CJEU Rules on Lawfulness of Video Surveillance in Residential Buildings

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

On 11 December 2019, the CJEU ruled that national provisions which authorise the installation of a video surveillance system on buildings, for the purpose of pursuing the legitimate interest of ensuring the safety and protection of individuals and property, without the consent of the data subjects, are not contrary to EU law if the processing of personal data carried out by means of the video surveillance system at issue fulfils the conditions laid down in Art. 7(f) of Directive 95/46/EC.

In the case at issue (Case C-708/18, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*), the referring Romanian Court had to deal with an action brought by an owner of an apartment located in a residential building. The apartment owner applied for an order that the association of co-owners take out of operation the building's video surveillance system and remove the cameras installed in the common parts of the building because the instalment is contrary to EU's data protection law (Art. 6(1) lit. c) and Art. 7 lit. f) Directive 95/46, and Arts. 7, 8, 52 of the Charter).

The CJEU stressed that video surveillance systems processing personal data are lawful under the following three conditions:

First, the data controller or by the third party or parties to whom the data are disclosed must pursue a legitimate interest. In the case at issue, this condition is generally fulfilled if the controller seeks to protect the property, health, and life of the co-owners of a building. The extent to which the interest must be "present and effective" at the time of data processing did not need to be decided by the CJEU because the video surveillance system was installed after thefts, burglaries, and acts of vandalism had occurred.

Second, personal data must be processed for the purpose of the legitimate interests pursued; it is settled case law in this regard that derogations and limitations in relation to the protection of personal data must apply only insofar as is strictly necessary. In other words, it must be ascertained that the legitimate data processing interests pursued by video surveillance cannot reasonably be as effectively achieved by other means that are less restrictive of the fundamental rights and freedoms of data subjects. In addition, the processing must adhere to the "data minimisation principle" enshrined in Art. 6(1) lit. c) of Directive 95/46. The CJEU considered the requirements in relation to proportionality to have been met in the present case because the co-owners had installed an intercom/magnetic card system at the entrance of the building as an alternative measure, which proved to be insufficient. The CJEU points out, however, that the referring court must assess whether aspects of the data minimisation principle were upheld, e.g., determine whether it is sufficient if the video surveillance operates only at night or outside normal working hours, and whether it blocks or obscures images taken in areas where surveillance is unnecessary.

Third, the referring court must ensure that the fundamental rights and freedoms of the person affected by the data protection do not take precedence over the legitimate interest pursued. This necessitates a balancing of opposing rights and interests, which depends on the individual circumstances of each particular case in question. According to the CJEU, the following guidelines come to the fore here:

- Member States cannot exclude (categorically and in general) the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in any particular case;
- Such balancing must take into account the seriousness of the infringement of the data subject's rights and freedoms. It is important whether the data are accessed from public or non-public sources. Processing of data from non-public sources implies that the infringement is more serious because information relating to the data subject's private life will thereafter be known by the data controller and possibly to third parties;
- Account must be taken, *inter alia*, of the nature of the personal data at issue, in particular of the potentially sensitive nature of these data, and of the nature and specific methods of processing the data, in particular of the number of persons having access to these data and the methods of accessing them;
- For the purpose of the balancing exercise, the data subject's reasonable expectations are also relevant, namely that his/her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data;
- Lastly, all these factors must be balanced against the importance (for all the co-owners of the building concerned) of the legitimate interests pursued in the instant case by the video surveillance system at issue, inasmuch as it seeks essentially to ensure that the property, health, and life of those co-owners are protected.

The final assessment of this balancing has been left to the referring Romanian court.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union