Personal data protection at the workplace

Laura Felicíssimo - 01.22.2018

/ Introduction

At the workplace, internet has intensified the mixture between the public and the personal life. Dating back to the 19th century when telephones emerged. until nowadays culminating with routinely connected workplaces.

On the legal point of view, there are many challenges in the regulation of new labor conditions propitiated by technology and media progress. This article will focus on employees´ rights to privacy at the workplace in a comparative law perspective.

/ Brazilian perspectives

Although Brazil does not yet have a general regulation for the personal data protection, the Superior Labor Court's Coordination of Documentation already has compiled an extensive bibliography [11] on the subject of privacy and the right to intimacy at the work environment being possible to find studies specifically addressing the question of the employee's personal data since 2012.

Nevertheless, Article 5, paragraph X, of the Brazilian Federal Constitution provides the inviolability of intimacy, private life, honor and image of people, ensuring the right to compensation for material or moral damages resulting from their violation. On this matter, in May 2017, the Brazilian Superior Labor Court convicted [12] a bank to compensation for moral damages by accessing the current account of its employee and at the same time, its own account at that bank , to verify the compliance with internal norms that prohibits bankers from having another paid activity other than that.

In this example, it was concluded that there was an undue breach of the bank secrecy, as this is an exceptional measure that requires the presence of sufficient evidence of employee's failure to comply with this rule. In this sense, the mere inspection of the employee's bank account, in order to verify the existence of another remunerated activity, or the receipt deposit from other sources of income was undue.

Additionally, Article 5, paragraph XII of the Brazilian Federal Constitution provides that the secrecy of correspondence and telegraphic communications, data and telephone communications shall be inviolable, except by a court order. In the workplace this is accomplished in the unfortunate monitoring of the employee's personal e-mail, which can often justify the employer decision of banning the access of personal content on professional desktop. At the same time, there is also the conclusion that this right is not extended to the corporate e-mail, as this is a work tool that can even be used by the employer as a legal proof of fair[13].

eSocial

A recent challenge to the employee's personal data protection is the Digital Bookkeeping System for Tax, Social Security and Labor Obligations (eSocial) [14] , instituted in 2014 by the Decree No. 8373.

The eSocial unifies the provision of information regarding the recording of tax, social security and labor obligations, standardizing its transmission, validation, storage and distribution. Currently, it is necessary to execute 15 different fiscal, social security and labor obligations, all of which will be centralized in this new public registration system.

Since October 2015 the platform is used by the domestic employer. The system´s implementation for companies will be done in two phases: the first one will be in January 2018, aimed at employers and taxpayers with a turnover of more than R$ 78 million in 2016; and the second phase will start in July 2018 covering other employers and taxpayers.

Decree 8373/14 states that members of the Steering Committee shall have shared access to the information that integrates the national environment of the eSocial and shall use them within the limits of their respective competences and attributions, moreover they are not able to transfer them to third parties or to disclose them, unless otherwise provided by law. [15] Nevertheless, the tax information and the Unemployment Compensation Fund (FGTS) must observe the rules of fiscal and banking secrecy[16].

However, the Brazilian government still has a lot to progress in relation to its security and efficiency policies in the provision of services offered within the Internet [17]. For example, in 2015 there was an attempt to adopt the Digital Workbook, which would completely replace the existent one, but today this initiative is only used as support [18] due to numerous system failures that was inspired by an analog processes.

/ The European scenario for the personal data protection at the workplace

European Union

Europe is longer familiar with the debate and regulation around security information, offering more accurate delimitations around the personal´s employee data protection.

The General data protection regulation of the European Union (Regulation (EU) 2016/679) will be in force on May 2018, but the broad personal data protection is not a EU recent concern because this Regulation will replace the Personal Data Protection Directive (Directive 95/46/EC), from 1995. Nevertheless, reference studies for the European Commission about the subject[19] date back from 1999.

In June 2017, the European Union adopted Opinion 2/2017[20] about data processing at work as a complement to other Opinions about the subject, produced before the General Data Protection Regulation. The Opinion is based on tree principles of the Directive: legality, transparency and the automation of decisions.

Due to power asymmetry at labor relations, the Opinion addresses that legal bases for data processing at the workplace should not rely on the employee's consent because this is provided they despite the purpose, in order to keep the job.

Nevertheless, data collection usually occurs to comply with legal requirements, so it goes beyond personal consent. Thus, the employer cannot rely solely on the authorization given by the employment contract to collect and process employee data. It is necessary

to rely on other authorized forms, such as legitimate interests or legal requirements, otherwise employee's data treatment may be considered illegal.

However, the employer must realize that the data processing must be based on legitimate interests, while methods and technologies used must be less intrusive as possible, limited to the compliance of legitimate interests.

The processing operations must also rely on transparency, which means that employees must be clearly informed about their personal data processing, including the existence of monitoring at the work place. Finally, the Opinion emphasizes that legal or sensitive decisions should not be based solely on automated processing, as this method often favors personal aspects such as the employee's performance, unless this procedure is necessary to fulfill a contract or if there is the explicit consent of the data subject.

