CONTROLES DE ACCESO A CCPP

Las nuevas tecnologías han permitido a las Comunidades de Propietarios aumentar la seguridad de las personas e instalaciones. No son pocas las Comunidades que, a día de hoy, cuentan con cámaras de videovigilancia, sistemas de tarjetas magnéticas o contraseñas de acceso privadas. Además, recientemente, se ha popularizado el **uso de sistemas de control de acceso a las instalaciones y recintos de las Comunidades de Propietarios a través de herramientas que tratan datos biométricos** (por ejemplo, la huella dactilar). Sin embargo, estos sistemas no están exentos de riesgo, puesto que tratan datos de carácter especial.

La instalación de estos nuevos métodos debe tener en cuenta la normativa de protección de datos personales: ¿pueden recabarse datos biométricos para realizar un control de acceso?, ¿qué medidas de seguridad se deben tener en cuenta? ,¿existen diferencias respecto a los controles aplicados a propietarios, trabajadores y proveedores o, incluso, terceros ajenos a la Comunidad?

01 Controles de presencia mediante sistemas biométricos

En primer lugar, tenemos que saber que los controles de presencia son un conjunto de tratamientos utilizados para realizar una vigilancia en el acceso a determinadas zonas. **El control de presencia puede tener como finalidad el control de acceso laboral, el no laboral o permitir el registro de la jornada laboral de personas trabajadoras.**

En la práctica, en las Comunidades de Propietarios pueden instalarse para supervisar el acceso de propietarios o terceros a determinados espacios como, por ejemplo, piscinas, gimnasios, trasteros o salas comunes, así como para controlar el acceso de empleados de la Comunidad y registrar su jornada laboral.

Adicionalmente, si mediante el uso de estos controles se recaban características físicas de los usuarios mediante, por ejemplo, las huellas dactilares o el reconocimiento facial, debemos tener en cuenta que se estarán tratando **datos biométricos.**

Datos biométricos

Son datos personales de carácter especial, según la definición del Reglamento de la Unión Europea 2016/679, de 27 de abril, relativo a la protección en el tratamiento de los datos personales de las personas físicas (en adelante RGPD), y pertenecen a una categoría de datos que, si no son tratados con las garantías adecuadas, supone un riesgo para los derechos y libertades de las personas.

Teniendo claros estos conceptos, vamos a conocer el criterio de la Autoridad de Control de Protección de Datos para el **tratamiento de los datos biométricos en los controles de acceso.**

02 Criterio de la Agencia Española de Protección de Datos

La **Agencia Española de Protección de Datos** (en adelante AEPD), publicó el pasado 23 de noviembre de 2023, la **"Guía sobre tratamientos de control de presencia mediante sistemas biométricos"**. En dicha guía, se establecen una serie de criterios a tener en cuenta en los controles de acceso que recaben y traten datos biométricos. En numerosas ocasiones, recabar esta tipología de datos es excesivo a la finalidad perseguida y puede quebrantar el principio de minimización de datos establecido en el artículo 5 del RGPD.

La AEPD considera que el tratamiento de datos biométricos en los controles de acceso supone un **tratamiento de alto riesgo**. Además, según el RGPD, debe tenerse en cuenta que se establece una prohibición general del uso de los datos biométricos, salvo en aquellos casos tasados en el propio artículo 9.2 del propio Reglamento Europeo.

"El tratamiento de los datos biométricos sólo deberá aplicarse en situaciones excepcionales, cuando sea absolutamente necesario para garantizar la finalidad perseguida y aplicando una de las condiciones previstas en el artículo 6 del RGPD que legitime el tratamiento de los datos"

03 Aspectos a tener en cuenta antes de realizar el control

Antes de proceder a instalar un control de acceso que recabe datos biométricos en una Comunidad, se deberá realizar una **Evaluación de Impacto para la Protección de Datos,** que tenga en cuenta y supere los **controles de idoneidad, necesidad y proporcionalidad del tratamiento.**

- **Control de acceso para fines no laborales** (puede aplicarse para los propietarios de la Comunidad, pero también para los proveedores o para cualquier tercero ajeno a la Comunidad): el tratamiento de los datos biométricos **no podrá ampararse en el consentimiento de los usuarios**, ni tampoco en la ejecución de un contrato o en un interés legítimo.
- **Control de acceso con fines laborales y al registro de la jornada laboral:** el tratamiento **no podrá ampararse en el cumplimiento de las obligaciones establecidas Estatuto de los Trabajadores**, ya que dicha normativa no prevé expresamente el uso de los datos biométricos.

La AEPD reconoce que **actualmente no existe en la normativa legal española una norma con rango de ley que permita utilizar datos biométricos con la finalidad de registrar la jornada laboral o permitir el control de acceso con fines laborales.**

04 Conclusiones

Por todo lo expuesto, el ámbito de actuación de las Comunidades de Propietarios a la hora de implementar un control de acceso que trate datos biométricos deberá tener en cuenta los criterios de la AEPD, que considera que pueden lograrse las finalidades de control de acceso sin necesidad de recabar los datos biométricos de las personas relacionadas con la Comunidad.

De existir medios alternativos que cumplan con las finalidades perseguidas, y supongan una afectación menos invasiva en los derechos de los propietarios, personas trabajadoras y terceros, **los controles de acceso que recaben datos biométricos no serán adecuados** y las Comunidades deberán abstenerse de su instalación.

Incumplir el criterio de la AEPD y la normativa en materia de protección de datos puede comportar sanciones por parte de la AEPD.

T. 902 153 500 | www.iesa.es