trabajador en el marco de la relación laboral (a la luz del nuevo Reglamento UE 679/2016)", LA 2017 - I International Congress Labour 2030 - "rethinking the future of work", *publicación en curso*, p. 17.

[125] Rec. núm. 137/2017.

[126] Jennifer BEL ANTAKI y Sergi GÁLVEZ DURAN, "Claves sobre la recogida de datos personales del trabajador en el marco de la relación laboral (a la luz del nuevo Reglamento UE 679/2016)", LA 2017 - I International Congress Labour 2030 - "rethinking the future of work", *publicación en curso*, p. 18.

trabajadores, que queda anulado en la práctica, aunque se diera consentimiento genérico al formalizar el contrato".[127]

En todo caso, téngase en cuenta que el artículo 7.2 RGPD exige que, cuando el consentimiento se solicite por escrito, ello se realice de forma "*inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo*".

9. ¿Qué información en el ámbito de la protección de datos personales está obligada la empresa a proporcionar a la representación legal de los trabajadores? ¿Cómo y con qué periodicidad?

El RGPD no prevé la obligación de informar a los representantes de los trabajadores sobre la recogida y tratamiento de datos personales de la plantilla.

Si bien el artículo 88 RGPD recomienda a los estados miembros una regulación específica "*mediante ley o convenio colectivo*" del tratamiento de datos personales en el ámbito laboral, el texto del Proyecto de Ley Orgánica de Protección de Datos que adaptaría la normativa española al RGPD no entra a desarrollar las especificidades en materia de cesión de datos personales a los representantes de los trabajadores.

Sentado lo anterior, debemos destacar que cualquier cesión de datos a los representantes de los trabajadores que exceda del legítimo ejercicio de las funciones de control que la ley (artículo 64, apartados 1, 7 y 9 ET) o el convenio colectivo aplicable atribuyen a la representación legal de los trabajadores debe contar con el consentimiento de los trabajadores afectados (el consentimiento sí ha sido modificado por el RGPD, en tanto que ahora debe ser prestado de forma inequívoca –no se admite el consentimiento tácito o por omisión–). En este sentido, la AEPD ha señalado en repetidas ocasiones que la labor de vigilancia y control de los representantes de los trabajadores puede entenderse cumplida sin necesidad de proceder a una información "masiva". Solo cuando esa vigilancia o control se refieran a un sujeto o sujetos concretos, será posible la cesión de datos específicos individualizados. En el resto de casos, esa labor quedará plenamente satisfecha mediante la cesión de datos disociados (es decir, sin referenciar a personas concretas). Por ello, habrá que analizar cada supuesto de hecho concreto para valorar si la base jurídica del tratamiento es adecuada al ámbito competencial de los representantes de los trabajadores[128].

[127] Jennifer BEL ANTAKI y Sergi GÁLVEZ DURAN, "Claves sobre la recogida de datos personales del trabajador en el marco de la relación laboral (a la luz del nuevo Reglamento UE 679/2016)", LA 2017 - I International Congress Labour 2030 - "rethinking the future of work", *publicación en curso*, p. 18.

[128] Al respecto, pueden verse los Informes Jurídicos de la AEPD núm. 300/2008, 437/2008, 491/2008, 524/2008, 604/2009, 71/2010, 154/2010, 187/2010, 327/2010, 384/2010).

En relación con el alcance de este deber de información, y habida cuenta de las últimas resoluciones de la AEPD[129] que han impuesto sanciones a empresas por entregar datos personales excesivos a la comisión negociadora de un procedimiento colectivo, es necesario encontrar un equilibrio entre la buena fe de la empresa en la negociación y los requisitos para la cesión legal de datos que impone el nuevo Reglamento.

10. ¿Existe un derecho a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo? En su caso, ¿debe la empresa definir la extensión y límites de este derecho conjuntamente con los representantes de los trabajadores o puede hacerlo mediante una política empresarial?

En España, el ordenamiento jurídico-laboral no reconoce un derecho específico del trabajador a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo. Es decir, no existe la obligación empresarial de garantizar que los trabajadores están desconectados de los dispositivos digitales y medios de comunicación durante el tiempo de descanso.

Ahora bien, como consecuencia de la obligación empresarial de respetar la normativa sobre tiempo de trabajo (artículos 34, 36 y 37 ET), de garantizar a los trabajadores su seguridad y salud en el trabajo (artículos 4.2.d), 19 ET y 14 LPRL) y de retribuir en atención al tiempo de trabajo –abonando, en su caso, la realización de horas extraordinarias– (artículos 4.2.f) y 35 ET), es posible defender que existe un deber empresarial genérico de adoptar mínimas medidas de control del tiempo de trabajo y del tiempo de descanso de los trabajadores.

La facultad (junto al deber) empresarial de control del artículo 20.3 ET permite a la empresa verificar tanto que los trabajadores cumplen con su jornada de trabajo, como que no exceden de la misma. En relación con ello, no existe un derecho individual del trabajador a determinar su tiempo de trabajo, por lo que no tiene capacidad para, unilateralmente y sin el consentimiento de la empresa, ampliar el número de horas trabajadas mediante la realización de horas extraordinarias u horas complementarias respecto los trabajadores a tiempo parcial.

[129] La Resolución de la AEPD de 15 de marzo de 2018 impone una sanción a una empresa por entregar datos personales excesivos a la comisión negociadora de un Expediente de Regulación Temporal de Empleo (ERTE). En concreto, se considera que la Empresa facilitó datos que no eran necesarios para la negociación del ERTE, tales como el DNI, la fecha de nacimiento, teléfono, o el número de afiliación a la seguridad social.

En principio, existe libertad empresarial en la determinación de la forma de control del tiempo de trabajo (en virtud de la facultad de control del artículo 20.3 ET), pudiéndose adaptar a las necesidades de la empresa y a las diversas fórmulas de tiempo de trabajo en ella existentes. A título ejemplificativo, en aquellas empresas en que los trabajadores están sujetos a un control horario con cierta fijeza, será posible emplear sistemas de control formales tales como el fichaje o el registro, mientras que en aquellas empresas que reconocen a sus trabajadores un grado acentuado de libertad en la gestión del tiempo de trabajo, podrían utilizarse fórmulas menos formalistas de control, como el autocontrol verificable.

IMPACTO LABORAL DEL USO DE DISPOSITIVOS TECNOLÓGICOS EN ARGENTINA

Vanesa Beatriz Lamamí,
Profesora Universidad Nacional de José C. Paz
Universidad Nacional de Buenos Aires

Introducción

El impacto de la tecnología en las relaciones de trabajo ha significado un cambio de paradigma en el equilibrio que la doctrina y la jurisprudencia habían considerado consolidado en relación a las facultades de control y dirección del empleador, y el respeto de los derechos humanos de los trabajadores. Careciendo de regulación especial se han desarrollado jurisprudencialmente, estándares que procuran compatibilizar el derecho de intimidad y las potestades de control y dirección.

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los Dispositivos tecnológicos en la empresa?

En Argentina no existe un cuerpo normativo que regule el uso de dispositivos electrónicos en las relaciones de trabajo. La jurisprudencia de la Justicia Nacional del Trabajo ha utilizado las normas generales de la Ley de Contrato de Trabajo N° 20.744 y de la Ley de Protección de Datos Personales N° 25.326 en adelante LPDP, para delinear los principales criterios que, fundamentalmente, procuran compatibilizar el ejercicio de la facultad de control del empleador y el derecho a la intimidad de las/los trabajadoras y trabajadores.

2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o de una política interna sobre el uso de estos dispositivos? En caso contrario, ¿cómo se regula el uso de los dispositivos tecnológicos en la empresa?

No existe una obligación legal de disponer de un código de conducta telemático sobre el uso de dispositivos en la empresa, sin embargo, la jurisprudencia ha valorado especialmente este aspecto al momento de fundar sus sentencias. Cabe citar la Disposición N° 10/2015 de la Dirección de Datos Personales, que en el marco de la reglamentación de la LPDP (N° 25.326) ha regulado las condiciones de licitud para la recolección de imágenes digitales con fines de seguridad. Dentro de las obligaciones a cargo del responsable del tratamiento de las imágenes obtenidas se encuentra la de contar con un manual de tratamiento de imágenes digitales.

3. ¿En qué supuestos y en qué condiciones es posible el acceso y la monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos propiedad de la empresa (e-mail, mensajería instantánea, etc.)?

El ordenamiento laboral Argentino no prevé la existencia de supuestos y las condiciones de licitud para la monitorización de las comunicaciones personales de los trabajadores. Al respecto, la jurisprudencia y la doctrina han centrado el debate en la monitorización de comunicaciones realizadas exclusivamente desde "casillas de mail laborales" provistas por el empleador, en el entendimiento de que dichas casillas de mail integran la categoría de herramientas de trabajo; "medios instrumentales provistos a los trabajadores" (Artículo 84 LCT). De la propiedad del empleador se derivan las facultades de control, por ello resulta inadmisible la posibilidad de monitorización de correos remitidos desde casillas personales. Fundamentalmente la controversia ha quedado circunscripta a la determinación de estándares que compatibilicen el derecho de intimidad de los dependientes y las facultades de control del empleador en cuanto a la protección de sus bienes (artículo 70 LCT) así como a sus facultades de dirección en el modo de prestación de servicios.

Con relación a los mecanismos de control, la LCT establece que;

a. En todos los casos deberán salvaguardar la dignidad del trabajador, y deberán practicarse con discreción
b. Deben realizarse por medios de selección automática destinados a la totalidad del personal (artículo 70 LCT).

Sobre el tema en particular la jurisprudencia ha considerado aplicables los siguientes estándares[130]:

a. La revisión de la cuenta de mail de los/as empleados/as requieren el expreso consentimiento del trabajador, como condición excluyente de licitud.
b. La inexistencia de reglamentos internos, y códigos de conducta que regulen el uso de herramientas laborales generan una expectativa de privacidad por parte del dependiente.
c. El otorgamiento de una clave de acceso solo de conocimiento del trabajador, refuerza la expectativa de privacidad.

130 GARCÍA, DELIA M. C. YACIMIENTOS PETROLÍFEROS FISCALES S.A. / VILLARRUEL, ROXANA I. C. VESTIDITOS S.A (CNTrabajo, Sala VII, "Pereyra, Leandro Ramiro c/ Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. s/ Despido". 27/03/2003).

4. ¿En qué circunstancias es posible instalar sistemas de video vigilancia de carácter permanente para controlar la actividad laboral?

Como ha sido adelantado, en virtud de la reglamentación de la LPDP (N° 25. 326), la Dirección de Protección de Datos Personales dependiente del Ministerio de Justicia ha dictado la Disposición N° 10/2015, en virtud de la cual se reglamenta la actividad de recolección y posterior tratamiento de imágenes digitales. En el ANEXO I, se prevé como requisito de licitud para la recolección de imágenes digitales con fines de seguridad la obligación de contar con el consentimiento del titular del dato.

El modo de obtener el consentimiento depende del nivel de intromisión en la intimidad, que la obtención de los datos signifique para la persona titular de los mismos. En el artículo primero del ANEXO I se determinan una serie de excepciones a la obligación de contar con un consentimiento informado, reemplazándolo por la colocación de un cartel que en forma clara indique al público la existencia de dichos dispositivos de seguridad (sin que sea necesario precisar su emplazamiento puntual), los fines de la captación de las imágenes y el responsable del tratamiento con su domicilio y datos de contacto para el correcto ejercicio de los derechos por parte del titular del dato. La utilización de cámaras de seguridad en el ámbito de la empresa se encuentra comprendida en dicha excepción, y la licitud en la utilización de las imágenes obtenidas mediante cámaras de seguridad se encontrará supeditada a la información previa de la persona afectada mediante la utilización de carteles.

La norma también prevé la obligación de contar con un manual de tratamiento de datos, y de inscribirse en el Registro Nacional de Base de Datos (artículos 6° y 7°). Cabe destacar que la norma reglamenta la recolección de imágenes con fines de seguridad "exclusivamente", el artículo 2° determina que las imágenes registradas no podrán ser utilizadas para una finalidad distinta. En el ámbito de las relaciones laborales no existe normativa específica, debiendo ajustar el control visual a las disposiciones de la norma analizada, asimismo rigen las pautas de buena fe, respeto a la dignidad del trabajador y justificación de la utilización de la medida, es decir; el control debe estar justificado en la necesidad del empleador para la organización del trabajo y/o por razones de seguridad. Sobre el particular, la Sala I de la CNAT se ha expedido en el siguiente sentido;

> "*El sistema de seguridad mediante cámaras de video implementado por la demandada y en el marco del debate de autos, no luce en el sub examine lesivo de la intimidad del trabajador. Ya que controlaba sólo los lugares de trabajo. No se probó que existieran en baños, vestuarios o lugares de descanso. Se trata de un control general del edificio por motivo de seguridad y no para vigilar el*

cumplimiento de las tareas por el personal (en el caso, se exhibió un audiovisual donde aparecía el actor, en un depósito reunido junto con otros trabajadores, donde se observaba que destaparon una botella de champagne, fumaban y charlaban, todo ello en horario de trabajo"[131].

5. ¿En qué circunstancias es posible instalar sistemas de videovigilancia ocultos para controlar la actividad laboral? En particular, ¿su instalación sólo es posible cuando la empresa sospecha que se ha cometido un ilícito penal o también cuando existen indicios de un incumplimiento laboral?

Conforme la reglamentación a la LPDP comentada (Disposición N° 10/2015) se concluye la imposibilidad del empleador de instalar sistemas de video vigilancia ocultos sin orden judicial previa.

6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?

La Sala IX de la CNAT se ha expedido en el caso "Pavolotzki Claudio y otros c/ Fischer Argentina S.A. s/ Juicio Sumarísimo", en el cual un conjunto de trabajadores viajantes de comercio inició una acción judicial con el objeto de reestablecer las condiciones de trabajo al momento anterior a la instalación de un sistema de geolocalización satelital en el celular de los trabajadores, que permitía a la empresa conocer en todo momento y en tiempo real, su ubicación geográfica. El tribunal entendió que la instalación de dicho sistema no solo había significado una ampliación de las tareas, sino una intromisión en las vidas privadas de los trabajadores, en tanto la empleadora conoce durante las veinticuatro horas del día la ubicación del personal. Para así decidir tuvo en cuanta que; los reclamantes podían utilizar el equipo de comunicación "Nextel" fuera de la jornada laboral (aunque ello se encuentre librado a su propia decisión y no sea un requisito impuesto por la empresa), en tanto les fue otorgado sin ninguna restricción de uso, pues cada dependiente se hace cargo de los gastos que ocasiona el aparato, aclarando que lo que se cuestiona no es la efectiva utilización de datos correspondientes a la vida extra laboral de sus trabajadores, sino la posibilidad de acceder a su ubicación geográfica en cualquier momento. Haciendo una aplicación de la LPDT, el tribunal agrega que aun sorteando la valla formal no ha logrado apreciarse en el caso:

"[L]*a razonabilidad que debe observar cualquier medida adoptada por la empleadora, no sólo desde la óptica de los arts. 62 y 63 de la LCT y demás normas invocadas en grado, sino también a partir de la exigencia establecida por*

131 (CNAT (Sala I), "Medina Ercila, Victorio A. c. Compañía de Servicios Hoteleros S.A.", sentencia del 25 de junio de 2004, La Ley On Line.)

> *el artículo 5º, inc. 2 "d" de la ley Nº 25.326 de Protección de los Datos Personales (B.O. 30/10/00), en tanto no puede soslayarse que la recurrente no explicó, de modo concreto, la necesariedad de un relevamiento de datos de la magnitud y extensión señaladas a los efectos del desarrollo o cumplimiento de las tareas de los reclamantes*".

Conforme la doctrina del precedente analizado, concluimos que la utilización de sistemas de geolocalización en las relaciones laborales solo será viable si; resulta necesario y razonable conforme las características de la prestación de servicios, si resulta estrictamente acotado a su utilización en la jornada de trabajo y, si existe previo consentimiento del trabajador.

