LABOR IMPACT OF TECHNOLOGICAL DEVICES CONCLUSIONS

Sergi Gálvez Duran
Labor lawyer, Cuatrecasas
PhD student, Universitat Ramón Llull, ESADE Law School

Andrés Camargo Rodríguez
PhD student, Universitat Pompeu Fabra

Abstract

The Comparative Labor Dossier (CLLD) in this issue 2/2018 of IUSLabor is dedicated to the impact of technological devices in the employment context. Aside from Spain, renowned academics and professionals from the following countries have participated in this publication: Belgium, France, Italy, Portugal, Poland, Slovenia, Argentina, Brazil, Colombia, Mexico, Dominican Republic and Uruguay. The following pages contain the 10 main conclusions reached in the comparative study. Nevertheless, it is highly recommended the detailed reading of the pertinent chapters to better understand the conclusions here indicated. Likewise, you will find attached to the conclusions a summary table with the answers of the different legal regimes to each one of the questions on labor impact of technological devices analyzed in this issue of IUSLabor.

El Comparative Labor Law Dossier (CLLD) de este número 2/2018 de IUSLabor está dedicado al impacto de los dispositivos tecnológicos en las relaciones laborales. Además de España, en esta publicación han participado académicos y profesionales de reconocido prestigio de los siguientes países: Bélgica, Francia, Italia, Portugal, Polonia, Eslovenia, Argentina, Brasil, Colombia, México, República Dominicana y Uruguay. En las siguientes páginas hemos incluido las 10 conclusiones principales que hemos alcanzado. No obstante, recomendamos encarecidamente una lectura detallada de los capítulos correspondientes para una mejor comprensión de los puntos aquí señalados. Asimismo, las conclusiones vienen acompañadas de un cuadro-resumen con las respuestas de los distintos ordenamientos jurídicos a cada una de las preguntas sobre el impacto laboral de los dispositivos tecnológicos analizadas en este número de IUSLabor.

Título: Impacto laboral del uso de dispositivos tecnológicos. Conclusiones.

IUSLabor 2/2018, ISSN 1699-2938, p. 140-172
DOI: 10.31009/IUSLabor.2018.i02.03

Keyworkds: technological devices, e-mail, surveillance systems, right to disconnect.
Palabras clave: dispositivos tecnológicos, correo electrónico, sistemas de videovigilancia, derecho a la desconexión.

Summary

1. «Top ten» conclusions

The Comparative Labor Dossier (CLLD) in this issue 2/2018 of IUSLabor is dedicated to the impact of technological devices in the employment context. Aside from Spain, renowned academics and professionals from the following countries have participated in this publication: Belgium, France, Italy, Portugal, Poland, Slovenia, Argentina, Brazil, Colombia, Mexico, Dominican Republic and Uruguay.

The CLLD emanates from the following questions answered by the international advisors of the journal*:*

1. Is there any regulation in your country regarding employees' use of technological devices in the company?
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?
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.)?
4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?
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?
6. In what cases is it possible to install geolocation systems (GPS) to control work activity?
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?
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?
9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?
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?

Following, and in the same order of the above questions, the reader will find the 10 main conclusions reached on the grounds of the answers given by the different academics and professionals on the impact of technological devices in the employment context.

1. None of the European legal regimes analyzed in the present comparative law study provide specific regulation on employee's use of the technological devices provided by the company to employees, with the exception of **Portugal**.

The different **European legal regimes** analyzed do not foresee specific regulations concerning the use of the technological devices in the company. In these countries, general regulations on employees' conduct (duties of good faith and care), as well as those related to employers' managerial powers, are relevant for the use of technological devices. Some countries, such as **Poland** and **Spain,** have regulations regarding telework or personal data protection, but there are no explicit regulations on the use by employees of technological devices in the company.

As indicated above, the only exception can be found in **Portugal**, where the Portuguese Labour Code dedicates some dispositions to employees' personal communications and information, namely those sent, received or consulted by means of electronic devices, as electronic mail systems. Among other issues, the Portuguese Labour Code explicitly recognizes that the employer is entitled to define the rules concerning the use of technological devices; at the same time, it establishes that employers are not allowed, in any case, to access the content of employees' personal communications.

Similarly, none of the analyzed legal systems in **Center and South America** establish legal rules regarding the use of electronic devises in the company. So, and given the legal vacuum on the matter, the majoritarian trend is to solve the related controversies by applying general norms (e.g. data protection), creating specific rules case by case (**Argentina**, **Brazil**, **Dominican Republic** and **Uruguay**), or through collective bargaining mechanisms. In the latter case, the **Uruguayan** case stands out, since collective agreements celebrated at the company level set provisions concerning the use of mobile phones, access to social networks, and the use of text messages systems in the work place and during working time.

2. As mentioned previously, **none of the European legal regimes analyzed includes a legal obligation to have a code of conduct or an internal policy** on the use of technological devices.

However, employers use codes of conduct or internal policies to regulate the matter of the use of technological devices in the company. In this point there are two patterns. **France**, **Italy**, **Spain** and **Portugal** allow the employer to limit or forbid the use of technological devices in the company in the rules of procedure, a memorandum or in an IT charter. For example, employers may establish that a professional email account shall not be used for personal purposes. On the contrary, in **Belgium** and **Slovenia** an employer cannot unilaterally determine work regulations regarding the use of technological devices, as work regulations shall be drawn up in consultation between the employer and his employees (as well as with the Work's Council, if it exists).

In the **Latin-American** countries analized, there are not specific provisions to adopt codes of conduct or internal policies regarding the use of technological devices. Hence, when the matter is regulated by rules applicable to the company level, these are usually set at employer's will.

3. Regarding the conditions to access and monitor employees' personal communications through the company's technological devices, **each legal system has its peculiarities**.

