CORPORATE MONITORING BY TECHNOLOGICAL MEANS IN SPAIN: OVERVIEW OF SUBSTANTIVE AND PROCEDURAL CONCEPTUAL CONSTRUCTION

Rodrigo Tascón López[*]
Rodrigo García Schwarz[**]

ABSTRACT

The incredible technological advances have found one of their most striking (and legally sensitive) manifestations in the resized capacity control by the employer regarding the provision of services performed by employees. Art. 20.3 of the Spanish Workers' Statute (WS) designated to set the limits of action in this matter, only diffusely refers to human dignity, without the legislator proceeding to update a pre-informative precept. In this context, case law (both of the Constitutional Court and of the Supreme Court) has been responsible for assuming quasi-legislative work and proceeds to exaggerate the limits of corporate monitoring power when they collide (real or potential) with the nonspecific fundamental rights (to privacy – Art. 18.1 of the Spanish Constitution (SC) –, communications secrecy – Art. 18.3 SC – or to the informational self-determination – Art.18.4 SC –) of employees. The present article aims, based on the analysis of the doctrines used by the high national courts in statements, whether classic or recent (proportionality of corporate measure, expectation of privacy, and informational self-determination of the employee), to build a synthesis rule that allows us to better shape the limits of corporate monitoring power through the use of new technologies. Over time, the main procedural problems raised by this issue are discovered.

KEYWORDS: *corporate monitoring; fundamental rights; informational self-determination of the employee; limits of corporate monitoring; new technologies*.

---

[*] Doctor of Laws, University of Leon (Spain). Professor of the University of Leon (Spain).

[**] Doctor of Laws, University of Castilla-La Mancha (Spain). Professor of the University of Antioquia (Colombia) and of the University of West of Santa Catarina (Brazil), Visiting Professor at International Doctoral School of the Association for International and Comparative Studies in the Field of Labour Law and Industrial Relations - University of Bergamo (Italy).

SUMMARY

1. Introduction: resizing corporate monitoring power through the incorporation of new technologies into the workplace. 2. Substantive analysis of the limits of corporate monitoring power by technological means. 2.1. The legal doctrines used by the courts to decide on the legality/illegality of the practice of corporate monitoring power. 2.1.1. The doctrine of the proportionality of the Constitutional Court as a general criterion for resolving conflicts between the fundamental rights of workers and corporate monitoring power. 2.1.2. The doctrine of the creation of a private space for the worker through confidence in the legitimacy of a reasonable use for technological tools. 2.1.3. The doctrine of corporate informational duty under the fundamental right of the employee's informational self-determination. 2.2. Conclusion: a conceptual attempt to fix a synthesis rule on the limits of corporate monitoring power through technology. 3. Analysis of several relevant procedural issues. 3.1. The nature and value of the technological test. 3.2. The possibility of pre-establishing the technological test. 3.3. The legal consequences of the illegality of the test.

1 INTRODUCTION: RESIZING CORPORATE MONITORING POWER THROUGH THE INCORPORATION OF NEW TECHNOLOGIES INTO THE WORKPLACE

An elementary idea present in the logic of work relations considers that the celebration of a work contract and its further development gives the employer management power to arrange the benefits due and ensure the normal development of the productive process (MELGAR, 1965; DE LA TORRE, 1992; LAMAS, 1998). In a similar prerogative, a large – though limited (PARRA, 1999) – bundle of powers are derived: among others, and for what it's worth now, the possibility of the employer to take "measures he deems appropriate to verify the workers' compliance with their obligations and job duties, maintaining in his adoption and application due consideration to human dignity" (Art. 20.3 WS).

In short, this monitoring power – an indispensable complement of management (SEIN:1989, PACHES, 1998; YANINI, 2004) –, despite granting a wide – perhaps too generous and in Spanish law a little vague (DAL-RE, 1990; LOPEZ, 1985) – margin of action to the employer, it pairs, on one hand, the duty of using respectful means with the fundamental rights of the worker (as these

appear without a doubt within the broad and generic concept of human dignity alluded to by the precept); on the other, the need to circumscribe monitoring activities – except justified exceptions – to audit the issues strictly related to work benefits (SEIN, 1989; PACHES, 1998; FONS, 2002).

Without fear of exaggerating, it is possible to state that the introduction of new technologies in the company, in addition to substantially changing modes and work and production patterns (FULLER, HARTMAN, RAMAN, 1996; BROWN, CAMPBELL, 2002), presents in its influence over management power one of its "most striking" expressions, taking into account those that are enabling (increasingly) sophisticated means capable of decisively "intensifying" (and in many cases even beyond what is lawful) possibilities of business enforcement of labour activity (ORIHUEL, 1990; FONS, 2002; ALONSO, 2015).

Attendance management, characterized by the space/time coincidence of the employer and employee, is part of the "artisanal past" (BAAMONDE, GRAU, RODRIGUEZ, 1990) of the labour law and is rapidly giving way to "technological monitoring" (DAWSON, 1986); thus the "peripheral, partial and discontinuous one performed by the human hierarchy gives way to a centralized and objective one verified in real time" (ORIHUEL, 1990, p. 72) but which over time, leaves – or can leave – a perpetual trace in the "memory" of the machine (EDWARDS, 1993).

It is worth recalling how new technological information and communications allow new forms of "almost limitless" monitoring (CAPRON, JOHNSON, 2004) which (and, in many cases, at least through a legally disturbing silence) are being used *de facto* by employers to intensify forms of knowledge of the behavior of workers (ORIHUEL, 1990), creating "virtual work" centers (IGBARIA, TAN, 1998) in which the Orwellian Big Brother prophecy acquires "laborized" dimensions – "the immense power of the mechanical business eye", according to Sein (2006, p. 15) – in which reality once again, and unfortunately, exceeds fiction (MCGRATH, 2004).

Consequently, new computer technologies, like almost any invention noted in the flow of human history, presents "ambivalent charges" (LOPEZ et al., 2003), as long as, in addition to being legitimate and extremely useful (primarily aimed at improving

productivity), through this can occur – and which in fact does occur – the most vile and deplorable actions–, not only by the employer – who will see in these means an "extended hand" for the "absolute monitoring "of the operators, according to Anton and Ward (1998, p. 897) – but also by the workers themselves, as long as they can use them – during work and at the workplace – for particular purposes able to distract them from their work duties, which, apart from being an undeniable economic loss for the company in the form of lost working hours – and in the consumption of services, even if the problem has lost entity once the so called "flat rate" has been generalized – we can assume an even greater one in the form of information and program destruction through possible viruses acquired by the negligence or recklessness of those who so acted and, ultimately and in more severe cases, provide the most egregious losses of contractual good faith under faster and quieter forms of industrial espionage (RUBERT, 2004; THORP, 2003; ZEKOS, 2002).

Focusing our attention of the speech on its subject matter, the potential monitoring technologies establish a virtually unlimited protean set (LÓPEZ, 2005), that goes on a list that must be *numerus apertus*, from the – relatively – most traditional video surveillance system (in its many possibilities), to the most sophisticated access and localization control mechanisms within the company, through personal cards or even biometric data (or outside, by using GPS tracking systems), through the increasingly common mechanisms of use control given the technological tool (a computer or, in its recent and more generalized version, a smart phone), such as inspection of employee e-mails or reviewing internet browser history, installation of spyware can reveal almost all aspects related to computer equipment assigned to the employee (from the programs or applications used to the number of beats per minute performed) and, finally, the interception of telephone conversations while providing services from company terminals (FRIED, 2000; WALKER, 2004; RAY, 2004; OLIVER, 2002).

We should also include, in recent times, one other technological possibility of monitoring (partially different from the previous ones, but also related to the technologies), which is monitoring the use of social networks carried out by the worker. Indeed, their growth has been unstoppable and in them, of course, the

worker reveals aspects that may have job relevance in many cases (from unsuitable attitudes or behaviors towards a situation – for example, from sick leave to criticism towards the company or coworkers – perhaps in the context of a labour dispute, which also reaches an incredible potential for diffusion, through data about his/her personal life – health, ideology... – that can serve as a criterion for evaluation – prone to discrimination – in any selection or promotion process), and the employer may be interested in locating (through a more or less straightforward investigation, due to the popularity of the network and the private or public nature of the information contained in the profile of the user) and use – with the implicit risk of injury to some fundamental workers' rights even with widespread approval of the courts, according to Torres (2014) – for decision-making (RUBERT, 2010; GUANTER, 2015).

We must also keep in mind that, along with the various monitoring means allowed by new technologies, one of the most precise and commonly used (strong complement of the above) is given, no doubt, by the one exerted through information obtained using data-processing techniques, something greatly facilitated by the "computer trail" that remains forever in the technological toolbox, allowing subsequent verification of their use.