7. En el caso de que la empresa haya realizado un despido incumpliendo los requisitos de control de comunicaciones por e-mail o de instalación de sistemas de video vigilancia, ¿cuál sería la calificación del despido y qué sanciones administrativas se podrían derivar?

Corresponde destacar que en la Argentina rige un sistema de estabilidad impropio, en virtud del cual el despido sin causa es un acto ilícito, violatorio del principio de continuidad (artículo 10 LCT), pero indemnizable mediante el pago de una suma de dinero determinable por la aplicación de la fórmula establecida en el artículo 245 de la LCT. Por ello, el criterio de procedencia de la reinstalación por la declaración de nulidad del acto de despido se ha construido sobre la base del artículo 1 de la Ley 23.592, es decir, por la determinación de la materialización de la discriminación en el acto de despido. Este criterio adoptado por nuestro máximo tribunal en el caso "Álvarez Maximiliano c. Cencosud" no goza actualmente de uniformidad habiendo sido objeto de reciente cuestionamiento en la actual composición de la CSJN. [132]

En virtud de lo expuesto, en los casos en que el empleador haya dispuesto el despido incumpliendo los estándares de protección del derecho a la intimidad de los/as trabajadores/as, el trabajador afectado podrá exigir el pago de la indemnización con fundamento en la arbitrariedad del despido, solicitar la reinstalación con fundamento en las normas del derecho común, y/o solicitar el pago de una indemnización de carácter civil. Asimismo, podrá realizar la denuncia penal con fundamento en lo dispuesto en los artículos 153 y ss. del Código Penal, cabe resaltar que en el ámbito de la justicia penal el criterio de aplicación de la norma resulta absolutamente estricto. En el caso ILIC, DRAGOSLAV del 05/06/07, la Sala II de la CNACyC, ha expuesto un criterio uniforme en la materia en virtud del cual:

132(CSJ 3194/2015/RHl Farrell, Ricardo Domingo e/ Libertad S.A. s/ despido. 06/02/2018)

> "*En un proceso penal, resulta inadmisible la utilización como medio de prueba de los mails obtenidos mediante el acceso ilegítimo a una cuenta de correo electrónico pues, más allá de que se considere o no al hecho como típico del delito de violación de correspondencia, lo que determina su exclusión como prueba es el hecho de que han sido obtenidos a través de la transgresión del derecho a la privacidad consagrado en el artículo 19 de la Constitución Nacional*".

La jurisprudencia laboral no ha sido uniforme al respecto, se pueden señalar dos líneas de análisis que se han construidos en sucesivos fallos; aquella mediante la cual los jueces se han basado en el análisis de la aptitud extintiva de la conducta del trabajador para fundar sus sentencias, y aquellas en las que el análisis se centró en la licitud del procedimiento llevado a cabo por el empleador para obtener evidencia del incumplimiento. En el precedente "Giménez, Victoria c/Crear Sistemas S.A. y otro", la Sala X expresó que:

> "*Es improcedente el despido dispuesto por el uso hecho por el dependiente de los servicios de email e Internet para cuestiones personales, pues más allá de no haber sido fehacientemente comprobada la conducta que se le imputa, aún de tenerse por cierta, no puede soslayarse que si bien el empleador goza de la facultad de imponer sanciones disciplinarias al trabajador desobediente o incumplidor, dicha potestad no debe ser abusivamente utilizada como alternativa válida del despido, no resultando ajustado a derecho que aplique la medida de mayor gravedad en forma intempestiva y sin recurrir previamente a otros medios que la ley le confiere a tal fin*."

En el precedente "VILORIA, MYRIAN A. c. ASEGURADORA DE CRÉDITOS Y GARANTÍAS S.A", la Sala VII, consideró justificado el despido de la trabajadora que remitió información confidencial a la principal competidora de su empleadora. Aquí nuevamente el análisis se centró en la valoración de la injuria para determinar la justificación del despido, con prescindencia del método utilizado para obtener las pruebas del hecho imputado a la trabajadora, al respecto la sentenciante se limita a manifestar que el proceder del empleador no resulta reprochable por haber sido la inspección estrictamente limitada a comprobar el incumplimiento de la dependiente.

Aquellos tribunales que se introducen en el análisis de la licitud en la obtención de la prueba, resaltan la necesidad de contar con el expreso consentimiento del trabajador declarando injustificados aquellos despidos que no cumplen con dicho requisito.

Con relación a la instalación de sistemas de video vigilancia, la LPDP establece una multa cuyo monto puede varias entre los $ 1.000 (MIL) hasta los $ 100.000 (CIEN MIL).

En el ámbito específicamente laboral, la Ley 25.212, modificada por la Ley 26.941, califica a los actos del empleador contrarios a la intimidad y a la dignidad de los trabajadores como una "infracción muy grave" (artículo 4 inc. d), disponiendo una sanción de multa del cincuenta por ciento (50%) al dos mil por ciento (2.000%) del valor mensual del Salario Mínimo, Vital y Móvil vigente al momento de la constatación de la infracción, por cada trabajador afectado.

8. ¿Qué datos personales pueden ser recogidos y tratados en el marco de la relación laboral? En particular, ¿es necesario el consentimiento del trabajador? ¿En qué casos no es necesario?

Al respecto rigen las disposiciones de la LPDP Nº 25.326, en virtud de la cual se establecen los principios de; consentimiento, información, licitud, lealtad, finalidad calidad, proporcionalidad y responsabilidad.

Ello significa que el empleador podrá recoger y conformar un archivo de datos siempre que; se encuentre debidamente inscripto en el Registro de Datos Personales, asegure la calidad de los datos archivados debiendo ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para el que los hubiere recogido, y se permita el acceso por parte de sus titulares.

En lo que refiere al contrato laboral, resulta aplicable el artículo 5 de la LPDP que exceptúa el consentimiento del titular del dato; en aquellos casos en que se deriven de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento (inc. d), o cuando se recaben en virtud de una obligación legal (b), entre otros supuestos. En todos aquellos casos en que la recolección de datos exceda a aquellos estrictamente necesarios para el desarrollo del vínculo laboral se deberá requerir el consentimiento expreso de su titular.

9. ¿Qué información en el ámbito de la protección de datos personales está obligada la empresa a proporcionar a la representación legal de los trabajadores? ¿Cómo y con qué periodicidad?

No se prevé en el ordenamiento vigente la obligación de informar a los representantes de los trabajadores, las actividades de recolección y tratamiento de los datos llevados a cabo por la empresa.

10. ¿Existe un derecho a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo? En su caso, ¿debe la empresa definir la extensión y límites de este derecho conjuntamente con los representantes de los trabajadores o puede hacerlo mediante una política empresarial?

El ordenamiento jurídico argentino no cuenta con una regulación específica sobre utilización de dispositivos tecnológicos, por ello debemos recurrir a la aplicación de las normas generales en virtud de las cuales las tareas realizadas fuera de la jornada normal de trabajo deben computarse como horas extraordinarias y abonarse conforme lo dispone el artículo 201 de la LCT.

Cabe agregar que la extensión de la jornada de trabajo se determina en virtud del tiempo en el cual el trabajador permanece "a disposición del empleador", circunstancia que no implica la efectiva prestación de servicios, sino la disponibilidad inmediata para dicha prestación.

IMPACTO LABORAL DEL USO DE DISPOSITIVOS TECNOLÓGICOS EN BRASIL

Carolina Pereira Lins Mesquita[133]
Profesora e investigadora
Universidad Federal de Rio de Janeiro - UFRJ.

Introducción

La Constitución Federal de la República Federativa del Brasil de 1988 dispone, en su artículo 5º, X, XII e XXIII, respectivamente, que: i) son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurado el derecho a indemnización por el daño material o moral resultante de su violación; ii) es inviolable el secreto de la correspondencia y de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en las hipótesis y en la forma que la ley establezca para fines de investigación criminal o instrucción procesal penal; iii) se garantiza el derecho de propiedad.

Por su parte, la Consolidación de las Leyes del Trabajo (que es similar a un Código del trabajo) presenta el concepto de empleador como "*la empresa, individual o colectiva, que asumiendo los riesgos de la actividad económica admite, asalaria y dirige la prestación personal servicios*" (artículo 2, CLT).

Entre las dimensiones del poder del empleador, mientras que el polo reverso de la subordinación, se ubica al derecho del empleador a fiscalizar la prestación de servicios. Sin embargo, las balizas para esta fiscalización no siempre son claras o fijadas en normas legales. En Brasil, no existe una regulación específica sobre estas cuestiones, recayendo sobre la jurisprudencia esta carga.

La alteración en la Consolidación de las Leyes del Trabajo, por la Ley nº 13.467, de 13.07.2017, la denominada "reforma laboral", no ha implicado cambios sustanciales en la cuestión del uso de los dispositivos tecnológicos en las relaciones laborales, aunque ha regulado expresamente el trabajo a distancia (artículo 75-A a 75-E, CLT). Antes de esta modificación, en 2011 (Ley nº 12.551), los medios telemáticos e informatizados de mando, control y supervisión fueron equiparados, para fines de subordinación jurídica, a los medios personales y directos de mando, control y supervisión del trabajo ajeno (artículo 6º, párrafo único, CLT).

[133] Phd en Derecho y Sociología por la Universidad Federal Fluminense - UFF. Master en Derecho por la Universidad Federal de Minas Gerais - UFMG. Asociada del Instituto de Ciencias Jurídicas y Sociales. Currículo: http://lattes.cnpq.br/4213026169005908

Sin embargo, ante la ausencia de reglamentación por medio de normas estatales, estas cuestiones pueden ser objeto de negociación colectiva de trabajo o reglamentos empresariales siempre que no violen las normas constitucionales relativas al respeto a la intimidad, a la vida privada y al secreto de las comunicaciones.

Aunque la práctica de utilización de dispositivos tecnológicos en las relaciones de trabajo es común, Brasil no tiene estadísticas detalladas sobre la temática.

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa?

En Brasil no existe una regulación específica sobre el uso por los trabajadores de los dispositivos tecnológicos que la empresa pone a su disposición para el desarrollo de la actividad profesional.

Por este motivo, ha sido la jurisprudencia, especialmente la del Tribunal Superior del Trabajo, la que ha establecido los requisitos relativos a la monitorización de los mensajes electrónicos de los trabajadores y al control de su actividad laboral mediante sistemas audiovisuales, ponderando i) los derechos fundamentales a la intimidad, la vida privada, la honor y la imagen de las personas (artículo 5º, X, CF/88) y ii*)* la inviolabilidad del secreto de la correspondencia y de las comunicaciones telegráficas, de datos y de las comunicaciones telefónicas (artículo 5º, XII, CF/88); con los derechos empresariales de i) garantía del derecho de propiedad y ii) de dirección de la prestación personal de servicios (artículo 2º, CLT).

2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o de una política interna sobre el uso de estos dispositivos? en caso contrario, ¿cómo se regula el uso de los dispositivos tecnológicos en la empresa?

En Brasil, como hemos visto, no existe una regulación específica sobre el uso por los trabajadores de los dispositivos tecnológicos que la empresa pone a disposición de los trabajadores y, por tanto, el ordenamiento jurídico-laboral no contempla una obligación legal de disponer de un código de conducta telemático o una política interna sobre el uso de estos dispositivos.

Igualmente, no hay uniformidad de entendimiento en cuanto a la necesidad de verificar si el empresario ha notificado clara y previamente a los trabajadores afectados sobre la posibilidad de monitorización y su naturaleza.

3. ¿En qué supuestos y en qué condiciones es posible el acceso y la monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos propiedad de la empresa (e-mail, mensajería instantánea, etc.)?

El ordenamiento jurídico del Brasil no establece los criterios para la monitorización de las comunicaciones personales de los trabajadores mediante dispositivos tecnológicos en la empresa.

La jurisprudencia del Tribunal Superior del Trabajo ha sido en el sentido de que el e-mail corporativo ofrecido a los empleados, puede ser monitoreado, sin que haya violación de los derechos fundamentales a la privacidad ya la intimidad. La fundamentación para este entendimiento es de dos órdenes: i) la previsión en el código civil de que el empleador responde civilmente por actos de sus empleados, en el ejercicio del trabajo o en razón de él (artículo 932, CC); ii) la comprensión de que el correo electrónico corporativo es instrumento (herramienta) de trabajo.

Por otro lado, el e-mail particular del empleado y herramientas de conversación como el MSN, aunque accedido en el ambiente de trabajo, conforme a la jurisprudencia mayoritaria en Brasil, no puede ser monitoreado por el empleador, caracterizando violación a la intimidad y al secreto de las correspondencias.

En este último caso, corresponde a la empresa, si lo considera necesario, prohibir el acceso de dichos programas en el ambiente de trabajo, pero, una vez autorizada su utilización, aunque tácitamente, los datos allí contenidos integran el ámbito privado del trabajador.

4. ¿En qué circunstancias es posible instalar sistemas de videovigilancia de carácter permanente para controlar la actividad laboral?

Sobre la instalación de sistemas de cámara de vigilancia en el ambiente de trabajo, en Brasil tampoco hay reglamentación específica, por medio de norma estatal, sobre esta cuestión. Las balizas para que el empleador las instale, con carácter permanente, con el fin de controlar la actividad laboral, son fijadas por la jurisprudencia del país.

La jurisprudencia mayoritaria ha establecido algunos requisitos para la validez de este sistema de vigilancia, visando la garantía del patrimonio de la empresa y la seguridad de sus empleados.

El primer requisito se refiere al lugar donde se instalan las cámaras. Hay una tendencia a considerar ilegal la instalación de cámaras en lugares donde hay riesgo de violación de

la privacidad de los empleados, como comedores, baños, vestuarios o locales destinados al descanso, por obligar a los trabajadores. Si, por otra parte, lícitas, cuando se fijan en el lugar de trabajo propiamente dicho.

El segundo se refiere a los empleados filmados. Hay una tendencia a considerar lícita las grabaciones generalizadas y no sobre uno u otro empleado en específico.

En cuanto a la necesidad de informar o advertir a los trabajadores o los representantes de éstos sobre su instalación y finalidad, los juzgados en su mayoría no hacen mención, mientras que una exigencia, a pesar del principio general de buena fe que impone el deber de transparencia en las relaciones de trabajo.

La indispensable de este sistema de vigilancia por cámaras tampoco es señalada por la jurisprudencia brasileña como un requisito de validez.

5. ¿En qué circunstancias es posible instalar sistemas de videovigilancia ocultos para controlar la actividad laboral? en particular, ¿Su instalación sólo es posible cuando la empresa sospecha que se ha cometido un ilícito penal o también cuando existen indicios de un incumplimiento laboral?

La jurisprudencia mayoritaria en Brasil no hace distinción de la instalación de cámaras ocultas o visibles para fines de verificación de ilicitud del procedimiento, ante la violación del derecho a la intimidad del trabajador. Es decir, el hecho de que haya o no ciencia de los empleados no es considerado por la jurisprudencia, limitándose ésta a los análisis ya mencionados del lugar de instalación de las cámaras y de la generalidad de los sujetos filmados.

Además de estos requisitos, en algunos pocos casos se verifica si hubo perjuicio concreto al trabajador, por ejemplo, mediante la divulgación de las imágenes captadas.

6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?

En Brasil, de una manera general, tampoco hay reglamentación específica sobre la instalación de sistemas de geolocalización (GPS) para fines de control de la actividad laboral.

En la jurisprudencia brasileña, esta forma de control no es discutida en cuanto a la violación o no de la intimidad del empleado. Por el contrario, la discusión se centra en

la posibilidad de pago de horas extras a los trabajadores que ejecutan sus actividades externamente, fuera de la sede de la empresa.

El ordenamiento jurídico nacional (artículo 62, I, de la CLT) excluye a los trabajadores externos del derecho a la recepción de las horas prestadas, por la imposibilidad del control de jornada de trabajo. De este modo, la jurisprudencia centra el análisis en la posibilidad de control de la jornada: si hay control, por ejemplo, por medio de geolocalización, el empleado tendrá derecho a la recepción de las horas extraordinarias prestadas.