In **Belgium**, the employer must respect the principles of purpose, proportionality and transparency in order to install a monitoring system, with the peculiarity that the employer who wants to install such system must inform the Work's Council in advance. **Poland** legislation expressly allows the control of employee's e-mail, if the employer respects the secrecy of correspondence and other employees' personal rights. In **Italy** and **Spain**, there is no specific regulation on this matter; therefore, 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. On the other hand, **Portugal** expressly forbids employers to access the content of employees' personal communications. In **France**, case law allows searching employees' professional messages but prohibits any access to his/her personal files and messages that are specifically identified and marked as "personal".

In the **Latin-American** countries analyzed, corporate accounts or e-mails are considered working tools and, therefore, they can be monitored. These legal systems set a wide range of criteria such as the necessity, the suitability or the proportionality of the measure (**Colombia** and **Dominican Republic**), the random selection of cases (**Argentine**) or the worker's knowledge or consent (**Uruguay**). Regarding the matter, the **Colombian** constitutional tribunal has developed an interesting approach to distinguish different categories of information such as: public (to be known by anyone and so by the employer within the labor relation frame), semiprivate (run by competent

authorities and to be known by people under authorization), private (to be known exceptionally, given its confidential character) and classified (just to be known by his/her holder).

Finally, personal data transmitted through e-mail or text messages cannot be surveilled in the legal systems of **Brazil** and **Uruguay**.

4. The majority of the European countries analyzed allow the employer to install camera surveillance to control work activity.

From these premises, however, each legal system regulates their proceeding differently, being ones more protective than others. For example, States that seem to have a more protective regime for workers are **Portugal** and **Belgium**. **Portuguese** legislation only allows the employer to install camera surveillance for people and property safety purposes, prohibiting to install permanent video surveillance systems to control work activity. In **Belgium**, there is a distinction between **continuous and temporary camera surveillance**. In this sense, if the purpose of the surveillance is the control of the production process concerning workers or the control of the worker's work, the camera surveillance can only be temporary. In **France** and **Italy**, the regulation is also protective, as the installation of video surveillance systems by employers requires administrative authorization. Finally, in **Slovenia** and **Spain**, the employer must notify the employees in writing of the intended video surveillance beforehand; and, in the case of **Slovenia**, it is also necessary toconsult with workers' representatives about the necessity of introduction of such video surveillance.

In **Latin-America**, the matter is most of the times regulated by case-law. In **Brazil**, **Colombia** and **Mexico**, there exist restrictions to install camera surveillance in places where worker's privacy is at risk, such as toilets and dressing rooms. In some countries, however, such as **Dominican Republic** and **Uruguay,** these devices can be installed if workers are aware of it.

5. Unanimity is nearly achieved among European countries analyzed in **prohibiting the use of hidden cameras** to monitor employees. In **Belgium**, **France**, **Poland** and **Portugal**, the employer is obliged to inform employees on the existence and purposes of the surveillance systems used. Nevertheless, unanimity is broken by **Slovenia** and **Spain**. In **Slovenia**, case-law has considered as legitimate the use of hidden cameras if used not for the monitoring and control of work performance but for the investigation if there is founded suspicion of commitment of a criminal offense. Different, however, is the **Spanish** case, where Courts have admitted the use of hidden cameras when there are signs of a breach of contract.

Regarding the **Latin-American countries** analyzed in this comparative study, it is possible to identify two patterns: the prohibition to install hidden systems of surveillance (**Argentina**, **Dominican Republic** and **Uruguay**); and the absence of rules (**Colombia** and **Mexico**). In **Brazil,** the matter follows the same criteria applicable to visible systems of surveillance.

6. In **most of the European countries** analyzed, it is possible to **install a geolocation system to control work activity** if the employer fulfils the proceeding requierements. However, these requirements vary in the different legal systems analyzed. In **France**, a geolocation system can be installed to control work activity after individual information to employees, information and consultation of the Social and Economic Committee and after the declaration of the National Commission for Data Processing and Liberties. In **Slovenia** and **Spain**, the employer must specifically determine which data he or she needs and for what purpose; therefore, if he or she does not prove that it is necessary for the exercise of rights and obligations of the employment relationship, it is not possible to obtain GPS data from employees.

In any case, it is important to highlight that employee geolocation data should be treated as personal data under the legal regime of Regulation (EU) 2016/679. Therefore, in **all the European countries analyzed**, the GPS must be used in compliance with data protection regulations.

The **Latin-American systems** analyzed report, again, few regulations on the matter, standing out, however, the **Argentinian** and **Colombian** systems. In both cases, it is possible if the measure has as purpose the control over working time and the due performance of obligations stemming from the employment contract. In this context, it is interesting to point out that a procedural dimension of the problem has also been identified. In the **Dominican Republic** the admission of records taken from GPS systems as means to legally proof the fulfilment of labor obligations is discussed.

7. All European countries analyzed foresee **consequences for companies that fire an employee without fulfilling the proceeding requirements** to control electronic communications or install video surveillance systems. However, these consequences vary in the different legal systems analyzed.

In most countries, there are economic sanctions based on the illegality of the information itself. Yet nullity and reinstatement of workers are foreseen in the great majority of cases. While in Spain there is still a judicial discussion regarding this matter, in countries such as **France**, **Portugal**, **Italy,** and **Slovenia** the dismissal is

declared null when prove has been obtained in violation of the requirements analyzed in the previous questions. In **France**, the employer that disrespects the conditions of employees' control can even be criminally condemned; in particular, in case of violation of worker's right to privacy or secrecy of communications. The only exception is found in **Belgium**, where the employer will only have to pay the normal dismissal compensation in addition to damages.

In the majority of countries analyzed in **Center and South America**, the breach of the requirements regarding control communications by e-mail or installation of video surveillance systems triggers the qualification of the act as unfair and, therefore, the employer has the obligation to pay an economic compensation. The exception is the **brasilian system**, where, in the case of unjustified acces to the worker's corporate e-mail or phone records, there is the obligation to reinstate the worker along with the compensation for damages and pain and suffering. Only in **Uruguay** administrative consequences are reported, such as: the surveilance of the system by administrative authorities, warnings, fines, suspension or, at last stage, closure of the control system.

