¿PUEDE UNA ORGANIZACIÓN REVISAR LOS EMAILS DE SUS EMPLEADOS?

Escrito por **Carlos Rozen** y **Martín Elizalde**

BDO

Carlos Rozen

Carlos Rozen es socio de BDO en Argentina y responsable para la Región de las prácticas de Compliance & Forensic Services.
Ha capacitado a más de 2000 responsables de compliance y ha contribuido en la creación de más de 50 áreas de compliance.
Fue socio fundador y Presidente de la AAEC Asociación Argentina de Ética y Compliance.
Dirige la CEC Certificación Internacional en Ética y Compliance (AAEC-Universidad del Cema – IFCA International Federation of Compliance Associations). Es profesor en temas de Compliance en 5 universidades de Argentina y 4 del exterior, incluyendo España. Especialista en tecnologías aplicadas a Compliance. Autor de 5 libros en temas de compliance e investigaciones.

Martín Elizalde

Abogado. Master in Law, LLM, Washington College of Law, American University, Washington D.C.
Certification de Kroll Ontrack , Minneapolis.
Profesor de Seguridad Informática en distintas universidades de la Región (Argentina, Colombia, Ecuador y Panamá). Socio Fundador de Foresenics.

Top ten

Si tuviéramos que armar un ranking de las consultas más frecuentes que recibimos de nuestros clientes antes de iniciar una investigación interna, la pregunta que titula este artículo podría liderar el podio.

Una consulta, varias preguntas:

Proponemos formular varias preguntas, en la búsqueda de una respuesta comprensiva:

¿Cuáles son las facultades legales del empleador para monitorear la actividad del empleado en internet y acceder a sus cuentas y redes en los ordenadores que utiliza?

No existe una disposición legal orgánica. La Constitución Nacional consagra el principio de la inviolabilidad de la correspondencia epistolar y los papeles privados. Este principio se extrapolaría al ámbito laboral y a las herramientas digitales utilizados por los trabajadores. Pero la correspondencia "epistolar" gráfica y los "papeles privados" no son lo mismo que un intercambio por Internet de documentos electrónicos - no son sobres cerrados en un armario con llave, desde luego. La trayectoria del documento digital es más expuesta y su acceso, en algunas condiciones, es mucho más vulnerable.

Por su parte, la **ley de Protección de Datos Personales 25.326** impone cuidados en la recolección y tratamiento de los datos personales y protege, desde esta perspectiva, su confidencialidad. Y condiciona estas tareas al consentimiento previo del titular del dato- que se encontraria formulado en un documento interno de la empresa, como veremos más adelante.

Para la recolección de documentos electrónicos del empleado y en su tratamiento se aplican **(a)** Principio de finalidad: los datos deben ser obtenidos y tratados para fines específicos y legítimos; **(b)** Principio de lealtad y licitud: la recolección y tratamiento de datos deben ser realizados de manera transparente y legal; **(c)** Principio de proporcionalidad: la acción de control debe ser idónea, necesaria y proporcionada al fin que se busca; **(d)** Principio de no discriminación: los controles no pueden ser arbitrarios, direccionados injustamente, o discriminatorios.

Más específicamente, el **artículo 63** de la **Ley de Contrato de Trabajo 20.744**, cuyo título es **"Principio de Buena fe"** establece que: "Las partes están obligadas a obrar de buena fe, ajustando su conducta a lo que es propio de un buen empleador y de un buen trabajador, tanto al celebrar, ejecutar o extinguir el contrato o la relación de trabajo". La mención de esta norma no es ociosa, es necesario enmarcar en ella la actividad de un empleado que usa una herramienta digital de la empresa y la de ésta, cuando ejerce un control sobre el uso. Asimismo, el control que de buena fe se ejerza sobre esa herramienta (un celular o PC, por ejemplo) importaría aplicar las disposiciones sobre controles sobre el empleado, que en cuanto a la protección y salvaguarda de los bienes y herramientas de trabajo de su propiedad, establecen los artículos 70, 71 y 72 de la **Ley de Contrato de Trabajo:**

Artículo 70 .- .Controles personales. Los sistemas de controles personales del trabajador destinados a la protección de los bienes del empleador deberán siempre salvaguardar la dignidad del trabajador y deberán practicarse con discreción y se harán por medios de selección automática destinados a la totalidad del personal. Los controles del personal femenino deberán estar reservados exclusivamente a personas de su mismo sexo.

Artículo 71 .- .Conocimiento. Los sistemas, en todos los casos, deberán ser puestos en conocimiento de la autoridad de aplicación. Texto reformado en este punto por la **ley 27.322.**

Artículo 72 .- .Verificación. La autoridad de aplicación está facultada para verificar que los sistemas de control empleados por la empresa no afecten en forma manifiesta y discriminada la dignidad del trabajador.

