

## CHANGES TO EMPLOYMENT LEGISLATION AS A RESULT OF THE LOPDP

The much-awaited Organic Act 3/2018, of 5 December, on the Protection of Personal Data and the guarantee of digital rights ("LOPD"), which entered into force on 6 December, has brought with it some significant changes to employment legislation in Spain, in addition to the important regulation on data protection matters.

We briefly set out here some urgent comments on the most relevant aspects of this Organic Act, which have an impact on employment legislation.

### 1. NEW ARTICLE 20.BIS OF THE WORKERS' STATUTE ("WS"): EMPLOYEES' RIGHTS TO PRIVACY IN THE DIGITAL ENVIRONMENT AND THEIR RIGHT TO DISCONNECT

The first and foremost change is the introduction of a new Article 20.bis in the Workers' Statute which aims to establish, in a generic way and as a counterpoint to the employer's faculty to management its business set forth in Art.20 WS, new rights granted to employees in this area: (i) employees' right to privacy deriving from the use of digital devices provided by the company and from the establishment of video surveillance, sound recording and geolocation systems, and (ii) the so-called "right to disconnect".

Thus, the new article states that *"Employees have a right to privacy while using the digital devices made available to them by their employer, the right to disconnect and the right to privacy from the use of video surveillance and geolocation devices in the terms established in the legislation in force on the protection of personal data and the guarantee of digital rights"*.

This is an article that announces a series of rights but does not regulate their contents; for that purpose it refers to the contents of the LOPDP itself.

Note that *"respect for their privacy and due consideration for their dignity"* was already generically set out as a right granted to employees in Art. 4.2.e) WS, although without specifically referring to the scope of the various electronic devices used when exercising the faculties of managing and supervising a business, for which extensive and varied case law does indeed exist which governs and guides the existence, exercise and extents of those rights and faculties.

On the contrary, the right to "disconnect" digitally is a new addition to Spanish law, having no precedent other than specific provisions included in some companies' collective bargaining agreements.

#### Key Aspects

- Employers must put in place a "digital disconnection policy", on which they must first consult with employee representatives
- Employers must develop criteria for the use of digital devices
- Employers must inform both the employee representatives and the employees themselves of existing video surveillance, sound recording and/or geolocation systems at the workplace

## 2. RIGHT TO DISCONNECT

The right to disconnect set out in Article 20.bis of the Workers' Statute is governed in Article 88 of the LOPDP. Such article establishes that *"Employees ... will have the right to disconnect digitally, so as to ensure respect, outside of their working hours agreed or established by law, for their free time, vacation and leave, and respect for their personal privacy and that of their family"*.

To specifically regulate this right and the ways in which it can be exercised, Article 88 of the LOPDP refers to the provisions of the company's collective bargaining agreement or, failing that, to the agreements reached between the employer and the employee representatives. This must in any event be consistent with the intended aim of the new article, which makes two basic assumptions in order for the right to be duly exercised: that the nature and object of the labour relationship be observed, and that the employee's right to reconcile his or her work and family life be encouraged.

Without clearly stating how this fits into the aforementioned collective bargaining agreements, section three of Article 88 adds that the employer *"must develop an internal policy"*, defining *"the ways of exercising the right to disconnect and the employee training and awareness actions regarding the reasonable use of technological tools to help prevent the risk of information overload"*. Developing such a policy first requires, however, *"meeting with the employee representatives"*.

As an initial approach, one could interpret that the employer is required to consult with the employee representatives in an attempt to reach an agreement. However, if no agreement is reached, the company would be obliged to develop a policy defining how this right can be exercised, which must in any event uphold any undertakings contained in the collective bargaining agreement in this regard, as the case may be.

The LOPDP states somewhat vaguely that the parties affected by this new law would be the *"employees, including those holding management positions"*. This could be understood to mean that not only those employees with an ordinary labour relationship have this right, but also senior executives who have a special type of labour relationship.

## 3. RIGHT TO PRIVACY

The possible subjection to, and due respect of, the right to privacy in the context of the use of digital devices, video surveillance equipment and geolocation systems is governed in Articles 87, 89 and 90 of the LOPDP.

- **Use of digital devices and right to privacy:**

Article 87 of the LOPDP establishes the employee's right to the protection of his or her privacy in the context of the use of digital devices made available by the employer. In particular, it states that the company is entitled to access the content deriving from the use of such digital means, only for the purpose of monitoring the employee's compliance with his or her labour obligations and to ensure the integrity of such devices.

