

Is it lawful to remotely monitor employees' work activities thorough the use of surveillance systems?

A recent Italian Supreme Court decision broadens scope of employments' right to use surveillance systems in the workplace

September 17 2012

By Saverio Cavalcanti and Marilita Piromalli

Italian legal framework

The acquisition and use of personal data from workplace surveillance systems is currently unregulated in Italy. Article 134 of Legislative Decree no. 196 (June 30, 2003), "Personal data protection Code" (hereinafter, "**Privacy Code**") states only that the Data Protection Authority (hereinafter, "the **Authority**") supports the introduction of a code of professional conduct "*for the acquisition and use of personal data obtained from surveillance systems.*" However, at present, no such code has been implemented by the relevant professional associations.

Consequently, the acquisition of personal data from surveillance systems is regulated under the Privacy Code which is supplemented by an order of the Authority ("Decision on Surveillance Systems") implemented on April 8, 2010.

Pursuant to the general principles set forth in the Privacy Code, the acquisition of personal data using such systems is lawful only if:

- (i) monitored subjects are properly informed, pursuant to Article 13 of the Privacy Code; and
- (ii) monitored subjects have expressed their free, informed and specific consent for the acquisition of personal data, pursuant to Article 23 of the Privacy Code.

With specific reference to the acquisition of employees' personal data from surveillance systems, the above-indicated general principles (i) and (ii) of the Privacy Code must be reviewed in conjunction with the applicable provisions of Law no. 300 (May 20, 1970), the so-called "**Workers Statute.**"

In particular, Article 4, Paragraph 1, of the Workers Statute provides that *“It is unlawful to remotely monitor employees’ work activities through the use of surveillance systems.”* Therefore, as specified by the Authority in the above-mentioned order, it is unlawful to use surveillance cameras to monitor employees merely for the purpose of ascertaining whether employees observe due diligence standards, such as punctuality and accuracy, in carrying out their work activities.

However, the same Article 4 of the Workers Statute allows the employer to use surveillance systems for organizational, productivity and security reasons. Because in such cases the employer could indirectly control employees’ work activities, even if inadvertently, it is provided that the employer must follow a specific procedure (i.e. co-determination with internal trade union representatives or - where there are no such representatives - with the relevant labor office). Therefore, surveillance equipment may be installed subject to an agreement between the employer and trade union representatives or the authorized labor office.

In addition, Article 8 of the Workers Statute forbids an employer from inquiring into an employee’s political or religious beliefs or trade union affiliations, as well as any other facts and opinions that are not relevant to an assessment of the employee’s professional skills. Therefore, the employer runs the risk of infringing upon its employee’s rights if such information is inadvertently obtained through the use of surveillance systems in the workplace.

Article 164, paragraph 2, et seq., of the Privacy Code establishes a fine of between 30,000.00 and 180,000.00 Euros for an employer that breaches the above-mentioned provisions. In addition, Article 171 of the Privacy Code (which refers to Article 38 of the Workers Statute) provides that the use of surveillance systems for the purpose of remotely controlling work activities carried out by employees or to investigate employees’ opinions is punishable by (i) a fine ranging between 154.00 and 1,549.00 Euros; or (ii), incarceration for a period of 15 days to 1 year, unless the violation falls within the criminal code and is punishable by criminal sanctions.

Furthermore:

- a. in the more serious cases, both sanctions (i) and (ii) can be imposed against the employer;
- b. a judge may increase the fine up to 7,745.00 Euros if, taking into account the employer’s means, the maximum fine under point (i) is not effective;
- c. the court can order publication of the sentence as an additional sanction.

Supreme Court Decision n. 22611 (April 17, 2012)

The case

In Decision No. 22611 (April 17, 2012) (the **“Decision”**), the Criminal Section of the Supreme Court ruled on an appeal filed by a company condemned for having mounted four video cameras – two of which focused directly on employees’ workspaces – in the absence of an agreement with trade unions, in breach of Article 4 of the Workers Statute.

In its defence, the company argued that it had asked for – and obtained – written consent of all employees to install the video cameras and, therefore, it lacked the intent to illegally control its employees. In addition, the company had installed signs in the workplace indicating the presence of

video cameras. As a consequence, according to the company, it could not be punished for a crime because it lacked the requisite criminal intent.

Decision

The Supreme Court ruled in favor of the company, stating that an employer may use surveillance systems, even video cameras directly focused on employees' workspaces – without following the procedure of co-determination with trade union representatives – if the company acquires its employees' express written consent to do so.

In light of the above, according to the Supreme Court, the company in question had not breached Article 4 of the Workers Statute because the express consent of all employees is adequate to lawfully replace the agreement between the company and trade unions.

In fact, according to the Supreme Court, in spite of the fact that the employer did not enter into any agreement with trade unions, *"it is rational that the greater includes the lesser, so that the effectiveness of a clear and express consent by all employees – and not only by their trade union representatives – has not been denied."*

Furthermore, the Supreme Court seems to assert – though not pronouncing directly on this point – that in the case in question there was no criminal intent on the part of the employer because there were signs mounted to warn of the presence of video cameras.

Conclusion: possible diminution of employment protection against surveillance system use by employers

The recent Supreme Court decision seems to indicate a new trend towards employee protection against surveillance system use by employers.

In fact, in the past, the Supreme Court has taken a different – more "formal" – approach to the enforcement of Article 4 of the Workers Statute, establishing the crime of illicit installation of surveillance systems in the absence of an agreement between the employer and trade unions (see Supreme Court, Criminal Section, No. 8042 (December 15, 2006)).

Therefore, the Decision could open up a new interpretation of the provisions of the Privacy Code and Workers Statute (and of the Authority's orders) on the use of surveillance systems in the workplace. This interpretation could be less favorable to employees than in the past, creating a diminution of their protection against surveillance system use by employers.

The Supreme Court opined that the employees' consent to the installation of video cameras was sufficient to replace the required (by Article 4 of Workers Statute) agreement between the employer and trade unions and found that such consent is more effective than such an agreement because it is given by all employees and not only by their trade union representatives.

The Privacy Code does not provide for the possibility of a "collective" expression of consent by a group of individuals, but rather only for the expression of consent by a trade union or labor office acting on the individual employees' behalf. In light of this general principle, it may be reasonable to assert that the individual consent of all employees (on the one hand) and an agreement with trade unions (on the other) do not objectively have the same effectiveness in terms of employee protection against a possible illicit use of their personal data by the employer.

Following a quantitative and formal approach, trade unions could be considered a “group of employees” numerically inferior to the total of all individual employees in the company. But, to the contrary, trade union consent should be considered using a qualitative approach: they have the role and the capacity to discuss and negotiate employees’ rights through agreements with employers, which are more protective towards the employees than a mere signature of the same employee on a document written unilaterally by the employer.

Finally, the installation by an employer of signs in the workplace indicating the presence of video cameras does not diminish the employer’s criminal intent. In fact, under these circumstances, the crime of illicit installation of surveillance systems could very well apply (similar to the situation where the employer installs surveillance systems without any awareness on the part of the employees). This is because, even if the employer installs warning signs (in compliance with the information obligation of the Privacy Code), the surveillance systems could be used to unlawfully obtain unauthorized information on its employees.

In order to assess the full extent of this innovative Decision, it is advisable to await other confirmatory decisions of the Supreme Court.

This article is intended solely to provide general information on the subject matter. Legal advice should be sought regarding your specific circumstances.