En particular, sobre los conductores profesionales, la Ley nº 13.103 / 2015 (que reproduce el artículo 1, V, de la Ley nº 12.619 / 2012, hoy revocado), expresamente prevé como derecho de los conductores profesionales tener la jornada de trabajo controlada de manera fidedigna mediante anotación en diario de a bordo, papeleta o ficha de trabajo externo, o de medios electrónicos idóneos instalados en los vehículos, a criterio del empleador.

Se observa que la adopción de sistemas electrónicos, incluso, el sistema de geolocalización (GPS) es señalado como un derecho de los conductores de haber controlado la jornada de trabajo, incluso, para fines de pago de las horas extraordinarias.

7. En el caso de que la empresa haya realizado un despido incumpliendo los requisitos de control de comunicaciones por e-mail o de instalación de sistemas de videovigilancia, ¿Cuál sería la calificación del despido y qué sanciones administrativas se podrían derivar?

La Constitución Federal de 1988 dispone que son inadmisibles, en el proceso, las pruebas obtenidas por medios ilícitos.

Por su parte, el Supremo Tribunal Federal firmó entendimiento en el sentido de que la grabación de conversación por uno de los interlocutores, a fin de rechazar conducta ilícita del otro, no se encuadra en el sellado previsto en el artículo 5. LVI, de la Carta Magna, constituyéndose, pues, ejercicio regular de derecho.

En este sentido, el acceso al correo electrónico corporativo, la grabación de conversaciones telefónicas, con el fin de rechazar conducta ilícita puede ser utilizado como medio de prueba para la dispensa por justa causa del empleado.

El artículo 482 de la CLT especifica las hipótesis de justa causa del trabajador, incluyendo, entre otros, acto de improbidad (robo de programa desarrollado por la

empresa); la incontinencia de conducta (divulgación de material de cuño sexual a otros empleados) y desidia (empleado que permanece horas navegando en Internet, perjudicando sus servicios).

Sin embargo, si la justa causa no se demuestra en juicio, podrá ser excluida, incluso, ante la demostración de violación del derecho a la intimidad ya la imagen del empleado, implicando la reintegración del trabajador e indemnización por daño moral y material.

8. ¿Qué datos personales pueden ser recogidos y tratados en el marco de la relación laboral? en particular, ¿Es necesario el consentimiento del trabajador? ¿En qué casos no es necesario?

En Brasil no hay previsiones específicas sobre estas cuestiones.

9. ¿Qué información en el ámbito de la protección de datos personales está obligada la empresa a proporcionar a la representación legal de los trabajadores? ¿Cómo y con qué periodicidad?

En Brasil, no existe la cuenta de informar con carácter previo a los representantes de los trabajadores sobre el tratamiento de datos que repercuten sobre el conjunto de los trabajadores de la empresa. Sin embargo, de forma específica, nada impide que dicha materia sea prevista en acuerdo o convención colectiva de trabajo.

10. ¿Existe un derecho a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo? en su caso, ¿Debe la empresa definir la extensión y límites de este derecho conjuntamente con los representantes de los trabajadores o puede hacerlo mediante una política empresarial?

El ordenamiento jurídico-laboral brasileiro no reconoce explícitamente un derecho específico del trabajador a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo. Ahora bien, como consecuencia de la obligación empresarial de respetar la normativa sobre tiempo de trabajo, de garantizar a los trabajadores su seguridad y salud en el trabajo y de retribuir en atención al tiempo de trabajo, es posible defender que existe un deber empresarial genérico de respeto al tiempo de descanso de los trabajadores. Además, la Constitución Federal tutela al trabajador frente a la automatización (artículo 7, XXVII, CF), asegurando también el derecho fundamental al ocio (artículo 6, *caput*, CF) y a la intimidad ya la vida privada (artículo 5, V, X, CF).

Sin embargo, la jurisprudencia laboral y La doctrina reconocen un derecho específico de desconexión, visando la preservación de la vida privada y de la salud del empleado. Se

trata de los casos de régimen de sobreaviso, caracterizado como el tiempo, previamente ajustado, en que el empleado permanece, fuera del horario normal de trabajo, a disposición del empleador, en espera de eventual llamada para el trabajo. Como en la hipótesis hay disminución de la libertad del empleado de disponer de su propio tiempo (destinado al descanso), ya sea en casa o en cualquier otro lugar, por aplicación analógica, las horas de sobreaviso deberán ser remuneradas a razón de 1/3 del valor del salario normal y las escalas de turno deberán ser de no más de 24 horas (artículo 224, CLT e súmula 428, TST).

En la jurisprudencia del TST (AIRR-2058-43.2012.5.02.0464), de 27/10/2017, el Ministro Relator Cláudio Brandão afirmó que "*el avance tecnológico y el perfeccionamiento de las herramientas de comunicación deben servir para la mejora de las relaciones de trabajo y optimización de las actividades, jamás para esclavizar al trabajador*".

Se destaca, sin embargo, que el uso de instrumentos telemáticos o informatizados suministrados por la empresa al empleado, por sí solo, no caracteriza el régimen de sobreviso, siendo necesario para la caracterización del sobreaviso, el régimen de turno o equivalente, aguardando en cualquier momento el llamado al servicio durante el período de descanso.

Bibliografía y pronunciamientos judiciales

CONSOLIDAÇÃO DAS LEIS DO TRABALHO. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452.htm. Acesso em 01/01/2018.

DELGADO, M. G. *Curso de Direito do Trabalho*. São Paulo: LTr Editora, 2018.

DE BARROS, A. M.. *Curso de Direito do Trabalho*. São Paulo: LTr Editora, 2005.

MESQUITA, C. P. L. *Teoria Geral do Direito do Trabalho: pela progressividade sociojurídica do trabalhador*. 1ª ed. São Paulo: LTr Editora, 2012.

TRIBUNAL SUPERIOR DO TRABALHO. RR: 976-82.2010.5.11.0015, Relator: Alberto Luiz Bresciani de Fontan Pereira, Data de Julgamento: 31/08/2011, 3ª Turma, Data da publicação: DEJT 09/09/2011.

TRIBUNAL SUPERIOR DO TRABALHO. RR: 952-16.2012.5.11.0005, Relator: Dora Maria da Costa, Data de Julgamento: 23/10/2013, 8ª Turma, Data da publicação: DEJT 25/10/2013.

TRIBUNAL SUPERIOR DO TRABALHO AIRR: 15598220165230091, Relator: Guilherme Augusto Caputo Bastos, Data de Julgamento: 09/05/2018, 4ª Turma, Data da publicação: DEJT 11/05/2018.

TRIBUNAL SUPERIOR DO TRABALHO. RR-1156-48.2013.5.09.0242, Relator Ministro: Emmanoel Pereira, ata de Julgamento: 15/04/2015, 5ª Turma, Data de Publicação: DEJT 24/04/2015.

TRIBUNAL SUPERIOR DO TRABALHO RR-648-84.2012.5.23.0004, Relator Ministro: Lelio Bentes Corrêa, Data de Julgamento: 15/04/2015, 1ª Turma, Data de Publicação: DEJT 17/04/2015.

TRIBUNAL SUPERIOR DO TRABALHO RR-2056-28.2010.5.03.0040, Relator Ministro: Alexandre de Souza Agra Belmonte, Data de Julgamento: 29/06/2015, 3ª Turma, Data de Publicação: DEJT 02/07/2015.

TRIBUNAL SUPERIOR DO TRABALHO. RR-1006-46.2012.5.15.0077, Relatora Ministra: Kátia Magalhães Arruda, Data de Julgamento: 13/05/2015, 6ª Turma, Data de Publicação: DEJT 19/06/2015.

TRIBUNAL SUPERIOR DO TRABALHO. RR-48200-64.2013.5.17.0008, Relatora Ministra: Maria Cristina Irigoyen Peduzzi, Data de Julgamento: 03/06/2015, 8ª Turma, Data de Publicação: DEJT 08/06/2015.

TRIBUNAL SUPERIOR DO TRABALHO. ARR-1185-30.2010.5.03.0094. 4ª Turma. Relator João Oreste Dalazen. Data de Julgamento: 13/05/2015, Data de publicação: DEJT 22/05/2015.

TRIBUNAL SUPERIOR DO TRABALHO. AIRR-2058-43.2012.5.02.0464. 7ª Turma. Relator: Cláudio Brandão. Data de Julgamento: 18/10/2017, Data de publicação: DEJT 27/10/2017.

TRIBUNAL SUPERIOR DO TRABALHO. Ag-E-ED-RR-169000-71.2009.5.02.0011. Relator Ministro Cláudio Brandão. Data do julgamento: 26/10/2017; Data da publicação: 31/10/2017.

IMPACTO LABORAL DEL USO DE DISPOSITIVOS TECNOLÓGICOS EN COLOMBIA

Juliana Patricia Morad Acero
Profesora Pontificia Universidad Javeriana – Bogotá.

Carlos Adolfo Prieto Monroy
Profesor Pontificia Universidad Javeriana – Bogotá.

Introducción

El uso de dispositivos tecnológicos en las relaciones laborales no ha tenido un exclusivo desarrollo normativo en el ordenamiento jurídico colombiano. No obstante, se puede rastrear un amplio marco regulatorio como pronunciamientos jurisprudenciales en torno al tema, en dos etapas de la relación laboral: en la contratación y durante su ejecución.

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa?

El Ordenamiento Jurídico Colombiano contempla un régimen normativo de protección del derecho a la intimidad de las personas en general, derivado de la consagración constitucional contenida en el artículo 15 de la Constitución Política de 1991, y desarrollado por la Ley 1581 de 2012, "*por la cual se dictan disposiciones para la protección de datos personales*", ley estatutaria en los términos del artículo 153 de la Constitución y declarada exequible mediante la Sentencia C – 1011 de 2011. Se trata, entonces, de un postulado normativo que establece un derecho fundamental, inherente al principio de dignidad humana y, por lo tanto, transversal en cualquier ámbito de relación social.

Por otra parte, el ordenamiento jurídico colombiano ha regulado el *documento electrónico*, por conducto de la Ley 527 de 1999, "*por medio de la cual se define y reglamenta el acceso y uso de mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones*." Este régimen, generalista, tiene aplicación en todas aquellas situaciones o circunstancias sociales en las que se generen documentos, definidos por el artículo 243 del Código General del Proceso (CGP).

En el ámbito del trabajo subordinado, la regulación, contenida primordialmente en el Código Sustantivo del Trabajo (CST), no contempla una normatividad aplicable de manera específica el uso de dispositivos tecnológicos en el ámbito laboral; lo que sí

establece es una serie de obligaciones para las partes de la relación laboral, concernientes a la que recae sobre el empleador en cuanto a suministrar las herramientas de trabajo necesarias para la ejecución de la labor contratada (artículo 57.3 CST), y la propia del trabajador, consistente en mantener la reserva respecto de aquella información a la que haya accedido con causa en la relación laboral, particularmente de aquella que tenga el carácter de reservada y cuya revelación pueda causar perjuicio al empleador (artículo 58.2 CST).

En cuanto a la ejecución de la relación laboral, y concretamente en función del uso de las tecnologías de la información y de la comunicación – TIC´s -, el ordenamiento jurídico colombiano ha regulado la figura del *teletrabajo*, por conducto de la Ley 1221 de 2008, reglamentada a su vez por el Decreto 884 de 2012. De este cuerpo normativo, se resalta el hecho de que concibe el teletrabajo como "*una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo*" (Congreso de la República, 2008)

Así pues, la reglamentación normativa del uso de dispositivos tecnológicos en el ámbito laboral, se concentra en el modo como el empleador pone a disposición del trabajador herramientas para la ejecución del trabajo.

2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o de una política interna sobre el uso de estos dispositivos? En caso contrario, ¿cómo se regula el uso de los dispositivos tecnológicos en la empresa?

Respecto al uso de los dispositivos tecnológicos en el entorno del trabajo, tal como se ha puesto de presente, el ordenamiento jurídico vigente en Colombia impone a todos los habitantes del territorio nacional la observancia del régimen de protección de datos establecido por la Ley 1581 de 2012, concretamente en lo referente al acceso y administración de la *información sensible* (artículo 5 Ley 1581/12), siendo tal la contenida en datos "*que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos*." (Congreso de la República, 2012)

En cuanto al respeto por la intimidad del trabajador, el ordenamiento jurídico laboral vigente en Colombia establece una cláusula general consistente en el respeto de la dignidad del trabajador, en función del ejercicio de la subordinación (artículo 23 CST), del cual se deriva una serie de obligaciones y de prohibiciones, así:

- "*Guardar absoluto respeto a la dignidad personal del trabajador, a sus creencias y sentimientos*" (artículo 57.5 CST).
- "*Limitar o presionar en cualquier forma a los trabajadores en el ejercicio de su derecho de asociación*" (artículo 59.4 CST).
- "*Imponer a los trabajadores obligaciones de carácter religioso o político, o dificultarles o impedirles el ejercicio del derecho del sufragio*" (artículo 59.5 CST)
- Emplear en las certificaciones de que trata el ordinal 7o. del artículo 57 signos convencionales que tiendan a perjudicar a los interesados, o adoptar el sistema de "lista negra", cualquiera que sea la modalidad que utilicen, para que no se ocupe en otras empresas a los trabajadores que se separen o sean separados del servicio (artículo 59.8 CST).
- "*Ejecutar o autorizar cualquier acto que vulnere o restrinja los derechos de los trabajadores o que ofenda su dignidad*" (artículo 59.9 CST).

En adición a lo anterior, por conducto de la Ley 1010 de 2006, "*por medio de la cual se adoptan medidas para prevenir, corregir y sancionar el acoso laboral y otros hostigamientos en la relación de trabajo*", se estableció un régimen legal de protección contra las conductas reiteradas y repetitivas tendientes a inducir al trabajador a la renuncia o a afectar su dignidad (artículo 1º), que consagra como bien jurídico a tutelar, entre otros, la intimidad de los trabajadores, y que al efecto establece como categorías de acoso laboral sancionables el *maltrato laboral* (artículo 2.1), la *discriminación laboral* (artículo 2.3), y el *entorpecimiento laboral* (artículo 2.4). Por último, esta disposición ordena que todo empleador adecúe su reglamento interno de trabajo con la proposición de una política de prevención del acoso laboral, así como a constituir un Comité de Convivencia Laboral (artículo 9.1), que sirva de instancia empresarial para evitar, instruir y sancionar los casos en los que eventualmente se configurasen tales comportamientos.

Con fundamento en estos antecedentes, se tiene que el ordenamiento jurídico laboral vigente en Colombia no contempla una obligación expresa, en el sentido de establecer códigos de conducta o políticas de manejo de herramientas informáticas o tecnológicas en el ámbito laboral. No obstante, si establece un régimen fuerte de protección de la intimidad de la persona del trabajador, el cual, a referirse a la información en tanto contenido, necesariamente impacta en los medios de difusión de tal información, dentro de los que se encuentran los dispositivos electrónicos, las bases de datos y, en últimas,

los medios de comunicación y de almacenamiento de información de los que el empleador disponga en el ejercicio de su actividad empresarial.

3. ¿En qué supuestos y en qué condiciones es posible el acceso y la monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos propiedad de la empresa (e-mail, mensajería instantánea, etc.)?

