

El Tribunal de Estrasburgo abre la puerta a examinar 'chats' y emails

## ¿Puede el empresario revisar el correo de los empleados?

En España es necesaria la autorización del trabajador para entrar en su ordenador

La inspección debe estar justificada y tiene límites

Manuel G. Pascual  
10-02-2016

### ¿Es legítimo usar el ordenador del trabajo para actividades ajenas a las profesionales?

La respuesta es afirmativa. El empleado tiene derecho a 15 minutos de descanso durante la jornada laboral, y durante ese tiempo puede hacer uso del equipo informático.

### ¿Puede el empleador inspeccionar los correos y demás comunicaciones electrónicas de sus asalariados, ya sean profesionales o privadas?

También, aunque con limitaciones. El Tribunal Europeo de Derechos Humanos de Estrasburgo publicó el pasado 12 de enero una sentencia en la que encuentra dentro de la ley que una empresa revise los correos electrónicos de su plantilla. El fallo, referido a un caso ocurrido en Rumanía, incluye los mensajes enviados desde el correo corporativo (en horario laboral) y los que se transmitan a través de cuentas privadas, pero operadas desde el ordenador del trabajo.

“El derecho español establece que el trabajador tiene que ser notificado antes de que se le monitorice el ordenador”, apunta Carlos Aldama, perito ingeniero informático y director de Aldama Informática Legal. Y a día de hoy, la legalidad de cada Estado va por delante de la comunitaria.

En el mes que ha transcurrido desde la publicación de la sentencia, que todavía pueden recurrir las partes implicadas, se han multiplicado las consultas a asesorías para conocer qué tipo de cláusula se debe incluir en el contrato de los trabajadores para poder revisar su correo. “Suele introducirse un anexo específico en la parte que versa sobre confidencialidad”, explica Aldama. Este experto asegura también que muchas compañías empiezan a notificar por la intranet que los empleados deben firmar un documento para aceptar las nuevas condiciones de privacidad, o incluso a ofrecer ligeros aumentos en el salario a quienes rubriquen su conformidad con esta política.

Si la autorización está firmada, el empresario puede examinar las comunicaciones del empleado cuando le plazca. “Los hay que analizan aleatoriamente a diez trabajadores todos los meses”, ilustra Aldama. El perito cuenta que recientemente investigó el caso de un trabajador que llevaba cinco años robando datos de su empresa. Pero solo se había podido aportar ante el tribunal la prueba hallada durante los últimos 11 meses, el tiempo transcurrido desde que firmó el citado documento. Al ver el delito, el juez autorizó a ampliar el foco del estudio más atrás en el tiempo.

Con los correos enviados desde la dirección corporativa, el proceso es más sencillo. No hace falta autorización alguna: al ser una herramienta de la empresa, esta es la dueña y responsable de todo lo que desde ella se dice.

#### Así se interviene un ordenador

**Autorización.** La clonación (copia del disco duro) de una máquina se puede realizar si su usuario ha firmado previamente un documento de la empresa en el que se avisa de la monitorización de las comunicaciones.

**Clonación.** El disco duro no se confisca, sino que se copia de una forma especial para ver qué contenía un día determinado (y qué se había borrado hasta esa fecha).

**Cadena de custodia.** En el momento de la clonación deben estar presentes el usuario habitual del ordenador, los representantes sindicales y un notario.

**Búsqueda ciega.** Como está prohibido entrar en la privacidad de los trabajadores, el perito realiza las llamadas búsquedas a ciegas: se examinan todos los datos (aquí entran redes sociales, emails y chats) del ordenador y se separa las que contengan una palabra determinada\_(por ejemplo, el nombre de la competencia si se sospecha que el investigado colabora con ella), pero que excluya otras de índole privada que aludan a la sexualidad, enfermedades o religión del sujeto.

## ¿Dónde está el límite?

Existen varios condicionantes que limitan las búsquedas de datos. “Está prohibido entrar en contenidos estrictamente privados. Cuando intervenimos un ordenador, no podemos leer las comunicaciones que hablen de religión, enfermedades o sexualidad”, explica Aldama. Solo una orden judicial, normalmente si se entra en la vía penal (asesinato, terrorismo), justifica traspasar esta frontera.

Las herramientas de análisis forense de equipos informáticos analizan todos los datos que han pasado por el ordenador. Incluyendo los de las redes sociales como Facebook, Twitter o incluso Whatsapp. A este último se accede (de forma legal) a través del rastro que deja en la computadora si se enchufa el teléfono a esta para cargarlo.