THE TOPIC OF VIDEO SURVEILLANCE AND ITS COUNTLESS REPERCUSSIONS

Xenia Camerini, Civil Lawyer and DPO in Naples

Abstract:

This focus is based to the analysis of the difficult issue concerning the video surveillance of workers and the necessary compliance with privacy legislation in this area.

In particular, first of all, the reference legislation, the interested parties, and the procedure to be respectful of the provisions of the new privacy regulation will be analyzed. Secondly, attention will be focused on specific aspects such as practical tips, useful advice concerning the positioning of the cameras, the possibility of installing fake or inactive cameras. In addition, three further problems related to the topic will be discussed: the eventuality of an impact assessment under artilce 35 GDPR, the related inspection activities, and finally any sanctions in case of violations. Finally, it will be necessary to deepen the guidelines adopted, nationally, by the Italian Data Protection Authority (Italian DPA) and in the supranational context, guidelines no. 3 of 2019 of the European Data Protection Board (EDPB). At the end of this paper, a particular case study concerning private video surveillance in public transit will be addressed.

Key-words: Video surveillance - Protection of workers' privacy - GDPR - Italian DPA - EDPB

Category: Legal area

Topic: Data Protection Law

1. Introduction

The issue of privacy protection, especially after the adoption of the European regulation n. 679/2016 is a much debated topic, in particular, as regards the search for the right balance of the relationship existing between the video surveillance of workers and the protection of their rights and freedoms, especially in light of the new "GDPR".

The matter raises numerous legal topics that will be investigated, after trying to clarify the salient aspects of the legislation: applicable discipline, stakeholders, and related procedure. Subsequently, the hypotheses in which it is necessary to carry out an impact assessment will be addressed, as well as any inspection activities and, if necessary, the application of any sanctions in case of non-compliance with the privacy legislation. Fundamental in this sector are the guidelines implemented both nationally and internationally, namely those of the Italian Data Protection Authority and the European Data Protection Board.

Finally, the Lazio Regional Administrative Court, recently, has faced the question of private video surveillance in public transit, establishing that the purpose of crime prevention and territorial control for the protection of urban security is entrusted only to the territorial Public Administration.

2.Video surveillance and the protection of workers' privacy

2.1 The reference standard

Given the complexity of the subject, it is necessary to clarify, *prima facie,* the regulations applicable to the case in question:

1) Workers' Statute (Law no. 300/1970),
2) Privacy Code (Legislative Decree no. 169/2003 as amended by Legislative Decree no. 101/2018),
3) EU Regulation 679/2016 (GDPR),
4) Provisions and guidelines of the Italian Data Protection Authority (Italian DPA),
5) INAIL Circulars (National Labor Inspectorate),
6) Guidelines of the EDPB (European Data Protection Board),
7) CCNL collective bargaining contracts - Corporate Contracts.

2.2 Interested subjects

About video surveillance in the workplace, it is first of all necessary to specify who are the subjects involved in the processing of data: these are all subordinate workers (according to article 2094 of the Italian Civil Code), therefore excluding other collaborators (*ex multis* consultants, professionals with VAT number). More specifically, two regulations are highlighted to determine the rights and duties of this area:

A) Labor law regulations

The personal rights of the workers are:

- the right to physical integrity and health (art. 2087 of the Italian Civil Code and art. 9 of the Workers' Statute);
- the right to freedom of opinion and protection of confidentiality (articles 1 and 8 of the Workers' Statute);
- the right to the dignity of the worker (articles 3-4 and 6 of the Workers' Statute).