8. Regarding what personal data can be collected and processed in the framework of the employment relationship, it is important to highlight that **all European Union countries must respect the principles related to the treatment of data foreseen in Regulation (EU) 2016/679**. Therefore, in the labor context, data treatment will be legitimate when it is necessary for the performance of the employment contract or because it is necessary for compliance with a legal obligation to which the controller (the employer) is subject.

For this reason, **none of the European countries analyzed attribute relevance to employees' consent** as an autonomous ground to legally collect and process data. Therefore, consent will only be necessary when there is no other legal basis that legitimizes the collection or processing of data.

In general, the **Latin-American legal systems** analyzed establish the possibility of collective worker's basic data (personal identification, home address, marital status, inter alia). Some countries (**Colombia** and **Uruguay**) prohibit collecting sensitive information, which could lead to discriminatory treatments in recruitment processes. That is the case of data related to political opinion, religious preferences or specific matters concerning worker's heath condition. Other systems, such as the **Dominican**, require an expression of consent to gather workers' financial information or criminal records.

9. Beyond what personal data can be collected and processed in the framework of the employment relationship, **in most of the European legal regimes** analyzed it is **not necessary to inform workers' representatives about the collection and processing of personal data** of the company's employees.

The great majority of **European countries directly do not foresee the obligation to inform workers' representatives** about the collection and processing of worker's personal data. However, in some cases employees' representatives must be informed and consulted about the implementation of technologies that use worker's data for their proper functioning. Hence, in **France**, the Social and Economic Committee must be informed and consulted on the implementation of new technologies that modify health, security and work conditions. Simlarly, in **Spain**, employees' representatives must be informed on the devices controlling employees' activity before their implementation in the company. Likewise, in **Belgium**, the Work's Council should be consulted on the adoption of necessary measures if camera surveillance appears to have an impact on worker's privacy. The only exception is found in **Slovenia**, where the employer has to send drafts of codes of conduct by which he or she regulates the use of technological devices by employees to workers' representatives beforehand. In **Portugal**, only the collection and processing of biometric data must be informed to the National Committee for Data Protection.

In this point, the **Latin-American legal systems** analyzed do not include provisions that impose the employer's duty of providing information to worker's representatives.

10. Finally, the **great majority of European countries** analyzed do **not recognize a specific right of employees to disconnect** from technological devices outside of working time.

The only exception can be found in **France**. In this sense, French companies must regulate the modalities of the right to disconnect in the context of the annual collective negotiation on professional equality between women and men and quality of work life with worker's representatives. In the absence of a collective bargaining agreement, the employer has to unilaterally implement a charter on the right to disconnect after the Social and Economic Committee's opinion.

In **Italy**, recent labour reforms have introduced a sort of right to disconnect applicable to the so-called *smart workers* or *lavoratori agili*, which is a particular way of working characterized by flexibility regarding the place and time of work. **Belgium** has introduced some provisions that are merely supporting the start of a debate between the employer and worker's representatives regarding this issue, although they do not

contain any real rights or obligations. In other countries such as **Poland**, **Slovenia** or **Spain**, an employee is entitled to some periods of rest specified in the labour law and the employer is only bound by general rules regarding providing safety and health at work.

The right to disconnect form technological devise is not regulation in the **Center** nor **South American** countries analyzed, although judicial bodies have studied the right to overtime payment when workers are out of the employer's premises but still available. However, **Uruguay** has reported a draft legislation on the matter.

2. «Top ten» conclusiones

El Comparative Labor Law Dossier (CLLD) de este número 2/2018 de IUSLabor está dedicado al impacto de los dispositivos tecnológicos en las relaciones laborales. Además de España, en esta publicación han participado académicos y profesionales de reconocido prestigio de los siguientes países: Bélgica, Francia, Italia, Portugal, Polonia, Eslovenia, Argentina, Brasil, Colombia, México, República Dominicana y Uruguay.

Para realizar este análisis comparativo, el CLLD se ha basado en las respuestas que los colaboradores internacionales de la revista han dado a las siguientes preguntas:

1. ¿Existe una normativa en su país que regule el uso por los trabajadores de los dispositivos tecnológicos en la empresa?
2. ¿Es obligatorio que la empresa disponga de un código de conducta telemático o
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.)?
4. ¿En qué circunstancias es posible instalar sistemas de videovigilancia de carácter permanente para controlar la 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?
6. ¿En qué supuestos es posible la instalación de sistemas de geolocalización (GPS) para controlar la actividad laboral?
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?
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?
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?
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?

A continuación, el lector encontrará, siguiendo el orden de las preguntas anteriores, las 10 conclusiones principales alcanzadas en base a las respuestas de los diferentes académicos y profesionales en materia del impacto laboral de los dispositivos tecnológicos.

1. Ninguno de los ordenamientos jurídicos europeos analizados en el presente estudio de derecho comparado **regula el uso por los trabajadores de los dispositivos tecnológicos** en la empresa, con la excepción de **Portugal**.

Los diferentes ordenamientos jurídicos europeos analizados no contemplan una regulación específica del uso de los dispositivos tecnológicos por parte de los trabajadores. Por ello, en estos países, las facultades de dirección empresarial y la normativa genérica sobre la conducta de los empleados (en particular, el deber de buena fe) son relevantes a la hora de analizar el uso de los dispositivos tecnológicos por los trabajadores. Algunos países, como **Polonia** y **España,** regulan el teletrabajo o la protección de datos, pero no contienen referencias especificas al uso de los dispositivos tecnológicos por los trabajadores.

Como hemos avanzado, la única excepción se encuentra en **Portugal**, cuya normativa laboral dedica de forma específica determinadas disposiciones a regular el acceso y consulta de las comunicaciones personales de los trabajadores mediante dispositivos tecnológicos, como el correo electrónico. Entre otras cuestiones, la normativa portuguesa reconoce expresamente que el empresario está legitimado para definir las reglas de uso de los dispositivos tecnológicos en la empresa, pero que en ningún caso podrá acceder al contenido de las comunicaciones personales de los trabajadores.

