

¿Cuándo puede (y cuándo no) la empresa espiar mis correos?

El TEDH fija que la empresa debe avisar al trabajador de que le investigará

Los protocolos telemáticos permiten hacerlo, pero bajo un buen número de condiciones

Javier García Ropero

Pablo Sempere

6 de septiembre de 2017

En enero del pasado año, el caso del ingeniero rumano Bogdan Barbulescu, despedido en 2007 por enviar desde el correo de la empresa mensajes de carácter personal y privado a amigos y familiares, llegó al Tribunal de Derechos Humanos de Estrasburgo (TEDH). Entonces, la Gran Cámara falló en favor de la compañía, aludiendo que la vigilancia de las comunicaciones por parte del empleador había sido razonable en un procedimiento disciplinar. Hoy, sin embargo, el citado caso volvió a dar que hablar, cuando el mismo tribunal tomó la determinación de enmendar la decisión y dar la razón al trabajador.

¿Puede una empresa acceder a los correos de sus trabajadores?

Sí, la empresa puede vigilar los correos internos de sus profesionales, así como las redes sociales utilizadas desde los dispositivos facilitados por el empleador. Pero no de cualquier forma. Hay una lista de matices que, si se descuidan, pueden terminar quitando la razón a la compañía, como ha terminado ocurriendo en el caso de Barbulescu. El primer aspecto a tener en cuenta, explica el jefe del área de laboral del despacho Pérez-Llorca, Daniel Cifuentes, es que el trabajador debe ser consciente mediante un aviso previo de la empresa de que sus equipos pueden ser monitorizados, algo que el TEDH estima que no sucedió en el caso del ingeniero rumano, pese al despido previo de otra compañera por motivos similares. Pero no todo vale. “Ese control debe ser proporcional, necesario y lo menos invasivo posible, evaluando el choque entre el derecho del interés empresarial y la privacidad del trabajador”, apunta.

¿Dónde establece la empresa esa capacidad?

En los llamados protocolos telemáticos, o en el propio convenio colectivo de la compañía. Con ellos, se arroga el derecho de investigar el uso que sus trabajadores hacen de las herramientas informáticas que les facilita. Pero no es una barra libre. Como explica Ignacio Jabato, socio de laboral de Cuatrecasas, Gonçalves Pereira, sentencias anteriores del Tribunal Supremo y del Constitucional en España dan como suficiente la existencia de ese protocolo para poder investigar, siempre que se justifique la proporcionalidad, la idoneidad y la necesidad de la medida. “La novedad de la sentencia del TEDH está en el aviso previo al trabajador de cómo y en qué periodo se va a investigar. Las empresas deberían revisar y validar si sus protocolos cumplen con esto”, afirma Jabato.

¿Cómo puede la empresa ver que no se usa el correo para fines laborales?

Daniel Cifuentes analiza algunas particularidades de la sentencia. “Deja claro que para que exista esta monitorización, la empresa debe tener sospechas fundadas de que el empleado está faltando a los acuerdos contractuales, pero sin invadir su intimidad”. Este experto lo ilustra con determinados supuestos, como un posible envío masivo de correos, alejado de lo que la compañía entiende como normal, una cantidad de archivos enviada que no concuerda con la media o el intercambio de mensajes con cuentas de dominios web con los que la empresa no trabaja.

¿Y qué ocurre con el contenido de los mensajes?

El TEDH le da la razón a Barbulescu, entre otras cosas, por desconocer que la empresa podía llegar a investigar hasta lo que decía en sus mensajes. “Esto supone una vulneración de la privacidad. Deben respetarse los principios de idoneidad y proporcionalidad”, recuerda el socio de Sagardoy Abogados, Alberto Sancho.

Sin embargo, el protocolo telemático de una compañía puede dejar claro que no hay expectativa de privacidad, es decir, que en tanto el trabajador usa herramientas proporcionadas por la empresa, esta puede investigar lo que se escriba siempre que tenga indicios de mal uso y de que supere el triple juicio de idoneidad, necesidad y proporcionalidad para hacerlo. “Si no, sería imposible demostrar que un empleado ha estado enviando información confidencial a una empresa de la competencia, por ejemplo. Lo que no se puede es, de forma indiscriminada, leerlo todo”, argumenta Ignacio Jabato.

¿Se puede hacer de forma sistemática e indiscriminada?

El socio director del área laboral de Abdón Pedrajas & Molero, Iván López, recomienda comunicar con asiduidad y de forma detallada cuáles son los controles, así como no generalizarlos y dirigirlos hacia el objetivo en cuestión: “Se pueden analizar los dominios de destino, el volumen de correos o la cantidad de tráfico, así como utilizar filtros que impidan el acceso total a los contenidos. Todo lo que no implique llevar a cabo un seguimiento exhaustivo y desproporcionado”. Porque convertir prácticas de este tipo en una política de recursos humanos no es lo más cómodo para un trabajador. “Cualquier empresa tiene cosas más importantes que hacer que controlar el correo de los empleados. Llegar a estos extremos solo debe ser para casos muy concretos e identificados”, explica Cristina Hebrero, directora de People Matters.

Protocolos detallados

Otro punto interesante que planea la sentencia, opina Daniel Cifuentes, es que cuestiona la política de la compañía rumana. “Parece que había comunicado que los equipos podían ser monitorizados, pero no había especificado cómo”. Es decir, no vale con que existan políticas generales, sino que deben estar reguladas y explicadas, de forma explícita, para cada medio y cada plataforma: “No es lo mismo Messenger, que el correo interno, el correo externo o las redes sociales. La empresa debe individualizar las normas y el supuesto de cada herramienta para que el empleado conozca todos los posibles a la perfección”, añade. “Cuanto mayor detalle tenga el protocolo telemático, sobre qué se puede hacer y qué no, qué es un uso abusivo, o de qué manera se va a monitorizar, mejor”, dice Ignacio Jabato, de Cuatrecasas,

¿Basta con que el protocolo sea público y accesible?

No. El abogado de Cuatrecasas avisa de que no solo basta con que el protocolo sea público para los empleados, por ejemplo, en una intranet. La empresa debe cerciorarse de que estos han accedido a él y, si es posible, que lo han leído. La frase de “el desconocimiento de la norma no exime de su cumplimiento”, en este caso no aplica. El empleado puede argumentar en un juicio que la empresa no le ha insistido, o no le ha informado de forma directa, de que debe cumplir con dicho protocolo.