B) Privacy Policy

Art. 114 of the Privacy Code as reformed by Legislative Decree no. 101/2018 refers to art. 4 of the Workers' Statute. In this case, the data subjects are all individuals, workers and third parties, who are filmed by the cameras. In the case of workers, art. 4 of the Workers' Statute provides (amended by Legislative Decree no. 151/2015 implementing the so-called "Jobs Act" referred to Law no. 183/2014 in compliance with the adaptation of the legislation to new technologies) the general prohibition of control over the activity of subordinate workers, except in cases expressly provided for namely: "Audiovisual systems":

1. paragraph: The audiovisual systems and other tools from which also the possibility of remote control of the activity of workers can be used exclusively for organizational and production needs, for worker safety, and the protection of company assets and may be installed following a collective agreement stipulated by the unitary union representation or by the company union representatives. Alternatively, in the case of companies with production units located in different provinces of the same region or several regions, this agreement can be stipulated by the comparatively most representative trade unions on a national level. In the absence of agreement, the systems and instruments referred to the first period can be installed prior authorization of the territorial offices of the National Labor Inspectorate or in the case of companies with production units located in the areas of competence of several territorial offices, of the headquarters of the National Labor Inspectorate. The measures referred to the third period are definitive.

2. paragraph: The provision referred to paragraph 1 does not apply to the tools used by the worker to perform work performance and to the tools for recording access and attendance.

3. paragraph: The information collected under paragraphs 1 and 2 can be used for all purposes related to the employment relationship provided that the worker is given adequate information on the methods of use of the tools and of carrying out controls and in compliance of the provisions of Legislative Decree, 30 June 2003, no. 196. Concerning this latter aspect, it is, therefore, necessary to prepare adequate information regarding the worker, where it must be clarified that all the information collected through the tools from which control of the workers may also derive can be used for all purposes connected to the relationship of work provided that adequate information is given to the worker; on how to use the tools; on the procedures for carrying out checks and in compliance with the provisions of the privacy legislation.

Therefore, in summary, it is necessary to keep in mind that:

Before proceeding with the installation of the video surveillance system, it must be borne in mind that there is a general prohibition of remote control of working activities. The installation of the cameras must not be

carried out to check the method of execution of the work. It is necessary to respect the sphere of intangibility of the fundamental rights and freedoms of people, including workers: obligation to provide information; obligation to keep images or data relating to the worker for no longer than a certain period; obligation to allow the exercise of the right of access to interested parties; obligation to activate a trade union or administrative procedure before installation. When video surveillance is made necessary by organizational, production, or work safety needs, the guarantee procedures are established under art. 4 of the Workers' Statute.

2.3. Procedure

Step 1: Understand the purposes of the processing; where the cameras will be placed; recording times and methods, if the camera has further potentially harmful functions.

Step 2: Evaluate whether to carry out an impact assessment according to art. 35 of GDPR and establish whether any prejudices for the person concerned emerge as a result of this examination.

Step 3: Stipulate a trade union agreement with the RSAs, or, failing that, submit a request for authorization to the competent Labor Inspectorate.

Step 4: Inform employees, collaborators, and customers of the presence of cameras with appropriate warning signs displayed both inside and outside the company premises and provide employees with appropriate information.

Step 5: Designate any internal appointees or external managers of the video surveillance management.

2.4. Practical tips

- Position the cameras in such a way that the camera angle frames only the parts of the premises most exposed to the risk of robberies or other criminal behaviors in compliance with the privacy of employees and aimed exclusively at protecting the safety of company assets or other legitimate ones reasons for installation. • Equip the cameras with an indicator light that indicates when they are in operation.
- Prepare a map of the rooms indicating the location of the cameras, their technical specifications, their shooting cone, and the location of the video recorder and monitor.
- Properly store recording equipment as well as accessories for operation with safety measures (e.g. closed box with a key).
- Keep the images collected for a maximum of 24 hours (except on holidays and for specific needs).
- View the recordings in the presence of the person in charge of video surveillance.

2.5. Regarding the positioning of the cameras:

- They cannot be installed in every company environment, for example in changing rooms, bathrooms, or similar.

- The employer cannot, at the end of the working day, watch - as if it were a film - the content of the filming because this would spill over into remote control, except in certain cases.
- The employer cannot constantly monitor the performance of workers through the video surveillance system but only e.g. their assets.
- The employer can only carry out a so-called control defensive (i.e. in those cases in which an event affecting the business or assets of the entrepreneur has already occurred, for example, the theft of objects in the office). Under this last aspect of the hidden defensive controls, the Grand Chamber of the European Court of Human Rights declared that the installation of hidden cameras without the knowledge of employees does not affect the right to privacy of workers if this activity is intended to verify any illegal acts to the detriment of the society. For example, a businessman can install hidden cameras without informing employees if he has the well-founded suspicion that they are robbing him and if the losses suffered for their conduct are substantial (for details see the ECHR judgment of 17 October 2019).