Similarmente, en ninguno de los ordenamientos que se analizan en **Centro y Suramérica** existen normas generales relacionadas con el uso de dispositivos electrónicos en la empresa. Así, frente al vacío normativo, la tendencia mayoritaria consiste en resolver las controversias relacionadas mediante la aplicación de normas generales (por ejemplo, protección de datos), la creación de reglas a través de la jurisprudencia (**Argentina**, **Brasil**, **República Dominicana** y **Uruguay**) o a mediante mecanismos de negociación colectiva. En este último ámbito, destaca la existencia de convenios colectivos por actividad en **Uruguay**, en donde ya se regula el uso del teléfono móvil, junto con el acceso a redes sociales y sistemas de mensajería instantánea dentro de la jornada y sitio de trabajo.

2. Como hemos indicado anteriormente, **ninguno de los ordenamientos jurídicos europeos** analizados incluye la **obligación empresarial de disponer de un código de**

conducta o de una política interna sobre el uso de los dispositivos tecnológicos por parte de los trabajadores.

No obstante, los empresarios suelen aprobar códigos de conducta o políticas internas para regular la extensión y límites del uso de los dispositivos tecnológicos en la empresa. En este punto podemos diferenciar dos tendencias. **Francia**, **Italia**, **Eslovenia**, **España** y **Portugal** permiten al empresario limitar o prohibir el uso de los dispositivos tecnológicos en la empresa mediante reglas de conducta (por ejemplo, la empresa puede prohibir el uso del correo electrónico corporativo para fines personales). Por el contrario, en **Bélgica** y **Eslovenia**, el empresario no puede regular unilateralmente tales reglas de conducta, en la medida en que debe consultar previamente con los trabajadores y, en su caso, con sus representantes.

Tampoco en los casos analizados en **Latinoamérica** existen disposiciones que impongan la obligación de adoptar códigos de conducta o políticas internas respecto al uso de dispositivos tecnológicos. Así, aun cuando la cuestión se regula, en la mayoría de supuestos, mediante normas aplicables al nivel de la empresa, éstas se adoptan por voluntad del empleador.

3. En relación con las condiciones para acceder y monitorizar las comunicaciones personales de los trabajadores mediante el uso de dispositivos tecnológicos, hemos observado que **cada ordenamiento jurídico tiene sus propias peculiaridades.**

En **Bélgica**, el empresario debe respetar los principios de finalidad, proporcionalidad y transparencia a la hora de instalar un sistema de control de las comunicaciones personales de los trabajadores, con la peculiaridad de que el empresario que pretenda instalar un sistema de este tipo debe informar previamente a los representantes de los trabajadores. La legislación **polaca** admite expresamente el control del correo electrónico de los trabajadores, siempre y cuando el empresario respete el derecho al secreto de las comunicaciones y otros derechos personales de los trabajadores que pudieran verse afectados. En **Italia** y **España,** no existe una regulación específica al respecto; por lo tanto, el control de las comunicaciones electrónicas personales de los trabajadores debe respetar los principios sobre el tratamiento de datos personales previstos en el Reglamento General de Protección de Datos, que resulta aplicable directamente sin necesidad de transposición interna. Por otro lado, **Portugal** prohíbe expresamente al empresario acceder al contenido de las comunicaciones personales de los trabajadores. En **Francia**, la jurisprudencia ha permitido realizar búsquedas en los correos electrónicos corporativos, pero ha prohibido cualquier acceso a los ficheros personales y a los mensajes que el trabajador haya identificado expresamente como "personales".

Por su parte, en los países **latinoamericanos**, las cuentas o los mensajes de correo electrónico alojados en cuentas institucionales pueden ser monitoreados, a partir de su consideración mayoritaria como herramienta de trabajo. A tal efecto, dichos ordenamiento establecen una amplia variedad de criterios como la necesidad, idoneidad o proporcionalidad de la medida (**Colombia** y **República Dominicana**), la selección aleatoria de casos (**Argentina**), el conocimiento o el consentimiento del trabajador (**Uruguay**). En este punto se destaca la doctrina del Tribunal constitucional **colombiano**, que ha desarrollado una tipología en la que se distingue entre información *pública* (que puede ser conocida por cualquier persona y que, por ende, puede ser monitoreada en el contexto de la relación laboral), *semiprivada* (manejada por autoridades competentes y con la posibilidad de ser suministrada al público con la debida autorización), *privada* (conocida excepcionalmente al gozar de la reserva) y *reservada* (solamente conocida por su titular), lo cual determina la posibilidad de acceso.

En lo que respecta a información estrictamente personal transmitida a través de correo electrónico o sistemas de mensajería instantánea, no se puede monitorear en los sistemas legales de **Brasil** y **Uruguay**.

4. La mayoría de los países europeos permiten la instalación de cámaras de videovigilancia de carácter permanente para controlar la actividad laboral.

Partiendo de lo anterior, cada Estado regula el procedimiento de instalación de estos sistemas de videovigilancia de forma diferente, existiendo regulaciones más exigentes que otras. Por ejemplo, los estados que parece que tienen un régimen más protector para los trabajadores son **Portugal** y **Bélgica**. La legislación **portuguesa** únicamente autoriza la instalación de sistemas de videovigilancia cuando la finalidad es la seguridad y protección de las instalaciones y personal de la empresa, prohibiendo expresamente la instalación de tales sistemas para controlar la actividad laboral. En **Bélgica**, se **distingue específicamente entre sistemas de videovigilancia de carácter permanente o temporal**. Así, si la finalidad de la videovigilancia es el control de la actividad laboral, la cámara únicamente puede ser temporal. En **Francia e Italia** la regulación es también fuertemente protectora, por cuanto la instalación de cámaras de videovigilancia requiere autorización administrativa previa. Finalmente, en **Eslovenia** y en **España**, la empresa debe notificar a los trabajadores sobre la finalidad del sistema de videovigilancia; aunque **Eslovenia** presenta la particularidad de que también se exige consultar previamente con los representantes de los trabajadores sobre la necesidad de introducir dicho sistema de videovigilancia.