This compared study is important because much of what the Opinion presents as best practices or legal requirements restricted to Europe are seen at the Brazilian general personal data protection Bills.

Regarding the Regulation, the Opinion emphasizes that the legal requirements of the Directive have been maintained besides the inclusion of new obligations that also covers labor relations, such as:

- Privacy by Design, in favor of techniques such as anonymization [21].

- prior evaluation of data protection impacting the implementation of new technologies [22].

Article 88 of the Regulation deals specifically with data processing at the workplace, giving freedom to Member States to set standards for data protection in the context of recruitment, employment contract's termination, work organization and management, diversity issues, equality, health, safety and protection of personal property in order to privilege the legitimate interests and employee´s fundamental rights.

In this matter, the Opinion highlights the risks of excessive and unjustified monitoring and data retention by setting examples of good practices, for instance, anonymity to report abuses on the work environment and immediate destruction of data from non-selected subjects in recruitment processes, which should be discarded as soon as this decision is made.

In September 2017, a decision of The Grand Chamber of the European Court of Human Rights considered unfounded [23] the fair dismissal of an employee that was using the company's network for personal communication, despite internal rules against that practice. The reason for the decision was because the employee was not aware about the monitoring with this purpose and even though the express prohibition, the employee's private life and correspondence secrecy shall be respected.

Nevertheless, the company has used the full content of personal communications to demand explanations from the employee, to proceed with the fair dismissal and to use the situation as an example of bad behavior to other employees.

United Kingdom

The Data Protection Act from 1998 is still in force at the UK. The country has also implemented the European Directive on Data Protection and the iCO (Information Commissioner's Office), which is UK's independent authority set up to uphold information rights in the public interest.

Regarding the employee's personal data protection, the iCO has produced several guides [24] that provide guidance on legal obligations to companies of all sizes. The guides approach legal matters on employees' rights, recruit and selections procedures, employee's historical data, especially concerning sensitive data like heath data, monitoring practices and others.

Despite the fact that UK is leaving the European Union, the guides also provide support to comply with the Regulation that will be in force in 2018. The fact that a regulation is replacing a directive about the subject in the EU demonstrates its increasingly importance in the last years because unlike a directive, a regulation needs to be fully enforced by the EU member states.

Such detail of obligations and legal care by the employer is still not mandatory in Brazil due to the absence of a general regulation for data protection, but it is not correct the conclusion that there are no obligations or rights related with privacy concerns and personal data protection here.

/ Conclusion

At this study, it was possible to realize that the highly-connected workplace in Brazil is requires further regulation and reflection. However, it is always important to be aware of constitutional rights such intimacy, correspondence secrecy and leisure.

Regarding the employee's personal data protection, many gaps could be fulfilled by a general data protection regulation that is currently subject of several Bills in progress at the National Congress. Until there, Baptista Luz Advogados is a step forward on the debate with the Privacy Hub, a project that defends the data protection as a competitive strategy. For instance, it can bring positive results in the labor sector resulting in the attraction and retention of the best work forces, reducing the risks of labor lawsuits originated from unfortunate personal data treatment.

[1] Available in: goo.gl/iyzsHT, accessed on: 13.12.2017.

[2] Decree-Law no 5,452/43.

[3] Law no 13,467/17.

[4] Article 6 of Decree-Law no 5,452/43.

[5] Article 62, III, of Decree-Law no 5,452/43.

[6] Article 62, II of Decree-Law no 5,452/43.

[7] Available in: goo.gl/sBRBP7, accessed on: 08.12.2017.

[8] Available in: goo.gl/VYf1Td, accessed on: 08.12.2017.

[9] Article 6.

[10] Available in: goo.gl/VYf1Td, accessed on: 08.12.2017.

[11] Selected biography about Privacy and the right to intimacy at the workplace. Available in: goo.gl/X4Q5At, accessed on: 07.11.2017.

[12] Available in: goo.gl/xUqkhs, accessed on: 06.12.2017.

[13] TST, ED-RR–996100-34.2004.5.09.0015 from 18.02.2009 and TST-RR-613/2000-013-10-00.7 from 10.6.2005.

[14] eSocial. Available in: goo.gl/kTX2o7, accessed on: 13.11.2017.

[15] Article 8, §2.

[16] Article 8, § 3.

[17] Learn more at: goo.gl/GJ8v6r, accessed on: 12.12.2017.

[18] Available in: goo.gl/V11H6G, accessed on: 12.12.2017.

[19] Available in: goo.gl/DVXfCW, accessed on: 03.11.2017.

[20] Available in: goo.gl/J6JfrN, accessed on: 15.01.2018.

[21] Article 25 of the EU General Personal Data Protection Regulation.

[22] Article 35 of the EU General Personal Data Protection Regulation.

[23] CASE OF BĂRBULESCU v. ROMANIA (Application no. 61496/08) of The European Court of Human Rights. Available in: goo.gl/2SRPPB, accessed on: 15.12.2017.

[24] Available in: goo.gl/7sKCk3, accessed on: 11.12.2017.