CASE NOTE

Is Your Video Surveillance Legitimate under EU Data Protection Rules?

Emma Flett
Partner, Kirkland & Ellis LLP

Jacqueline Clover
Associate, Kirkland & Ellis LLP

CCTV; Common parts; EU law; Legitimate processing; Right to respect for private and family life; Romania; Surveillance

On a reference from a Romanian court, the Court of Justice of the European Union (CJEU), in ruling on the compatibility with EU laws of national legislation allowing the use of CCTV in the common parts of a resident building for safety and security purposes, has provided useful guidance for data controllers on assessing whether they can rely on the legitimate interests lawful basis for processing personal data.[1]

Background

In April 2016, the association of co-owners of an apartment block, M5A, approved the installation of video surveillance cameras in the common parts of the building. The claimant, TK, who owned an apartment in the building, objected and brought an action in the Romanian courts seeking the removal of the cameras on the ground that the CCTV system constituted an infringement of the right to respect for private life.

The association's case was that it had been necessary to install a video surveillance system in order to monitor as effectively as possible who entered and left the building, since the lift had been vandalised on many occasions and there had been burglaries and thefts in several apartments and the common parts. The association also stated that other measures which it had taken previously, specifically the installation of an intercom/magnetic card entry system, had not prevented repeat offences of the same nature being committed.

The Romanian court decided to refer the case to the CJEU for guidance on whether arts 6(1)(c) and 7(f) of the Data Protection Directive (95/46) (the Directive),[2] read in light of arts 7 and 8 of the EU Charter of Fundamental Rights, precluded national law from allowing installation of a system of video surveillance installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the data subjects' consent.

Decision

The CJEU began by observing that the surveillance in the form of a video recording of persons, which is stored in a continuous recording device, i.e. the hard disk drive, constituted automatic processing for the purposes of art.3(1) of the Directive.[3] Consequently, such processing must comply, first, with the principles relating to data quality set out in art.6 and, secondly, with one of the criteria for making processing legitimate listed in art.7.[4]

Three cumulative conditions

The relevant criterion in this case was legitimate interests (art.7(f)). Following its ruling in *Rīgas*,[5] the court identified three cumulative conditions in order for processing of personal data to be lawful under that provision: first, the pursuit of a legitimate interest by the data controller or by a third party or parties to whom the data is disclosed; secondly, the need to process personal data for the purposes of the legitimate interest pursued; and thirdly, the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued.

Processing for the purpose of the legitimate interest

The CJEU was satisfied that the objective which the data controller essentially sought to achieve by installing the CCTV system, namely protecting the property, health and life of the co-owners of the building, was likely to be characterised as a "legitimate interest" within the meaning of art.7(f). The Romanian court, however,

[1] *TK v Asociația de Proprietari bloc M5A-ScaraA* (C-708/18) EU:C:2019:1064; [2020] 2 C.M.L.R. 17.
[2] Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
[3] See *Ryneš v v Urad pro ochranu osobnich udaju* (C-212/13) EU:C:2014:2428; [2015] 1 W.L.R. 2607.
[4] See *Google Spain SL v Agencia Espanola de Proteccion de Datos (AEPD)* (C-131/12) EU:C:2014:317; [2014] 3 C.M.L.R. 50.
[5] See *Valsts Policijas Rigas Regiona Parvaldes Kartibas Policijas Parvalde v Rigas Pasvaldibas SIA Rigas Satiksme* (C-13/16) EU:C:2017:336; [2017] 3 C.M.L.R. 39.

questioned whether art.7(f) meant that the interest pursued by the controller must, first, be "proven" and, secondly, be "present and effective at the time of the data processing". In that regard, the CJEU agreed with the submissions of the Romanian and other governments that the controller responsible for the processing of personal data or the third party to whom that data is disclosed must pursue legitimate interests justifying that processing, and those legitimate interests must be present and effective as at the date of the data processing and must not be hypothetical at that date. The court was, however, clear that this did not necessarily require, at the time of examining all of the circumstances of the case, that the safety of property and individuals was previously compromised.