En **América Latina**, se trata de un asunto mayoritariamente regulado mediante reglas de carácter jurisprudencial. En **Brasil**, **Colombia** y **México** existen restricciones para la instalación de cámaras de seguridad en aquellos sitios en donde se pone en riesgo la intimidad del trabajador, tales como baños o vestidores. Por su parte, en la **República Dominicana** y **Uruguay** es posible la instalación de dichos dispositivos siempre que sea conocida para el trabajador.

5. En la **práctica totalidad de ordenamientos jurídicos europeos** analizados se **prohíbe el uso de sistemas de videovigilancia ocultos**. Así, en **Bélgica**, **Francia**, **Polonia** y **Portugal**, el empresario está obligado a informar a los trabajadores sobre la existencia y la finalidad de tales sistemas de control. La unanimidad la quiebran **Eslovenia** y **España**. En **Eslovenia** la jurisprudencia ha considerado como legitimo el uso de cámaras ocultas si estas no se utilizan para el control de la actividad laboral del trabajador, sino para investigar la posible comisión un ilícito penal. Diferente es el caso **español**, cuya jurisprudencia ha admitido el uso de cámaras ocultas cuando existan indicios de un incumplimiento laboral.

Respecto a los países de **Latinoamérica** analizados en el presente estudio de derecho comparado, es posible identificar dos tendencias: la prohibición de instalar sistemas ocultos en **Argentina**, **Republica Dominicana** y **Uruguay**; y la anomía en **Colombia** y **México**. Por su parte, en el ordenamiento jurídico **brasileño**, el asunto sigue los mismos criterios que regulan la instalación de sistemas de vigilancia visibles.

6. En **la mayoría de los países europeos** analizados, es posible **instalar un sistema de geolocalización para el control de la actividad laboral** cuando el empresario cumpla con los requisitos pertinentes. Ahora bien, estos requisitos son distintos en función del sistema legal analizado. En **Francia**, para proceder a la instalación de un sistema de geolocalización cuya finalidad sea el control de la actividad laboral es necesario informar previamente a los trabajadores afectados, informar y consultar al Comité Económico y Social, y obtener la declaración previa de la Comisión Nacional sobre Tratamiento de Datos y Libertades. En **Eslovenia** y **España**, el empresario debe determinar específicamente qué datos necesita y para que finalidad; por tanto, si no acredita que tales datos son necesarios para el ejercicio de derechos y obligaciones propios de la relación laboral, no puede obtener información sobre la geolocalización de sus trabajadores.

En cualquier caso, es relevante subrayar que los datos sobre la geolocalización de los empleados deben ser considerados como datos personales a la luz del Reglamento General de Protección de Datos. Por tanto, **en todos los países europeos analizados**, el

uso empresarial de sistemas GPS deberá respetar la normativa sobre protección de datos personales.

Los **ordenamientos latinoamericanos**, una vez más, reportan escazas regulaciones en la materia, siendo destacables las excepciones de **Argentina** y **Colombia**. En ambos casos, la finalidad de la medida consiste en ejercer control sobre el tiempo de trabajo y la debida ejecución de las obligaciones derivadas del contrato. En este ámbito, debe identificarse también una dimensión procesal del problema. Así, en la **República Dominicana** se discute la admisibilidad de los reportes obtenidos de dichos sistemas como medio de prueba para acreditar válidamente el cumplimiento de los deberes del trabajador.

7. Todos los países europeos analizados prevén **consecuencias** para las empresas que procedan a un **despido sin cumplir con los requisitos** establecidos para el control de las comunicaciones electrónicas o la instalación de cámaras de videovigilancia. No obstante, estas consecuencias varían en los diferentes sistemas legales analizados.

Mayoritariamente, se contemplan sanciones económicas basadas en la ausencia de información a los trabajadores sobre tales medidas. Igualmente, se prevé la nulidad del despido y la obligación de reintegrar al trabajador en la empresa en muchos casos. Así, mientras que en **España** existe una discusión jurisprudencial sobre este aspecto, en países como **Francia, Portugal, Italia** y **Eslovenia** se declara la nulidad del despido por obtención de la prueba en vulneración de los requisitos correspondientes. En **Francia**, el empresario que incumple las condiciones para el control de la actividad laboral puede incluso ser condenado penalmente por ello, en particular, si se acredita la vulneración del derecho a la privacidad y al secreto de las comunicaciones. La única excepción se encuentra en el ordenamiento **belga**, donde el empresario solo tendrá que abonar la indemnización por despido y los daños y perjuicios que la medida haya podido originar.

En la mayoría de países de **Centro y Suramérica** analizados, el despido efectuado al margen de las obligaciones en materia control de comunicaciones o sistemas de vigilancia genera la calificación del acto como injusto, y en consecuencia, la obligación de resarcir sus efectos mediante el pago de la respectiva indemnización laboral. En ese contexto, desataca el **ordenamiento brasileño** que se separa de la tendencia y en el que, ante el supuesto de acceso injustificado del empleador a la cuenta de correo corporativa del trabajador o a sus conversaciones telefónicas, se genera el derecho a la reincorporación, junto con el pago de los daños morales y materiales. Solo en **Uruguay** se reportan consecuencias en ámbito administrativo, que incluyen: el sometimiento del respectivo sistema a observación por parte de una entidad administrativa (*Unidad Reguladora y de Control de datos personales*), el "*apercibimiento*", la imposición de

sanciones económicas, la suspensión o, en última instancia, la clausura del respectivo sistema de control.