Using these data-processing techniques the employer can obtain and systematize information, whether it is work-related or not, regarding the worker's persona, ranging from the most banal acts to his/her most intimate secrets (union or political affiliation, religion, health status...) and return such information when a decision on the worker is necessary. Thus, the road to some of the most despicable discriminations condemned by law is expedited, while allowing developing categories (true "labour castes") that recall, in this case, the Alphas and Betas written by Huxley, allowing the employer to diversify their choices based on convenience or ability (or even attitude) of the worker concerned (DOMINGUEZ, ESCANCIANO, 1997).

The activity of the employee and the information about his/her activity constitute an "indissoluble whole" (GAETA, 1992), allowing "total" monitoring (LLOYD, 2000) – or, at least, "nearly total" monitoring (O'BRIEN, 2002) – of the employee's performance in the workplace – and even outside of it, wherever the employer – and, ultimately, the development of all types of reports or profiles –

according to the case – about not only their professional character but also, ultimately, their own personal details (DOMINGUEZ, ESCANCIANO, 1997).

Anyone who knows that they are being watched clearly loses the most basic skills of organizing their own work with a minimum margin of initiative and is subject to an almost unbearable pressure, capable of putting their own physical and psychic equilibrium in obvious danger (which puts into question one of the most basic obligations of prevention of risks associated with the employment contract, *ex* Art. 14 Spanish Health and Safety Work Law, LPRL), ultimately forcing them to radically change their behavior by trying to adapt to performance control standards (DWORKIN, 1990; BAETHGE, OBERBECK, 1995).

By increasing the potentiality of the power of surveillance and limiting the employee's performance, subjecting him/her to strict and dense work sequences, the modernization of the company elevates the business position to a higher level than that arising from its mere management power (BROWN, CAMPBELL, 2002), and, according to Dominguez and Escanciano (1997, p. 87), "introduces a new element into the contractual synallagma capable of causing a rupture in the necessary balance of interests" and jeopardizing the ("nonspecific") fundamental rights of the employee's persona in an obvious way, especially those of dignity and privacy (Art. 18.1 SC), in its classic versions, but also of the secrecy of communications (when what is being monitored are the employee's emails or phone calls, Art. 18.3 SC) and the recent information freedoms or self-determination information set forth in Art. 18.4 SC.

Additionally, this profound impact, which has been realized, has taken its toll not only on large companies – "real modern Leviathans capable of being equated to the most incisive State", according to Lloyd (2000, p. 240) –, but also, and due to lower costs and substantial improvement derived from their application, on small and medium ones, creating a "panoptic" situation (UGUINA, 2001) – in which everything can be monitored and recorded – quickly passing from the so-called "Information Society" to the most worrisome "Surveillance Society", according to Flaherthy (1998, p. 377) – which raises serious risks for those who have somehow come into contact with their normal activity cycle, mainly their

customers (actual or potential), their suppliers, and their employees (MCGRATH, 2004).

Such a technology warp has largely complicated the development of work relations, creating a scenario that differs greatly from the other whose reference was given by the fordist-taylorist model in which the concentration of employees prevails in the factory, and upon which the foundations of the initial labour law were settled at the dawn of the modern age. However, in light of the scenario described, Spanish legislators (unlike what happened in neighboring countries, such as Portugal and Italy, where the labour law has tried to provide concrete guidelines for action) have not intervened to clarify the legitimacy frameworks in a confusing situation like few others, maintaining, literally, Art. 20.3 WS, which has not been altered in recent years despite the substantial change occurred in practice.

2 SUBSTANTIVE ANALYSIS OF THE LIMITS OF CORPORATE MONITORING POWER BY TECHNOLOGICAL MEANS

The ambiguity of the legislation on this point, combined with the rapid growth and development of new forms of monitoring protected by information and communications technology (ANTON, WARD, 1998), have led the courts to establish adequacy guidelines between these new systems and (nonspecific) fundamental rights (FRANCO, 1999; SEIN, 2004), whereby "the questionable legislative imprecision requires creative, quasi-legislative work by the courts capable of achieving sometimes striking contradictions that cause, ultimately, a remarkable degree of legal uncertainty", according to Franco (1999, p. 205); but it will be "after these statements when one can start building any general doctrine, *a posteriori*, of the consequences with regard to the causes", according to Guanter (2015, p. 30); a goal that, from the recent and very important statements by the highest courts existing in the field, aims to contribute (humbly but boldly) to this present work.

2.1 The legal doctrines used by the courts to decide on the legality/illegality of the practice of corporate monitoring power

As noted, in recent times some statements of great interest on the issue now under consideration have emanated from the highest national courts trying to respond to many and varied situations in which corporate monitoring power has conflicted with the fundamental rights of employees. Legal doctrines used as arguments in such statements will supplement (if they do not enter into partial conflict with) other classic statements. Different statements (more classical and older, and more recent and innovative) must be analyzed systematically in this speech, in order to try to articulate the construction of a synthesis rule on corporate monitoring power in the technological context on their basis.

Perhaps it is appropriate to point out that the statements below that are to be explained are the result of the circumstances in this particular case (as it could not have been otherwise) and, consequently, it is somewhat difficult to relate them to each other with the intention of finding a storyline that gives coherence to the whole, although it will be attempted (after the exegesis of said statements) as a final and conclusive summary of this essay.

2.1.1 The doctrine of proportionality of the Constitutional Court as a general criterion for resolving conflicts between the fundamental rights of employees and corporate monitoring power

The general doctrine, which has been applied since ancient times to solve the conflict between the corporate monitoring power established in Art. 20 WS and the fundamental rights of employees set forth directly or non-specifically in the Constitution, is given, as it is well known, by the principle of proportionality, as set by the Constitutional Court in separate notorious cases in which the matter of corporate surveillance had to be addressed.

In accordance with the above principle, “the constitutionality of any measure restricting fundamental rights is determined by the strict observance of the principle of proportionality. To verify whether an action passes or fails the proportionality judgment, it is necessary to ascertain whether it meets the three following requisites or conditions: if such a measure is likely to achieve the proposed

goal (judgment of suitability); if, in addition, it is necessary, in the sense that there is no other more moderate measure to achieve that purpose as effectively (judgment of need); and finally, if it is weighted and balanced, and from more benefits or advantages are derived for the general interest than damages on other goods or conflicting values (proportionality in the strict sense)" (STCo 98/2000)[1].

Based on this well-known general construction, the high court was doomed (a decade and a half ago) when deciding on the constitutionality of both corporate monitoring measures consisting in recording the work behavior of employees via video-cameras. In one of the cases, a conclusion was reached, according to which the installation of a video surveillance system is in line with constitutional parameters if there is "reasonable suspicion" by the employer to be experiencing thefts by employees, constant alarming discrepancies in section yields, and when the measure was also limited to recording their own register area and had a limited duration until the unlawful conduct was proven, with failure to provide information on the installation of this measure to the representatives of employees having no constitutional significance *ex* Art. 64.1.3. WS (STCo 186/2000).

By contrast, on the other hand, and based on reasonable criteria (FONS, 2002), it is understood as a disproportionate measure, and therefore contrary to the right to privacy of employees, when the company, without providing any good reason beyond the ambiguous reason of "adequate labour activity monitoring," proceeds to complete an operational monitoring system consisting of a closed circuit television, with the installation of microphones that allow for collecting and recording conversations that might occur (STCo 98/2000).

In short, even if it is possible to find the "common denominator [principle of proportionality], the task requires in each case an additional reflection of specific cases" (GUANTER, 2015, p. 10) without it being possible to claim that "there are safe rules (...) and should any aprioristic attempt of monolithic reconstruction without fractures between the compatibility of fundamental rights and the rights and obligations arising from the employment contract

[1] STCo, Spanish acronym: Constitutional Court Decision.

be rendered ineffective (...) becoming forced, in any case, to address the specific issue that is already being considered and the circumstances surrounding it" (LALLANA, 1999, p. 21).

Therefore, as a result of this need for a specific case trail, according to Fons (2002, p. 27), "it can be said that personal privacy will not be infringed upon by the mere decision-making instruments of audiovisual control, but mainly by the existing circumstances which, in its precise application, contextualize the decision to install it" and may even violate, in some cases, the fundamental rights of employees.

Consequently, the application of the doctrine of proportionality will never fail to arouse the deepest of doubts regarding those in the position to make a claim against corporate actions, requiring that a "specific case trial" be held (DACRUZ, 2000), in which it will be necessary to address "not only the workplace where audiovisual monitoring systems are installed by the company [even though the installation of such media in places of rest and relaxation, changing rooms, toilets, cafeterias and others, adversely affects, *a fortiori*, in any case the right to privacy of workers for obvious reasons], but also other criteria in evidence, such as whether the installation was done indiscriminately and massively or not, whether the systems are visible or have been secretly installed, the actual purpose for the installation of such systems, and whether there are safety reasons due to the type of activity carried out in the workplace in question, etc." (STCo 98/2000).

