G A _ P

Gómez-Acebo & Pombo

# La procedencia del despido disciplinario y la protección de la información empresarial

**Francisco Pérez Bes**

*Of counsel*

Director del Área de Derecho y Economía Digital de Gómez-Acebo & Pombo

*El Juzgado de lo Social de Gijón dicta una sentencia en la que acuerda la procedencia del despido disciplinario de un trabajador que descargaba información empresarial sin autorización.*

Uno de los conflictos que comienzan a tener mayor incidencia en el ámbito empresarial es el relacionado con la responsabilidad del trabajador de acatar y respetar las medidas organizativas que implanta el empresario en cumplimiento de sus obligaciones de tratamiento de información personal, cuyo deber de custodia recae en la empresa.

Esta responsabilidad también se refleja en el deber del trabajador de mantener la buena fe contractual y de evitar el abuso de confianza en el desempeño del trabajo, tal y como establece el artículo 54.2*d* del Estatuto de los Trabajadores.

En el caso objeto de análisis, el Jugado de lo Social de Gijón, en su Sentencia de 21 de agosto del 2019, consideró acorde a derecho, por transgredir la debida lealtad hacia su empleador, el despido disciplinario de un trabajador que fue descubierto efectuando copias, sin permiso, de información sobre la actividad de la empresa (en este caso, de una asesoría jurídica) en la que se encontraban —entre otros relacionados con expedientes y similares— datos de carácter confidencial dotados de especial protección.



*N. de la C.*: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

Además, el volcado de la información se había llevado a cabo por medio de una plataforma a la que el empresario no podía tener acceso, lo que configuraba una situación en la que dicho empleado podría utilizar con posterioridad la información copiada para fines ajenos a la actividad de la empresa. En tal caso, se estaría poniendo en grave peligro la confidencialidad de esos datos, lo que podría comportar graves consecuencias para la empresa al ser ella la responsable de custodiar y proteger esa información, así como de hacer de ésta un adecuado tratamiento, conforme dispone la normativa aplicable.

En efecto, en lo que a las obligaciones del responsable del tratamiento se refiere, el artículo 24 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), obliga al responsable del tratamiento a aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de los datos personales es conforme con el mencionado reglamento. Para ello —añade—, el responsable deberá tener en cuenta la propia naturaleza del tratamiento y los riesgos para los derechos y libertades de las personas físicas.

Entre estas medidas se cuentan el desarrollo e implementación de políticas de protección de datos —que deberán ser proporcionadas en relación con las actividades de tratamiento—, así como otras iniciativas que permitan reducir al máximo el tratamiento de los datos personales, seudonimizarlos lo antes posible o dar transparencia a las funciones y al tratamiento de tales datos, permitiendo a los interesados supervisar el tratamiento de los datos y al responsable del tratamiento crear y mejorar elementos de seguridad.

En el caso que ahora nos ocupa, la titular de la asesoría observó que el ordenador del empleado incumplía las instrucciones acordadas y conocidas por los empleados, según las cuales todos los ordenadores de los trabajadores debían permanecer apagados, por motivos de seguridad, a partir de cierta hora.

Al acceder casualmente a la pantalla del ordenador, descubrió que se estaba ejecutando, de manera no autorizada, una descarga de toda la información de la asesoría a un servicio externo (la conocida aplicación «mega» ubicada en Nueva Zelanda) por medio de una cuenta abierta con una dirección de correo electrónico de la empresa, pero a cuya contraseña no tenía acceso la titular del negocio afectado, como tampoco lo tenía a la dirección de vinculación utilizada por el empleado para poder acceder a esa información llegado el caso de que no pudiera acceder de forma directa mediante la propia cuenta de usuario.

La argumentación del juez a la hora de valorar si la actuación del empresario contraviene los derechos fundamentales del trabajador es clara. Y, aunque recuerda que la jurisprudencia europea (así como la española) acota y restringe la posibilidad de que los empresarios fiscalicen los medios informáticos que ponen a disposición de los trabajadores en la medida en que

pueden llegar a conocer hechos que afecten a la intimidad de los trabajadores, en este caso no entiende que la actuación del empresario demandado haya afectado —ni siquiera potencialmente— a datos personales del empleado ni a otros sobre los que el derecho a la intimidad extienda su protección.

Por el contrario —continúa—, nos encontramos ante un encuentro casual provocado en el momento en el que el empresario se disponía a apagar el ordenador del trabajador, conforme a las órdenes e instrucciones que todos conocían, siendo ése el momento en que se percató de que se estaba llevando a cabo una copia de información sin autorización —lo que incumplía las obligaciones recogidas en la ley de protección de datos personales— a la que la empresa, en cuanto responsable del tratamiento, no tenía acceso.

Tal circunstancia se engloba, a juicio del juez, en un supuesto de grave deslealtad hacia el empleador, por lo que considera que el despido disciplinario es procedente conforme al artículo 54 del Estatuto de los Trabajadores.

Este caso vuelve a poner de manifiesto la importancia de contar con políticas claras y conocidas por los empleados en las que se establezcan instrucciones de uso de los activos informáticos de la empresa que estén alineadas con los principios de protección de la información empresarial en general y de los datos personales en particular, así como la conveniencia de implementar otras medidas técnicas y organizativas con las que se garantice la adecuada custodia y seguridad de la información.