Tal y como se indicó previamente en Colombia no existe normativa sobre el acceso y monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos que son propiedad del empleador, no obstante esta posibilidad debe comprenderse dentro del marco regulatorio ya indicado de la Ley 1581 de 2012, "*por la cual se dictan disposiciones para la protección de datos personales*"; los artículos relativos a las obligaciones y prohibiciones del empleador frente a sus trabajadores tales como, guardar absoluto respeto a la dignidad personal del trabajador, a sus creencias y sentimientos.(artículo 57.5 CST) y evitar ejecutar o autorizar cualquier acto que vulnere o restrinja los derechos de los trabajadores o que ofenda su dignidad (artículo 59.9 CST). La propia del trabajador, consistente en mantener la reserva respecto de aquella información a la que haya accedido con causa en la relación laboral, particularmente de aquella que tenga el carácter de reservada y cuya revelación pueda causar perjuicio al empleador (artículo 58.2 CST). El derecho a la intimidad (artículo 15 Constitución Política) y libertad de empresa que justifica constitucionalmente el ejercicio de la facultad subordinante del empleador (artículo 333 CP) y (artículo 23.1.b. CST).

Ahora bien, teniendo en cuenta que durante la ejecución del contrato el trabajador puede verse expuesto a intromisiones por parte del empleador quien verifica el cumplimiento de sus obligaciones, debe efectuarse un juicio de proporcionalidad sobre el derecho a la intimidad del trabajador. Este juicio construido por nuestra Corte Constitucional involucra tres criterios: la necesidad y constitucionalidad de la medida que en este caso sería la manera cómo el empleador supervisa los dispositivos tecnológicos otorgados al trabajador; la idoneidad de esta medida para lograr la supervisión y la proporcionalidad de la misma, esto es: que la misma no suponga una desproporcionada vulneración al derecho de intimidad del trabajador.

De otra parte, según el desarrollo jurisprudencial, existen cuatro tipos de información que deben ser tenidos en cuenta al momento de analizar la afectación o no al derecho a la intimidad en cualquier momento, incluyendo la inspección de herramientas tecnológicas suministradas al trabajador: la pública que puede ser conocida por cualquier persona; la semiprivada que solo es manejada por autoridades competentes pero que con todo puede ser suministrada al público, previa autorización; la privada que

es aquella que por solo puede ser conocida excepcionalmente al gozar de reserva; y la reservada que sólo puede ser conocida por su titular. (Sentencia de tutela 427, 2013)

Junto a esto y de la mano del desarrollo jurisprudencial, la Corte Constitucional en muy pocas sentencias se ha pronunciado sobre el control que puede existir sobre dispositivos tecnológicos suministrados por el mismo empleador. En la sentencia de tutela 405 del año 2007 por ejemplo, examinó un caso de una trabajadora que había guardado en una carpeta personal abierta para sus documentos dentro de un computador suministrado por su empleador, unas fotos en las que su hija aparecía desnuda. Su empleador hizo públicas estas fotos para mostrar que el computador era de carácter empresarial y no podían guardarse documentos personales. La Corte concluyó en este caso la vulneración al derecho a la intimidad de la trabajadora (Sentencia de tutela 405, 2007).

Con todo, en virtud del artículo 2349 del Código Civil que le atribuye a los empleadores los daños ocasionados por sus trabajadores en ejercicio de la labor desplegada, podría decirse que el secreto de las comunicaciones cedería ante la responsabilidad que asume el empleador.

4. ¿En qué circunstancias es posible instalar sistemas de videovigilancia de carácter permanente para controlar la actividad laboral?

Nuevamente cabe indicar lo expuesto en anteriores puntos, sobre la inexistencia de normativa que se concentre en este asunto en particular; existiendo no obstante un marco regulatorio que permitiría analizar cada caso.

Sin embargo, sobre este punto vale resaltar la sentencia de tutela 768 del año 2008, en donde la Corte Constitucional examinó el caso de un trabajador de un banco que tapó el acceso de unas cámaras de vigilancia al percatarse que estaba siendo monitoreado. El empleador entonces instaló otro dispositivo que no fue conocido por el trabajador y que lo filma dándose muestras de afecto con una compañera del trabajo. Tras este hecho, el trabajador fue despedido. En este caso, la Corte señala que las cámaras instaladas en lugares tales como lugares de descanso, baños, vestuarios, o donde se graben situaciones íntimas de los trabajadores, violan el derecho a la intimidad; pero las que se emplean para la vigilancia de la empresa, para que no se atente contra el derecho de propiedad o la seguridad, están permitidas. Frente al caso concreto, la Corte encuentra proporcional el uso de cámaras en los bancos para proteger la seguridad de los trabajadores y de la institución, encontrando ajustado el despido del trabajador por la obstrucción de las cámaras y no acatar órdenes sobre seguridad y vigilancia en las instalaciones del Banco. (Sentencia de tutela 768, 2007)

5. ¿En qué circunstancias es posible instalar sistemas de videovigilancia ocultos para controlar la actividad laboral? En particular, ¿su instalación sólo es posible cuando la empresa sospecha que se ha cometido un ilícito penal o también cuando existen indicios de un incumplimiento laboral?

Indicando que caben las mismas apreciaciones realizadas en puntos precedentes, cabe resaltar que, en el caso previamente citado, el empleador instaló un sistema de videovigilancia oculto. Sin embargo, en esta sentencia la Corte Constitucional concluyó que del conocimiento previo de cámaras se infiere el conocimiento de un sistema de videovigilancia, así se desconozca el lugar exacto de instalación de otras cámaras. (Sentencia de tutela 768, 2007)

Con todo no se rastrean pronunciamientos jurisprudenciales diferentes en el que el máximo tribunal constitucional se concentre exclusivamente en sistemas de video vigilancia ocultos.

6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?

Tal como se ha puesto de presente previamente, el ordenamiento jurídico laboral vigente en Colombia, imbricado como está en el ordenamiento constitucional vigente y desarrollado en el país, impone un límite material respecto de la posibilidad de afectar la intimidad de las personas, consistente en el respeto de la intimidad personal como componente esencial del derecho fundamental al buen nombre (artículo 15 C.P).

Es así como se proscribe cualquier posibilidad de intervención unilateral en esa intimidad sin que medie razón suficiente u orden judicial más se permite la posibilidad de afectar tal privacidad siempre que tal intervención esté vinculada con lo que la jurisprudencia constitucional ha identificado como la "intimidad social", y que define en estos términos:

> "(la intimidad social) *involucra las relaciones del individuo en un entorno social determinado, tales como, las sujeciones atenientes a los vínculos labores o públicos derivados de la interrelación de las personas con sus congéneres en ese preciso núcleo social, a pesar de restringirse -en estos casos- el alcance del derecho a la intimidad, su esfera de protección se mantiene vigente en aras de preservar otros derechos constitucionales concomitantes, tales como, el derecho a la dignidad humana* (…)" (Sentencia de constitucionalidad 602, 2016)

Acceso que va a estar limitado, necesariamente, a la información sensible de la persona, y concretamente en el caso de la relación laboral, que no tenga relevancia en el decurso de las actividades propias del trabajo.

Así las cosas, la posibilidad de imponer a la persona del trabajador, la obligación de portar un dispositivo geolocalizador, se ve enmarcada en el límite material que presupone el respeto por su intimidad asociada con la información sensible del titular.

Sin embargo, y a partir de la consagración de la ya mencionada subordinación como elemento esencial del contrato de trabajo, con las limitaciones establecidas por la Ley (artículo 23.1.b. CST), existe la posibilidad de que el empleador, dentro de ese marco jurídico, imponga al trabajador la obligación de portar dispositivos geolocalizadores, con el único propósito de facilitar el ejercicio de este atributo, dentro de la jornada laboral y en función exclusiva de la prestación del servicio por parte de aquél, siempre respetando la intimidad del trabajador y en ningún caso afectando información sensible. La imposición de este tipo de obligaciones tiene una causa eminentemente contractual, y siempre asociada al cumplimiento de las obligaciones que asume el trabajador en virtud de la relación de trabajo y circunscrita concreta y exclusivamente a ese ámbito.

Por último, es importante poner de presente que, en el evento en el que el ejercicio de las funciones del trabajador requiera la geolocalización, ésta deberá llevarse a cabo mediante el uso de dispositivos suministrados por el empleador, en cumplimiento de la obligación patronal establecida por el artículo 57.1 CST.

7. En el caso de que la empresa haya realizado un despido incumpliendo los requisitos de control de comunicaciones por e-mail o de instalación de sistemas de videovigilancia, ¿cuál sería la calificación del despido y qué sanciones administrativas se podrían derivar?

Conforme con la dinámica de la normatividad laboral vigente en Colombia, concretamente la contenida en los artículos 61, 62 y 64 CST, el despido, como modalidad de terminación del contrato de trabajo, contempla dos posibilidades: a) el despido con justa causa; y b) el despido sin justa causa.

Se estará en presencia de un despido con justa causa, en el evento en el que el trabajador haya incurrido en alguna de las causales previstas al efecto por el artículo 62.a CST.; por el contrario, si el despido no se sustenta en ninguna de tales causales, será calificado como uno sin justa causa, y la consecuencia jurídica en ese evento será el reconocimiento de la indemnización prevista por el artículo 64 CST.

Por otra parte, y trayendo a colación lo dicho al responder los interrogantes Nos. 1 y 2, el hecho de que el empleador haya realizado un despido basado en la afectación del derecho fundamental al buen nombre y a la intimidad, implicará la vulneración de este derecho subjetivo, mas no derivaría en la nulidad de la desvinculación. El efecto jurídico, que deberá ser declarado por un Juez Laboral, será el de calificar la desvinculación como una sin justa causa, y como consecuencia, llevar al reconcomiendo de la indemnización prevista por el artículo 64 CST.

En el marco normativo vigente en Colombia, la afectación del derecho a la intimidad del trabajador no deviene en la nulidad del despido, en la medida en que tal derecho fundamental no está asociado con las garantías laborales tales como el mínimo vital y móvil ni con el acceso a la seguridad social. En otras palabras, la afectación a la intimidad del trabajador no es un criterio generador de estabilidad laboral reforzada. Es un asunto muy concreto en la relación laboral individual y, en consecuencia, no puede plantearse un criterio judicial o doctrinal que sirva de precedente para calificar el caso.

8. ¿Qué datos personales pueden ser recogidos y tratados en el marco de la relación laboral? En particular, ¿es necesario el consentimiento del trabajador? ¿En qué casos no es necesario?

Sobre el particular y sin ahondar en el marco regulatorio reiterado señalado concretamente en los puntos del uno al seis, vamos a centrarnos en dos momentos de la relación laboral para exponer de qué manera, a la luz del Ordenamiento Jurídico Laboral Colombiano, el empleador debe manejar la información obtenida del trabajador: en el momento de la contratación y en la ejecución de la relación laboral.

Para seleccionar su personal el empleador puede desarrollar una serie de pruebas para escoger al mejor candidato, que eventualmente podrían estar orientadas a conocer aspectos no necesariamente laborales pero que sí podrían impactar en la ejecución de las funciones a desplegar. Existen no obstante temas que jurisprudencialmente han merecido una especial atención por el cuidado que deben tener como por ejemplo datos relacionados con la ideología, la religión, las creencias, la salud o la comisión de delitos o infracciones administrativas, que podrían eventualmente generar tatos discriminatorios a la hora de vincular nuevo personal.

Sobre las pruebas médicas que puede exigir el empleador, en ejercicio de su obligación a brindar seguridad a sus trabajadores (artículo 56 CST), la Corte Constitucional se ha pronunciado sobre la prueba de embarazo, señalando que sólo puede solicitarse cuando el cargo al que se aspira sea incompatible con este estado, al poder incidir negativamente en el que está por nacer. (Sentencia de tutela 1219, 2005)

En esta misma línea, no se podrán relevar aspectos relacionados con la salud del trabajador y con todo, la Corte Constitucional ha indicado que es facultativo del trabajador revelar o no aspectos relacionados con su salud, a menos que sean necesarios para garantizar su debida protección. Esta información sin embargo sólo será conocida por el médico tratante quien indicará al empleador el trato debido al trabajador sin comunicar la afección que se padezca (Sentencia de tutela 513, 2006)

Sobre los trabajadores portadores de VIH, según el artículo 2.8.1.5.6. del Decreto Único Reglamentario 780 del año 2016, no están obligados a informar su condición a sus empleadores. Al respecto, la Corte Constitucional se ha pronunciado en diversas sentencias reiterando que esta condición no puedo justificar un trato discriminatorio y mucho menos la desvinculación del trabajador. (Sentencia de Tutela 1218, 2015)
En salud, la Corte Constitucional proscribió de otra parte la posibilidad de solicitar la historia clínica de los trabajadores junto a la incapacidad por ausencia justificada al trabajo, dado el carácter reservado del que goza esta información. (Sentencia de tutela 669, 2009)

Finalmente cabe resaltar que en sentencia de constitucionalidad 326 del año 1997, indicó la Corte que no resultaba violatorio del derecho de intimidad la creación de una base de datos con la información de funcionarios del Estado que incluyese formación académica como cargos desempeñados, que el permitiesen al Estado verificar eventuales inhabilidades o incompatibilidades. (Sentencia de constitucionalidad 326, 1997)

9. ¿Qué información en el ámbito de la protección de datos personales está obligada la empresa a proporcionar a la representación legal de los trabajadores? ¿Cómo y con qué periodicidad?

En el ordenamiento jurídico Colombiano no existe la obligación de informar con carácter previo a los representantes de los trabajadores sobre aquellos tratamientos de datos que repercuten sobre el conjunto de los trabajadores de la empresa.

No obstante, deberá analizarse en cada caso la posibilidad de suministrar información de cara a la naturaleza de la información requerida, para facilitar los procesos de negociación colectiva.

10. ¿Existe un derecho a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo? En su caso, ¿debe la empresa definir la extensión y límites de este derecho conjuntamente con los representantes de los trabajadores o puede hacerlo mediante una política empresarial?

Del mismo modo como sucede en otras legislaciones, la laboral colombiana establece una regulación detallada en materia de limitación de la jornada laboral (artículo. 161 y s.s. CST), en la medida en que constituye un derecho mínimo, cierto e indiscutible para los trabajadores. Del mismo modo, regula lo referente al trabajo suplementario, o en día de descanso obligatorio (artículo. 172 y s.s. CST). Esta regulación se justifica en la medida en que establece un límite temporal para el ejercicio de la subordinación, por parte del empleador.

En ese sentido, se establece una regla conforme con la cual el empleador solo puede ejercer la subordinación dentro del lapso – diario de 8 horas; semanal de 48 horas – correspondiente a la jornada, de tal suerte que el trabajo, esto es, la actividad personal, subordinada y remunerada, ejecutada por el trabajador a favor del empleador, que se ejecute por orden de éste en un tiempo distinto a la jornada laboral, constituirá trabajo suplementario, y causará a favor del trabajador el derecho a cobrar un recargo consistente en el pago de horas extras (artículo 159 CST). En el evento en el que ese trabajo suplementario se ejecute en un día de descanso obligatorio, se causará, a su vez, el recargo correspondiente, además de la posibilidad de disfrutar de un descanso compensatorio (artículo 179 CST).

El ordenamiento jurídico laboral colombiano no establece una regla positiva en el sentido de "desconectar" al trabajador, en el sentido de privarlo del acceso a la información relacionada con el trabajo, puesta a su disposición por conducto de dispositivos tecnológicos; lo que si se establece, como ya se ha expuesto es un régimen de limitación de la jornada de trabajo, superado el cual el empleador no está facultado para ejercer la subordinación, salvo en el modo previsto en el caso del trabajo suplementario o de horas extras, o en el del trabajo en día de descanso obligatorio.

En ese sentido, lo que se prevé es una "desconexión" de la actividad laboral por fuera de la jornada laboral, antes que el "bloqueo" del acceso a datos o el uso de dispositivos electrónicos. Así lo ha puesto de presente la Sala de Casación Laboral de la Corte Suprema de Justicia, mediante la sentencia SL 5584 del 5 de abril de 2017, cuando, al referirse al concepto de "disponibilidad", estableció que el solo hecho de que el empleador imponga al trabajador un régimen que implique la simple posibilidad de exigir la prestación del servicio, aún sin que esta se materializara, genera al trabajador el derecho a cobrar los recargos correspondientes al trabajo suplementario.