Estos artículos reconocen una facultad de control al empleador, estableciendo modalidades y trazando límites. Si bien no mencionan las herramientas informáticas debido a que son anteriores a Internet, ahora se extienden a sus efectos. Y es así porque cuando el **artículo 5** de la Ley citada define a la empresa, lo hace como "la organización de medios personales, materiales e inmateriales, ordenados bajo una dirección para el logro de fines económicos". Dentro de los inmateriales, resulta correcto considerar al correo electrónico, el GPS, la información almacenada en una PC o servidores. Todos ellos son herramientas de trabajo, como lo es un rodado perteneciente a la empresa o una sierra manual. De hecho, son herramientas de mayor utilidad.

Asimismo, el **artículo 84** de la la Ley establece que "El trabajador debe prestar el servicio con puntualidad, asistencia regular y dedicación adecuada a las características de su empleo y a los medios instrumentales que se le provean". Resulta claro que el correo electrónico, la PC, laptop o servidor que la empresa pone a disposición del empleado para que realice su función laboral, son "instrumentos de trabajo, o, como lo denomina el texto legal "medios instrumentales"

¿Los documentos que están almacenados en los ordenadores de los empleados tienen valor de prueba en nuestros tribunales?

No siempre. Solo los que son resguardados de un modo forense serán considerados prueba documental en el expediente. La cadena de custodia es el procedimiento mediante el cual se asegura la integridad del documento desde su toma, hasta la presentación en juicio. Funciona como una especie de bitácora donde se asientan todos los procedimientos y herramientas que se siguieron y utilizaron desde un principio. Solo con el procedimiento descrito, admitirá el Juez que el documento que se presenta en el marco de un acta judicial es el mismo que estaba en la PC o el servidor.

¿De qué se trata en definitiva la expectativa de privacidad?

La clave reside en la "expectativa de privacidad" que tiene el empleado respecto del uso de las herramientas informáticas proporcionadas por el empleador (principalmente computadoras, correos electrónicos corporativos; espacio de guardado en la nube y demás software).

1. Existencia de una política clara: Si la empresa cuenta con una política interna documentada que advierte a los empleados sobre la posibilidad de monitoreo y control de los equipos y comunicaciones corporativas, y que prohíbe explícitamente la utilización de las herramientas para fines ajenos al laboral, la expectativa de privacidad del empleado se reduce. Para que este factor se active, la citada política debe ser conocida por el empleado, de manera demostrable, desde el inicio de la relación laboral o al momento de su implementación.

2. Uso personal tolerado: Si, a pesar de no haber una política expresa, la organización tolera -o incluso consiente- el uso personal de las herramientas, la expectativa de privacidad del empleado puede ser mayor y el control por parte del empleador más restringido. Un ejemplo podría ser preguntarse: ¿la organización ha actuado en los últimos X años respecto del uso inapropiado del correo electrónico corporativo?

3. Carácter de la comunicación: Se distingue entre el correo electrónico corporativo y el correo electrónico personal. Al respecto, existirá una mayor expectativa de privacidad sobre el correo personal, incluso cuando se acceda al mismo desde equipos de la empresa, que sobre el correo corporativo.

¿Cómo hacemos entonces para que un acceso sea considerado "lícito" ante la sospecha de un fraude?

Para que el acceso y constitución de la la prueba sean válidas en juicio, el empleador debe cumplir con ciertas condiciones:

Fundamento razonable y sospecha fundada: No puede tratarse de una actividad de control indiscriminada o falta de motivo. Debe existir una sospecha fundada y objetiva de que el empleado está cometiendo un ilícito o un incumplimiento grave de sus obligaciones laborales que justifique la injerencia. Ej.: una denuncia recibida podría contribuir, como así también entrevistas documentadas, documentación que revele esquemas fraudulentos, entre otros elementos.

Advertencia previa y política de uso: Como se mencionó anteriormente, la existencia de una política de uso que informe al empleado sobre la posibilidad de monitoreo se torna un requisito fundamental.

Proporcionalidad de la medida: La revisión debe limitarse a lo estrictamente necesario para la investigación del fraude, evitando una intromisión en exceso en la privacidad del empleado. Aquí entran en discusión aquellas nuevas tecnologías que permiten un monitoreo amplio y que disparan alertas ante sospechas.

