

El control empresarial y el uso de la tecnología



Laura Morató | Abogada

lmorato@marimon-abogados.com

Imagínese grabar como uno de sus empleados tiene una conducta inapropiada, o tener prueba de que uno de sus exempleados, antes de comunicar su baja, se descargó la base de datos de los clientes de la empresa. Ahora, piense en tener esas pruebas y no poderlas utilizar.

Este escenario no es meramente hipotético; constituye una realidad frecuente en el mundo corporativo, originado principalmente por el desconocimiento de la empresa en esta materia.

Así surge la pregunta, ¿puede el empresario controlar a sus trabajadores?

El control de la actividad laboral lo encontraremos regulado en el artículo 20.3 del Estatuto de los Trabajadores, que faculta al empresario para adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Podemos estar hablando de medidas de geolocalización, videovigilancia, controles en los dispositivos electrónicos y hasta cierto punto, del correo electrónico.

Sin embargo, la implementación de estas medidas conlleva, en muchas ocasiones, un tratamiento de datos personales, obligando al empresario a cumplir la normativa de protección de datos y a estar atento a los siguientes requisitos esenciales:

1. Videovigilancia

La imagen de una persona se considera un dato personal cuyo tratamiento exige cumplir con el deber de informar. En el ámbito de la videovigilancia, es común que las empresas notifiquen de sus derechos a las personas afectadas a través de señalizaciones amarillas que anuncian la existencia de cámaras de seguridad.

Cuando se recurre a la videovigilancia no solo para asegurar la protección de los bienes e instalaciones, sino también para el control laboral, resulta imprescindible notificar tal hecho, de manera anticipada, expresa y clara, tanto a los trabajadores como a sus representantes legales. También es fundamental que la empresa cuente con evidencia documental de este proceso de información, como podría ser la firma de un documento por parte de los empleados.

2. Geolocalización

La normativa específica, como el artículo 90 de la LOPDGDD, permite el empleo de sistemas de geolocalización para el control de los trabajadores siempre y cuando se realice una notificación previa al empleado. Es relevante subrayar que el propósito de la geolocalización debe ser el seguimiento de herramientas de trabajo pertenecientes a la empresa, como pueden ser teléfonos móviles, ordenadores o vehículos, y no la propia persona trabajadora. Respecto a esta medida, cabe tener en cuenta dos aspectos para limitar su uso: (i) cuando se permite el uso del dispositivo para fines personales, y (ii) cuando los empleados no disponen de herramientas de empresa y utilizan sus propios dispositivos. En estos casos, se deben definir excepciones en el seguimiento para salvaguardar la privacidad del empleado.

3. Control de los dispositivos electrónicos

El control sobre los dispositivos electrónicos por parte de los empleadores presenta un desafío creciente para la privacidad de los trabajadores. Para que esta vigilancia sea legítima, debe adherirse a principios de transparencia, proporcionalidad, mínima intervención y adecuación, garantizando que se realice exclusivamente para comprobar el cumplimiento laboral.

La LOPDGDD enfatiza que los trabajadores tienen derecho a su intimidad incluso cuando usan dispositivos digitales en el trabajo, salvo que anteriormente se les haya informado del uso estrictamente profesional de estos dispositivos. Además, los empleadores deben desarrollar políticas de privacidad y uso de los dispositivos y poseer evidencia concreta de que estas políticas han sido comunicadas.

4. El deber de informar de las medidas de control

Un caso reciente en el Tribunal Superior de Justicia de Madrid (STSJ M 13457/2023) ilustra la importancia de este requisito. La corte anuló como prueba en un procedimiento de despido disciplinario unos correos electrónicos que evidenciaban irregularidades por parte de un trabajador, debido a que la empresa no pudo demostrar que el trabajador había sido debidamente informado sobre la política de protección de datos. A pesar de que existían políticas internas establecidas, la falta de un acuse de recibo por parte del empleado despojó a la empresa del derecho a acceder a los correos electrónicos del trabajador.

Este fallo pone de manifiesto la tensión continua entre la autonomía privada y los derechos fundamentales de los trabajadores, y cómo la interpretación de los límites del poder de supervisión del empleador sigue siendo un área llena de incertidumbre. En este contexto, es necesario que cada situación sea evaluada individualmente, teniendo en cuenta no solo las regulaciones existentes sino también los principios éticos subyacentes que rigen nuestra sociedad.

En resumen, mientras las empresas navegan por las aguas turbulentas del control mediante dispositivos electrónicos, es crucial que mantengan un enfoque equilibrado, fundamentado en el respeto por la privacidad de los empleados y en la comunicación clara de las políticas.

El control empresarial y el uso de la tecnología

Departamento de Tecnología y Protección de Datos

Este documento es una recopilación de información jurídica elaborada por Marimón Abogados. La información que se incluye en el mismo no constituye asesoramiento jurídico alguno. Los derechos de propiedad intelectual sobre este documento son titularidad de Marimón Abogados. Queda prohibida la reproducción en cualquier medio, la distribución, la cesión y cualquier otro tipo de utilización de este documento, ya sea en su totalidad, ya sea de forma extractada, sin previa autorización. **Marimón Abogados © 2024**