Así las cosas, no existe una reglamentación que permita la "desconexión" del trabajador por fuera de la jornada laboral; lo que existe es un régimen de trabajo suplementario, que causa sus efectos en el evento en el que el trabajador, por cualquier medio – y esto incluye los dispositivos tecnológicos y el acceso a las tecnologías de la información – preste un servicio en sede del ejercicio de la subordinación, por parte del empleador.

11. Otras cuestiones relevantes en materia del impacto laboral de los dispositivos tecnológicos en el ámbito laboral

El mundo económico, que incorpora en sus dinámicas lo laboral, se enfrenta actualmente a lo que se ha dado en llamar la cuarta revolución industrial, la incursión de las tecnologías de la información y de los sistemas ciberfísicos en el mundo empresarial, que, desde luego, generan un impacto directo en el ámbito laboral, cuestionando incluso el concepto mismo de *trabajo*, con las consecuentes implicaciones sociales, políticas, económicas, y desde luego, jurídicas.

Sin embargo, este es un fenómeno que, propio de las sociedades en las que la economía de mercado ha alcanzado su máxima expresión – de hecho, es un resultado de esa evolución -. Colombia es un país en el que, si bien el modelo económico es uno propio de economía de mercado, la oferta de trabajo subordinado industrial no es suficiente para absorber la demanda, por lo que la informalidad empresarial y laboral prevalece y, en consecuencia, el concepto de *trabajo decente*, promovido por la OIT, aún parece una aspiración para muchas personas.

En este entorno, en el que el concepto de *trabajo* dependiente está en crisis ante la irrupción de la cuarta revolución industrial, mientras que por otra parte prevalece la informalidad empresarial y laboral, la irrupción de los dispositivos tecnológicos plantea un desafío en el ámbito de las actividades económicas, generadoras de ingresos para aquellos que, por alguna circunstancia, no se incorporan al circuito laboral formal.

Es así como la Ley 1780 de 2016 contempla una modalidad económica que aún está en ciernes, denominada *Trabajo decente para las empresas de los nuevos tiempos* (artículo 24), en los siguientes términos:

> "*Las empresas que presten bienes o servicios a través de plataformas electrónicas, deberán incorporar a los mismos mecanismos para realizar los procesos de afiliación, cotización o descuentos al Sistema de Seguridad Social Integral*".

La redacción de la norma, antes de promover el uso de nuevas tecnologías, procura que, en el evento en el que un empresario establezca una industria de cuarta generación, concretamente en el campo de las economías colaborativas mediante el uso de aplicaciones informáticas, cuente con un mecanismo que garantice el recaudo de aportes al sistema de seguridad social de quienes presten efectivamente los servicios ofrecidos. Como se ve, no se trata de la aplicación de los dispositivos tecnológicos en la relación laboral, sino más bien de la imposición de una exigencia, dirigida al recaudo de aportes, impuesta al desarrollador de aplicaciones o de emprendimientos que se basen en el uso de dispositivos tecnológicos.

Bibliografía

CÓDIGO CIVIL COLOMBIANO.

CÓDIGO SUSTANTIVO DEL TRABAJO.

CONGRESO DE LA REPÚBLICA. (2006). Ley 1010 de 2006.

CONGRESO DE LA REPÚBLICA. (2008). Ley 1221 de 2008. Artículo 2º.

CONGRESO DE LA REPÚBLICA (2012). Ley 1581 de 2012. Artículo 5º.

CONGRESO DE LA REPÚBLICA (2012) Ley 1564 de 2012. Código General del Proceso.

CONSTITUCIÓN POLÍTICA DE COLOMBIA.

CONGRESO DE LA REPÚBLICA. (2016) Ley 1780 de 2016.

CORTE CONSTITUCIONAL. Sentencia de constitucionalidad 326, 326 (10 de Julio de 1997).

CORTE CONSTITUCIONAL Sentencia de constitucionalidad 602, 602 (2 de Noviembre de 2016).

CORTE CONSTITUCIONAL Sentencia de tutela 1218, 1218 (28 de enero de 2015).

CORTE CONSTITUCIONAL Sentencia de tutela 1219, 1219 (24 de Noviembre de 2005).

CORTE CONSTITUCIONAL Sentencia de tutela 405, 405 (24 de Mayo de 2007).

CORTE CONSTITUCIONAL. Sentencia de tutela 427, 427 (10 de Julio de 2013).

CORTE CONSTITUCIONAL. Sentencia de tutela 513, 513 (6 de Julio de 2006).

CORTE CONSTITUCIONAL Sentencia de tutela 669, 669 (16 de Febrero de 2009).

CORTE CONSTITUCIONAL Sentencia de tutela 768, 768 (31 de Julio de 2007).

CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN LABORAL. Sentencia 5584 (5 de abril de 2007)

DECRETO ÚNICO REGLAMENTARIO 780 del año 2016.

IMPACTO LABORAL DEL USO DE DISPOSITIVOS TECNOLÓGICOS EN MÉXICO

José Alfonso Aparicio Velázquez
División de Estudios de Posgrado, Facultad de Derecho de la UNAM

Oscar Zavala Gamboa
Profesor de la Facultad de Derecho de la UNAM

Introducción

El desarrollo tecnológico vinculado al derecho humano a la comunicación, aparece como uno de los grandes temas en nuestro país; basta con observar la importante función que realiza la Unión Internacional de Telecomunicaciones, organismo especializado de la Organización de las Naciones Unidas y el impacto de sus políticas en México, por conducto del Instituto Federal de Telecomunicaciones, para dimensionar la importancia que tiene este tema en nuestra sociedad y el interés - tanto del sector público como el privado- para que se discutan y posicionen avances y retos en esta materia.

Una de las razones es que las telecomunicaciones se han convertido en una de las claves para la prestación mundial de servicios; aspectos como la industria bancaria, el turismo, el transporte y la industria de la información dependen de sistemas de telecomunicación, que además de ser confiables y eficientes, deben ser globales.[134]

Durante las últimas dos décadas, las revoluciones tecnológicas han tenido impactos en todos los ámbitos de la actividad en sociedad y el campo del trabajo no es la excepción. Tal y como ocurrió en la Revolución industrial, nuevamente la mano de obra se encuentra inmersa en un proceso de transformación que coloca a trabajadores y empleadores en una situación de modernidad que no en todos los casos es comprendida o aceptada por quienes están acostumbrados a desarrollar sus labores de manera tradicional.

Según indica el Banco Mundial[135] las Tecnologías de la Información y las Comunicaciones (TICs) transforman al mundo del trabajo mediante dos modalidades

[134] Departamento de información Pública, *ABC de las Naciones Unidas,* Organización de las Naciones Unidas, Nueva York, 1998, p. 166.

[135] "Conectarse para trabajar: Cómo las TIC amplían las oportunidades de empleo en todo el mundo", consultado en http://www.bancomundial.org/es/news/feature/2013/09/10/how-icts-are-expanding-job-opportunities.

distintas: la creación de nuevas oportunidades de empleo y el aumento de la innovación, inclusión y globalización de los mercados laborales. Sin embargo, al constituir estas trasformaciones tecnológicas otros esquemas en el ámbito laboral, las implicaciones no se limitan a la prestación del trabajo, si no que abarcan otros aspectos de la relación laboral, como la interacción entre trabajadores y empleadores por medios electrónicos; la utilización de nuevos mecanismos de control y vigilancia en los centros de trabajo; así como la evolución del derecho procesal que incorpora mecanismos en las legislaciones para la valoración de pruebas "aportadas por la tecnología", situaciones que obligan a reflexionar sobre un tema fundamental como es la protección de datos y privacidad de los trabajadores.

Es en este sentido, donde la legislación laboral mexicana[136] ha sido nula en el uso de tecnologías en las relaciones laborales, por lo que sigue siendo una agenda pendiente de adecuación frente a los escenarios actuales, con el objeto de garantizar la igualdad de oportunidades para la permanencia, promoción y desarrollo en el centro de trabajo; pero también como mecanismo para garantizar el derecho a la intimidad y a la privacidad. Es por ello, que responderemos las preguntas, en la mayoría de los casos, haciendo referencia a derechos inespecíficos laborales, como lo es la regulación en materia de protección de datos personales en posesión de particulares.

A manera de advertencia, señalamos que en el presente análisis solo se hará referencia a las relaciones laborales en el sector privado, sin desconocer que existe una regulación laboral particular para los trabajadores al servicio del Estado, donde si bien tampoco se cuenta con un marco normativo específico sobre uso de tecnologías en el trabajo, lo cierto es que las obligaciones que se derivan de otras materias como el acceso a la información y la rendición de cuentas, permiten escenarios de mayor publicidad en entornos que para el sector privado resultarían cuestionables, como es la información que se comparte en el correo electrónico institucional, donde al final de cuentas el trabajador se constituye en servidor público.

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa?

En México, no existe norma expresa, ni interpretación jurisprudencial que se refiera al uso de dispositivos tecnológicos por parte de los trabajadores en la empresa. No obstante, en la regulación laboral mexicana se pueden considerar por extensión temas relacionados al uso de las tecnologías en el trabajo, mencionamos tres esencialmente:

[136] Nos referimos a la legislación laboral que regula las relaciones laborales del sector privado (Ley Federal del Trabajo) que data de 1970 y si bien, en el 2012 hubo una reforma importante, en ella no se consideraron aspectos como el uso de la tecnología.

i. La jornada laboral, que se vincula expresamente con las legislaciones de otros países para referirse al tema tan particular de la "desconexión laboral". En el artículo 58 de la Ley Federal del Trabajo, se define expresamente como "el tiempo durante el cual el trabajador está a disposición del patrón para prestar su trabajo".

ii. El trabajo a domicilio, que se vincula generalmente con el teletrabajo y éste realizado por medios electrónicos. En el artículo 311 de la Ley Federal del Trabajo es considerado "*como trabajo a domicilio el que se realiza a distancia utilizando tecnologías de la información y la comunicación*".

iii. La capacitación y adiestramiento en el trabajo, que puede vincularse con una capacitación en el uso de dispositivos tecnológicos dentro de la empresa. En el artículo 153-A de la Ley Federal del Trabajo prevé que "*los patrones tienen la obligación de proporcionar a todos los trabajadores, y éstos a recibir, la capacitación o el adiestramiento en su trabajo que le permita elevar su nivel de vida, su competencia laboral y su productividad, conforme a los planes y programas formulados, de común acuerdo, por el patrón y el sindicato o la mayoría de sus trabajadores*"; y el artículo 39-B. de la misma Ley, prevé una contratación especializada para la capacitación para el trabajo que define como "*aquella por virtud de la cual un trabajador se obliga a prestar sus servicios subordinados, bajo la dirección y mando del patrón, con el fin de que adquiera los conocimientos o habilidades necesarios para la actividad para la que vaya a ser contratado*".

2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o de una política interna sobre el uso de estos dispositivos? En caso contrario, ¿cómo se regula el uso de los dispositivos tecnológicos en la empresa?

Como se ha dicho antes, en México no existe regulación particular respecto del uso de tecnología en el trabajo; no obstante, existen los reglamentos interiores de trabajo que son un conjunto de disposiciones obligatorias para trabajadores y patrones en el desarrollo de los trabajos en una empresa o establecimiento (tal como se prevé en el artículo 422 de la Ley Federal del Trabajo), en el que se podría contemplar el tema materia de la pregunta.

De igual manera, podría regularse el uso de estos dispositivos, mediante la negociación colectiva, en alguna cláusula del Contrato Colectivo de Trabajo.

Por último, existen buenas prácticas o autorregulación en materia de protección de datos personales, mediante el establecimiento de un esquema de autorregulación vinculante (validado o certificado, que consiste en el establecimiento de un Sistema de Gestión de

Datos Personales) o bien de reglas para adaptar normativa, de conformidad con los "Parámetros de Autorregulación en materia de Protección de Datos Personales", que son de adhesión voluntaria, pero de cumplimiento obligatorio, una vez adheridos los empleadores, en los que podría regularse el uso de dispositivos tecnológicos en la empresa.

3. ¿En qué supuestos y en qué condiciones es posible el acceso y la monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos propiedad de la empresa (e-mail, mensajería instantánea, etc.)?

Ni la norma mexicana ni su jurisprudencia laboral prevén los criterios para la monitorización de las comunicaciones personales de los trabajadores mediante dispositivos tecnológicos en la empresa.

No obstante, en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, se establece expresamente la "expectativa razonable de privacidad", misma que podría ser aplicable, entre otras, a las relaciones laborales y en especial en el acceso y monitorización de trabajadores por parte del empleador mediante tecnologías. Dicha expectativa, que ha servido en otros países para delinear el tema cuestionado, se define como: "*En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley*" (Cfr. Artículo 7, último párrafo).

4. ¿En qué circunstancias es posible instalar sistemas de videovigilancia de carácter permanente para controlar la actividad laboral?

Como se expresó en la respuesta a la pregunta anterior, no existen normas ni jurisprudencia que expresamente en materia laboral regule el uso de la tecnología, por lo que tampoco las circunstancias para el control de la actividad laboral.

No obstante, como igualmente se expresó, en la Ley Federal de Protección de Datos Personales, hay regulación que prevé la "expectativa razonable de privacidad" que es el estándar para el tratamiento legítimo de los datos personales, que entre otros son del trabajador en su actividad laboral.

5. ¿En qué circunstancias es posible instalar sistemas de videovigilancia ocultos para controlar la actividad laboral? En particular, ¿su instalación sólo es posible cuando la empresa sospecha que se ha cometido un ilícito penal o también cuando existen indicios de un incumplimiento laboral?

Como se ha indicado en respuestas previas, no hay legislación ni jurisprudencia laboral respecto al uso de tecnologías. No obstante, como también se advirtió, existe legislación que complementa la laboral, y que prevé las condiciones del tratamiento legítimo de datos personales por parte de un responsable de éstos. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, es clara en determinar en su artículo 15 que el responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad. Y se detalla en su artículo 17, fracción II, que cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos, la identidad y domicilio del responsable que los recaba y las finalidades del tratamiento de datos.

Razones por las que, bajo dicha legislación en protección de datos, no sería posible la videograbación oculta, en ninguna hipótesis.

6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?

En el derecho mexicano, la geolocalización es objeto de análisis interesantes, por un lado, pero limitados por otro, ya que su regulación apunta mucho más hacia cuestiones vinculadas con entes gubernamentales que de aquellas permitidas a los particulares, y en el caso concreto, en el sector laboral.

El 14 de julio de 2014 se publicó en el Diario Oficial de la Federación, la Ley Federal de Telecomunicaciones y Radiodifusión, misma que regula entre otros aspectos relevantes, tanto la intervención de las comunicaciones, como al sistema de geolocalización, o como lo denomina la propia ley "localización geográfica en tiempo real", entendida como la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada.

Por su parte, el Código Nacional de Procedimientos Penales, establece en su artículo 303 que habrá localización geográfica en tiempo real, cuando exista denuncia o querella, y el servidor público facultado para ellos solicite a los concesionarios o permisionarios o comercializadoras del servicio de telecomunicaciones o comunicación

vía satélite, la localización geográfica en tiempo real de los equipos de comunicación móvil asociados a una línea que se encuentren relacionados con los hechos que se investigan en términos de las disposiciones aplicables.

Como se observa, la legislación mexicana establece presupuestos jurídicos encaminados a regular la geolocalización, para casos en los que intervengan autoridades, sea como entes reguladores, o como persecutores de delitos. Cabe señalar, que estas determinaciones evidentemente fueron objeto de controversias jurídicas, como la Acción de inconstitucionalidad 32/2012, promovida por la Comisión Nacional de los Derechos Humanos, en la que la Suprema Corte de Justicia de la Nación validó las normas que sustentan la geolocalización de los equipos de comunicación móvil vinculados a delitos considerados graves.

En el caso de nuestra materia, en realidad son escasas las regulaciones sobre la geolocalización, no obstante su uso frecuente y cotidiano al interior de las empresas y como parte de las actividades de los trabajadores, sin que la legislación o la jurisprudencia hayan emitido criterios en los que se impongan límites o determinaciones al respecto.