2.6 Fake or inactive cameras

The Italian Supreme Court of 1986, with sentence no. 1490 established that the prohibition imposed by art. 4 of the Workers' Statute it is not excluded either from the fact that such equipment has been installed but is not yet functional or from any notice given to workers or that the control is intended to be discontinuous because it is exercised in premises where the workers are only occasionally. In addition, the Italian Supreme Criminal Court, with the sentence no. 4331 of January 30, 2014, stated that the installation of cameras inside the company and aimed directly at the employees, carried out without waiting for the authorization of the DTL or the agreement with the trade union representatives, involves the criminal liability of the employer of work, even if they are off. The judge also highlights the possibility of sanctioning the company even if "fake" cameras are mounted, without the prescribed rules, for the sole purpose of deterrence. Therefore, it is possible to state that even the mere fact of having installed equipment without having subsequently activated them constitutes a violation of art. 4 of the Workers' Statute.

3. Possible need for the data protection impact assessment under art. 35 GDPR

In the cases established by Article 35 of the GDPR, it is necessary to carry out an impact assessment, and in fact, paragraph 3 establishes: "*The data protection impact assessment referred to in paragraph 1 is required in particular in the following cases:*

a) a systematic and comprehensive assessment of personal aspects relating to natural persons, based on automated processing, including profiling, and on which decisions are based that have legal effects or similarly significantly affect said natural persons;

b) the large-scale processing of particular categories of personal data referred to in Article 9, paragraph 1, or of data relating to criminal convictions and offenses referred to in Article 10; or

c) systematic large-scale surveillance of an area accessible to the public ".

4. Inspection activities

The inspector, once verified the installation of audiovisual systems in the event of a failure to agree with the trade unions or in the absence of the authorization issued by the Labor Inspectorate, must issue a prescription under art. 20 of Legislative Decree no. 758/1994 to stop the unlawful conduct and have the audiovisual systems themselves removed. Once these obligations have been carried out, they will be able to eliminate the infringement ascertained. Within the inspection report, a deadline must also be set for compliance and therefore for the removal of illegally installed systems. The deadline must be adequate, due to the actual technical time really necessary for the uninstallation of the audiovisual systems. To limit the criminal sanction, the company may, in the meantime, sign the trade union agreement or request the issuance of the ministerial authorization. If in this time, the trade union agreement is signed or the administration is released, the inspector may admit "*the offender to pay, within 30 days from the fulfillment of the prescription contained in the report, a sum equal to one-quarter of the maximum fine, established for the offense committed* " as established by art. 21 of Legislative Decree no. 758/1994.

5. Fines

For non-compliance with the provisions of the Workers' Statute, a fine from € 154 to € 1,549 or arrest from 15 days to 1 year is established according to Articles 4 and 38 of Law no. 300/1970. (Articles 114 and 171 of Legislative Decree no. 196/2003, unless the fact constitutes a more serious crime). In the most serious cases, the penalties are applied jointly, and if the penalty of the fine is ineffective, the judge can fix it five times more. If there is the presence of an RSA in the company, we must not forget the possibility that the Union promotes an action under art. 28 of Law no. 300/70 against the entrepreneur who, by not involving the RSA, actually carries out conduct likely to be judged anti-union. For non-compliance with the provisions on privacy, the fines laid down by the GDPR according to art. 83 are: up to € 10ml or 2% of the annual worldwide turnover of the previous year if higher. In case of violation of the disclosure obligations: under labor law it will not be possible to use the data collected for disciplinary purposes and according to the new privacy regulation, the owner will be subject to the highest level penalties of € 20 million and, if necessary, 4% of the revenue.