Presencia del empleado o un tercero imparcial: Es altamente recomendable que la apertura o revisión de mails y/o archivos sea realizada en presencia del empleado afectado o, en su ausencia, con la presencia de un representante gremial o un tercero imparcial (escribano público, por ejemplo) para garantizar la transparencia y la legalidad del procedimiento. Esto es fundamental para evitar nulidades. Respecto de este punto, debo aclarar que nada resulta menos práctico para una investigación. Por dicha razón nos quedaremos con el "tercero imparcial" como la contratación de una firma o investigador de renombre en la materia, que disponga también de asesores en materia legal.

No interceptación en tránsito: La jurisprudencia tiende a considerar que la interceptación de comunicaciones "en tránsito" (en ocasión de que se estén enviando o recibiendo) no es legal sin que medie una orden judicial. En todo caso será preferible el acceso a comunicaciones ya "almacenadas" (recibidas o enviadas), siempre bajo las condiciones mencionadas.
Garantías de privacidad y confidencialidad: La información obtenida debe ser tratada con confidencialidad y utilizada únicamente para los fines del proceso investigativo.

¿Qué consecuencias podría tener un acceso que sea considerado ilícito?

Si el empleador accede a los archivos o correos electrónicos del empleado de forma ilegítima, sin cumplir con los requisitos legales y técnicos del caso, las consecuencias son ser graves:

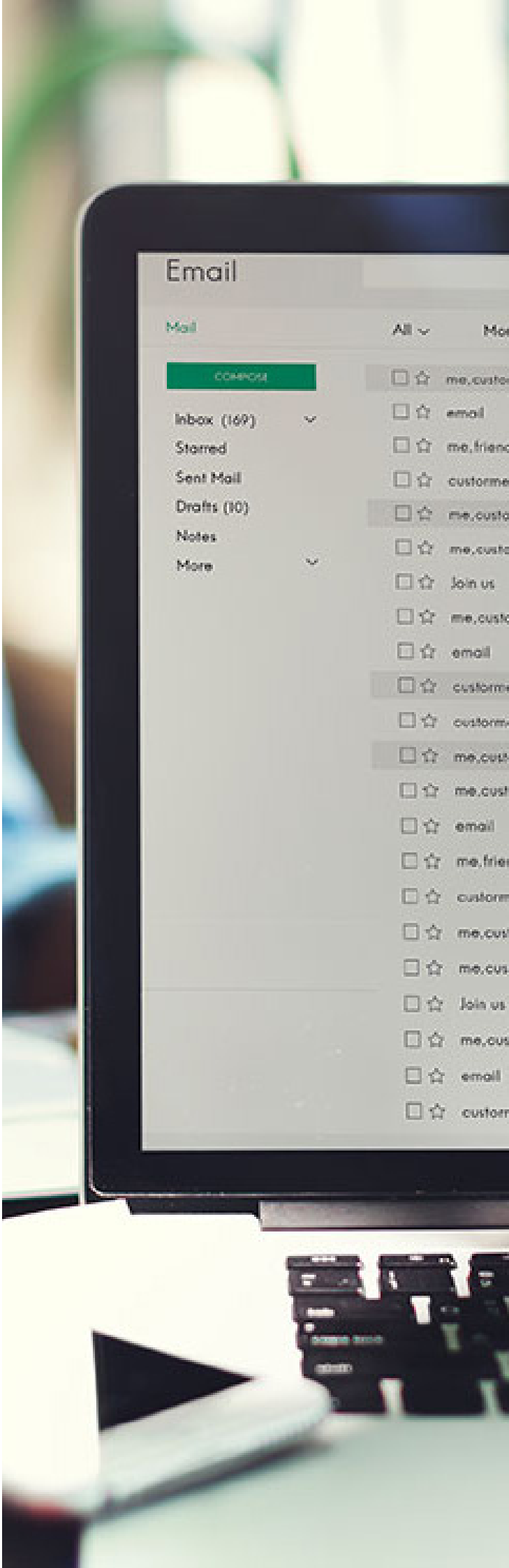
- **Nulidad de la prueba:** La prueba obtenida de forma ilícita (es decir, que se interprete como violación al derecho a la privacidad) puede ser declarada nula en un proceso judicial y, por lo tanto, no podrá ser utilizada para fundamentar una sanción y/o un despido.