Since it could not been otherwise, companies' massive use of these means of monitoring has triggered proposals for numerous lawsuits before the labour courts over the years, after which a *corpus* was formed that took as a decision criterion the mentioned doctrine of proportionality, even though there are plenty of statements fraught with gaps and contradictions. Sometimes, when the appeals courts learned about the legality of the installation of monitoring systems through video surveillance, they considered that the measure was proportionate and adapted to the relevant circumstances (they normally justified such action based on the suspicion of the employer regarding certain labour breaches) and, on other occasions (perhaps quantitatively minor), they considered it excessive and disproportionate (STSJ *Cantabria* 18/1/2007, Appeal n. 107/2007; STSJ *Madrid* 12/3/2012, Appeal n. 123/2012).

Looking for significant examples other than video surveillance in which labour courts applied the doctrine of proportionality, it can be noted how the legality of software tools for access control have been accepted, through the most common system of ID card readers (which becomes a normal mechanism that replaces the traditional signature log book), through more advanced systems, used in this case by a Public Administration, consistent with biometric readings through infrareds of certain data in the hands of officials and employees, which were used as a way to verify timetable control (WALKER, 2004), considering and from the proportionality standard, "it is ideal for achieving the proposed objective that is none other than that of reaching a higher level of efficiency in public administration, which passes through an effective monitoring of compliance with employees' obligations, which start as from the moment of timely access of their work stations and remains in strict observance during the working day" (STSJ *Cantabria* 21/2/2003, J. 122751).

In another exemplary demonstration, regarding measures to monitor the employee when he/she has to provide his/her services outside of the workplace, there are conformity statements with which a GPS movement control system is installed in the company vehicle used by employees during travel can be considered legal when no other effective mechanism to verify compliance with the benefit because it takes place outside of the workplace (STSJ *Galicia* 14/2/2013, Appeal n. 5195/2012); but, equally, acquires disproportionate characters when it also allows control outside of working hours, even in the privacy of the employee's home (STSJ *Cataluña* 23/5/2012, Appeal n. 6212/2012)[2].

A third example would be given by the controls on the use and content of telephone conversations of employees (NAVARRO, MAZZUCONI, 2002). As with the exerted control over e-mails (as will be discussed below), in this case not only the right to privacy of the employee is affected, but also the right to privacy of communications (BONETE, RUIZ, 2012). For this reason, while there can be no objection to the employer auditing external call data (recipient's number, duration, etc.), there should be a limit to the possibility of intervening in the content of the communication (STCo

[2] STSJ, Spanish acronym: Superior Court of Justice Decision.

114/1984). This being in general, however, the Supreme Court has found no objection to allowing the employer to know the content of those conversations as long as, in accordance with the principle of proportionality, there was a legitimate purpose justifying the intrusion, as in this case that was, in an alleged telemarketing situation, to analyze the commercial techniques of the employees in order to provide relevant instructions to improve them (STS 05/12/2003, RJ 2003/313).

The issue regarding records on the computer used by the employee (about its different contents, such as work e-mail, Internet surfing, files used, etc.) has been developing for over a decade, which is perhaps the most controversial aspect, as the most absolute contradiction was the characteristic note of the numerous statements on the subject issued by the High Courts of Justice (ALBELLA, 2004).

Thus, as a first line of statements the essential fact to be considered was given by corporate ownership of the computers used as a work tool and therefore, the right to privacy of communications established in Art. 18.3 SC cannot defend a situation in which the particular communication has been made through a business medium, and during and at work, especially in the absence of an express order prohibiting such activity, resulting in the disregard of the duties of good enforceable faith in an employment relationship (STSJ *Cataluña* 5/7/2000, Appeal n. 3452; STSJ *Cataluña* 6/6/2003, Appeal n. 2003/2272; STSJ *Castilla y León – Burgos* 10/5/2006, Appeal n. 2007/682).

For another line of pronouncements, however, the e-mail of the worker in the company was an appropriate channel to transmit personal information – thus giving validity to the resignation of the worker made through the e-mail if it was clear and final (STSJ *Madrid* 13/3/2001, Appeal n. 1733) – and, therefore, should be protected by Art. 18.3 of the Constitution, although, like all fundamental rights, it should allow certain adjustments given that the employer also has a legitimate interest in exercising its powers of control to prevent deviant or abusive use.

In that trial they applied as a standard to be considered the familiar principle of proportionality – which is shown, again, as a generally true doctrine on the matter – in order for corporate control over employees' e-mail when there is a justified objective and

reasonable need for such to be considered applicable [for example, a suspicion about the use of company computers to perform work for third parties with activities in competition with the producing organization (STSJ *Andalucía – Sevilla* 9/5/2003, RJ 2840), or evidence of sending large amounts of e-mails from company computers (STSJ *Cataluña* 14/11/2004, RJ 3444; STSJ *Madrid* 12/6/2001, RJ 2953; STSJ *Castilla y León – Burgos* 10/5/2006, Appeal n. 2007/682)] and there were no other – less aggressive – moderate measures to achieve that purpose (STSJ *Galicia* 4/10/2001, RJ 3366; STSJ *Madrid* 13/5/2003, RJ 3649). On the other hand, the installation of spyware programs that monitor communications carried out by employees surreptitiously and without previous suspicions is not considered to be proportionate (STSJ *C. Valenciana* 19/7/2005, Appeal n. 3205).

No doubt, this second interpretation was more in line with the Constitutional Court's understanding of Art. 18.3 of the *norma normarum*, by making a broad interpretation of the concept of communication – without circumscribing traditional media *ad exemplum* of the precept – to adapt it to the current developments within communications and data processing (STCo 70/2002). Thus, the protective environment of the fundamental right to privacy of communications – specific guarantee of the right to privacy but, at the same time, an independent fundamental right (STCo 34/1996) – must be extended, evidently, to those made via e-mail, and its guarantee also applies to company employees (ALBERTOS, 2004).

However, accepting e-mail as a communication medium protected by the fundamental right, this second interpretative line was shown to be clearly inconsistent with the concept of "protected secret," which, according to the Constitutional Court, has "a formal character, in what is being said from what is being stated, whatever its content may be and the purpose of the communication itself belonging or not to the realm of the personal, the intimate or the reserved (...) and also can only be intercepted by court order," and not, obviously, – and as the appeals judgments allow in an attempt to reconcile the general dogma of the right to privacy of communications with the capacity of corporate control – by a decision of the employer, provided however that it could become such (STCo 34/1996). Although it is now noted, notwithstanding future elaboration, in its last statements, the

Constitutional Court has understood that the information provided through an "open channel" is excluded from such construction (which seems to be the classification deserved by the company media made available to the employee for the provision of services), and that prevents the communication from being confidential (STCo 241/2012; STCo 170/2013).

Meanwhile, regarding controls over the Internet browser, or files and software used by the worker, contrary to what occurred in the previous case, the basis of the protection of employees against monitoring Web pages visited during the working day cannot be justified by the right to privacy of communications. In this case, there is access to information, but no true objectively protected interpersonal communication (FONS, 2002; ALBERTOS, 2004). Consequently, the corporate power game will be broader at the time of verifying possible breaches of contract by the employee, consisting of consulting web pages or the use of other kinds of computer resources for private purposes – or to perform other kinds of work violations (STSJ *Cantabria* 15/7/2005, Appeal n. 1918) – during the working day, even though we should not ignore their attachment to the unwavering limit constituted by the right to privacy (MOSTERIO, 2001).

Recently, the courts have also been in the position to assess the legality of the monitoring carried out through the supervision or inspection of personal social networks of employees (but only if work-related information has been shared), accepting, in general, its realization, when the employer has obtained the information from networks accessible to the public, without infringing on private profiles or access keys (STSJ *Madrid* 25/11/2010, Appeal n. 2865/2010; STSJ *Cataluña* 30/5/2011, Appeal n. 1170/2011; STSJ *Andalucía – Granada* 10/11/2011, Appeal n. 2333/2011; STSJ *Aragón* 9/5/2012, Appeal n. 162/2012; STSJ *Asturias* 14/6/2013, Appeal n. 214/2013); although, however, it is obvious that there are situations in which the use of sensitive information can be, *per se*, damaging to the right to non-discrimination (Art. 14 SC) (TORRES, 2014).

2.1.2 The doctrine of the creation of a private space for the worker through confidence in the legitimacy of a reasonable use for technological tools

In a context such as that briefly described in the preceding pages

(where the principle of proportionality had been the only standard for a possible solution), the process of agreeing on the limits of corporate monitoring power found the unified doctrine of the Supreme Court relevant, if not decisive, or at least very significant in seeking to provide solutions precisely to one of the issues that, until that date had proved more controversial, which is the corporate power over the records of computers used as a work tool by employees.

As a *de facto* assumption, the Supreme Court faced a situation in which an employee serving in an office, without a key, with a computer available and lacking an access code and connected to the company network. As a result of information failures detected on that computer, the company resorted to a computer technician who, in the presence of the company manager (but without the employee or personal representation present), detects the presence of computer viruses as result of browsing unsafe websites. In this regard, the inspection of the temporary files folder allows the discovery of older access to pornographic sites, whose data were copied into a USB device and delivered to a notary. Once repaired (and perhaps to provide some formal inspection), the search scene is repeated, but this time in the presence of personal representatives, after which they proceed to dismiss the employee.