6. Guidelines on video surveillance

6.1. Decision of the Italian Data Protection Authority on video surveillance of 2010.

The Italian DPA intervened on the topic with the guidelines of 8 April 2010, clarifying some points:

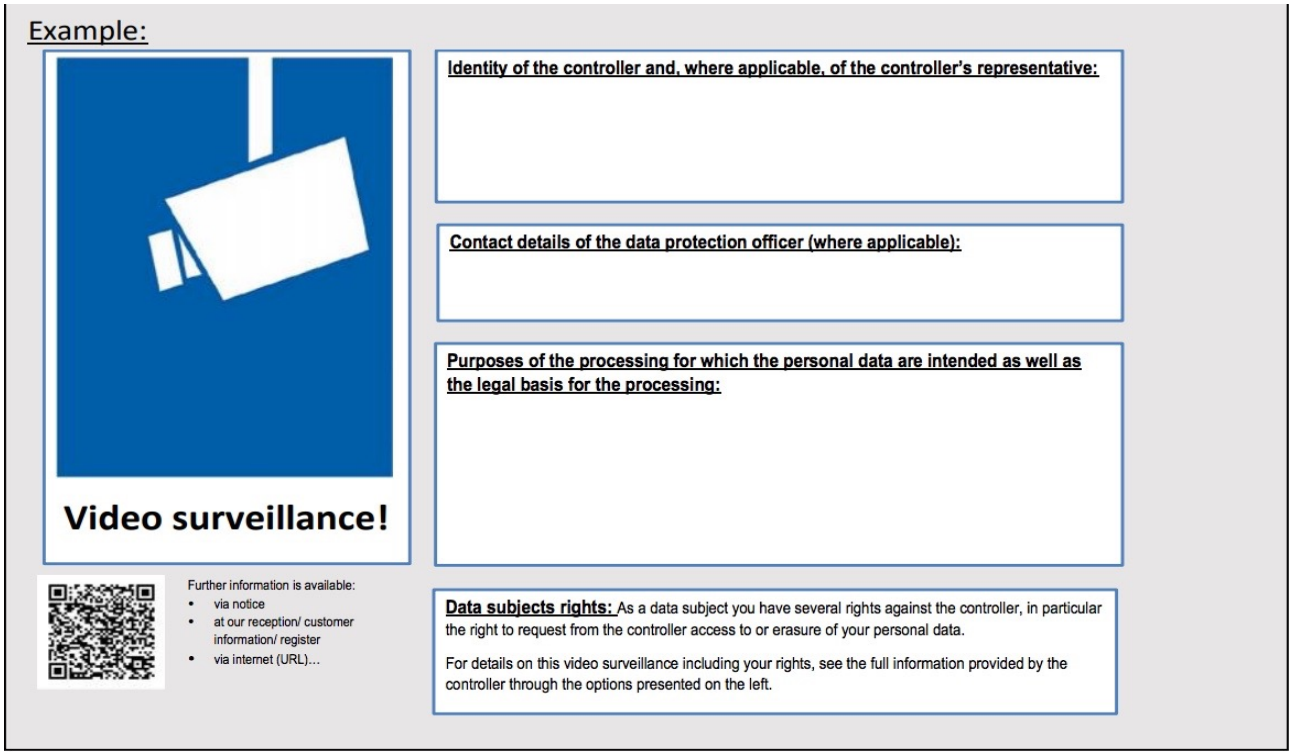
- interested parties must always be informed that they are about to enter into a video surveillance area;
- to this end, the Authority believes that the simplified model of "minimum" information can be used, indicating the data controller and the aim pursued;
- the sign must be placed before the range of action of the camera, even in its immediate vicinity;
- it must have a format and a position such as to be visible in all environmental lighting conditions, even when the video surveillance system is possibly active at night;
- can incorporate a symbol or stylization of explicit and immediate understanding;
- the Italian DPA also considers it desirable that the information, rendered in simplified form, then refers to a complete text containing all the elements referred to the relevant legislation.