7. En el caso de que la empresa haya realizado un despido incumpliendo los requisitos de control de comunicaciones por e-mail o de instalación de sistemas de videovigilancia, ¿cuál sería la calificación del despido y qué sanciones administrativas se podrían derivar?

De la revisión de los artículos 51 (establece las causas de rescisión de la relación de trabajo, sin responsabilidad para el trabajador) y 133 (establece las obligaciones de los empleadores) de la Ley Federal del Trabajo, no se advierte alguna causal de despido relacionada con el incumplimiento de control de comunicaciones o de sistemas de video vigilancia; sin embargo, esto no quiere decir que sea inviable explorar la posibilidad de establecer la obligación a los empleadores de proteger los datos personales de los trabajadores y de sancionar el incumplimiento.

En ese sentido, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece los principios básicos para el tratamiento de los datos personales, mismo que debe ser cumplido por todos aquellos que traten datos personales, entre los que podemos incluir a los empleadores.

Así, esta disposición debe analizarse e interpretarse conjuntamente con el derecho procesal del trabajo, especialmente con la posibilidad de ofrecer como pruebas dentro de un proceso laboral, a las fotografías, cintas cinematográficas, registros

dactiloscópicos, grabaciones de audio y de video, o las distintas tecnologías de la información y la comunicación, tales como sistemas informáticos, medios electrónicos ópticos, fax, correo electrónico, documento digital, firma electrónica o contraseña y, en general, los medios aportados por los descubrimientos de la ciencia (artículo 776, VIII Ley Federal del Trabajo), por lo que resulta claro que en una interpretación sistemática de la norma, el empleador deberá allegarse de los elementos probatorios, sin dejar de salvaguardar los datos personales de los trabajadores, pues éste tiene prohibido ejecutar cualquier acto que restrinja a los trabajadores los derechos que les otorgan las leyes (artículo 133, fracción VII de la Ley Federal del Trabajo).

Cabe señalar, que hasta el momento son nulos los criterios jurisprudenciales o interpretativos al respecto, por lo que es necesario explorar mecanismos en ese sentido[137].

8. ¿Qué datos personales pueden ser recogidos y tratados en el marco de la relación laboral? En particular, ¿es necesario el consentimiento del trabajador? ¿En qué casos no es necesario?

Si bien no existe una regulación expresa, el artículo 25 de la Ley Federal del Trabajo establece que el documento en el que consten las condiciones de trabajo se deberán contener el nombre, nacionalidad, edad, sexo, estado civil, Clave Única de Registro de Población, Registro Federal de Contribuyentes y domicilio, tanto del trabajador como del empleador.

[137] En cuestión de tecnología, son escasos los pronunciamientos del Poder Judicial, no obstante se rescatan algunos criterios como el siguiente, en relación con el correo electrónico: Tesis: I.7o.T.79 L, Época: Novena Época, Fuente: Semanario Judicial de la Federación y su Gaceta, Tomo XIX, Junio de 2004, página: 1425. CORREO ELECTRÓNICO TRANSMITIDO POR INTERNET, OFRECIDO COMO PRUEBA EN EL JUICIO LABORAL. VALOR PROBATORIO. El artículo 776 de la Ley Federal del Trabajo establece que son admisibles en el proceso todos los medios de prueba que no sean contrarios a la moral y al derecho, entre ellos, aquellos medios aportados por los descubrimientos de la ciencia; consecuentemente, es permisible ofrecer el correo electrónico transmitido por internet, que constituye un sistema mundial de diseminación y obtención de información en diversos ámbitos. Por otra parte, dada su naturaleza y la falta de firma de la persona a la que se le imputa un correo electrónico, ello trae como consecuencia que no se tenga la certeza de que aquel a quien se atribuye su envío a través de la red sea quien efectivamente lo emitió y dirigió al oferente, por lo que si es objetado no puede perfeccionarse mediante la ratificación de contenido y firma, de conformidad con el artículo 800 del mismo ordenamiento legal, que dispone que cuando un documento que provenga de tercero ajeno a juicio resulta impugnado, deberá ser ratificado en su contenido y firma por el suscriptor. De lo que se sigue que ese medio de prueba por sí solo carece de valor probatorio ante la imposibilidad de su perfeccionamiento, además, si dicho correo electrónico no es objetado, ello no trae como consecuencia que tenga valor probatorio pleno, aunque sí constituirá un indicio, cuyo valor será determinado por la Junta al apreciarlo con las demás pruebas que obren en autos.

Cabe señalar que para el cumplimiento de obligaciones de seguridad social, el empleador debe recabar otro tipo de información relacionada con antecedentes familiares e incluso de salud (datos sensibles) sin que exista alguna regulación expresa.

En la actualidad vemos que los empleadores para contar con elementos que le permitan hacer una selección del personal, en aras de ese derecho a la libertad de contratación, recaban datos personales de distinta índole que en ocasiones vulneran el respeto a la esfera individual del trabajador a la que no cualquiera puede tener acceso. Y es que la relación laboral puede llegar a condicionar el ejercicio de algunos derechos del trabajador, pues se busca justificar con dicha condicionante o restricción la ejecución del trabajo, de tal forma que en otros contextos seguramente no sucedería[138].

Un aspecto positivo, es el hecho de que algunas empresas han comenzado a adoptar avisos de privacidad, en términos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en los que se prevé el tratamiento a los datos personales de los trabajadores, no obstante sigue siendo un tema en el que la legislación laboral se encuentra varios pasos por detrás.

9. ¿Qué información en el ámbito de la protección de datos personales está obligada la empresa a proporcionar a la representación legal de los trabajadores? ¿Cómo y con qué periodicidad?

No existe una regulación al respecto, aunque resulta interesante resaltar que los empleadores son sujetos regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, ya sea como personas físicas o morales, al no situarse en los supuestos de excepción antes transcritos, ya que no recolectan y almacenan datos personales para uso exclusivamente personal y sin fines de divulgación, pues dada la naturaleza del empleador es indudable que divulgará los datos personales de sus trabajadores para cumplir con las obligaciones que tiene en materia de seguridad social y hacendaria, sólo por citar un ejemplo[139].

Es importante señalar que el sindicato, entendido como una especie de representación de los trabajadores, es un sujeto expresamente regulado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, por lo que deberá sujetarse a los mismos principios y deberes que se les impone a otros responsables y responder en caso de un incumplimiento.

[138] HERNÁNDEZ GONZÁLEZ, A. B. y ZAVALA GAMBOA, O. "Datos personales en las relaciones laborales del sector privado", en *Revista Latinoamericana de Derecho Social,* Número 27, julio-diciembre de 2018, p. 227.
[139] *Idem.*

10. ¿Existe un derecho a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo? En su caso, ¿debe la empresa definir la extensión y límites de este derecho conjuntamente con los representantes de los trabajadores o puede hacerlo mediante una política empresarial?

El derecho a la desconexión laboral, en los términos en que ha sido concebida en otros países como Francia, no tiene una referencia directa ni en la legislación, ni la jurisprudencia mexicana. Aunque algunas empresas han adoptado códigos de buenas prácticas en los que se incluye esta figura, cuestión que resulta plausible, máxime que no existe obligación legal para hacerlo.

11. Otras cuestiones relevantes en materia del impacto laboral de los dispositivos tecnológicos en el ámbito laboral

Sin lugar a dudas, el tema de la tecnología siempre será motivo de análisis en el derecho laboral, particularmente por sus implicaciones, tanto en la prestación del trabajo, como en la interacción con los trabajadores. Es por ello, que resulta necesario analizar otras cuestiones relevantes como el teletrabajo, en el que la tecnología es un elemento fundamental y donde la regulación jurídica también resulta incipiente.

En 2017, se realizó en la Ciudad de México el Primer Foro sobre el Teletrabajo, en el que resultan oportunas las palabras de Noémie Feix[140], Oficial Nacional de Empleo "*El teletrabajo representa una oportunidad para ayudar a mejorar el equilibrio entre vida profesional y personal, pasar menos horas en los medios de transporte y más horas con la familia es un beneficio para la mayoría de los trabajadores, sobre todo en ciudades como la Ciudad de México*", pero destacando que si bien hay bondades en la prestación de estos servicios, también hay que tomar en consideración los aspectos negativos para los trabajadores (horas de trabajo sin pago, estrés y agotamiento) y empleadores (falta de vigilancia en las funciones desempeñadas), este último elemento muy relacionado con la utilización de dispositivos tecnológicos en el ámbito laboral.

[140] Véase: "CDMX lidera el tema del teletrabajo en México", en http://www.ilo.org/mexico/noticias/WCMS_561787/lang--es/index.htm

IMPACTO LABORAL DEL USO DE DISPOSITIVOS TECNOLÓGICOS EN REPÚBLICA DOMINICANA

Gina María Polanco Santos
Abogada laboralista, Estrella & Tupete, Abogados

Introducción

La República Dominicana ha presentado una evolución jurisprudencial acorde con los cambios de las tecnologías y la modernización del trabajo. En este sentido, a pesar de que aún no contamos con las legislaciones formales al respecto, las empresas dominicanas han sabido adecuarse al funcionamiento actual y los requisitos y retos que estos exigen.

En consecuencia de lo antes expuesto, cabe destacar el importante papel que juegan los códigos y reglamentos de conducta de las empresas, que son los que actualmente llevan la carga de regular los usos de los dispositivos tecnológicos en las relaciones laborales.

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa?

En el ordenamiento jurídico laboral de la República Dominicana no existen normas que regulen el uso por parte de los trabajadores de dispositivos tecnológicos dentro de la empresa y en su horario laborable, ni de carácter privado ni los pone a su disposición la empresa para la ejecución de sus labores. Sin embargo, resulta razonable que, si la empresa otorga un dispositivo que debe ser utilizado como obligatorio para el buen desempeño de las funciones de un trabajador, la empresa debe permitir su uso.

Los rasgos de una posible regulación vienen dados por la jurisprudencia, al momento en que, a través de la Sentencia número 40 emitida por la Suprema Corte de Justicia en fecha 18 de diciembre de 2013, establece los requisitos necesarios para que la empresa pueda verificar y revisar los correos electrónicos institucionales, salvaguardando el derecho a la intimidad de los trabajadores.

2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o de una política interna sobre el uso de estos dispositivos? En caso contrario, ¿cómo se regula el uso de los dispositivos tecnológicos en la empresa?

En República Dominicana no existe un carácter de obligatoriedad legal para la implementación de un código interno que reglamente el uso de los dispositivos. Las

empresas sí hacen efectivo el uso de reglamentos o políticas internas que van dirigidas al establecimiento de las todas directrices que deberán seguir todos los trabajadores.

Dichos códigos de conducta, en su mayoría, incluyen lo relativo al uso de dispositivos tecnológicos, y los mismos son aceptados al momento de incumplimiento de alguna de las normas contenidas, los trabajadores sean pasibles de despido, pero siempre con el apoyo de una de las causas contenidas en el artículo 88 del Código de Trabajo Dominicano, siendo este el régimen sancionador que garantiza el buen manejo de las reglas pautadas por la empresa.

Las empresas no tienen que seguir requisitos más allá que los de garantizar que las normas y reglas que implementen o exijan a los trabajadores no transgredan sus derechos fundamentales.

3. ¿En qué supuestos y en qué condiciones es posible el acceso y la monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos propiedad de la empresa (e-mail, mensajería instantánea, etc.)?

Las comunicaciones personales de los trabajadores cuentan con la protección constitucional del derecho a la intimidad de cada persona, sin embargo, cuando estas comunicaciones son realizadas desde dispositivos que son propiedad de la empresa, esta cuenta con la facultad para la verificación de los fines para los cuales son utilizadas las herramientas de trabajo que proporciona.

De acuerdo con la Sentencia indicada en la pregunta 1, los requisitos que debe procurar toda empresa que desee monitorear las comunicaciones de sus trabajadores dentro de los dispositivos que les otorga, son: a) la necesidad de un propósito específico, explícito y legítimo; b) que la supervisión sea una respuesta proporcionada sobre una situación; y c) la mínima repercusión sobre los derechos a la intimidad del trabajador.

4. ¿En qué circunstancias es posible instalar sistemas de videovigilancia de carácter permanente para controlar la actividad laboral?

Las empresas pueden implementar sistemas de videovigilancia para proteger su propiedad, siempre que esta vigilancia a los trabajadores no transgreda con sus derechos fundamentales, es decir, que no vaya en contra de su derecho constitucional a la intimidad.

Nuestra Suprema Corte de Justicia ha dado cabida a la utilización de cámaras en los puestos o centros de trabajo, a través de varias Sentencias (Número 279 de fecha 18 de

mayo de 2016, número 47 de fecha 2 de abril de 2012), bajo el aclarando de que no sean colocadas en sitios que evidentemente sean privados o íntimos, como son las áreas de aseo, descanso, vestuarios, comedores, entre otras. Así también, debe ser informado al trabajador que la empresa cuenta con las cámaras de vigilancia e instalarlas en lugar visibles.

5. ¿En qué circunstancias es posible instalar sistemas de videovigilancia ocultos para controlar la actividad laboral? En particular, ¿su instalación solo es posible cuando la empresa sospecha que se ha cometido un ilícito penal o también cuando existen indicios de un incumplimiento laboral?

En República Dominicana no existe permisibilidad alguna para la instalación de cámaras de manera oculta, por lo que los requisitos para la implementación de sistemas de vigilancia en el área de trabajo están condicionados a lo expresado en la pregunta anterior, es decir, que sea de forma pública y con la debida información a los trabajadores de que serán monitoreados.

6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?

A pesar de que no se han manejado situaciones que impliquen el establecimiento de las condiciones o la forma en que la empresa pueda instalar un sistema de geolocalización, nuestra jurisprudencia ha aceptado como medios de pruebas válidos, para la comprobación de la justificación o no de un despido, los informes que son emitidos por este tipo de sistema. De esta forma, nos encontramos con la Sentencia número 386, de fecha 27 de julio de 2016, dictada por la Suprema Corte de Justicia, que acogió un despido como justificado tomando como prueba el sistema de posición global (GPS), que indicó la falta cometida por el trabajador.

Tomando en cuenta, la preservación de los derechos fundamentales de los trabajadores, consideramos que, igual que todos los otros dispositivos tecnológicos dentro de las empresas, el uso de un GPS debe ser informado al trabajador.

7. En el caso de que la empresa haya realizado un despido incumpliendo los requisitos de control de comunicaciones por e-mail o de instalación de sistemas de videovigilancia, ¿cuál sería la calificación del despido y qué sanciones administrativas se podrían derivar?

En nuestro ordenamiento jurídico laboral, la consecuencia de que la empresa ejecute un despido habiendo violentado las directrices que se han pautado para el monitoreo de los

correos electrónicos y de sistemas de vigilancia, sería la declaración de injustificado del despido, toda vez que las causas de nulidad de la terminación de un contrato por despido se encuentran expresamente señaladas en el Código de Trabajo, no dejando apertura para dar ese mismo tratamiento a otras causas.

Nuestro ordenamiento de justicia no cuenta con una fase administrativa, por lo que las sanciones a las que puede verse comprometida la empresa que incumpla con los derechos fundamentales de sus trabajadores, estarán sujetas a la decisión de un Tribunal que podrá, además de las indemnizaciones y prestaciones que le corresponden al trabajador, imponer un monto en reparación de daños y perjuicios.

8. ¿Qué datos personales pueden ser recogidos y tratados en el marco de la relación laboral? En particular, ¿es necesario el consentimiento del trabajador? ¿En qué casos no es necesario?

La Ley número 172-13 sobre protección de datos, la cual tiene como objeto fundamental "*la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, así como garantizar que no se lesione el derecho al honor y a la intimidad de las personas*". Así como también regula, además, "*la constitución, organización, actividades, funcionamiento y extinción de las Sociedades de Información Crediticia (SIC), así como la prestación de los servicios de referencias crediticias y el suministro de la información en el mercado, garantizando el respeto a la privacidad y los derechos de los titulares de la información*".

