MORRISON | FOERSTER

Legal Updates & News

Bulletins

Spain's Strict New Limitations on Video Surveillance

March 2009
by Teresa Basile, Janelle J. Sahouria, Christine E. Lyon

Privacy and Data Security Update, March 25, 2009

In recent months, Spain has imposed substantial new restrictions on video surveillance and other types of videotaping of individuals without their consent. These developments underscore important differences between U.S. and Spanish privacy law.

Related Practices:

- Privacy and Data Security
- Technology Transactions

Spain's approach to video surveillance is illustrated by a recent enforcement action, in which Spain's Data Protection Authority (the "AEPD") fined a 20-year-old for posting a video on YouTube without the consent of the individual shown in the video.[1] This case received significant media attention, as the video showed a group of teenagers harassing a disabled person, and led to public outrage over the mistreatment of the victim. The AEPD investigated the incident and determined that the videotaping violated Spain's Data Protection Law (the "LOPD") because the victim had not consented to being recorded. In a subsequent statement, the AEPD explained that the LOPD generally requires a person or entity making a video recording to obtain the consent of each person who can be identified in the video recording: "The collection of images of a person, as long as [the images] allow the identification of that person, is regulated by [the LOPD] and requires the consent of the person involved."[2] This consent obligation applies even if the individual is videotaped in a public location, as discussed below.

Applicability of Spain's Data Protection Law to Video Surveillance

The LOPD provides that "the processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law."[3] Processing is broadly defined to include collection, recording, storage, or transfer of personally identifiable information.[4] The AEPD has explained that "collecting the images of a person in a public place constitutes data processing" as long as the images allow identification of that person.[5] In other words, Spain recognizes an inherent right not to be videotaped without consent, even in public locations. This is a noteworthy difference from U.S. law, which generally recognizes a privacy interest only if the individual had a reasonable expectation of privacy in the location where the video surveillance occurred.

This leads to the question of whether a company operating in Spain may use video surveillance within its facility. In general, video surveillance may serve multiple functions: protecting the safety of employees and customers in publicly accessible areas (such as retail areas), identifying theft by customers or employees, and deterring theft and other misconduct. The AEPD recently issued guidelines for video surveillance,[6] which attempt to balance individual privacy rights with the legitimate purposes served by video surveillance.

New Video Surveillance Guidelines

The new Video Surveillance Guidelines ("the Guidelines") must be read as a complement to Instruction 1/2006[7] on the processing of personal data when using cameras or video cameras for security purposes.

In general, the processing of personal data by means of video surveillance systems requires the data subject's consent. Exceptions to this rule can be found in the Spanish Private Security Law[8] and in section 20 of the Labor Statute[9] as described in more detail below.

When using video surveillance systems for security purposes, private companies must comply with certain requirements.

First, before creating any databases that contain video surveillance files, private companies must notify the AEPD of their intention to create video surveillance files. In comparison, there is no need to notify the AEPD when video surveillance systems are used to simply play or broadcast images in real time (without storing such images as files).

Second, private companies have a duty of information vis-à-vis those individuals whose images are to be captured. Organizations must place at least one sign in zones that are under video-surveillance, notifying individuals that they are under surveillance. These signs must be placed "in a sufficiently visible zone, in open as well as enclosed spaces." In addition, organizations must provide affected individuals with certain information as required under the LOPD.[10]

Third, organizations must ensure that technical and organizational measures are in place to guarantee the security of the data, and to protect against alteration, loss, or unauthorized processing or access to the video surveillance files.

Lastly, the video surveillance files can be stored for a maximum of one month, unless data are needed for purposes of criminal or administrative investigations.

In addition to the above rules, another set of requirements is prescribed for those organizations wishing to use video cameras for monitoring purposes in the workplace. Section 20.3 of the Spanish Labor Statute allows the video monitoring of employees, without their consent, in order to check that employees are fulfilling their labor obligations. Nonetheless, there are minimum requirements to be observed by the organizations:

- There must be no other alternatives or more appropriate means to accomplish this purpose than the use of such video surveillance;
- The implementation of video surveillance systems must be strictly limited to the uses and locations necessary for fulfilling the purpose of the employee monitoring;
- Video surveillance systems cannot be located in facilities meant for employees' private use (*e.g.*, toilets, restrooms, or recreation rooms);[11]
- Employees' right to their private lives must be respected, and private conversations cannot be recorded;
- Organizations must fully respect their employees' information rights (i) by notifying the employees' union representatives that a video surveillance system is to be put in place, (ii) by placing the information sign described above as set out in the Instruction 1/2006, and (iii) by means of a personalized notice;
- In cases where video surveillance files are created, the notification requirement described above applies;
- Employees' images must be deleted within 30 days, unless these data are needed for investigative purposes (crimes or non-compliance with labor obligations);
- Employees' rights of access to and erasure of their images must be guaranteed;
- Organizational and technical measures to secure data must be implemented; and
- The company retained to install the video surveillance equipment must comply with specific requirements pursuant to Spanish sector-based law.

