

Extended Abstract

Processing of personal data in the context of video surveillance towards the new General Data Protection Regulation (GDPR)

Jorge Miguel do Vale Martinez Batalha

Instituto Superior Técnico, Portugal

Summary

The current text is the result of a research carried out in the field of citizens' fundamental rights, particularly, with respect to Personal Data Protection.

Nowadays, despite Portugal's national legislation ensuring special care in relation to Personal Data Protection, one notes that, the recent approval by the European Union, of the «General Data Protection Regulation», all Member States will have to comply with tighter rules. In this context, the intention is to answer the following question: in the light of the «General Data Protection Regulation» when handling personal data obtained using video surveillance systems, in private spaces, what are the main changes imposed on data subjects, especially in the work context, what measures should those in charge of these processing take and what type of additional legislation requirements should the Portuguese State respond to?

At the end, with a special focus on the personal data protection in the work context, and considering the finding derived from the research work carried out, two proposals are suggested aimed at addressing the existing gaps in the regulation of the processing of personal data obtained using video surveillance systems in private spaces.

Key words: RGPD, GDPR, Data processing, Video surveillance, CCTV, Personal data protection.

Introduction

The Official Journal of the European Union, published in 2016 the new «General Data Protection Regulation» (GDPR), which shall be applied by 25 May 2018. It is a binding document on all Member States, which primary objective is to guarantee an equivalent level of protection of individuals to allow the free flow of personal data in the European Union.

In fact, the Regulation repeals Directive 95/46/EC, with effect from 25 May 2018. However, it should be emphasized that the said Directive forms the basis of data protection laws in the Member States. These naturally include the Portuguese State, which transposed the directive, about nineteen years ago, into the national legal system, through the publication of Law 67/98, of October 26th, which is commonly mentioned as Law of Protection of Personal Data that currently regulates, in general, the processing of personal data in the Portuguese legal system.

It is essential to understand that *“the processing of personal data must be designed to serve the people”*¹. We speak of individuals who, by a large majority, were unable to perceive how quickly they became vulnerable, particularly concerning the protection of personal data.

In this context, this research focuses on finding the answer to the following question: in the light of RGPD and within the scope of the processing of personal data obtained using video surveillance systems in private spaces, What are the main changes imposed on data subjects, especially in the work context, what measures should those in charge of the treatment take and what type of additional legislation requirements should the Portuguese State respond to?

During the research, for the national scope, we gave special relevance to the Constitution of the Portuguese Republic, the Law of Protection of Personal Data (Law 67/98), and the Labor Code, to deliberations, opinions and commitments from the National Data Protection Commissioner and to the legislation regulating private security activities. In the international context, the emphasis was on Directive 95/46/EC, the Charter on Fundamental Rights of the European Union, the Universal Declaration of Human Rights and the General Data Protection Regulation.

¹ Cf. Considering nº. 4, UNIÃO EUROPEIA, *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*, in: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679&from=EN>, consulted on May 2016.

1. Framework

The «National Committee for Data Protection» (CNPD), an independent administrative authority, states the following: “since 1976 that the Constitution of the Portuguese Republic has enshrined the protection of personal data in the light of the use of Information Technology as a fundamental right, under the article 35th”².

Please note that, according to the no. 1 of the article 35th of the Constitution of the Portuguese Republic (CPR), “all citizens have the right to access the electronic data that concern them, and may demand its rectification and updating, along with the right to acknowledge the purpose the data are intended to, in the terms of the law”³. Moreover, in the case of Portugal, it was a pioneer in the “express constitutionalisation of the Information Technology/fundamental rights ratio”⁴.

Currently, through the consultation of the most recent annual reports of the CNPD, “the data processing has continued to increase steadily when it comes to video surveillance systems”⁵. Besides, when it comes to decision-making, video surveillance has a notorious relevance within the national context. Actually, in 2015, its percentage was of about 70.

In fact, according to Catarina Sarmiento e Castro, “there will be a processing of video surveillance, namely in the cases when the collection of images originated from web cameras, or when the Internet was used to disseminate them, but also when this data collection was conducted in a closed circuit television (CCTV)”⁶.