Both judgments issued by the Judicial Court and the Superior Court of Justice (STSJ *Galicia* 25/1/2006, Appeal n. 2006/844), understand those guarantees provided in Art. 18 WS for searching the worker's locker from the analogous application of supposed corporate inspections of the worker's computer, and, given that they have not been observed in the present case, the evidence obtained as a result of the search conducted is invalid.

To appeal for a unification of doctrine, the company seeks as a contrasting statement one of several in which, in sharp contrast to the previous line, it is considered that the guarantees referred to in Art. 18 WS cannot be demanded in the search of a computer installed by the company and available to the employee to perform his/her services, due to the fact that it is not personal property of employees, but rather a work tool (STSJ *Madrid* 13/11/2001, Appeal n. 2002/471).

The Supreme Court is responsible for clearly specifying how the guarantees referred to in Art. 18 WS regarding the search of the employee's locker result, in any way, analogically applicable to the

control performed by the employer regarding the technological means that are provided for employees in order to perform their duties, banishing once and for all any doubts and solving the existing contradiction between a line of conformity statements under which such guarantees were to be observed analogously (STSJ *Andalucía – Málaga* 25/2/2000, Appeal n. 626; STSJ *Castilla y León – Burgos* 11/6/2003, Appeal n. 2526; STSJ *Cantabria* 26/8/2004, Appeal n. 2513; STSJ *Cataluña* 21/9/2004, Appeal n. 2880), and another that it is not considered appropriate (STSJ *Cataluña* 5/7/2000, RJ 3452; STSJ *Madrid* 2/12/2002, RJ 789/2003; STSJ *Cataluña* 6/6/2003, RJ 2272; STSJ *Castilla y León – Burgos* 10/5/2006, Appeal n. 2007/682).

However, the most significant aspect of this great change in trends by the Supreme Court is given by such reasoning according to which it is established on a jurisprudential level since the doctrine referred to a "social use" of the technological means of the company by the employee, as a result of which the Supreme Court agrees to a private space for the worker, whose invasion would assume an unspecified injury of the right established by Art. 18.1 SC.

Indeed, based on that famous thesis according to which "the right to privacy implies the existence of its own environment and is reserved against the action and knowledge of others and is necessary according to the guidelines of our culture, to maintain minimum quality of life," (STCo 209/1988; STCo 197/1991; STCo 99/1994; STCo 207/1996; STCo 98/2000) the Supreme Court understands that, assuming that "there is a custom and not merely occupational or professional use of computer media provided by the company. That personal use is a result of the practical difficulties of establishing an absolute prohibition of the use of the computer (as it is with the telephone conversations of the company) and the generalization of a certain tolerance for moderate use of this media. At the same time, we must bear in mind that these media are owned by the company and that such are used by the employee in carrying out the provision of services, and so such use is covered within the surveillance environment of the employer in Art. 20.3 WS" (STS 26/9/2007, RJ 2007/7514; STS 8/3/2011, RJ 2011/932).

However, as continued by the high court, "the business tolerance of the corporate use creates a general expectation of confidentiality of those uses, which are expectations that cannot be

ignored, but nor do they represent a permanent impairment of corporate monitoring, because, even if the worker has the right to the respect of his/her privacy, he/she cannot assert that respect when using a medium provided by the company against the instructions established by such. Consequently, according to the requirements of good faith, the company must set the rules of use of those mediums in advance (with implementation of absolute or partial bans), and inform workers that there will be monitoring and of the means to be applied in order to ensure their proper use. Thus, if the medium is used for private use against these prohibitions and with knowledge of the existence of applicable controls and measures, it may not be understood that when the control is carried out there is an infringement of the "reasonable expectation of privacy" (STEDH 25/06/1997 – C. Halford; STEDH 03/04/2007 – C. Copland)[3].

When there are no such indications from the employer, it is clear that the reasonable expectation of privacy arises, something which is particularly obvious when it comes to private telephone conversations or communications by e-mail (both with extra protection under the fundamental right to secrecy of communications), but also when it comes to employees' personal files or temporary files (automatically saved copies on the hard disk of the webpages visited on the Internet). These are "navigation trails or prints, and not personal information that can be understood to fall under the protections of privacy, notwithstanding what has been said about the warnings by the company (...) and these files may contain extremely sensitive data in the area of privacy (STEDH 03/04/2007 – C. Copland), as they may contain revealing information on certain aspects of private life (ideology, sexual orientation, personal hobbies, etc.)" (STS 26/9/2007, RJ 2007/7514; STS 8/3/2011, RJ 2011/932).

Consequently, corporate performance represents an intrusion into the intimate environment of the worker and therefore evidence obtained in this manner is invalid. "It is true that the initial entry in the computer can be justified by the existence of a virus, but corporate performance does not stop at repair tasks, but continues in the analysis of the computer (...). Thus, it is inconceivable being in the presence of what is considered in the criminal environment as a

[3] STEDH, Spanish acronym: European Court of Human Rights Decision.

'serendipitous finding,' because it has gone beyond what was justified for regular admission for repair" (STS 26/9/2007, RJ 2007/7514; STS 8/3/2011, RJ 2011/932).

The legal construct used by the Supreme Court is extremely clever and quite clearly defines the profiles of the fundamental right to privacy in the context of the development of the provision of services. As is well known, it has been a long time since fundamental rights definitively entered the company, banishing the last redoubts of "industrial feudalism" (STCo 88/1985); it is necessary to consolidate the foundation needed to speak of a true "labour citizenship" (PÉREZ, 1996; GRAU, 1991) in which, even during and at work [and not only in the rest and dressing areas], even while using the work tools owned by the company, even with such (and everything) there is a private space for the employee, regarding his/her person, with his/her reasonable expectation of seeing a minimally respected bastion of independence outside corporate control and interference.

Without a doubt, the efforts of the courts to try to extend the fundamental rights to the reasonably possible extent under the employment contract are praiseworthy (DAL-RE, 1990; SEIN, 1989); however, in this case an employee's privacy is presented as fluctuating, able to expand or shrink depending on the previous behavior of the subjects involved.

Indeed, the Supreme Court itself, in a subsequent judgment that confirms the doctrine but adds refinements, recognizes that this new area of privacy defined in its judgment "may decline when the employer has detailed the specific instructions of the technological tool, either fully or partially prohibiting the personal use of company resources, in which case we cannot speak of a reasonable expectation of privacy" (STS 11/10/2011, RJ 2011/932). In other words, there is no objective right to privacy, but rather corporate tolerance, which creates a mere expectation that obviously can be destroyed (VÁZQUEZ, 2015).

In any case, the doctrine of the construction of an expectation of the employee’s privacy from a certain degree of tolerance was necessarily conditioned, logically, depending on the opinion of the ultimate interpreter of the Constitution. And based on that fact it has recently come to be pronounced in two statements, to ratify it as

doctrine, even though it is completed it in some terms in a somewhat restrictive manner.

In the first case, the company accessed the records of electronic communications of two employees using a computer messaging application that had been installed on a public computer (without a personal password), contrary to the express prohibition of installing programs on the computer. According to the supreme interpretation of the *norma normarum*, "there is no doubt that the management and regulation over the use of corporate owned means of technology by the employee, and the corporate power of surveillance and enforcement of obligations relating to the use of the means in question, provided with full respect for fundamental rights is admissible (...). The intensity or degree of rigidity by which corporate surveillance and control must be assessed is variable depending on the configuration of the conditions of the provision and use of tools and instructions that might have been provided by the employer for that purpose" (STCo 241/2012).

The Constitutional Court recalls the formal character of the right to privacy of communications (STCo 11/1984; STCo 70/2002), but it reiterates that this construction is excluded from the information communicated through an "open channel" (which apparently is the classification deserved by the company media made available to the operator for the provision of services), and that prevents the communication from being confidential. Furthermore, the same monitoring of message content is considered to be justified in this case (as once proposed by the doctrine to try to provide for corporate interference in employee areas) (FONS, 2015) as "mere access to other elements of communication such as the identification of the sender or recipient, as such on their own do not serve as evidence to illicitness," is inefficient (STCo 241/2012).

Consequently, this ruling of the Constitutional Court is in perfect line with the construction of the expectation of privacy previously incorporated by the Supreme Court, following the foundations established by the European Court of Human Rights. Based on this, it is assumed that corporate monitoring powers are "coextensive to a clear policy on the use and destination of information technology production (...) as the existence of a company policy on the use of computers will be the fundamental

interpretive element in determining the legitimate authority of employees" (FONS, 2015, p. 345).

Therefore, the predetermination of the employer (corporate policy set in internal instruments more or less formalized; the "corporate rules" for computer issues) takes on an absolutely crucial dimension, becoming the decisive factor in determining the legality or illegality of the particular use of computers, and also by extension, of the eventual intrusion into the privacy of the employee (O'BRIEN, 2002).