Additionally, video surveillance systems installed by financial entities are governed by separate sector-specific laws.[12]

Penalties for Non-Compliance

The AEPD is empowered to enforce the LOPD and levy fines for violations. Penalties are based on the severity of the infringement, but the fines can be very harsh compared to those imposed in other European Union Member

States. In 2007, the AEPD collected €19.6 million in fines.[13] Additionally, the Spanish Criminal Code allows imprisonment for certain violations of the LOPD (*e.g.*, unauthorized access to personal data, use, or theft of such data).[14]

Practical Implications

While Spain has stricter rules on video surveillance than many other EU Member States, Spain's approach demonstrates general principles that apply in all EU Member States:

1) Privacy rights in the EU are not limited to situations in which an individual has a reasonable expectation of privacy, or a reasonable expectation that he or she will not be observed. To the contrary, EU data protection laws recognize an inherent right of privacy against surveillance, even in the workplace or other public places.

2) A company cannot diminish these EU privacy rights simply by announcing its intent to conduct surveillance or monitoring. Notice is a fundamental requirement of EU data protection laws, but notice does not in itself suffice, because other obligations arising under those laws must also be met.

For these reasons, companies operating in Spain or other EU Member States should exercise caution in implementing video surveillance or other monitoring practices, even if the same practices are acceptable in the U.S. or other countries.

Footnotes

[1] See Resolution R/01800/2008 of December 30, 2008 ("December 30, 2008 resolution"), available in its Spanish version at: https://www.agpd.es/portalweb/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00479-2008_Resolucion-de-fecha-30-12-2008_Art-ii-culo-6.1-LOPD.pdf.

[2] See AEPD statementof February 4, 2009, available in its Spanish version at: https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2009/notas_prensa/common/febrero/040209_AEPD_sanciona_responsables_grabacion_discapacitado.pdf.

[3] Organic Law on Data Protection 15/1999 of December 13, Art. 6. The law defines personal information as "any information concerning identified or identifiable natural persons." *Id*. at Art. 3(a). However, there is an exception for a natural person in the course of a purely personal or household activity. *Id*. at Art. 2(2)(a).

[4] Specifically, processing of data is defined as "operations and technical processes, whether or not by automatic means, which allow the collection, recording, storage, adaptation, modification, blocking and cancellation, as well as assignments of data resulting from communications, consultations, interconnections and transfers." *Id*. at Art. 3(c).

[5] See points of law of December 30, 2008 resolution, para. II, at page 8.

[6] Guía de Videovigilancia available in Spanish at: https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf.

[7] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, available in English at: https://www.agpd.es/portalweb/english_resources/regulations/common/pdfs/Instruccion_videovigilanci_EN.pdf.

[8] Ley 23/1992 de 30 de Julio, de Seguridad Privada, available in Spanish at: http://noticias.juridicas.com/base_datos/Admin/l23-1992.html.

[9] Available in its Spanish version at: http://noticias.juridicas.com/base_datos/Laboral/rdleg1-1995.t1.html.

[10] Section 5.1 of the LOPD requires the following information to be provided to the data subject: (i) that a file or personal data processing operation exists, including the purpose of collecting the data and the recipients of the information; (ii) the obligatory or mandatory nature of the reply; (iii) the consequences of obtaining the data or

refusing to provide them; (iv) the possibility of exercising rights of access, rectification, erasure and objection, and (v) the identity and address of the data controller (that is, the decision-maker as to why and how personal data must be processed) or its representative, if any.

[11] Within the U.S., many states also have laws prohibiting video surveillance or audio surveillance in restrooms, locker rooms, and changing rooms.

[12]Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana available in Spanish at: http://noticias.juridicas.com/base_datos/Admin/lo1-1992.html; and Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, available in Spanish at: http://noticias.juridicas.com/base_datos/Admin/rd2364-1994.html.

[13] See https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/memoria_AEPD_2007.pdf.

[14] Spanish Criminal Code 1995, Articles 197-201. The 1995 Criminal Code is available in Spanish at: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html.