A raíz de dicha ley, las empresas no pueden de manera voluntaria acceder a los datos e informaciones de carácter personal de los trabajadores que se encuentren en los burós de información. Sin embargo, para poder insertar a los trabajadores dentro del sistema de nóminas bancarias, el Sistema Dominicano de la Seguridad Social y demás obligaciones que tiene a su cargo, necesitan de los datos privados de los trabajadores, siempre que sean para este uso.

Cuando se trate de informaciones de carácter investigativo, como son los antecedentes penales o crediticios de la persona, debe existir un consentimiento escrito por parte del trabajador a que sean manejados dichos datos por su empleador.

La Organización Internacional de Trabajo (OIT) ha establecido los principios a los cuales debe acopiarse toda empresa para el manejo de los datos e informaciones de carácter personal de sus trabajadores, a saber:

1. El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador.
2. En principio, los datos personales deberían utilizarse únicamente con el fin para el cual hayan sido acopiados.
3. Cuando los datos personales se exploten con fines distintos de aqueellos para los que fueron recabados, el empleador debería cerciorarse de que no se utilizan de un modo que sea incompatible con esa finalidad inicial y adoptar las medidas necesarias para evitar toda interpretación errada por causa de su aplicación en otro contexto.
4. Los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información, no deberían servir para controlar el comportamiento de los trabajadores.
5. Las decisiones relativas a un trabajador no deberían basarse exclusivamente en un tratamiento informático de los datos personales que a él se refieran.
6. Los datos personales obtenidos por medios de vigilancia electrónica no deberían ser los únicos factores de evaluación profesional del trabajador.
7. Los empleadores deberían evaluar periódicamente sus métodos de tratamiento de datos, con el objeto de:
   a. Reducir lo más posible el tipo y el volumen de datos personales acopiados; y
   b. Mejorar el modo de proteger la vida privada de los trabajadores.
8. Los trabajadores y sus representantes deberían ser informados de toda actividad de acopio de datos, de las reglas que la gobiernan y de sus derechos.
9. Las personas encargadas del tratamiento de datos personales deberían recibir periódicamente una formación que les permita comprender el proceso de acopio de datos y el papel que les corresponde en la aplicación de los principios enunciados en el presente repertorio.
10. El tratamiento de datos personales no debería conducir a una discriminación ilícita en materia de empleo u ocupación.
11. Los empleadores, los trabajadores y sus representantes deberían cooperar en la protección de los datos personales y en la elaboración de una política de empresa que respete la vida privada de los trabajadores, con arreglo a los principios enunciados en el presente repertorio.
12. Todas las personas tales como los empleadores, los representantes de los trabajadores, las agencias de colocación y los trabajadores que tengan acceso a los datos personales de los trabajadores deberían tener una obligación de confidencialidad, de acuerdo con la realización de sus tareas y el ejercicio de los principios enunciados en el presente repertorio.
13. Los trabajadores no pueden renunciar a su derecho a proteger su vida privada.

9. ¿Qué información en el ámbito de la protección de datos personales está obligada la empresa a proporcionar a la representación legal de los trabajadores? ¿Cómo y con qué periodicidad?

Las empresas de la República Dominicana deben cumplir con los requisitos legales que les ordena el Código de Trabajo Dominicano y sus normas complementarias, como por ejemplo en artículo 15 del Reglamento para la Aplicación del Código de Trabajo, exige la presentación de una Planilla de Personal fijo, dentro de los primeros 15 días del mes de enero de cada año, por lo que los datos que tienen la obligación de proteger y proporcionar son los contenidos en dicho formulario.

Sin embargo, no existe obligación de informar a la representación legal de los trabajadores el tratamiento de los datos a los que legalmente tiene acceso la empresa.

10. ¿Existe un derecho a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo? En su caso, ¿debe la empresa definir la extensión y límites de este derecho conjuntamente con los representantes de los trabajadores o puede hacerlo mediante una política empresarial?

En la legislación laboral dominicana no se ha establecido el derecho de los trabajadores a desconectarse de los dispositivos tecnológicos que le son proporcionados por la empresa para la ejecución de sus labores, no obstante, dentro de la protección del derecho al descanso que le asiste a los trabajadores, entendemos que las empresas, deberían reglar a través de sus códigos o reglamentos de conducta o con la negociación colectiva, el tiempo en que existe obligatoriedad de conexión a estos dispositivos

IMPACTO LABORAL DEL USO DE DISPOSITIVOS TECNOLÓGICOS EN URUGUAY

Leticia Iglesias Merrone[141]
Profesora Adscripta de Derecho del Trabajo y Seguridad Social
Universidad de la República.

Introducción

Resulta indudable el creciente impacto de la utilización de dispositivos tecnológicos en las relaciones de trabajo, tanto apreciado desde un punto de vista cualitativo como cuantitativo, al punto que RASO ha postulado la existencia de "*tecnosubodinación*"[142].

Sin perjuicio de ello, en el Uruguay tal incidencia de la tecnología en el mundo laboral ha sido tímidamente abordada por normas heterónomas.

Igual parquedad se advierte de analizar los distintos instrumentos emanados de la negociación colectiva, tanto por sector de actividad, como a nivel de empresa.

Ante tal ausencia regulatoria, ha sido particularmente relevante el rol de la doctrina y la jurisprudencia sobre el particular, las cuáles han contribuido a delinear tendencias que guían la actuación de los distintos operadores de las relaciones laborales.

Desde ambas perspectivas ha quedado de manifiesto la necesidad de articular el ejercicio legítimo del poder de dirección en su más amplio sentido, que entre otros habilitaría la utilización de dispositivos tecnológicos con fines laborales, con la tutela de la intimidad de los trabajadores, derecho en cierto modo fundamental, del cual éstos no pueden ser desprovistos en el marco de una relación de trabajo.

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa?

Al presente no existe normativa en el Uruguay que a nivel general regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa.

[141] Magister en Derecho del Trabajo y Seguridad Social la Facultad de Derecho de la Universidad de la República

[142] RASO DELGUE, J., "La tecnosubordinación", en XIX Jornadas Uruguayas de Derecho del Trabajo y de la Seguridad Social, FCU, Montevideo, 2008, p. 34.

En función de la carencia de parámetros normativos integrales, el abordaje del tema se ha nutrido tanto de aportes doctrinarios, como jurisprudenciales.

Corresponde precisar que inicialmente el debate mayormente giraba en torno a la utilización de los equipos informáticos conferidos para el desarrollo de la tarea, en particular el alcance del uso del correo electrónico corporativo, así como la posibilidad de fiscalizar su empleo.

Posteriormente, la contraposición entre los poderes del empleador y derecho a la intimidad del trabajador, también se advirtió con relación a la implementación de sistemas de videovigilancia y más modernamente de los sistemas de ubicación geográfica, tanto aquellos empleados para constatar la actividad fuera del establecimiento laboral, como muy especialmente los que permiten conocer el lugar en el que se encuentra en tiempo real y a distancia cada empleado en las propias instalaciones de la empresa.

Asimismo, es del caso reseñar que contemporáneamente ha despertado atención la posibilidad de limitar la utilización de teléfonos celulares durante el horario de trabajo, lo cual implica ponderar el uso de dispositivos tecnológicos no provistos por el empleador, teniendo en consideración las desatenciones a las funciones que su empleo lleva asociadas, lo cual sabido es puede redundar tanto en una menor productividad, como incrementar el riesgo de incurrir en accidentes laborales.

En esa línea, en algunos casos a nivel de negociación colectiva por sector de actividad se han convenido parámetros al respecto, sea prohibiendo el uso de celular durante el horario de trabajo[143], sea en forma programática aludiendo a una futura regulación del tema[144].

[143] Grupo No. 18 “Servicios culturales, esparcimiento y comunicaciones", subgrupo 03 "Radios de AM y FM y sus ediciones periodísticas digitales", capitulo "Radios del Interior" 24.03.17, artículo 21: “*Durante el horario de trabajo no se podrá hacer uso del teléfono celular, facebook, twitter, whatsap, chat u otras formas de mensajería personal, salvo en los casos en que la empresa los considere necesarios para el desempeño de las tareas. Los trabajadores deberán permanecer durante su horario de trabajo en el puesto que efectivamente les corresponde ocupar*” o Grupo No. 19 "Servicios Profesionales, Técnicos Especializados y aquellos no incluidos en otros grupos", subgrupo N° 17 "Estudios Contables Profesionales y no profesionales", 6.12.16, artículo. 20: “*Uso de teléfonos celulares: Visto los problemas de distracción (con el consiguiente perjuicio para las empresas) que acarrea el uso de teléfonos celulares en los lugares de trabajo y en horas laborables, no se autoriza su utilización durante el desempeño del trabajo. El trabajador podrá mantener en su poder su celular pero no utilizarlo mientras desarrolla efectivamente su labor*.”

[144] Grupo 10 “Comercio en General”, Subgrupo No. 18 “Supermercados”, 21.12.16, artículo 20**: “***Uso de teléfonos móviles en ocasión del trabajo. Se creará una comisión que elaborará un protocolo sobre uso de celulares, con la participación de la Inspección General del Trabajo y Seguridad Social*”.

2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o de una política interna sobre el uso de estos dispositivos? En caso contrario, ¿cómo se regula el uso de los dispositivos tecnológicos en la empresa?

No existe obligación alguna de disponer de un código de conducta telemático o de una política interna sobre el uso de dispositivos tecnológicos.

Sin perjuicio de ello, resulta cada vez más habitual incluir pautas de actuación al respecto en los Reglamentos internos que discrecionalmente otorgan las distintas organizaciones.

A nivel judicial, usualmente se aprecia como deseable se expliciten a los trabajadores tantos los parámetros de uso de los dispositivos, como la política de monitoreo o fiscalización al respecto.

No obstante, la omisión patronal en tal sentido no ha sido considerada extremo determinante en un proceso en el cual un trabajador alegó como defensa que efectúo un uso extralaboral del correo electrónico del dominio de su empleadora pues ello no se le había expresamente prohibido, sosteniéndose en el fallo judicial que: "*aún cuando no existan directivas específicas en cuanto al uso de computadoras, correo electrónico e internet en el lugar y horario de trabajo, el sentido común y los principios que rigen las relaciones aborales indican que no pueden utilizarse las referidas herramientas y bienes de la empresa con fines diversos para los cuales fueron puestos a disposición del trabajador y mucho menos en beneficio personal con un potencial perjuicio para la empleadora*"[145].

3. ¿En qué supuestos y en qué condiciones es posible el acceso y la monitorización de las comunicaciones personales de los trabajadores realizadas con dispositivos tecnológicos propiedad de la empresa (e-mail, mensajería instantánea, etc.)?

Parte de la doctrina[146] y en menor medida la jurisprudencia, han considerado que el monitoreo de los correos institucionales se encuentra vedado pues ello implicaría una afectación a la inviolabilidad de la correspondencia tutelada a nivel constitucional[147].

[145] Juzgado Letrado del Trabajo de Décimo quinto Turno, Sentencia No. 39/2008 del 16 de diciembre de 2008.

[146] Entre ellos GIUZIO quien sostiene que: "*el correo electrónico constituye una forma de correspondencia (…) el hecho de que el soporte de la comunicación no sea material – papel – sino virtual – electrónica – no cambia su naturaleza*". GIUZIO, G., "*Tecnología, poder de dirección y protección de la intimidad del trabajador*", en XIX Jornadas Uruguayas de Derecho del Trabajo y de la Seguridad Social, FCU, Montevideo, 2008, p. 26.

[147] El artículo 28 de la Constitución establece: "Los papeles de los particulares y su correspondencia

Desde la perspectiva inversa, la doctrina y jurisprudencia a nuestro modo de ver mayoritarias, admiten tales pesquisas, fundando tal prerrogativa en la titularidad patronal de la casilla en cuestión y en los poderes de dirección y fiscalización que detenta el empleador[148].

No obstante, se ha planteado como deseable que los trabajadores sean informados de la posibilidad de ser pasibles de tales contralores. Hemos sostenido que si bien sería admisible el monitoreo de la casilla institucional proporcionada a cada trabajador por la empresa, en aras del principio de buena fe, impera que el trabajador tenga conocimiento de tal facultad patronal, los términos de la misma y en su caso, si la casilla en cuestión puede o no ser utilizada para fines personales[149].

Sin embargo, debe notarse que en algún fallo aislado se ha asimilado el "*chateo*" a través de servicio mensajería instantánea interno de la empresa a una conversación privada, cuestionándose por ende su monitorización[150].
En otro orden, es del caso subrayar que se ha admitido la instalación de programas centinelas para verificar el uso que del ordenador efectuaba un trabajador tras la sospecha de que utilizaba el equipo para fines extralaborales[151].

Finalmente, corresponde reseñar que respecto de los trabajadores de centros de atención telefónica para terceros ("call centers"), expresamente se establece el deber de informar a los dependientes si las "*escuchas*" serán utilizadas como procedimientos de auditoría utilizados por el empleador[152].

---

epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general".

[148] RAFFO Y LARRAÑAGA afirman que: "*el empresario cede a sus empleados, el uso de las herramientas informáticas para que desarrollen su trabajo. la empresa puede controlar que este uso sea aplicado a fines laborales*". RAFFO, V, Y LARRAÑAGA, Z N, "Control de uso de correo electrónico e internet en la empresa", en XIX Jornadas Uruguayas de Derecho del Trabajo y de la Seguridad Social, FCU, Montevideo, 2008, p. 113.

[149] IGLESIAS MERRONE, L, El principio de buena fe en el derecho del trabajo, FCU, Montevideo, 2017, p. 180.

[150] Sentencia del Tribunal de Apelaciones del Trabajo de Primer Turno, No. 71/2011, de fecha 9 de marzo de 2011.

[151] Sentencia del Tribunal de Apelaciones del Trabajo de Tercer Turno, SEF-0014-000338/2014, de fecha 30 de setiembre de 2014.

[152] Decreto No. 147/012 de fecha 3 de mayo de 2012, artículo 34.

4. ¿En qué circunstancias es posible instalar sistemas de videovigilancia de carácter permanente para controlar la actividad laboral?

La instalación de cámaras de videovigilancia permanente en el ámbito laboral, queda comprendida en los parámetros generales sobre la implementación de sistema de captación de imágenes y sonido, considerándose la misma una base de datos cuya registración corresponde ante la Unidad Reguladora y de Control de Datos Persona[153], requiriéndose paralelamente colocar señalética alusiva dando cuenta de la instauración de tal sistema, de quién es el responsable de éste y lugar en dónde se pueden ejercer los derechos de consulta respetivos.

Analizado el punto desde la perspectiva laboral, según postula dicha dependencia, no se requiere el consentimiento de los trabajadores para la implementación de sistemas de videovigilancia, pues se considera que su implementación es requerida para el desarrollo de la relación laboral, no obstante lo cual corresponde preavisar al personal tal instalación[154].

Corresponde señalar que si bien usualmente se asocia su disposición a la salvaguarda de la seguridad de bienes y personas presente en el establecimiento laboral, también se ha admitido su utilización como vía de control de la actividad laboral, aun cuando muchas veces tal extremo sea indirecto o derivado de los fines anteriores. En tal contexto, se acogió la existencia de notoria mala conducta[155], en un caso en el que las cámaras de seguridad ubicadas en un establecimiento comercial dieron cuenta de que varios trabajadores efectuaban una maniobra que implicaba entregar mercadería como beneficios de promoción pero a su vez facturarla al cliente[156].

En algunos casos asimismo se ha valorado el rol de los sistemas de videovigilancia como forma de verificar el horario realizado por cierto trabajador. Así lo trasuntado en una litis en la que se dirimía el horario extraordinario efectuado por un asalariado, en la

[153] El Dictamen No.10/010 del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales del 16 de abril de 2010 considera a la videovigilancia: "*como toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo. Las imágenes y sonidos mencionados constituyen información personal y por tanto es de aplicación la LPDP y sus normas complementarias*".