On the other hand, as Alexandre Sousa Pinheiro teaches, “the total domain of space by cameras would lead to a security Eden”⁷. However, although the human being is imperfect by nature and consequently crimes generator, one cannot go so far as to judge all citizens as suspects of being suspects. Despite this, Portuguese society remains silent regarding this issue.

Regarding processes of administrative misconduct opened by CNPD, there is an increase of over 50% in the period between 2011 and 2015⁸. Of these, “the participations made by GNR and PSP stand out, mainly regarding the operating conditions of video surveillance systems”⁹, which led to the opening of

² Cf. CNPD [Comissão Nacional de Protecção de Dados], *História da CNPD*, in: <https://www.cnpd.pt/bin/cnpd/historia.htm>, consulted on January 2016.

³ Cf. PORTUGAL, *Constituição da República Portuguesa*, Coimbra: Almedina, 2011, p. 23.

⁴ Cf. PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015, p. 666.

⁵ Cf. CNPD, *Relatório de atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consulted on January 2017.

⁶ Cf. CASTRO, Catarina Sarmiento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Edições Almedina, 2005, p. 125.

⁷ Cf. PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015, p. 185.

⁸ Cf. CNPD, *Relatório de atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consulted on January 2017.

⁹ Cf. CNPD, *Relatório de atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf,

603 processes. As for the reasons for complaints, “it’s possible to identify some areas where complaints are most recurrent, such as on video surveillance systems of neighbors or that of employers”¹⁰.

As a general principle, regarding the statements of 2nd article of the Personal Data Protection Law (PDPL), “the personal data treatment must be processed in a transparent manner and in strict respect for the privacy reserve, as well as fundamental rights, freedoms and guarantees”¹¹.

2. The need for a code of conduct for the purposes of processing the personal data of video surveillance in the labor context in compliance with GDPR

The setting up of codes of conduct was already suggested in Directive 95/46/EC of the European Parliament and the Council, of 24 October 1995¹². Nowadays, the use of this element is encouraged at various points of the GDPR. Consider the following references:

- 1) In Article 24, in what concerns to the responsibility of the person in charge of processing, paragraph 3 notes that “the compliance with the approved code of conduct (...) can be used as an element to demonstrate compliance with the obligations of the controller”¹³.
- 2) In Article 28, concerning the subcontractor, paragraph 5 notes that “the fact that the subcontractor complies with the approved code of conduct (...) can be used as an element to demonstrate the sufficient guarantees taken pursuant to paragraphs 1 and 4 of this Article”¹⁴.
- 3) In Article 32, concerning the security of the processing, paragraph 3 notes that “the compliance with an approved code of conduct (...) can be used as an element to demonstrate the fulfilling obligations set out in paragraph 1 of this Article”¹⁵.
- 4) In Article 35, concerning the data protection impact assessment, paragraph 8 notes that, “In assessing the impact of treatment operations carried out by data controllers or by subcontractors, particularly for the purpose of assessing the impact on data protection, due account is taken of the compliance with the approved codes of conduct referred to in article 8

consulted on January 2017.

¹⁰ Cf. CNPD, *Relatório de atividades da Comissão Nacional de Protecção de Dados, 2013-2014*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201314.pdf, consulted on January 2017.

¹¹ Cf. DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, N.º 247, 26 de outubro de 1998, p. 5536.

¹² Cf. UNIÃO EUROPEIA, *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, in: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>, consulted on April 2016.

¹³ Cf. Article 24 of the GDPR.

¹⁴ Cf. Article 28 of the GDPR.

¹⁵ Cf. Article 32 of the GDPR.

*40 on the part of those responsible or subcontractors*¹⁶.

The previous citations lead to the conclusion that compliance with an approved code of conduct may be an important element, both for controllers and subcontractors in terms of the GDPR.

Besides this, as stated in the GDPR, if there is a minor infringement, for the controller or the subcontractor to comply with a code of conduct, will be of great value, for it can attenuate the application of penalties imposed by the control authorities¹⁷. In other words, if there is a minor infringement of the video data processing of video surveillance in the workplace but compliance with the specific code of conduct for data treatment, this will be a valid factor in the mitigating of sanctions imposed by the authority.