In this sense, it is perhaps not trivial to show how representatives of workers are called to play – in this as in anything else where there are professional interests of those providing self-employment services – a starring role, not only in monitoring corporate performance but, correspondingly, in the negotiation in search of court settlements (GARRIDO, 2003), whose concrete joint tasks are in each case, at least, complicated (GREENE, HOGAN, GRIECO, 2003; FIORITO, BASS, 2002). For this reason the lack of importance that is, very lightly, assigned at the time of the absence of communication of the installation of a surveillance system to workers' representatives (required *ex* Art. 64.1.3. WS) is particularly discouraging (STCo 186/2000).

It is necessary to consider how, when the company established an appropriate policy – through the establishment of a code of conduct or procedural statement (NEILA, 2004) – allowing the employee such coveted "social use" of his/her mail, the operator usually responds positively, establishing those limits (O'BRIEN, 2002). A poorer working environment can be assumed if the employer strongly refuses to allow any personal use. From the individual point of view, it has been clearly shown how "it is unreasonable to require from the employee an almost heroic conduct by giving up a medium to which he/she is given easy access" (CARRO, 2001, p. 36; ALBERTOS, 2004, p. 26).

In any case, this is a legal index to bear in mind when the company does not say anything about it (neither allowing nor forbidding it); it seems that this omission must be understood (in a specific legal version of the Spanish assertion according to which "silence means consent") as a tacit concession that legitimate social use of technological company media [which, while it may be

revoked by the employer, does not allow a sudden and unexpected change, but forewarned and gradual, would subvert that principle of law that prohibits *venire contra factum proprium*] (STSJ *Madrid* 16/7/2002, RJ 3036) and, from that reasoning, considers a degree of personal use of a company computer (and probably other elements such as a mobile phone made available by the company) to be tolerable for particular purposes; the question would then (and this is something that can only be fully resolved in each case being) be determining when the employee performs a use or an abuse (NINET, 2001; VILLAZON, 2004).

However, this idea is somewhat blurred in view of the second case in which the Constitutional Court has had to pronounce over corporate monitoring of the use of technological tools, applying the doctrine of the expectation of privacy, which features additional, somewhat restrictive elements. The supposition to be evaluated consists in that the company proceeded to carry out an inspection of the contents of the employee's mobile phone and computer, discovering that he/she was sending strategic content to another company in the sector.

The Constitutional Court begins its reasoning by recalling, again, the formal character of the right to privacy of communications (STCo 11/1984; STCo 70/2002), but it reiterates that such construction is excluded from the information communicated through an "open channel" (which apparently is the classification deserved by the means of the company made available to the operator for the provision of services), and which prevents the communication from being confidential.

Next, and fully entering into the issue, it is understood that there is no expectation of privacy because the applicable collective agreement classified as a minor fault, the use of information technology that was property of the company for purposes other than those related to the content of the employment relationship. From such data (and even if the particular company had not forewarned the employees), the Court assumes as a fact that any expectation of privacy has been destroyed, since the definition in the agreement represents an express prohibition of non-occupational use of such means (STCo 170/2013).

With this, of course, the High Court formally accepts the

thesis that in the context of development of the employment contract there may be an expectation of privacy (which may limit corporate control), which clearly shows that it is relatively weak and can be switched off by almost anything that shows the employee the illegality of his/her conduct while using corporate technological mediums for personal use (eliminating the potential tolerance for a reasonable use), not only as a direct instruction of the employer, but rather the more remote disapproval incorporated into the collective agreement (TOVAR, 2013; PÉREZ, INSUA, 2014).

In addition, the Constitutional Court retrenched in this case the thesis that they had used in several appeals statements, under which a "double warning" was necessary (VÁZQUEZ, 2015) to destroy the expectation of privacy by the employee: on one hand, a ban on personal use of technological instruments; on the other, a notice of the intention to carry out a monitoring and control system to verify the correct use of such media (STSJ *Cantabria* 18/1/2007, Appeal n. 187/2007). This is because "the conventional express prohibition of a non-occupational use of e-mail and the subsequent limitation to professional purposes, implied the ability of the company to control its use in order to verify compliance by the worker with his/her obligations and work duties" (STCo 170/2013).

2.1.3 The doctrine of corporate informational duty under the fundamental right of the employee's informational self-determination

Recently, the Constitutional Court has come to bring a new doctrine to be considered in the assessment of the issue of whether corporate monitoring power exercised through technological means is harmful (or not) to fundamental rights. In the course of fact, the company (in the case of the University of Seville) used, as evidence to justify the disciplinary sanction imposed on the employee for breach of their working hours, the images obtained through a video camera located not specifically in the workplace, but at the access to the area, without having shown that its objective could serve the purpose of controlling the services performed. In this case, the statement of the High Court runs from the infringement of the fundamental right to protection of personal data, established in Art. 18.4 SC, ultimately granting the requested protection (STCo 29/2013). In this regard, it should be recalled that the Constitutional

Court had previously understood that the mentioned provision of the charter contained a true fundamental right (STCo 290/2000; STCo 292/2000) and the rules for its implementation (currently, Act 15/1999, on the Protection of Personal Data and its Implementation Regulations, Royal Decree 1729/2007) are fully applicable to the field of work relations (RUBERT, 1999), serving to correct the abuse of information processing in the field of paid employment (STCo 11/1998; STCo 202/1999).

The scientific doctrine had forewarned that the direct weighing of the limits of corporate monitoring power required taking into account the perspective of the protection of personal data as long as most of the technological control mechanisms have a method for systematizing the data (including images, sounds, or other types of information) that reasonably cause such mechanisms to be submitted to the rules (constitutional and legal) governing such matters (SIMITIS, 1991; NAPIER, 1992; BROWN, CAMPBELL, 2002). They had collected some pioneer statements on the subject, although the approach was still far from being a majority, perhaps because the defensive strategies of employees in the judicial area were based on other fundamental rights (SEIN, 2008; LÓPEZ, 2006).

So far the High Court has not had occasion to rule on this question, but that judgment has entered fully into the matter, clearly confirming this perspective (AROCHENA, 2015; MOYA, 2013). Thus, "it is beyond doubt" that the images captured by the cameras are of personal data (under the broader concept contained in Art. 3 of the Organic Law on the Protection of Personal Data and 5.1 RD 1720/2007 and, specifically, the instruction 1/2006 of November 8th, from the Spanish Data Protection Agency), and that the means of corporate control "offer multiple data processing means" (STCo 29/2013).

Next, the Court will make a dogmatic effort to appraise the duties of information regarding data processing, perhaps to outline the differences with the previous precedent, in which it was understood that the absence of information to employee representatives on the means of corporate control –Art. 64.1.3 WS– was strictly a matter of ordinary law that did not affect the judgment of constitutionality (STCo 186/2000).

Thus, "a restrictive interpretation of the right to information can not affect the case concerning Art. 18.4 SC (...) which also operates

when there is legal authorization to collect the data without consent (as occurs in the field of development of the employment relationship, *ex* Art. 6 LOPD), it is clear that one thing is the need for consent and another, which is different, the duty to report the purpose of such treatment (...). There is no explicit legal authorization for the omission of the right to information about data treatment in the field of work relations... and neither could it stand its ground in the corporate interest to control work activity through surprise or unannounced data processing systems to ensure maximum effectiveness of the monitoring goal (...) because that logic founded in the corporate utility or convenience would break the effectiveness of the fundamental right in its essential core" (STCo 29/2013).

Precisely the fact that the employees had not been informed about the "usefulness of work supervision," but rather, on the contrary, it would appear that the surveillance answered purposes of "public safety" (and, indeed, for this purpose it was granted to the Agency for Data Protection), and therefore not for "a declared and specific purpose to control work activity" leads the high Court to grant the requested protection.

In short, the Constitutional Court has accepted under all terms, the question under which, while the development of an employment relationship can lead the employer (in the normal development of such and *ex* Art. 20.3 WS) to collect data (and perform subsequent treatments thereof) without obtaining the consent of employees (Arts. 6 and 11 LOPD), such does not relieve them from complying with the information requirements established in Art. 5 LOPD, as the affected party [in this case, the controlled employee] must be informed explicitly, precisely, and unequivocally by the responsible person or his/her representative, within three months following the time of the search – which term seems too long for the workplace (RUBERT, 1999), an obvious manifestation of the many problems caused by the lack of a specific labour regulation on this issue (SIMITIS, 1999) – of the origin of the data as well as the existence of a file or processing, as well as the purpose of collecting the data, recipients of information, the possibility of exercising rights of access, rectification, cancellation, and opposition, and the identity and address of the controller, concluding that company omission of such information curtails the fundamental right of informational self-

determination referred to in Art. 18.4 SC (SEIN, 1989; PACHES, 1998; FONS, 2002).