8. En relación con qué datos personales pueden ser obtenidos y tratados en ámbito de la relación laboral, es importante subrayar que **todos los países de la Unión Europea deben respetar los principios relacionados con el tratamiento de datos previstos en el nuevo Reglamento General de Protección de Datos.** Por tanto, en el ámbito laboral, el tratamiento de datos será legitimo cuando éste sea necesario para la ejecución del contrato de trabajo o porque sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (el empresario).

Precisamente por este motivo, **ninguno de los países europeos** analizados le otorga una especial relevancia al consentimiento de los trabajadores como base jurídica autónoma para la obtención y el tratamiento de datos personales. De este modo, el consentimiento únicamente será necesario cuando no exista otra base jurídica que pueda legitimar la recogida de datos personales.

En términos generales, los **ordenamientos latinoamericanos** estudiados contemplan la posibilidad de los empleadores de recaudar información básica de los trabajadores (identificación personal, lugar de residencia, estado civil, entre otros). Algunos de los países analizados (**Colombia** y **Uruguay**) proscriben el recaudo de información que se considera sensible y que puede dar lugar a un trato discriminatorio en el proceso de reclutamiento. Es el caso de la información relativa a opinión político, preferencias religiosas, o determinadas cuestiones referidas al estado de salud del trabajador. Por su parte, ordenamientos como el de **República Dominicana** exigen una manifestación del consentimiento para el recaudo de información financiera o de antecedentes criminales.

9. Más allá de determinar qué datos personales pueden ser obtenidos y tratados en la relación laboral, en la **mayoría de los regímenes europeos** analizados **no resulta necesario informar a los representantes de los trabajadores** sobre la recogida y el tratamiento de datos personales de los empleados.

La gran mayoría de los países europeos no prevé específicamente la obligación de informar a los representantes sobre la recogida y el tratamiento de datos personales. No obstante, en algunos casos, los representantes de los trabajadores deben ser informados y consultados en relación con la implementación de tecnologías que utilizan datos de los empleados para su correcto funcionamiento. Así, en **Francia**, es necesario informar al Comité Económico y Social sobre la introducción de nuevas tecnologías que puedan modificar la salud, la seguridad y las condiciones laborales. De la misma forma, en

España es necesario informar a los representantes de los trabajadores acerca de la adopción de nuevos sistemas de control del trabajo (por ejemplo, sistemas de videovigilancia). Igualmente, en **Bélgica**, los representantes de los trabajadores deben ser consultados en caso de que las cámaras de videovigilancia puedan tener un impacto en el derecho a la privacidad de los trabajadores. La única excepción se encuentra en **Eslovenia**, donde el empresario tiene que remitir previamente a los trabajadores y, en caso, a los representantes de los trabajadores, los códigos de conducta en los que regula el uso de los dispositivos tecnológicos. En **Portugal**, únicamente es necesario informar al Comité Nacional sobre Protección de Datos acerca de la recogida y tratamiento de datos biométricos.

En este punto, en los países analizados en **Latinoamérica** no se reportan disposiciones que impongan al empleador la obligación de suministrar información a los representantes de los trabajadores.

10. Finalmente, **la mayoría de los países europeos** analizados **no reconoce un derecho especifico a la desconexión digital** de los trabajadores fuera de su jornada laboral.

La única excepción se encuentra en **Francia**. En este sentido, las empresas francesas deben regular las modalidades de ejercicio del derecho a la desconexión en el ámbito de la negociación colectiva anual sobre la igualdad profesional entre mujeres y hombres y la calidad de vida en el trabajo, junto con los sindicatos. En defecto de un acuerdo en sede de negociación colectiva, el empresario debe implementar unilateralmente una carta sobre el derecho a la desconexión, tras la preceptiva opinión del Comité Económico y Social.

En **Italia**, las recientes reformas laborales han introducido una suerte de derecho a la desconexión aplicable a los denominados *smart workers* o *lavoratori agili*, que constituye una forma particular de trabajo caracterizada por la flexibilidad entre el lugar de trabajo y el tiempo de trabajo. Por su parte, **Bélgica** ha introducido algunas previsiones dirigidas a introducir el debate del derecho a la desconexión en las negociaciones entre la empresa y los representantes de los trabajadores, pero sin reconocer expresamente ningún derecho u obligación al respecto. En otros países, como **Polonia**, **Eslovenia** o **España**, el trabajador tiene derecho a determinados periodos de descanso reconocidos en la normativa laboral y el empresario está obligado a respetar las reglas generales sobre seguridad y salud en el trabajo, si bien no existe un derecho específico a la desconexión.

El fenómeno planteado carece absolutamente de regulación en **Centro y Suramérica**, aunque los respectivos órganos jurisdiccionales han desarrollado la materia al estudiar el derecho al pago de remuneración en aquellos periodos en los que, pese a estar ausente del sitio de trabajo, el trabajador está obligado a estar a disposición del empleador mediante el uso de dispositivos tecnológicos. En todo caso, se destaca el avance de un proyecto de Ley que se ocupa de la materia en **Uruguay**.

3. Summary table

3.1. Europe

	Belgium	France	Italy	Poland	Portugal	Slovenia	Spain
1. Is there any regulation in your country regarding employees' use of technological devices in the company?	No.	No.	No.	No.	Yes.	No.	No.
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	No. Peculiarities: Work regulations shall be drawn up in consultation between the employer and his employees.	No. Peculiarities: Employer can unilaterally limit or forbid the use of the technological devices in the rules of procedure or in a IT charter	No. Peculiarities: Employer can unilaterally limit or forbid the use of the technological devices in the rules of procedure or in a IT charter	No. Peculiarities: The procedure of monitoring must be set in a collective labour agreement, in the workplace regulations or in the notice	No. Peculiarities: Employer can unilaterally limit or forbid the use of the technological devices in the rules of procedure or in a IT charter	No. Peculiarities: Work regulations shall be drawn up in consultation between the employer and his employees.	No. Peculiarities: Employer can unilaterally limit or forbid the use of the technological devices in the rules of procedure or in a IT charter