Article 40, of the GDPR contains clear examples of rules to include in a code of conduct. Thus, taking into account the suggestions made by the GDPR for the code of conduct, the following are examples of what is essential not to omit from a draft code of conduct that deals with systems of data processing of video surveillance in a workplace.

3. Draft Code of Conduct

Due to the national legal order, the proposed Code refers to the data processing operations related to video surveillance systems in a labour context, applied in the whole of Portugal.

The proposal comprises 22 articles. Besides the above, this code complies with the Constitution of the Portuguese Republic and the labour legislation. This summary highlights the following articles:

Principle of transparency

Considering the data protection regime established in the GDPR, the principle of transparency must be respected by the personal data processing controller.

The data processing controller commits to ensure that the processing in question is carried out in a transparent manner and in strict respect for privacy, as well as for the fundamental rights, freedoms and guarantees of the data subject, i.e., the employee, under the scope of video surveillance system use, in particular in the work context.

The fact that this Code applies to the data processing under the scope of video surveillance system use in the work context implies that the data processing controller is the employing entity or the public employment body, which determines the purposes and means of processing.

It is required that the controller takes the necessary measures, including by contract with the outsourced

¹⁶ Cf. Article 35 of the GDPR.

¹⁷ Cf. Considering no.148 of the GDPR.

entity, in order to ensure that the data collected through video surveillance system use in the work context are not used for any other purpose.

Prohibition of professional performance control

The data collected through video surveillance system use in the work context cannot be used by the data processing controller or by outsourced entities to control the professional performance of the employee, as requested in #1 of article 20th of the Labor Code, since this is not a legitimate purpose. For this reason, the personal data, even if collected for other legitimate purposes, cannot be used directly or indirectly to evaluate the employee performance.

Training on the protection of personal data

Public and private entities are obliged to promote the initial training and annual review, with a minimum duration of 4 (four) hours, in the field of personal data protection, with an evaluation that must necessarily be positive, to workers who have, or may come into contact, with data obtained through the use of video surveillance systems in a labour context.

Subcontracted entities, if any, have to fully comply with the provisions of the previous paragraph.

Violation of data

In the event of a violation of the data obtained through the use of video surveillance systems in a labour context, as soon as the responsible person is aware of a breach of such personal data, he/she shall notify the supervisory authority without undue delay and, whenever possible, within 72 hours of being aware of the event, unless he/she is able to demonstrate, in accordance with the principle of liability, that such breach is not liable to entail a risk to the rights and freedoms of specific persons. If notification cannot be made within 72 hours, the notification shall be accompanied by the reasons for such delay, and the information may be provided in stages without undue delay.

The person responsible for processing the data obtained through the use of video surveillance systems in a labour context is obliged to keep on record incidents of violation of personal data.

Impact assessment on data protection

Public and private entities wishing to resort to the use of video surveillance systems in a labour context are obliged to carry out an impact assessment of the use of technologies regarding the privacy of workers, in accordance with the provisions of Article 35 of the GRDP and, subsequently, to use the most appropriate and least intrusive means for achieving the legitimate objectives.

Compulsory signs

To all responsible for the data processing obtained through video surveillance systems in a work context, it is compulsory, the display, in very visible places, of informative notices about the existence of video

surveillance, with the requisites and technical specifications for the signs and its dimensions in the same terms as the ones disposed in article 115, decree n° 273/2013, from August 20, and according to its annex VIII, resorting to the following symbol:



The signs should be placed at the outer perimeter of the place or area under surveillance with resource to surveillance electronic equipment by video cameras, without exceeding 2 meters from the ground and in the most convenient way in order to ensure its immediate recognition by the workers.

The same informative signs should be replicated inside the building, without exceeding 2 meters from the ground.

The responsible for the data processing obtained through video surveillance systems in a work context has the obligation to, together with the symbols and the terms previously defined, post the following information:

- a) The existence and location of the video cameras;
- b) The reference «For your protection, this place is under video surveillance»;
- c) If it applies, the private security company authorized to operate the system, by identifying its name and its permit or license;
- d) The responsible for the collected data processing to whom the access and rectification right may be exercised.

