



## ENTREVISTA

# Es posible fijar procedimientos para supervisar las herramientas de comunicación otorgadas al trabajador



*Miguel MORACHIMO\**

*Para Miguel Morachimo, solo se puede acceder a las comunicaciones que los trabajadores hayan sostenido, empleando las herramientas que les ha provisto su empleador a través de una orden judicial. De lo contrario, no solo se trataría de medios ilícitos (en caso se trate de usarlos para demostrar la comisión de una infracción), sino que además se vulneraría el derecho al secreto y la inviolabilidad de las comunicaciones. Sin embargo, ello no impide que el empleador supervise que los instrumentos que provee sean utilizados adecuadamente.*

### 1. ¿Cuál es el contenido constitucionalmente protegido del derecho al secreto y la inviolabilidad de las comunicaciones?

Conforme está definido por nuestra Constitución, este derecho protege a las comunicaciones y sus instrumentos de cualquier intrusión, acceso o alteración no autorizada previamente por el emisor o receptor de la misma. El contenido de este derecho es amplio y no se agota exclusivamente en prevenir que terceros lean o escuchen nuestras comunicaciones, sino que también protege otros elementos, como su integridad (que no sean alteradas o mutiladas) o la libertad de los individuos de elegir el mecanismo de comunicación (ej. uso de cifrado). Incluso, tribunales internacionales han considerado que el simple registro o conservación de las comunicaciones, sin necesidad de que alguien tenga acceso directo a ellas o las alcance a conocer, implica en sí mismo una vulneración a este derecho.

### 2. ¿Solo está prohibido acceder al contenido de la comunicación o también podrían incluirse los metadatos?

Tradicionalmente se entendía como información protegida exclusivamente al contenido mismo de una comunicación, como las conversaciones telefónicas o el contenido de una carta. Sin embargo, las nuevas formas y medios de comunicación interpersonal con los que contamos actualmente nos obligan a ampliar el ámbito de lo que entendemos como información protegida para incluir otros elementos, como los registros geográficos asociados a la comunicación, la información identificadora de los terminales utilizados, los números de IP, entre otros. Protegemos estos datos porque a través de su lectura es posible obtener información acerca del comportamiento, identidad o hábitos del agente de dichas comunicaciones.

(\*) Abogado por la Pontificia Universidad Católica del Perú. Director de la ONG Hiperderecho, asociación civil dedicada a la defensa de los derechos humanos en entornos digitales.

En esos términos, considero protegido por el derecho a la inviolabilidad y el secreto de las comunicaciones a cualquier información relacionada con el proceso de comunicación de una persona o grupo de personas, siempre que no haya sido hecha pública previamente. Esta definición incluye no solo el contenido mismo de las comunicaciones, sino también otros elementos relacionados con el desarrollo de la comunicación, tales como su oportunidad, frecuencia, ruta, origen y destino. Ello en concordancia con el criterio establecido por la Corte Interamericana de Derechos Humanos, la cual ha señalado que la definición elegida no solo alcanza al contenido mismo de las comunicaciones, sino también cualquier otra información accesoria al contenido mismo, como “cualquier otro elemento del proceso de comunicación”.

### **3. ¿Qué implica el mandato constitucional de que ninguna relación laboral puede limitar el ejercicio de los derechos constitucionales?**

Esta afirmación es una extensión de la tesis planteada por nuestra Constitución según la cual los derechos fundamentales son irrenunciables. Por ende, su respeto no solo es plenamente exigible entre particulares, sino que los contratos entre particulares como los de naturaleza laboral no pueden apartarse o desconocer los derechos fundamentales.

### **4. La información obtenida con vulneración del derecho al secreto y la inviolabilidad de las comunicaciones, ¿puede tener algún valor?, ¿podría ser usada por un empleador para sancionar a un trabajador?**

Nuestro sistema jurídico contempla diversos escenarios en los cuales resulta posible y plenamente

legal que se afecte el derecho al secreto y la inviolabilidad de las comunicaciones. Como cualquier otro derecho fundamental, su ejercicio puede verse restringido en situaciones específicas. Estos son los casos de la interceptación de comunicaciones ordenada por un juez en el marco de una investigación penal o cuando la información se obtiene a través de un procedimiento de obtención de datos bajo el sistema nacional de inteligencia. Sin embargo, la jurisprudencia internacional en materia de derechos humanos ha dejado claro que cualquier afectación de este derecho debe de seguir un objetivo legítimo, resultar necesaria y ser proporcional.

En el marco de una relación laboral, como parte del poder de dirección del empleador, considero posible establecer reglas de conducta y fijar procedimientos en virtud de los cuales se supervise que las herramientas de comunicación otorgadas al trabajador, como teléfonos móviles, cuentas de correo o sistemas de mensajería, son utilizados apropiadamente. Estas políticas deben ser efectivamente comunicadas antes del inicio de la relación laboral e idealmente deben describir el nivel de granularidad<sup>(\*)</sup> que abarcará el monitoreo por parte del empleador. De lo contrario, las pruebas o documentación obtenidas libremente por el empleador a través de la vulneración de las herramientas de comunicación electrónicas otorgadas al empleador serán ilegales. Por un lado, constituirán una afectación evidente del derecho al secreto y la inviolabilidad de sus empleados que pueden haber usado dichas herramientas para comunicaciones personales. Por otro, al ser pruebas generadas por fuera de un procedimiento establecido y sin las garantías necesarias para su obtención o conservación, carecen de la confiabilidad suficiente como para ser tomadas como pruebas irrefutables por cualquier juez o tribunal.

<sup>(\*)</sup> Nota de *Diálogo con la Jurisprudencia*: en informática, este término alude al nivel de detalle al que se desea almacenar información.