[154] Unidad Reguladora y de Control de Datos Personales, Videovigilancia en el ámbito laboral, p. 5. Disponible en: https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/91f30070-80f6-4499-8fd1-238e32adbef1/Guia%2Bambito%2Blaboral.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=91f30070-80f6-4499-8fd1-238e32adbef1. Último acceso: 5 de julio de 2018.

[155] De acuerdo a lo previsto por el artículo 10 de la ley No. 12.597 la configuración de notoria mala conducta exime al empleador del pago de indemnización por despido.

[156] Sentencia del Tribunal de Apelaciones del Trabajo de Segundo Turno, SEF Nº 0013-000224/2017, de fecha 16 de agosto de 2017.

cual se entendió: "era carga de la empleadora en base al principio de disponibilidad probatoria el acreditar el número de horas efectivamente trabajadas por el actor, máxime teniendo presente que se controlaba el horario mediante reloj existían cámaras de seguridad y ello no fue agregado en autos"[157].

No obstante ello, cabe reseñar que en doctrina Panizza ha sido muy crítica en cuanto a la posibilidad de instalar sistemas de videovigilancia: "*salvo que existan otros derechos fundamentales en juego como pueden ser la vida o la seguridad de las personas*", agregando que: "*si no están en juego otros derechos constitucionales, deberían buscar otros mecanismos de vigilancia menos lesivos de la intimidad de los trabajadores*"[158].

Debe notarse que en atención a la afectación a la intimidad a que ello conllevaría, es pacíficamente admitido que los sistemas de videovigilancia no pueden ser instalados en áreas de esparcimiento, comedores, servicios sanitarios y/o vestuarios.

Ello quedó de manifiesto en el Dictamen No. 19/2012 del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, de fecha 6 de setiembre de 2012, expedido a raíz de una consulta referida a las eventuales consecuencias jurídicas que tendría contratar un sistema de videovigilancia en un domicilio particular a efectos de controlar la actividad laboral de una niñera, en el cual se sostuvo que el mismo resultaba admisible, empero se subrayó que: "deberán respetarse los espacios privados de la trabajadora (baños, dormitorios o vestuarios), pues la videovigilancia en estos casos afecta su intimidad y privacidad y no se ajusta al principio de proporcionalidad".

5. ¿En qué circunstancias es posible instalar sistemas de videovigilancia ocultos para controlar la actividad laboral? En particular, ¿su instalación sólo es posible cuando la empresa sospecha que se ha cometido un ilícito penal o también cuando existen indicios de un incumplimiento laboral?

En función de lo expresado en el numeral precedente, en principio no sería posible instalar sistemas de videovigilancia en forma oculta.

No obstante, la legitimidad de su empleo ante un caso puntual en donde existan indicios concretos de que cierto trabajador se encuentra incurriendo en irregularidades de entidad, corresponderá sea apreciado judicialmente, ponderando los distintos derechos en contraposición.

[157] Sentencia del Tribunal de Apelaciones del Trabajo de Segundo Turno, SEF Nº 0013-000317/2017, de fecha 25 de octubre de 2017.
[158] Panizza Dolabdjian, Carolina, Los derechos laborales inespecíficos, FCU, Montevideo, 2017, p. 82.

De allí que consideramos que desde la doctrina Dieste plantea el tema en sus justos términos señalando que: "*la presencia o ausencia de la publicidad no se corresponden necesariamente con la licitud o ilicitud del control. En ciertos casos, un control encubierto u oculto puede ser legítimo, y, la inversa, un control evidente, notorio o pronunciado puede, en otras circunstancia, resultar ilícito*"[159].

6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?

No existe regulación general sobre la posibilidad de instalar sistemas de geolocalización.

Sin perjuicio de ello, no encontrándose tampoco prohibido su uso, tales dispositivos se emplean con fines laborales, principalmente asociados a trabajadores que en razón de su función transportan valores y en menor medida, para el control horario de aquellos dependientes que no prestan servicio en el establecimiento principal de la empresa. Desde esta última perspectiva, recientemente uno de los Tribunales de Apelaciones del Trabajo ha valorado negativamente que una empresa no agregara al contestar la demanda los registros del GPS como mecanismos para sustentar el horario realizado por el trabajador accionante y por ende descartar la realización de horario extraordinario, sosteniendo: "*nada justifica que la demandada no aportara la documentación relativa a los controles de horario, en GPS con la contestación, de modo tal de acreditar los horarios de trabajo del actor. La omisión en que incurre la demandada en el punto genera una presunción relativa en su contra. (artículo 142.2 C.G.P), además de colidir con el paradigma del litigante que actúa de buena fe y diligentemente*"[160].

Sin embargo, consideramos que al igual que respecto de los correos electrónicos y los sistemas de videovigilancia, debe valorarse especialmente que el trabajador haya sido avisado de la instalación del dispositivo, así como las finalidades para las cuales ellos se disponen.

[159] DIESTE, J.F., "Control multimedia de la actividad laboral y derecho a la privacidad del trabajo", en XIX Jornadas Uruguayas de Derecho del Trabajo y de la Seguridad Social, FCU, Montevideo, 2008, p .75 y 76.

[160] Sentencia del Tribunal de Apelaciones del Trabajo de Tercer Turno, SEF-0014-000047/2018, del 21 de febrero de 2018.

7. En el caso de que la empresa haya realizado un despido incumpliendo los requisitos de control de comunicaciones por e-mail o de instalación de sistemas de videovigilancia, ¿cuál sería la calificación del despido y qué sanciones administrativas se podrían derivar?

El hecho de que se incumpla con el registro del sistema de videovigilancia o en su caso, la no publicidad del anterior o de la posibilidad de monitoreo de los correos electrónicos corporativos, no conllevan de por sí a cuestionar el despido resuelto en base los anteriores.

No obstante, debe tenerse presente que el considerar ilícito un medio probatorio que ha sido capital para sustentar un despido por notoria mala conducta, puede redundar en la imposibilidad de acreditar medió la eximente legal y por vía consecuencial, que se condene al pago de la indemnización por despido correspondiente.

Tal lo trasuntado en una litis en la cual se sostuvo que una trabajadora incurrió en notoria mala conducta al simular una enfermedad, extremo que fue advertido por la empleadora al acceder a la cuenta de Skype de la asalariada desde el ordenador que esta última utilizaba en la empresa, tomando conocimiento de un intercambio de mensajes que la anterior había mantenido fuera del horario laboral con su esposo, sosteniendo sobre el particular que: "*corresponde concluir que tratándose las conversaciones entre la actora y su esposo de prueba asimilable a cartas misivas, no existiendo consentimiento al menos de uno de los intervinientes, conforme a lo dispuesto en el artículo 175.2 del CGP se trata de prueba inadmisible. Sin perjuicio de ello, se comparte asimismo el análisis que hace la sentenciante A quo en cuanto a la ponderación de los derechos en juego para determinar a cual darle preeminencia, teniéndola en el caso el derecho a la intimidad de la trabajadora, frente al derecho del empleador en el uso de la potestad disciplinaria, para lo que cuenta con otros mecanismos*"[161].

Del punto de vista procesal, ello trae a colación la contraposición existente entre quienes sostienen que la prueba obtenida de manera ilícita no puede ser considerada en el proceso. Tal lo entendido por uno de los Tribunales de alzada expresando: "*la grabación obtenida con la participación de quien y contra quien se hará valer dicha prueba, sin su conocimiento ni consentimiento, debe reputarse ilícita; violatoria de*

[161] TRIBUNAL DE APELACIONES DEL TRABAJO DE TERCER TURNO, Sentencia SEF-0014-000278/2017, del 16 de agosto de 2017. Dicha sentencia es comentada por PIZZO N, en "El debate sobre el derecho a la intimidad y la utilización sistemas de mensajería informático desde ordenadores proporcionados por el empleador en base a un caso jurisprudencial", en *Revista Derecho del Trabajo*, Año V, No. 17, octubre-diciembre 2017, p. 249 a 266, dónde también se publica el texto íntegro de dicho fallo.

derechos inherentes a la personalidad humana, tales como los derechos a la intimidad, privacidad, etc. (artículo 72 de la Constitución de la República) así como vulneratoria de la moral y buenas costumbres. Por ende, resulta carente de eficacia probatoria en el plano jurídico. La prueba ilícita, así como su efecto más próximo (que se conoce como la "doctrina del fruto del árbol envenenado" o "fruit of the poisonous tree doctrine" configuran medios de prueba inválidos, ineficaces, totalmente improductivos a la hora de poder ser valorados por el órgano jurisdiccional para fundar una decisión, incumbiendo al Tribunal el poder-deber de impedir su incorporación al proceso, por inadmisibilidad, en base a lo establecido por los artículos 6, 24 apartados 6.y 9, 146.2, 144.1, 341 numeral 6 y concordantes del Código General del Proceso)"[162].

Y otros magistrados que han sido más laxos, ponderando contextualmente el medio probatorio en cuestión, aludiéndose a la posibilidad de valorar la cuestión de la licitud o ilicitud de la prueba, no solamente de modo liminar, sino también en oportunidades posteriores, una vez acreditadas las circunstancias justificantes de lo actuado clandestinamente cuando se invocaren[163].

Del punto de vista administrativo, las omisiones de los registros de bases de datos, como ser los sistemas de videovigilancia, podrían deparar sanciones por parte de la Unidad Reguladora y de Control de Datos Personales, que oscilan entre observación, apercibimiento, sanciones económicas, suspensión de la base datos y la clausura de la misma[164].

Por otra parte, ante casos de flagrante afectación a la intimidad de los trabajadores, por ejemplo, ante la colación de cámaras en servicios sanitarios, podría el empleador ser pasible de sanciones administrativas por parte del Ministerio de Trabajo y Seguridad Social.

8. ¿Qué datos personales pueden ser recogidos y tratados en el marco de la relación laboral? En particular, ¿es necesario el consentimiento del trabajador? ¿En qué casos no es necesario?

De acuerdo con la Ley de Protección de Datos Personales, No. 18.331[165], a nivel general se requiere el consentimiento libre, previo, expreso e informado del titular cuyos datos

[162] TRIBUNAL APELACIONES DEL TRABAJO DE TERCER TURNO, Sentencia No. 541/2012, de fecha 3 de octubre de 2012.

[163] JUZGADO LETRADO DE PRIMERA INSTANCIA DEL TRABAJO del 2º. Turno, Sentencia No. 6, del 5 de marzo de 2014.

[164] Ley No. 18.331, artículo 35.

[165] Ley promulgada el 11 de agosto de 2008, reglamentada por el decreto No. 414/009.

pretenden recabarse. No obstante, ello no resulta necesario en caso de que "*se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento*" o "*deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento*"[166].

El análisis de tales postulados desde la perspectiva de las relaciones de trabajo implica que no se requiera consentimiento expreso para recabar los datos antes enunciados, mas si respecto de aquellos que excedan lo anterior[167].

Respecto de los datos que sean suministrados en el marco de la relación de empleo, corresponderá efectuar un tratamiento acorde a los principios recogidos en el artículo quinto la ley citada, lo cual apreciado desde la perspectiva laboral, entre otros aspectos implicará: solicitar aquellos datos estrictamente necesarios para los fines laborales, utilizándolos exclusivamente a los efectos requeridos en la relación de empleo, guardando la más estricta reserva sobre los mismos y teniendo derecho el trabajador a rectificar, suprimir o actualizar los datos recabados.

Debe asimismo tenerse presente, que, de acuerdo a la ley relacionada, ninguna persona puede ser obligada a proporcionar "*datos sensibles*", entendiendo por tales a aquellos que revelen: i) origen racial y étnico, ii) preferencias políticas, iii) convicciones religiosas o morales, iv) afiliación sindical, y v) informaciones referentes a la salud o a la vida sexual. Concomitantemente, por imperio de igual cuerpo normativo se encuentra vedada la conformación de bases de datos que recojan los anteriores[168].

Tales premisas generales resultan de indudable aplicación en materia laboral, en cuyo mérito no resulta posible obligar a proporcionar datos sensibles, ni en instancias precontractuales, ni durante el devenir de la relación de trabajo.

---

[166] Ley No. 18.331, artículo 9, en especial literales c. y d).

[167] CASTELLO sostiene que en materia laboral el consentimiento se encontraría implícito en la celebración del contrato de trabajo, con la excepción de los datos sensibles. Véase CASTELLO, A, "Aplicación de la Ley No. 18331 sobre protección de datos personales al ámbito de las relaciones de trabajo", en revista Derecho Laboral, Tomo LI, No. 231, julio-setiembre 2008, p. 622. MARIEZCURRENA, *et al* sostienen que: "*para la recolección y tratamiento de los datos identificatorios del trabajador y toda aquellas información con trascendencia para la ejecución del contrato de trabajo, no se requiere el consentimiento previo*". En: MARIEZCURRENA, P ;*et al*, "Protección de los datos personales del trabajado", en AA VV, Cuarenta estudios sobre la nueva legislación laboral uruguaya, Grupo de los Miércoles, FCU, Montevideo, 2010, p. 262.

[168] Ley No. 18.331, artículos 4. lit. e) y 18.

Debe notarse que la doctrina asimismo asocia la no solicitud de este tipo de datos al respecto de la intimidad del trabajador. Tal el caso de MANGARELLI, quien alude a que: "[a]*l empleador le está vedado solicitar al trabajador datos sobre aspectos de la vida privada como por ejemplo, convicciones religiosas, opinión política o sindical, orientación sexual, situación familiar. Ello deriva justamente de la obligación del empleador de respetar la vida privada del trabajador y su intimidad personal, que surge de la naturaleza del contrato de trabajo*"[169].

A lo expresado corresponde agregar los postulados de la ley No. 18.868[170], según la cual se encuentra prohibido exigir la realización o presentación de test de embarazo o certificación médica o declaración de ausencia de estado de gravidez en el ámbito laboral.

9. ¿Qué información en el ámbito de la protección de datos personales está obligada la empresa a proporcionar a la representación legal de los trabajadores? ¿Cómo y con qué periodicidad?

Desde la perspectiva de las tutela de los datos personales no existe obligación de proporcionar información a los representantes de los trabajadores.

10. ¿Existe un derecho a desconectarse de los dispositivos tecnológicos fuera de la jornada de trabajo? En su caso, ¿debe la empresa definir la extensión y límites de este derecho conjuntamente con los representantes de los trabajadores o puede hacerlo mediante una política empresarial?

No se encuentra regulado en el Uruguay a nivel general el derecho a los trabajadores a desconectarse de los dispositivos tecnológicos una vez finalizado el horario de trabajo. Tampoco es habitual que a través de la negociación colectiva por sector de actividad, ni aún a nivel de cada organización en particular, se aborde la temática.

En los estrados judiciales el punto mayormente se ha considerado desde la perspectiva de cómo corresponde remunerar el tiempo que el trabajador permanece de algún modo "*conectado*" a la empresa fuera de su horario laboral, en cuyo análisis en usualmente se pondera si el asalariado tenía el derecho a negarse a recibir la comunicación o si por el contrario, es decir ante su negativa, es pasible de sanciones disciplinarias.

[169] MANGARELLI, C., "El derecho fundamental a la protección de los datos personales de los trabajadores", en *Revista Derecho del Trabajo*, Año III, No. 8, julio- setiembre 2015, p. 56 y 57.
[170] Ley promulgada el 23 de diciembre de 2011.

No obstante, cabe señalar que el 15 de marzo de 2017 se presentó en el Parlamento un proyecto de ley denominado "*Derecho del trabajador a desconectarse del trabajo fuera del horario laboral*", en el cual se reconoce tal derecho, con el fin de garantizar el respecto del tiempo de descanso, aun cuando ello no se efectúa de manera absoluta, pudiendo cesar ante algunos supuestos, como ser notificaciones, citaciones o urgencias manifiestas, remitiendo a la reglamentación su determinación.