The High Court unequivocally so concluded when stating that "otherwise it would confuse the legitimacy of the purpose of treatment (in this case, the verification of compliance with work obligations through data processing Art. 20.3 WS, which is exempt from the need to obtain consent *ex* Art. 6.2 LOPD) with the constitutionality of the act, which requires previous provision of the necessary information under Art. 5 LOPD (...) when the truth is that it should proclaim the legitimacy of that purpose (even without the employee's consent, Art. 6.2 LOPD), but, in the same manner, declaring that the use of such to carry out covert means to deny employees of the required information damages Art. 18.4 SC (STCo 29/2013).

It is necessary to emphasize that the approach recently taken by the Constitutional Court (regarding the necessary consideration of Art. 18.4 SC on the assessment of the exercise of corporate monitoring power) has found rapid application by ordinary jurisprudence, which has spoken about an assumption in which the dismissal of an employee had been supported by video evidence obtained with a camera whose purpose was for other than controlling work activities (STS 13/5/2014, Appeal n. 1685/2013), warning, in addition, of the possibility following the entry into force of the Regulatory Law on Labour Jurisdiction (LRJS, Spanish acronym) of trying to test the technology, precisely to avoid violations of the fundamental rights of employees, with the authorization of the judicial authority, *ex* Art. 90.4 LRJS, as it was pointed out previously in this essay (CRESPO, 2014).

2.2 Conclusion: a conceptual attempt to fix a synthesis rule on the limits of corporate monitoring power through technology

A systematic look at the amalgam of assumptions and doctrines that have just been glossed over can lead the reader to a sense of unease, given the various statements of the courts that have come to decide on the exercise of corporate monitoring power exercised through (or over) technological devices containing arguments difficult to reconcile, which sometimes seem contradictory and it is not very clear to assess whether they are

overcome or simply supplemented by other previous ones.

As the legislator, at this point, is not, nor is expected, and his/her intervention, although "ideal, in this case, appearing utopian", according to Arochena (2015, p. 415), the work of the employee must focus around the possibility of a logical inductive reasoning (from the particular to the general), to provide a synthesis rule to try to harmonize the various statements (scattered and passed, of course, attending to the present circumstances of each case and the defense strategies used by the legal advisers of the concerned employees) and reach a general validity as a guide and concerning a matter which has proved more difficult than others. For this task, the following guidelines are intended to help, offered as a conclusive culmination of the exegesis study being completed:

1. – When the company remains silent and does not expressly adopt a decision or instruction in the use and control of technological work environments, it is understood that the employee acquires a "reasonable expectation of privacy" (STCo 241/2012) and therefore, can enjoy a "social use" of the instruments and working tools without the employer moving from tolerance to a ban, abruptly and unexpectedly, for in that case the limits of the fundamental rights of employees (to privacy, Art. 18.1 SC or even to the secrecy of communications, art. 18.3 SC) would be broader and more stringent conditions of business activity.

2. – In this case, that expectation of privacy does not have an objective existence in itself, but derives from the previous attitude of the parties and therefore can be limited (but probably not completely destroyed), either directly by the employer, through an instruction or a regulation establishing clear and specific conditions of use and prohibitions (total or partial) for the tools to be used by the employee (STCo 241/2012; STS 26/9/2007, RJ 2007/7514; STS 8/3/2011, RJ 2011/932); or through other instruments (such as the collective agreement) (STCo 170/2013) that conclusively demonstrate the illegality of the use for personal purposes of the technological tools made available to the employee by the company.

3. – However, even in this case where the rules are set out to be observed by the employee in the management of technological tools, further control by the employer can be carried out through the establishment of a permanent monitoring system of work activities

via technological means (whether to verify the use of this software tool, or to directly monitor all of the work performed through a technological contrivance), it seems that it must be subject – on a second level, recalling the previously mentioned construction of the "double forewarning", according to VÁZQUEZ (2015, p. 359) – to proper observance by the employer of the following obligations:

a) On one hand, to provide proper information on both the installation of the control measure to the representatives of employees *ex* Art. 64.1.3. WS [even if its omission was considered devoid of constitutional significance too lightly, as the reader will recall] (STCo 186/2000); as a concrete and necessary form, for the affected worker on the collection of data (images, sounds, or any other captured and/or – observing the matrix –information processed by the control means used) and its purpose (control of worker labour and as a means of activity testing for the accreditation of illegal work that justifies the adoption of future hypothetical sanctions), as provided for in Art. 5 LOPD (STCo 29/2013).

b) On the other hand is respect for the principle of proportionality, as this doctrine cannot be taken as a reference in the assessment of possible damage to the fundamental rights through corporate control, even if it is to be relocated as a criterion for shutting the system down. Consequently, even established rules of use and informed adoption of the control measures may not be unreasonable or disproportionate, since in that case it would certainly deserve legal reproach, and it could be challenged, neither by the representatives of the employees, if they have been informed or have knowledge of such – through a process of collective bargaining, nor the individual employee affected – normally fighting a corporate disciplinary measure (AROCHENA, 2015).

The dogmatic question of which employee's fundamental right has been violated in this case needs to be analyzed; in principle, it seems that the expectation of privacy will have been destroyed, although it is doubtful whether the employer can, by its own will completely destroy this fundamental right, and there would always be an applicable minimum stronghold in the field of work relations that prevents intensive and abusive control by the company; certainly it would not be the secrecy of communications, since the use of an "open channel" [as would a computer-work tool whose use has been

severely restricted by the company for personal purposes] is not protected by Art. 18.3 SC (STCo 241/2012; STCo 170/2013); in short, a system of abusive and exhaustive control, at least and ultimately seems to be contrary in that regard due to the dignity of employees established in Art. 10.1 SC and established as a limit to the power of management in Art. 20.3 WS.

4. – The question arises, then, in order to finish this construction, whether there is any exception to the general rules to be observed by the company (informational and proportionality) in using a measure of technological control. Since then, observance of the rules outlined above seems necessary in general in those cases where the employer intends to install *ad futurum* a permanent surveillance system in the productive organization (STCo 29/2013).

However, it is possible that the aim is not so definitive, but simply a timely and detailed check based on a "reasonable suspicion" of a breach of the work contract and in order to specifically establish a test as proof of illegal for purposes of dismissal or other disciplinary action, which falls squarely within the orbit of enshrined effective judicial protection, as well as within the range of the fundamental right in Art. 24 SC, which includes the right to make use of the necessary and convenient means of testing (AROCHENA, 2015).

Perhaps with these assumptions one could support, strongly, the employer being able to waive the rule that requires the provision of information and proceed to develop the test with greater freedom and capacity; as such it was recognized by the Constitutional Court specifically in this case, which commented many times that if the employer had "reasonable suspicion" of having suffered theft from the obvious cash discrepancies it sustained, with due regard to the obligation to inform the workers' representatives (Art. 64.1.3 WS).

So it could also be understood, perhaps, regarding direct information to the affected employee (Art. 5 LOPD), even if the high court has not expressly ruled on this matter as it is not the subject of the de facto situation addressed in the statement in which the analysis ensuring employee informational self-determination in cases of corporate control had to be faced (STCo 29/2013). At least, in this exceptional case it is worth justifying the delay in fulfilling this duty for the time strictly necessary and taken (in this case with legal basis)

within three months following the registration of the data referred to in Art. 5.4. LOPD.

In any case, to avoid this uncertainty, so that it may be resolved in the future by the supreme interpreter of the Constitution, a solution would be provided by the use of the possibility provided for in Art. 90.4 LRJS to try to enlist the aid of the court in the pre-constitutionality of the test and thus ensure to the extent possible, its lawfulness in the future process, as expressly encouraged by the Supreme Court and will be discussed at another point in this essay (STS 13/5/2014, Appeal n. 1685/2013).

3 ANALYSIS OF SEVERAL RELEVANT PROCEDURAL ISSUES

It is appropriate to assess specifically the procedural issues raised (or which may arise) on the use of evidence obtained by the employer through technological monitoring in the course of proceedings against an employee. In this regard, it should highlight an important issue from a legal point of view: namely that most of the conflicts in this field between workers and employers (which give rise to multiple legal rulings having occurred in the matter) are produced as part of the challenge of a penalty (usually a dismissal) imposed by the company on an employee as a result of a breach of the work agreement detected and recognized through evidence obtained by means of computer technology (VÁZQUEZ, 2015).

In that context, the court is compelled to determine whether such evidence is lawful to prove such breach (and therefore to declare the employer's action applicable) or, conversely, adversely affects a fundamental right of the employee, in which case it is not valid *ex* Art. 90 of the Labour Procedure Law (ESCARTIN, 1993). Even more rarely do disputes arise (if at all of a collective nature) by which employees try to directly fight a means of corporate control through a special process on the protection of fundamental rights (Arts. 171 ff. LPL). In any case, this panorama leads to a reflection on several technical and legal elements that deserve to be weighed on the fair assessment of the issue.