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.)?	The employer must respect the principles of purpose, proportionality and transparency in order to install a monitoring system. He must inform the works council in advance.	The employer can searching an employee's professional messages, except personal messages marked as "personal".	No specific regulation. Monitoring employees' personal communications must respect the principles of data foreseen in Regulation (EU) 2016/679.	The employer must respect the secrecy of correspondence and other personal rights of an employee.	Labor regulation expressly forbids employers to access the content of employees' personal communications.	Monitor employees' personal communications only is possible if it such possibility is provided in an employer's code of conduct.	No specific regulation. Monitoring employees' personal communications must respect the principles of data foreseen in Regulation (EU) 2016/679.
4. Under what circumstances is it possible to install permanent video	(i) the employer has to inform the works council and provide	The installation requires administrative authorization.	The installation requires administrative authorization.	Objectives, scope and method of the surveillance must be set in a	The employer cannot install permanent video surveillance to control work	The employer must notify the employees in writing and consult with the	(i) The employer must notify the employees in writing and consult with the

surveillance systems to control work activity?	information in work regulations (ii) if the purpose of the surveillance is control worker's activity, the camera can only be temporary.			collective labour agreement, in the workplace regulations or in the notice	activity.	representative trade unions.	representative trade unions. (ii) If the purpose of the surveillance is control worker's activity, the camera can only be temporary.
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 employer cannot install hidden cameras to control work activity; they must inform the employees on the existence and purposes of the surveillance systems used.	The employer cannot install hidden cameras to control work activity; they must inform the employees on the existence and purposes of the surveillance systems used.	Cameras can only be installed after an agreement with workers' representatives or the authorization by the Labour Inspectorate.	The employer cannot install hidden cameras to control work activity; they must inform the employees on the existence and purposes of the surveillance systems used.	The employer cannot install hidden cameras to control work activity; they must inform the employees on the existence and purposes of the surveillance systems used.	The employer can only install hidden cameras if there is a founded suspicion of commitment of a criminal offense.	The employer can only install hidden cameras when there are signs of a breach of the employment contract.

6. In what cases is it possible to install geolocation systems (GPS) to control work activity?	Install a GPS system requires: comply with data protection regulations.	Install a GPS system requires: (i) the individual information of the employees; (ii) the information and consultation of the Social and Economic Committee and; (iii) the declaration to the National Commission for Data Processing and Liberties.	(i) Normally used to protect an employer's good, for safety reasons, or to a better management of the work performance. (ii) where the GPS are used as working tools or as systems for registering presence at work, they can be used without the need of any agreement or authorization, but in compliance with data protection regulations.	Only if it is necessary to ensure the safety of employees or to protect property or to control production.	The principles regarding privacy protection, mainly the principle of proportionality, have to be accomplished.	The employer must specify the use of GPS devices in its codes of conducts.	(i) Only if it is necessary to ensure the safety of employees or to protect property or to control production. (ii) The employer must inform the employee about which GPS data he needs and for what purpose.
7. In the event that the company fires an employee in breach of the conditions regarding	The employer will only have to pay the normal dismissal compensation plus certain	Nullity and reinstatement of workers	Nullity and reinstatement of workers	Depending on the circumstances, labor general provisions may apply to this matter.	Nullity and reinstatement of workers	Nullity and reinstatement of workers	Case-law discussion. .

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?	damages.						
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 necessary for the (i) performance of an employment contract; or (ii) the necessary for compliance with the legal obligation to which the employer is subject. Consent: only necessary when there is no other legal basis that	The necessary for the (i) performance of an employment contract; or (ii) the necessary for compliance with the legal obligation to which the employer is subject. Consent: only necessary when there is no other legal	(The necessary for the (i) performance of an employment contract; or (ii) the necessary for compliance with the legal obligation to which the employer is subject. Consent: only necessary when there is no other legal basis that	The necessary for the (i) performance of an employment contract; or (ii) the necessary for compliance with the legal obligation to which the employer is subject. Consent: only necessary when there is no other legal	The necessary for the (i) performance of an employment contract; or (ii) the necessary for compliance with the legal obligation to which the employer is subject. Consent: only necessary when there is no other legal basis that	The necessary for the (i) performance of an employment contract; or (ii) the necessary for compliance with the legal obligation to which the employer is subject. Consent: only necessary when there is no other legal basis that	The necessary for the (i) performance of an employment contract; or (ii) the necessary for compliance with the legal obligation to which the employer is subject. Consent: only necessary when there is no other legal basis that

	legitimizes the collection or processing of data.	basis that legitimizes the collection or processing of data.	legitimizes the collection or processing of data.	basis that legitimizes the collection or processing of data.	legitimizes the collection or processing of data.	legitimizes the collection or processing of data.	legitimizes the collection or processing of data.
9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?	There is no a specific obligation. Peculiarities: Works council should be consulted if camera surveillance have an impact on the privacy of employees.	There is no a specific obligation. Peculiarities: Social and Economic Committee must be informed and consulted on the implementation of new technologies which modifies the health, security and work conditions.	There is no a specific obligation. Peculiarities: obligation to negotiate an agreement for the installation of technological equipments and tools when they entail the possibility for an indirect control of the workers' activities.	There is no a specific obligation.	There is no a specific obligation. Peculiarities: collection and processing of biometric data must be informed to the National Committee for Data Protection.	There is no a specific obligation. Peculiarities: The employer has to send the drafts of codes of conduct by which he regulates the use of technological devices.	There is no a specific obligation. Peculiarities: the employees' representatives must be informed on the devices controlling the employees' activity before their implementation in the company.
10. Is there a right to disconnect from technological devices outside working time?	No.	Yes. The Company must settle the modalities of the right to disconnect in	No.	No.	No.	No.	No.

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 annual collective negotiation on professional equality between women and men and quality of work life with the union representatives. Absence collective agreement: employer to unilaterally implement charter on the right to disconnect after the Social and Economic Committee's opinion.					