4. The need for video surveillance general legislation

The CNPD, as a supervisory authority, as from 25 May 2018, will not continue to exercise a prior control, in general, on data processing, in the view of the established date for the applicability of the GDPR. However, the allocated authorizations to process personal data remain valid, provided that they adapt to the new rules.

Despite the rules set out in the GDPR, there is a continuous need for specific regulations concerning video surveillance. In fact, the Portuguese national legislator should have to draft legislation that, among other aspects, defines the following:

1. Admissible purposes for the processing of data taken from the use of video surveillance systems;
2. Requirement of an impact assessment on personal data protection;
3. Time limits for data retention;
4. Principles to be respected by entities, responsible for processing data, and subcontractors;
5. Obligation to attend annual and periodic sessions of training concerning personal data protection, for a minimum duration of 4 (four) hours, in the case of entities responsible for data processing;
6. Obligation to attend annual and periodic sessions of training concerning personal data protection, for a minimum duration of 4 (four) hours, in the case of subcontractors who are involved in data processing, namely, private security firms and entities that are subjected to prior registration (surveillance systems installers);
7. Dissuasive sanctions, providing the worsening of those ones in case of recurrence;
8. Obligation to indemnify the data subjects in the event of a security breach;
9. Definition of the limits of areas that are covered by the cameras;
10. Definition of the limits of areas covered by the video surveillance systems, in line with the specific characteristics of each public or private entity;
11. Definition of prohibited areas for the cameras scope;
12. Specification of mandatory security measures that have to be adopted by the entity responsible for processing and subcontractors;
13. Definition of limits for the video surveillance systems remote control, particularly in the labour context;
14. Definition of a platform for the presentation of complaints concerning illegal processing but ensuring the complainant anonymity;
15. Obligation to appoint a person responsible for protection who has the qualifications listed in the «General Data Protection Regulation» or, alternatively, through recourse to hiring external services, defining a minimum number of hours that will have to be contracted annually.

Conclusion

The unlawful use of personal data by third parties may have unimaginable effects, to the detriment of data owners. Just as people commonly say: if you are not in fault you have nothing to fear. But, as we have seen, in relation to video surveillance, even those who are not in fault, have reason to fear.

With a focus on the rights of personal data holders, the emphasis given here on the use of these video surveillance systems in a labour context results, on the one hand, from the Portuguese national legislation, in particular as regards the employment relationship; from the Constitution of the Portuguese Republic; the jurisdiction of higher courts, in this matter; and the guidelines produced by the National Data Protection Commission. On the other hand, account has been taken of the various European-level legislative documents concerning the rights of personal data holders, with a substantial emphasis on the «General Data Protection Regulation» (GDPR).

This latest legislative document, which has a compulsory nature for all Member States, has already entered into force, and shall apply from 25 May 2018. Therefore, the study of this legislation, the weighting of the various aspects that involve it, the obligatory interpretation, and the repercussion in the most varied sectors of activity, resulted in two potential contributions that could be recognized by the Portuguese State, with a view to promoting citizens' awareness of the risks, rules, guarantees, and rights associated with the processing of personal data.

The first of these contributions consists of a draft code of conduct. Their non-existence and necessity were both found. In other words, it has been proven that the GRDP has repeatedly suggested the creation of this type of instrument, so that data controllers and subcontractors might have the possibility to adhere to it, thus demonstrating their willingness to comply with established rules.

As for the second contribution, it consists in the presentation of a set of items considered relevant, which should be included in national legislation, due to the lack of a general law on the use of video surveillance systems in Portugal.

Finally, it should be noted that there is no obligation to provide specific training in the field of personal data protection in the context of the exercise of private security, knowing that it is the guards, officials of the entities subcontracted by the controller in the use of video surveillance systems, who play a professional role of greater physical proximity and access to the collected images.

Parallel to this group, there are entities subject to prior registration, within the scope of the legislation applicable to the private security activity, which carry out the study and design, installation, maintenance or technical assistance of security material and equipment, such as or video surveillance systems. Naturally, due to their activities, they have easy access to the personal data recorded in the collected images, therefore, they must have adequate and obligatory training in the protection of personal data.