3.1 The nature and value of the technological test

If, as has been mentioned, the main virtue of technological monitoring is to be used as proof of a breach by the employee, a major issue for the proceedings is to clarify the type of test involved in terms of its legal nature. Note that in some cases (and which is of slight significance) the court rules *ad hoc* on the validity of the introduction of a monitoring system using technological devices aimed at monitoring the overall development of the work performed, while in other cases it is forced to assess the monitoring (also technological, or by hand, perhaps by an expert inspector or supervisor, in which case it is worth the corresponding probative value) of specific use (or abuse) carried out in the owned computer tool made available to the employee who, as noted, leaves a trace or mark in the memory of the machine (FONS, 2015).

Unified jurisprudence has come to the conclusion that the videotape evidence (in an argument that would be extensible without too much trouble to other possible forms, which has been called "technical evidence") is not considered documentary evidence, but rather constitutes an autonomous test (STS 16/6/2011, Appeal n. 3983/2010; STS 26/11/2012, Appeal n. 786/2012). As the reader has surely deduced, this has significant legal consequences: on the one hand, with regard to the inability to substantiate requests for reversal (Art. 193 LRJS) or appeal (Art. 207 LRJS) in possible errors in its assessment with regard to the facts found (TORRES, 2014).

On the other hand, its evaluation is no longer assessed, but rather left to the discretion of the court under the rules of sound judgment (Art. 384.3 of the Civil Procedure Act, LECiv.). Subsequently, an issue of interest is how far the technological test, which is usually made from a systematization of data, can conclusively confirm an employee's behavior. A judgment has raised this issue, *obiter dicta*, to show "the difficulty of attribution of authorship to the complainant" (STS 26/9/2007, RJ 2007/7514; STS 8/3/2011, RJ 2011/932), as long as it is extremely easy to override the employee for this purpose.

Indeed, even in cases in which evidence obtained from a corporate search of the employee's computer is legal, in many cases there should be reasonable doubt about whether such evidence is

sufficient to establish the true authorship of the conduct detected through it, especially when the computer is found in a place with unrestricted access and use and has no access code.

This situation opens the door to a remarkable helplessness of being admitted as irrefutable proof of the charge since, on one hand, there is no sure awareness of who the person was who used the computer for the illicit activity (STSJ *Madrid* 17/10/2001, RJ 24276; STSJ *Cataluña* 11/6/2013, Appeal n. 2516) – it not being required that personal passwords be used – and, on the other, some alleged breaches, such as access to web pages or impermissible applications, may well have been automatically produced – a frequent circumstance in navigation on the Internet – from another used strictly for business purposes (STSJ *Galicia* 14/2/2013, Appeal n. 5195/2012).

Consequently, logic invites the judge to require from the company a broader activity, consisting not only of showing that there has been illicit activity, but that it was the employee himself/herself who personally led them to this evidentiary effect. When this does not come from the data obtained by the control means by itself, additional evidence will be necessary, that is, expert evidence from a computer expert attesting authorship of the materials presented; thus, in short, an affidavit will be required, even if only what the notary witnesses may be proven, rather than the absolute truth about who carried out a certain activity (TORRES, 2014).

3.2 The possibility of pre-establishing the technological test

It is perhaps a result of the conflicts that the use of this technological test was causing and the exacerbating casuistry that led to legal uncertainty, when in 2011, Act 36/2011 was adopted to regulate the labour law, the legislator wanting to contribute to new legal qualifiers and guarantees. On the one hand, it reiterates (albeit updated to the new legal doctrines applicable) the generic clause that allows for its use as evidence at trial of the means of reproduction of picture and sound, provided they had not been obtained by systems in violation of fundamental rights (Art. 90.2).

But also a new power (encouraged in its use by a recent ruling of the Supreme Court) (STS 13/5/2014, Appeal n. 1685/2013) with

the objective that the company seeking to prove wrongful conduct by the employee through the "access to documents or files, in any medium, which may affect personal privacy or other fundamental rights," turn to the judicial organ in advance for permission, by court order, "as long as no alternative means of testing exist and after balancing the interests affected by a judgment of proportionality and with minimal sacrifice, determining the conditions of access and guarantees for the conservation of and input into the process" (Art. 90.4 LRJS).

This allows the company to provide proof of its intention to rely on the process, with due guarantees and ensuring (if possible) its legality, which does not seem to exclude, however, ordinary and autonomous control that the employer can carry out extrajudicially (BONETE, RUIZ, 2012), and may even be a complement or reinforcement of it, because certainly if it intends to “regularize” future proof through court approval, it is because it will have prior knowledge (in perhaps spurious ways) of improper work activities committed by the employee (VÁZQUEZ, 2015).

Of course, in any case it is necessary that the court make some initial considerations prior to authorization, which is "a declared expression of the legislative will to assign a labour judge as ordinary guarantor of fundamental rights of the labour process" (CRESPO, MOLINA, ASTARBURUAGA, 2011). In any case, authorization of access to archives by the court *ex* Art. 90.4 LRJS does not appear to prevent the employee from alleging the illegality of the proof being harmful to certain fundamental rights by virtue of Art. 90.2 LRJS, but it will certainly be difficult for his/her claim to succeed, at least at present, by having prior consent from the judge (BONETE, RUIZ, 2012).

3.3 The legal consequences of the illegality of the test

When, in the course of a particular process, the employee has alleged that a particular test is adversely affecting any of his/her fundamental rights, and the judge, *ex* Art. 90.2 LRJS has accepted this statement, it remains an issue to be clarified, and the sense that such constitutionality of proof must be based on the corporate action (dismissal or sanction) adopted thereunder.

In this regard, the idea seems to have been accepted, perhaps in a somewhat uncritical form, that a decision to terminate business in such circumstances must be deemed null and void (STS 13/5/2014, Appeal n. 1685/2013). However, such a determination "does not appear to be entirely correct. Indeed, one thing is the wrongfulness of the test and another, the nullity of the dismissal or sanction.

In this regard, if the test has been obtained unlawfully, it should determine the admissibility of such, but this illegality should not necessarily translate into a qualification for dismissal (or corporate penalty) rending it null and void, but it should be valued regardless of the factual evidence provided by the annulment in question and declared appropriate, inappropriate, or invalid in light of the other evidence. Otherwise, according to Torres (2014, p. 385), "the incident referred to in Art. 90.2 LRJS is meaningless".

While this discussion has not yet been the subject of a serious reflection on the part of the courts, and certainly deserves a specific study, such as that which is invited to be undertaken in this essay, it is necessary to note how a reversal of judgment already exists that has sustained the thesis favorably and is now so succinctly defended (STSJ *Madrid* 21/3/2014, Appeal n. 1952/2014).

REFERENCES

ALBELLA, R. A. El uso del correo electrónico en el lugar de trabajo. *Datos Personales, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n. 11, 2004.

ALBERTOS, S. R. Facultades de control por medios informáticos. *Tribuna Social*, n. 162, 2004.

ALONSO, D. Protection of employees' privacy and personal information in Spain: general patterns and case law trends. In: AA.VV., *Protection of employees' personal information and privacy*. London: Walter Kluwerts, 2015.

ANTON, G.; WARD, J. J. Every breath you take: employee privacy rights in the workplace; an orwellian prophecy come true? *Labor Law Journal*, Vol. 49, n. 3, 1998.

AROCHENA, J. F. Derecho fundamental a la protección de datos

personales *vs* facultad empresarial de videovigilancia. In: DACRUZ, E. B. (Org.). *Controversias vivas del nuevo derecho del trabajo*. Madrid: La Ley, 2015.

BAAMONDE, M. E.; GRAU, A. B.; RODRIGUEZ, R. E. El Estatuto de los trabajadores. Diez años después: pervivencias, insuficiencias, desviaciones y reformas. *Relaciones Laborales*, n. 6-7, 1990.

BAETHGE, M.; OBERBECK, H. *Nuevas tecnologías y perspectivas profesionales de la gerencia empresarial*. Madrid: MTSS, 1995.

BONETE, A. D.; RUIZ, A. B. *Control informático, vigilancia y protección de datos personales de los trabajadores*. Valladolid: Lex Nova, 2012.

BROWN, C.; CAMPBELL, B. A. The impact of technological change on work and wages. *Industrial Relations*, Vol. 41, n. 1, 2002.

CAPRON, H. L.; JOHNSON, J. A. *Computers: tools for an information age*. Upper Sadle River: Prentice Hall, 2004.

CARRO, M. C. Desdramatizando el uso de internet en el trabajo. *Aranzadi Social*, n. 15, 2001.

CRESPO, J. A. Vídeovigilancia de los trabajadores: es preceptivo informales sobre su finalidad disciplinaria (Comentario de la STS 13-5-2014). *La Ley*, n. 8365, 2014.

CRESPO, J. A.; MOLINA, F. S.; ASTARBURUAGA, M.L. *Comentarios a la Ley Reguladora de la Jurisdicción Social*. Valladolid: Lex Nova, 2011.