3.2. Latin-America

	Argentina	Brasil	Colombia	México	Dominican Republic	Uruguay
1. Is there any regulation in your country regarding employees' use of technological devices in the company?	No. General rules of labor law used by jurisprudence.	No. Rules regarding supervision of e-mails and control by audiovisual means set by jurisprudence.	No. Application of general rules of right to privacy, and electronic documents.	No. General rules of labor law applied in matters such as: i) working time, ii) homework and telework, iii) training.	No. Rules regarding supervision of e-mails set by jurisprudence.	No. Rules set by jurisprudence and legal studies Collective bargained rules regarding the use of mobile phones.
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?	No.	No. No uniform rules on employers' duty of informing workers of supervision.	No. Application of general rules concerning worker's privacy	No. Codes of conduct, internal regulations or collectives agreements are voluntarily made	No. Internal regulations or policies.	No. Internal regulations or policies.
3. In which cases and under what conditions is it	Rules set by jurisprudence and legal studies.	Rules set by jurisprudence	Rules set by jurisprudence:	"*Reasonable expectation of privacy*"	Rules set by jurisprudence:	Rules set by jurisprudence and legal studies. (No

possible to access and monitor employees' personal communications through the company's technological devices (e-mail, instant messaging, etc.)?	Corporate e-mail may be monitored by the employer under the following rules: i) Keep worker's dignity and discretion ii) Random selection of cases iii) Workers consent is delivered iv) No internal regulation or code of conduct creates an expectation of worker`s privacy v) Delivery access code workers: expectations of privacy.	Corporate e-mail may be monitored by the employer on grounds of: i) liability for employee's acts; ii) corporate e-mail is a working tool. Personal email and message services cannot be supervised.	Criteria: i) necessity and constitutionality; ii) suitability and iii) proportionality. Access depends on the kind of information (public, semi-private, private and reserved).	(worker's information is presumed to be treated according to law).	Criteria: i) necessity (specific, explicit, and legitimate purpose); ii) proportionality; iii) minimum repercussion on the worker privacy.	agreement) E-mail: worker knowledge of the supervision. Chat has been considered private (no supervision). Phone calls (Call centres). Workers are to be informed that records could be used by the employer to carry out audit.
4. Under what circumstances is it possible to install permanent video surveillance systems to control work activity?	- Consent for collecting digital images is required (It may be replaced by a public ad under specific circumstances) - Data protection manual, and registration in a national database is to be kept. - Expression of reasons	Rules set by jurisprudence. Cameras cannot be installed in spots where workers privacy is at risk (toilets, locker rooms). Records of several workers are allowed.	Rules set by jurisprudence Cameras cannot be installed in spots where workers privacy is at risk.	N/A "*Reasonable expectation of privacy*"	Rules set by jurisprudence. Cameras cannot be installed in spots where workers privacy is at risk (toilets, locker rooms). Workers are to be informed about cameras	General rules regarding audio and video records. Signs regarding the installation of systems are to be visible. No worker's consent is required.

	on which the measure is grounded.				installation. Cameras are to be visible.	
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?	No possible without judicial order.	No distinction between visible and hidden system is made.	No regulation.	No regulation.	Not allowed.	Not allowed. Control by means of hidden cameras can be legitimate as a matter of interpretation.
6. In what cases is it possible to install geolocation systems (GPS) to control work activity?	When necessary and reasonable. It is to be used to control working time and requires worker's consent.	No regulation. Discussions about the matter concern the payment of extra-time.	- Respecting worker's privacy (sensitive information). - To exert control over the working time and the performance of duties.	No labor regulation.	No regulation. Jurisprudence has admitted reports based on GPS services as proof in trial.	No regulation.
7. In the event that the company fires an employee in breach	Administrative sanctions: fine.	Access to corporate e-mail and recording of	Unfair dismissal. No administrative	No related legal cause.	Unfair dismissal. No administrative	Unfair dismissal. Procedural

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?	Labor law: Unfair dismissal, compensation; reincorporation; civil law: economic compensation; criminal prosecution under restrictive criteria.	phone calls to refuse an illegal conduct of the employee is allowed. If the illegal conduct is not proven in trial, the employer is obliged to reincorporate the workers and damages and pain and suffering.	sanctions are reported.		sanctions are reported. Labor and civil consequences.	effects in trial (no admission of means of proof). Administrative sanctions: surveillance, warning, economic sanction, suspension and closure (of the system).
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?	Data can be collected as far as the employer: i) be registered in the national database, ii) assure quality of data collected, iii) allow access to data subjects.	N/A	Restrictions in the collection of sensitive data during recruitment to avoid discrimination.	Personal data (name, nationality, age, sex, marital status). Social security (family and health data).	Companies cannot access worker's personal data. Written expression of consent is required to check criminal or financial records.	General frame of data protection (name, DNI, nationality, home address and data of birth). Consent is necessary to collect further information. Prohibition to collect sensitive data (ethinc origin, political preferences, religious and

						moral believes, trade union status and health and sexual related data). Information about pregnancy status cannot be required.
9. What information in the field of data protection must the company provide to workers' representatives? How and with what periodicity?	No regulation.	N/A	No regulation.	No regulation.	No regulation.	No obligation.
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?	No. Working time is that in which a worker is available to the employer (no matter performances of tasks).	No. The employer duty of respecting working time and affording proper health and work conditions could be understood as a matter of interpretation. Disconnection	No. Payment for overtime when worker is not at employer premises but still available.	No. Commonly adopted by codes of conduct.	No. Right to take rest.	No. Controversy regarding the payment for overtime when worker is not at employer premises but still available. Draft legislation under discussion.

		right afforded by jurisprudence Payment for "*sobreaviso*" (time in which the worker is not at employer premises but still available).				
11. Other relevant aspects regarding the labor influence of the technological devices in the workplace			Companies using electronic platforms must contribute to social security.			