MARK AIRS (GETTY IMAGES)

ATENCIÓN: SU EMPRESA LE VIGILA

El interés del empresario por supervisar la actividad de sus trabajadores choca con el derecho de estos a su intimidad

POR **RAMÓN OLIVER**

Tenía usted que vivir (...) con la seguridad de que cualquier sonido emitido por usted sería registrado y escuchado por alguien y que, excepto en la oscuridad, todos sus movimientos serían observados". Este pasaje de *1984,* la inmortal novela de George Orwell, describe un mundo en el que los ciudadanos son sometidos a un asfixiante control por parte del Estado, hasta el punto de anular por completo su privacidad. Trasladado al entorno empresarial, el legítimo derecho del empresario a supervisar la actividad y rendimiento de sus trabajadores se topa con los límites que le impone el derecho fundamental de estos, reconocido por la Constitución española, a que sea respetada su intimidad.

El caso de Edward Snowden ha venido a demostrar que las organizaciones necesitan tomar medidas para proteger su información sensible. Porque si la mismísima NSA (Agencia de Seguridad Nacional) norteamericana no está a salvo de que uno de sus empleados filtre datos confidenciales al exterior, ¿quién lo está?

"El 55% de los ataques informáticos que tienen lugar en las organizaciones provienen de empleados con intenciones maliciosas y otras personas en las que la empresa confiaba", destaca Deepak Daswani, experto en ciberseguridad de Deloitte CyberSOC y profesor del máster en Ciberseguridad de IMF Business School. El descontento de estos *insiders* —como se les conoce en el argot— con su situación laboral o sus desavenencias con la dirección suelen estar detrás de estos ataques.

Pero impedir que un empleado hostil se descargue la lista de clientes o pase información a la competencia no es la única preocupación de las empresas. Medir la productividad de la plantilla es otra de sus viejas aspiraciones, un campo en el que los avances tecnológicos han abierto enormes posibilidades. La empresa española WorkMeter ha desarrollado una herramienta que registra el tiempo de conexión de un empleado a aquellas aplicaciones, redes corporativas o dispositivos que utiliza para su trabajo. Es el propio profesional quien decide cuándo se pone en marcha o se detiene la medición, y recibe información del sistema sobre cómo está gestionando su tiempo. Para su fundador y presidente, Joan Pons, la tecnología ha desdibujado el concepto de empleo tradicional. "Ya no es un puesto y un horario. Es una actitud, un esfuerzo y un objetivo".

Internet o las redes sociales son vistas por algunos empresarios como una peligrosa fuente de distracciones. Suprimirlas, sin embargo, no parece una opción. En primer lugar, recuerda Gabriel de Diego, director de Estrategia y Planificación de Recursos Humanos de Telefónica, porque "son herramientas de trabajo que facilitan al profesional estar al tanto de lo que sucede en su área de conocimiento o contexto de negocio". Además, añade Joan Pons, "¿de qué sirve bloquear el acceso a Facebook en la empresa si ahora el trabajador puede conectarse con su móvil? Eso sí, luego no le cuentas la media hora que pasó en su casa a las nueve de la noche contestando a correos de trabajo urgentes". Ambos especialistas coinciden en que existen otras prácticas mucho más perniciosas para la productividad que las redes sociales, como el exceso de reuniones o la insuficiente información que reciben los profesionales acerca del desempeño de sus funciones.

Acceso a los datos

Los expertos vaticinan que el imparable aterrizaje del *big data* en la gestión de personas va a permitir en muy corto espacio de tiempo anticipar futuros problemas. "Los datos permitirán detectar y analizar muchas de las conductas, competencias y comportamientos humanos, entre ellos, la honestidad", asegura Pau Hortal, consejero delegado de Facthum Cat. Se trata, ahonda Enrique Benayas General, de ICEMD (ESIC), de minimizar riesgos "intentando saber qué tipo de personas estoy metiendo en mi organización y cuáles son sus valores y actitudes frente a la vida".

¿Atentan estos sistemas contra la privacidad de las personas? Gabriel de Diego opina que no y apuesta no tanto por controlar como por medir. "El *big data* maneja la información de manera agregada y anónima; lo que se trabaja son perfiles con relación a su productividad para detectar posibles mecanismos de mejora". Pau Hortal, en cambio, sí piensa que los trabajadores tienen motivos para sentirse observados, aunque no más que en otros ámbitos de la vida. "No se pueden poner puertas al campo. Lo relevante no es desterrar la tecnología, sino gestionar adecuadamente su uso".

Y ¿qué piensan los empleados? Para Deepak Daswani, la clave está en la transparencia. "Si la compañía informa a los trabajadores de que el correo electrónico, la información del equipo o el tráfico que generan por Internet pueden ser monitorizados para garantizar la seguridad de la información, no habrá problemas". No obstante, agrega, es difícil delimitar dónde está el equilibrio. "Las medidas deben ir en sintonía con que los trabajadores puedan desarrollar su labor en un clima de trabajo óptimo. Los mecanismos de control no pueden ser ni tan rígidos que acaben ralentizando el trabajo ni tan laxos que carezcan de efectividad".

Entonces, ¿se fían las empresas de sus trabajadores? Para De Diego, así debería ser. "La flexibilidad que impera en las fórmulas de trabajo actuales requiere establecer mecanismos más o menos explícitos de confianza entre empresa y trabajador", explica.

LO QUE DICE LA LEY

¿Puede un empleado utilizar el ordenador de la empresa para enviar un tuit, entrar en su banco *online* o leer el periódico? En septiembre de 2007 una sentencia del Tribunal Supremo reconocía "la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores". Si bien, apunta Enrique Ceca, socio del área laboral de Ceca Magán Abogados, esa misma sentencia y otras posteriores obligan al empresario "a establecer las normas que regulen dicho uso y medidas preventivas que deben ser debidamente informadas a los empleados y sus representantes".
De hecho, la legislación permite al empresario prohibir completamente su utilización "sin que por ello sean vulnerados los derechos fundamentales del trabajador, al no existir una expectativa de intimidad". Aunque, advierte Enrique Ceca, "demasiadas restricciones generan rechazo y pueden ser contraproducentes". En su lugar, recomienda:

1
Delimitar qué puede y qué no puede hacer la empresa en materia de control.

2
Procurar que las medidas sean lo menos invasivas posible.

3
Establecer mecanismos preventivos como:
—Bloquear determinadas páginas web.
—Limitar o impedir las descargas de *software* desde Internet.
—No permitir la recepción de correos a partir de un determinado tamaño.

4
Informar a los empleados para que conozcan claramente las reglas.