Bibliography

- ABRANTES, José João, *Direitos Fundamentais da Pessoa Humana no Trabalho, em especial, a reserva da intimidade da vida privada (algumas questões)*, Coimbra: Almedina, 2014.
- CASTRO, Catarina Sarmiento e, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra: Edições Almedina, 2005.
- CNPD [Comissão Nacional de Protecção de Dados], *História da CNPD*, in: <https://www.cnpd.pt/bin/cnpd/historia.htm>, consulted on January 2016.
- CNPD, *Relatório de atividades da Comissão Nacional de Protecção de Dados, 2013-2014*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_201314.pdf, consulted on January 2017.
- CNPD, *Relatório de atividades, 2015*, in: https://www.cnpd.pt/bin/relatorios/anos/Relatorio_2015.pdf, consulted on January 2017.
- CONSELHO DA EUROPA, *Convenção Europeia dos Direitos do Homem*, in: http://www.echr.coe.int/Documents/Convention_POR.pdf, consulted on May 2016.
- DIÁRIO DA REPÚBLICA, *Decreto-Lei nº 135/2014 de 8 de setembro*, 1ª série - Nº 172, 8 de setembro de 2014, pp. 4802-4805.
- DIÁRIO DA REPÚBLICA, *Decreto-Lei nº 35/2004 de 21 de Fevereiro*, 1ª série-A, Nº 44, 21 de Fevereiro de 2004, pp. 932-941.
- DIÁRIO DA REPÚBLICA, *Lei n.º 98/2015 de 18 de agosto*, 1ª série - Nº 160, 18 de agosto de 2015, pp. 6081-6108.
- DIÁRIO DA REPÚBLICA, *Lei nº 34/2013 de 16 de maio*, 1ª série - Nº 94, 16 de maio de 2013, pp. 2921-2942.
- DIÁRIO DA REPÚBLICA, *Lei nº 52/2013 de 25 de julho*, 1ª série - Nº 142, 25 de julho de 2013, pp. 4365-4387.
- DIÁRIO DA REPÚBLICA, *Lei nº 67/98 de 26 de Outubro*, 1ª série - A, N.º 247, 26 de outubro de 1998, pp. 5536-5546.
- DIÁRIO DA REPÚBLICA, *Lei nº 72/2015 de 20 de julho*, 1ª série - Nº 139, 20 de julho de 2015, pp. 4909-4911.
- DIÁRIO DA REPÚBLICA, *Portaria nº 106/2015 de 13 de abril*, 1ª série - Nº 71, 13 de abril de 2015, pp. 1811-1812.
- DIÁRIO DA REPÚBLICA, *Portaria nº 273/2013 de 20 de agosto*, 1ª série - Nº 159, 20 de agosto de 2013, pp. 4956-4988.

GUERRA, Amadeu, *A Privacidade no Local de Trabalho*, Coimbra: Livraria Almedina, 2004.

PINHEIRO, Alexandre Sousa, *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, Lisboa: AAFDL, 2015.

PORTUGAL, *Código do Trabalho*, in: <http://cite.gov.pt/asstscite/downloads/legislacao/CT25092017.pdf>, consulted on October 2017.

PORTUGAL, *Códigos Penal e Processo Penal*, Porto: Porto Editora, 2015.

PORTUGAL, *Constituição da República Portuguesa*, Coimbra: Almedina, 2011.

UNIÃO EUROPEIA, *Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs')*, in: https://iapp.org/media/pdf/resource_center/WP29-2017-04-DPO-Guidance.pdf, consulted on August 2017.

UNIÃO EUROPEIA, *Carta dos Direitos Fundamentais da União Europeia*, in: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf, consulted on May 2016.

UNIÃO EUROPEIA, *Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*, in: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT>, consulted on April 2016.

UNIÃO EUROPEIA, *Opinion 2/2017 on data processing at work*, in: http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjUm72n_prWAhXKyRoKHfBnBQQQFggmMAA&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D45631&usg=AFQjCNFL9EUmcaORV7p_Z6N12WltBgUlaA, consulted on August 2017.

UNIÃO EUROPEIA, *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados)*, in: <http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32016R0679&from=EN>, consulted on May 2016.