DACRUZ, E. B. Derechos fundamentales y casuismo. *Actualidad Laboral*, n. 29, 2000.

DAL-RE, F. V. Poderes del empresario y derechos de la persona del trabajador. *Relaciones Laborales*, T. I, 1990.

DAWSON, P. M. *Computer technology and the redefinition of supervision*. Southampton: University of Southampton, 1986.

DE LA TORRE, M. R. *Poder de dirección y contrato de trabajo.* Valladolid: Grapheus, 1992.

DOMINGUEZ, J. J.; ESCANCIANO, S. R. U*tilización y control de datos laborales automatizados*. Madrid: APD, 1997.

DWORKIN, T. M. Protecting private employees from enchaced monitoring: legislative aproches. *American Bussiness Law Journal*, Vol. 28, 1990.

EDWARDS, R.: *The transformation of the workplace; debates on the labour process*. London: McMillan, 1993.

ESCARTIN, I. G. *La prueba en el proceso de trabajo*. Madrid: Civitas, 1993.

FIORITO, J.; BASS, W. The use of information technology by national unions: an exploratory analysis. *Industrial Relations Journal*, Vol. 41, n. 1, 2002.

FLAHERTHY, D. H. The emergence of surveillance societies in the Western World. *Government Information Quarterly*, Vol. 5, 1998.

FONS, D. M. *El poder de control del empresario en la relación laboral*. Madrid: CES, 2002.

FRANCO, T. S. El derecho a la intimidad y a la propia imagen y las nuevas tecnologías de control laboral. In: DACRUZ, E. B. (Org.). *Trabajo y libertades públicas*. Madrid: La Ley, 1999.

FRIED, C. Perfect freedom or perfect control? *Harvard Law Review*, Vol. 114, n. 2, 2000.

FULLER, S.; HARTMAN, A.; RAMAN, S. Bell meets Taylor: desmytifying knowledge work. In: ORLIKOWSKI, W. J. et al. (Org.). *Information technology and changes in organizational work*. London: Chapman & Hall, 1996.

GAETA, L. La dignidad del trabajador y las perturbaciones de la innovación. In: TOVAR, J. A.; GRAU, A. B. (Org.). *Autoridad y democracia en la empresa*. Madrid: Trotta, 1992.

GARRIDO, L. R. Los nuevos sistemas de comunicación electrónica y la representación colectiva de los trabajadores en la empresa. In: BARO, M. F. (Org.). *Derecho colectivo*. Madrid: CGPJ, 2003.

GREENE, A. M.; HOGAN, J.; GRIECO, M. Commentary e-collectivism and distributed discourse: new opportunities for trade union democracy. *Industrial Relations Journal*, Vol. 34, n. 4, 2003.

GUANTER, S. R. Nuevas perspectivas de la libertad de expresión e información en las relaciones laborales: contrato de trabajo y redes sociales. In: DACRUZ, E. B. (Org.). *Controversias vivas del nuevo derecho del trabajo*. Madrid: La Ley, 2015.

IGBARIA, M.; TAN, M. *The virtual workplace*. London: Idea Group, 1998.

LALLANA, M. C. Vulneración del derecho a la libertad sindical mediante uso desviado de datos informatizados sobre la afiliación del trabajador. Libertad sindical y derecho a la intimidad informática. *Aranzadi Social*, T. V, 1999.

LAMAS, J. R. Art. 20. Dirección y control de la actividad laboral. In:

PEREZ, J. L. (Org.). *Comentario al estatuto de los trabajadores*. Granada: Comares, 1998.

LLOYD, I. J. *Legal aspects of the information society*. London: Butterworths, 2000.

LOPEZ, F. J. et al. Los sistemas de control de la actividad laboral mediante las nuevas tecnologías de la información y las comunicaciones. *Relaciones Laborales*, n. 12, 2003.

LOPEZ, M. F. Libertad ideológica y prestación de servicios. *Relaciones Laborales*, n. 7, 1985.

LÓPEZ, R. T. El poder de control empresarial en la era tecnológica: visión panorámica de una cuestión inacabada. *Revista de Trabajo y Seguridad Social (CEF)*, n. 267, 2005.

_____. *El tratamiento por el empresario de los datos personales de los trabajadores*. Madrid: Civitas, 2006.

MCGRATH, J. E. *Loving big brother: performance, privacy and surveillance space*. London: Routledge, 2004.

MELGAR, A. M. *El poder de dirección del empresario*. Madrid: IES, 1965.

MOSTERIO, R. L. Despido por uso de correo electrónico e internet. *Actualidad Laboral*, n. 41, 2001.

MOYA, R. G. El derecho fundamental a la protección de datos y la vídeo-vigilancia empresarial *Revista de Derecho Social*, n. 62, 2013.

NAPIER, B. Computeritation and employment rights. *Industrial Law Journal*, Vol. 21, n. 1, 1992.

NAVARRO, A. V.; MAZZUCONI, C. M. *Nuevas tecnologías y relaciones laborales*. Pamplona: Aranzadi, 2002.

NEILA, E. C. Elementos para la construcción de una teoría general sobre el uso y control del correo electrónico corporativo. In: CARACUEL, M. R.; LEGARRETA, R. E. (Orgs). *Nuevas tecnologías de la información y de la comunicación y derecho del trabajo*. Albacete: Bomarzo, 2004.

NINET, J. I. Sobre el uso y abuso del teléfono, del fax, del ordenador y del correo electrónico de la empresa para fines particulares en lugar y tiempo de trabajo. Datos para una reflexión en torno a las nuevas tecnologías. *Tribuna Social*, n. 127, 2001.

O'BRIEN, C. N. The impact of employer e-mail policies on employee rights to engage in concerted activities protected by the National Labor Relations Act. *Labor Law Journal*, Vol. 53, n. 2, 2002.

OLIVER, H. E-mail and internet monitoring in the workplace: information privacy and contracting-out. *Industrial Law Journal*, Vol. 31, n. 4, 2002.

ORIHUEL, F. P. *Nuevas tecnologías y relación de trabajo*. Valencia: Tirant lo Blanch, 1990.

PACHES, F. V. *El derecho del trabajador al respeto de su intimidad*. Madrid: CES, 1998.

PARRA, M. L. *Los límites jurídicos de los poderes empresariales*. Barcelona: Bosch, 1999.

PÉREZ, J. L.; INSUA, M. M. El control empresarial del correo electrónico tras la STC 170/2013. *Aranzadi Social*, n. 11, 2014.

RAY, J. E. Geolocalisation, donness personnelles et droit du travail. *Droit Social*, n. 12, 2004.

RUBERT, M. B. *Informática y contrato de trabajo*. Valencia: Tirant lo Blanch, 1999.

_____. La utilización de las redes sociales en el ámbito de la empresa. *Revista de Derecho Social*, n. 52, 2010.

_____. Relaciones laborales y tecnologías de la información y de la comunicación. *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n. 9, 2004.

SEIN, J. L. *La videovigilancia empresarial y la protección de datos personales*. Madrid: Civitas, 2008.

_____. Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos y archivo de datos. *Justicia Laboral*, n. 17, 2004.

_____. *El respeto de la esfera privada del trabajador*. Madrid: Civitas, 1989.

SIMITIS, S. Developments in the protection of workers personal data. *Contitions of Work Digest*, Vol. 10, 1991.

_____. Reconsidering the premises of Labour Law: prolegomena to an EU regulation on the protection of employees' personal data. *European Law Journal*, Vol. 5, n. 1, 1999.

THORP, J. *The information paradox: realizing the business benefits of the information technology*. Toronto: McGraw-Hill Ryerson, 2003.

TORRES, L. E. Algunas cuestiones sobre la utilización de las redes sociales como medio de prueba en el proceso laboral. *Actualidad Laboral*, n. 3, 2014.

TOVAR, J. A. Los derechos fundamentales y el juicio de proporcionalidad

degradados a mera retórica (a propósito de la SCT 170/2013, de 17 de octubre. *Revista de Derecho Social*, n. 64, 2013.

UGUINA, J. R. Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica? *Relaciones Laborales*, n. 10, 2001.

VÁZQUEZ, Y. M. La vigilancia y control del trabajador a través de las nuevas tecnologías. Doctrina judicial reciente sobre su empleo como medio de prueba. In: DACRUZ, E. B. (Org.). *Controversias vivas del nuevo derecho del trabajo*. Madrid: La Ley, 2015.

VILLAZON, L. A. A vueltas con el control empresarial sobre la actividad laboral: test de honestidad, telemarketing, registro de terminales y uso -o abuso- de internet. *Tribuna Social*, n. 168, 2004.

WALKER, J. P. Algunos aspectos sobre la utilización de datos biométricos en el sector privado. *Datos Personales, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n. 12, 2004.

YANINI, M. M. Las facultades empresariales de vigilancia y control en las relaciones de trabajo. *TS*, n. 158, 2004.

ZEKOS, G. Cyberspace and globalization. *Law, Social Justice and Global Development Journal*, n. 1, 2002.