6.2. Guidelines n. 3/2019 of the EDPB on data processing through video devices

The main innovations adopted by the EDPB, regarding the processing of personal data will be described as follows:

- identification of cases of processing of personal data through video surveillance systems to which the current privacy legislation does not apply: fake cameras, high-altitude video recordings, park assist cameras, the processing carried out by competent authorities under EU Directive 2016/680, processing of personal data by a natural person for purely personal or domestic purposes.
- The importance of the data minimization principle is emphasized; therefore the Board believes that the use of video surveillance should be limited only to cases where the owner's needs prevail over the rights and freedoms of the data subjects.
- because of the principle of transparency, it is necessary to provide suitable information to interested parties about the existence of a video surveillance system, both through first-level information (so-called short information) and through extended information. The brief information, the so-called *vignette*, allows interested parties to know in advance which personal data are processed by entering the range of action of the cameras. The Committee, in this regard, suggested the inclusion of QR Codes or web addresses that refer directly to the extended information, where all the information required by the Regulations will be available.
- The legal basis has been identified: either in the legitimate interest that must always be balanced, or in the public interest. The consent of the interested party is confirmed as a residual legal basis. The possibility of using video surveillance systems for the processing of particular data was also confirmed as long as there is an adequate legal basis.
- Regarding the retention period, the EDPB found that the term of one or two days is consistent with the need to detect any damage or accidents.

- Particular attention was paid to the processing of biometric data, also with reference to cases in which the templates created by the recognition systems allow a profiling of the habits of the data subjects for marketing purposes.
- The guidelines also provide a specific indication of the technical and organizational measures that the Data Controller should implement to constantly maintain control of the tools used and to enable data subjects to be able to exercise their rights at any time.
- Lastly, the Committee underlines that in the event of a request for access to delete the registrations, the interested parties must provide the Data Controller with some indications to facilitate the identification of the frames that concern them.



7. A Case study: Private video surveillance in public transit

Private individuals may not install video surveillance cameras facing areas accessible to the public without first agreeing with the local authority which can order the immediate removal of the system by reporting the abuse directly to the Italian DPA. The purpose of crime prevention and territorial control for the protection of urban security is entrusted only to the territorial Public Administration. Therefore, even where private individuals install cameras facing public areas, the processing of personal data is regulated not by the GDPR but by Directive 2016/680 (Directive on public security treatments) implemented with Legislative Decree no.

51/2018. This is what was stated by the Lazio Regional Administrative Court, section II-bis, with sentence no. 3316 of March 17, 2020.

In particular, according to the Italian Data Protection Authority, the private video surveillance system must not frame the areas subject to public transit; for the latter, only the Municipality would be competent to arrange the installation of video surveillance systems pursuant to Legislative Decree no. 11/2009 converted into law no. 38/2009, in order to prevent crimes and control the territory. The Authority specifies that, if the systems used by the Municipalities are intended for the protection of urban security, the rules on the protection of personal data are dictated by directive 2016/680 (Police directive) and not by European regulation 2016/679 (GDPR).

Even private individuals can install cameras facing public areas, but in this case, a formal agreement with the Municipality is required which limits the use of external filming to the Municipalities for police purposes only with the further clarification that the local Police forces have exclusive access to installed the cameras for security reasons. The Court of First Instance, then adds that in order to install the systems in question, it is necessary to prepare the minimum security measures, in particular, the data must be stored in such a way as to guarantee the loss, even accidental destruction, and above all access of persons not authorized to them (possibly by setting up data encryption methods). In addition, organizational measures must be put in place for the deletion of data upon expiry, or of data that is no longer necessary. Finally, the interested parties, that is the subjects filmed, must be able to access the filming concerning them and verify the methods of use of the data collected. The unlawfulness of the filming involves not only the unusability of the recordings but also the provision of blocking and prohibition of data processing by the Italian DPA.

Conclusions

It is evident, from all the considerations put in place in the previous paragraphs, such as the legislation concerning the video surveillance of workers, presents major and current problems regarding compliance with the protection of the personal data of the workers themselves. Therefore, it is clear that, on the one hand, it is necessary to deepen the knowledge of the topics dealt with given the countless repercussions, and on the other hand, how it is appropriate to rely on professionals in the sector to comply with the numerous provisions dictated on the subject of video surveillance of workers. And it is precisely in this way that it will be possible to avoid incurring the high penalties provided for by art. 82 and the remainder of the GDPR.