To implement this right, Article 87 requires the employer to develop *"criteria for the utilisation of the devices"*, which must take into account the *"minimum standards"* for the protection of privacy in accordance with social uses of the devices. Although the employee representatives are to *"participate"* in developing these criteria for use, Article 87 does not specify what the extent of such *"participation"* is to be, as general Spanish labour legislation makes a distinction between the employee representatives' right to information and their right to be consulted. If one interprets that such *"participation"* required in developing these criteria for use will normally involve a certain degree of consultation, that would entail negotiating with such representatives in an attempt to reach an agreement. But if no agreement is reached, this is also open to the interpretation that the company is to develop these criteria for use unilaterally.

If the employer has permitted its digital devices to be used *"for private purposes"*, then in order to be able to access the content of such devices, the criteria for use must include a specific list of the uses authorised, and have guarantees in place to preserve the employees' privacy.

Lastly, Article 87 of the LOPDP adds that employees must be informed of the criteria for use mentioned.

A clear connection can be made between this article of the new law and the requirement already existing in Spanish case law opinions whereby, in order to eliminate or lower the "*expectation of privacy*" in the use of these devices and establish means for monitoring them, companies must put in place specific policies regarding the use of these devices and the means the company can use to monitor them.

- **Video surveillance and sound recording at the workplace**

Article 89 of the LOPDP clearly establishes that companies may process the images obtained through the use of cameras in order to monitor employees' compliance with their duties. However, in order to be able to do so, employee representatives and the employees themselves must first be informed of this, in an express, clear and concise manner, although it is understood that it will suffice for this purpose to display the devices visibly in the places where the cameras are located. This is notwithstanding the right to information and the right to be consulted established, in general, in Art. 64 WS.

In line with existing judicial precedents in this regard, the installation of cameras in employees' relaxation and leisure facilities (changing rooms, lunchrooms, etc.) is expressly prohibited.

Lastly, this article more restrictively regulates the use of sound recording systems, which will only be permitted "*when significant risks exist to the security of the premises, goods and persons as a result of the activities carried out at the workplace*", while always upholding the principles of proportionality and of minimum intervention and the guarantees applicable to video surveillance.

- **Geolocation systems**

Article 90, in turn, governs the use of geolocation systems, permitting their use and the processing of the corresponding data in order to monitor employees' compliance with their duties. Again, as established in the case of video surveillance, employee representatives and the employees themselves must first be informed of this, in an express, clear and unequivocal manner.

## **4. WHISTLEBLOWING**

Article 24 of the LOPDP governs the creation, maintenance and management of internal reporting channels, and furthermore enables such reporting to be done anonymously. Employees must be informed of the existence of these channels and may use them to report to the company any "*acts or conduct not complying with the general or sectorial regulations applicable to them*".

## **5. SUMMARY**

Although these provisions may later be developed through their implementing regulations and/or agreements and through case law and legal opinion on the subject, which will undoubtedly clarify the many current *lacunae*, some initial conclusions can be reached:

- Employers must put in place a "*digital disconnection policy*", on which they must first consult with employee representatives, in addition to the law referring in this regard to collective bargaining agreements or, failing that, to agreements reached between the company and the employee representatives;
- Employers must develop criteria for the use of digital devices, and employee representatives are to "*participate*" in developing these criteria;
- Employers must inform both the employee representatives and the employees themselves of existing video surveillance, sound recording and/or geolocation systems at the workplace.

## CONTACTS

**Juan Calvente**  
Counsel

**T** +34 91 590 7546  
**E** [juan.calvente@cliffordchance.com](mailto:juan.calvente@cliffordchance.com)

**Jorge Martín-Fernández**  
Senior Associate

**T** +34 91 590 4101  
**E** [jorge.martin-fernandez@cliffordchance.com](mailto:jorge.martin-fernandez@cliffordchance.com)

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

Clifford Chance, 10 Upper Bank Street,  
London, E14 5JJ

© Clifford Chance 2018

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street,  
London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to [nomorecontact@cliffordchance.com](mailto:nomorecontact@cliffordchance.com) or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Bangkok •  
Barcelona • Beijing • Brussels • Bucharest •  
Casablanca • Doha • Dubai • Düsseldorf •  
Frankfurt • Hong Kong • Istanbul • Jakarta\* •  
London • Luxembourg • Madrid • Milan •  
Moscow • Munich • New York • Paris • Perth •  
Prague • Rome • São Paulo • Seoul •  
Shanghai • Singapore • Sydney • Tokyo •  
Warsaw • Washington, D.C.

\*Linda Widyati & Partners in association with Clifford Chance.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.