In the current case, the CJEU was satisfied that the condition relating to the existence of a present and effective interest seemed in any event to be fulfilled, since the referring court noted that thefts, burglaries and acts of vandalism had occurred before the CCTV system was installed and that despite the previous installation, in the entrance of the building, of a security system comprising an intercom/magnetic card entry.

Necessity

Further, insofar as art.7(f) also required that the processing of the personal data was necessary for the purposes of the legitimate interest pursued, the CJEU was clear that the legitimate interests of ensuring the security of property and individuals and preventing crime could not reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of individuals, in particular the rights to privacy and the protection of personal data. In this respect, the CJEU noted that the processor must also comply with the data minimisation principle under art.6(1)(c) of the Directive, according to which personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". Here, it was common ground that alternative measures were initially put in place but proved insufficient. In addition, the video surveillance device was limited only to the common parts of the building and the approach to it.

However, as the court also observed, the proportionality of the processing by a video surveillance device should be assessed by taking into account the specific methods of installing and operating that device which must limit its effect on the rights and freedoms of individuals while ensuring the effectiveness of the system. Consequently, the controller must examine, for example, whether it is sufficient that the video surveillance operates only at night or outside normal working hours, and must block or obscure the images taken in areas where surveillance is unnecessary.

Balancing rights and interests

Finally, insofar as art.7(f) required a balancing of opposing rights and interests, the CJEU observed that this depended on the individual circumstances of a particular case and that the processing of data obtained from non-public sources is likely to constitute a more serious infringement of the individual's rights which must be taken into account and balanced against the legitimate interest pursued by the data controller. Account must also be taken of the nature of the personal data, in particular of its potentially sensitive nature, and of the nature and specific methods of processing the data, in particular of the number of persons having access to the data and methods of accessing the data. The court stressed that the individual's reasonable expectations that the personal data will not be processed when, in the circumstances of the case, that person cannot reasonably expect further processing of those data, were also relevant for the purposes of the balancing exercise. However, in the current case those factors must be balanced against the importance of all the co-owners of the building of the legitimate interest pursued by the video surveillance system, inasmuch as it sought essentially to ensure that the property, health and life of those co-owners were protected.

Conclusion

Applying these principles, the CJEU concluded that the Directive, read in the light of the Charter, did not preclude national law which authorised the installation of a video surveillance system such as the system in this case, in the common parts of a residential building for the purposes of pursuing the legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects, where processing of the personal data by that system fulfilled the conditions laid down in art.7(f) (that being a matter for the Romanian court to determine).

Comment

Romanian law aside (indeed the CJEU stressed that "Member States cannot definitively prescribe … the result of the balancing of the opposing rights and interests" for the purpose of legitimate interest),[6] the value in this CJEU judgment lies in the court's reiteration and further illustration of the conditions that sustain legitimate interests as a lawful basis for processing personal data, particularly its exposition of the factors that may apply to the assessment of whether those conditions are fulfilled in the context of CCTV and video surveillance. Although the proceedings were governed by the Directive, which has since been repealed and replaced, the legitimate

[6] *TK v Asociația de Proprietari bloc M5A-ScaraA* (C-708/18) EU:C:2019:1064; [2020] 2 C.M.L.R. 17 at [53].

interests provision under the GDPR is in similar terms.[7] Indeed, in its guidance on legitimate interests under the GDPR, the UK Information Commissioner's Office (ICO) applies the three-part test formulated in the *Rīgas* case. For data controllers this means ensuring, through carrying out a legitimate interests assessment, that there is a legitimate interest behind the processing (the "purpose test"); ensuring the processing is necessary for that purpose (the "necessity test"); and assessing whether the legitimate interest is overridden by the individual (the "balancing" test). As the guidance states, and as this latest case demonstrates, it is not sufficient for you to simply decide that it is in your legitimate interest to process personal data. All parts of the test must be examined and satisfied in a legitimate interests assessment, and what is required of the data controller will vary from case to case. This means ensuring that there are no alternative ways of achieving the objective of the processing and, potentially, actually deploying alternative measures to test whether or not they are, in fact, sufficient, before deploying a system which involves the processing of personal data and carrying out a balancing exercise to determine whether the legitimate interests are overridden by the rights and freedoms of the individuals concerned.

[7] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 [2016] OJ L119/1.