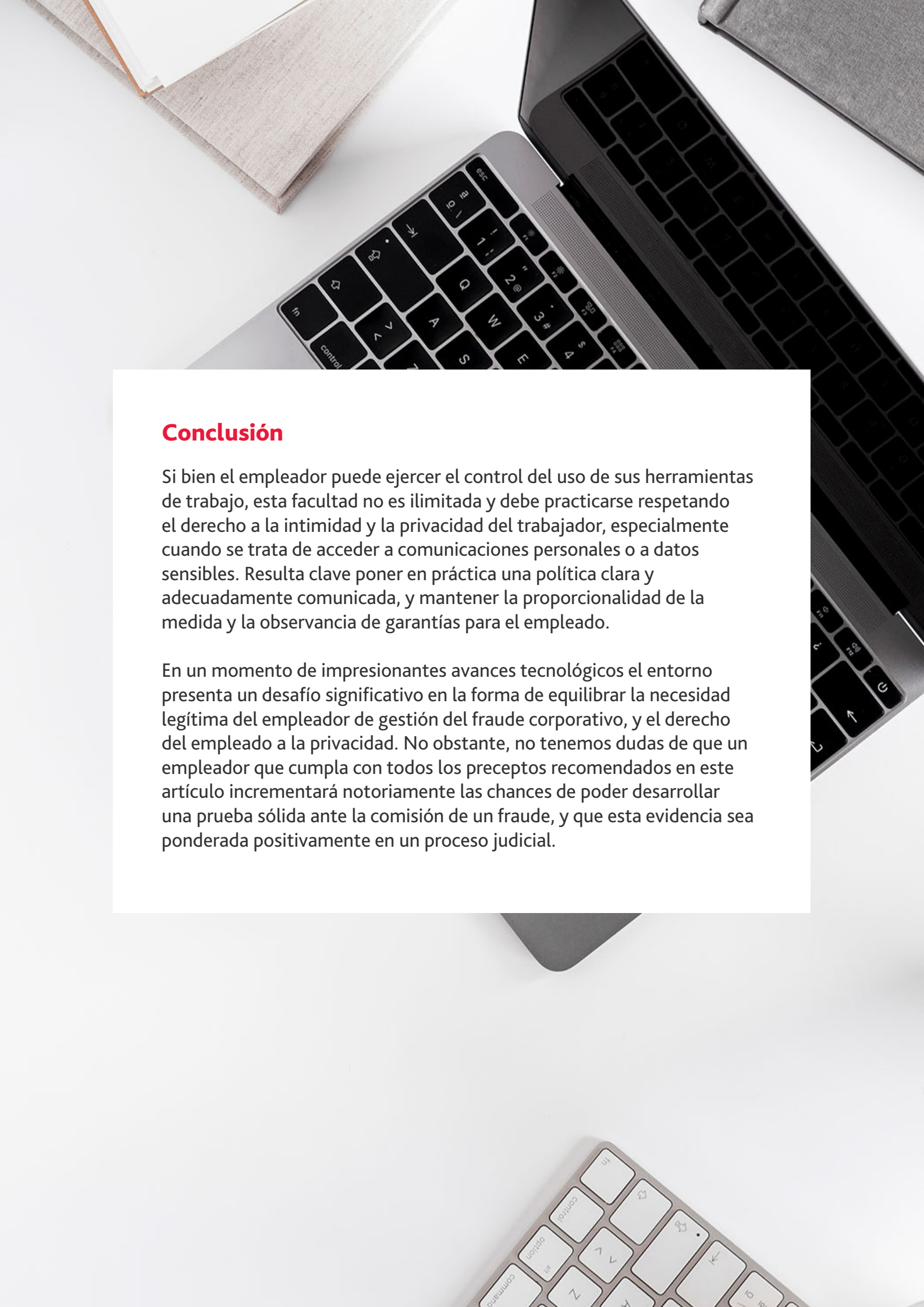
- **Acciones legales del empleado:** El empleado podría acciones legales por daños y perjuicios contra el empleador por violación de su derecho a la intimidad y privacidad. Además, tendría altas chances de ser la parte vencedora.

- **Responsabilidad penal:** En casos extremos, y dependiendo del modo y la profundidad de la intromisión, los directores podrían incurrir en delitos penales como violación de correspondencia o acceso indebido a datos **(Arts. 153 y 153 bis del Código Penal)**. Este tipo de delitos prevé penas de prisión.

¿A quién suele asistir más el derecho? ¿Qué chances tiene cada parte?

La jurisprudencia argentina ha ahondado esta problemática en diversos fallos, aunque con criterios bastante disímiles. En general, se prioriza el derecho a la intimidad del trabajador. Incluso se resolvió que la aceptación del control por parte de los empleados no constituye motivo suficiente para que el empleador utilice el contenido de la correspondencia privada del empleado. Se ha enfatizado la necesidad de que el empleador justifique con motivos razonables y sospechas fundadas, y que la revisión de información esté en proporción al fin buscado.





Conclusión

Si bien el empleador puede ejercer el control del uso de sus herramientas de trabajo, esta facultad no es ilimitada y debe practicarse respetando el derecho a la intimidad y la privacidad del trabajador, especialmente cuando se trata de acceder a comunicaciones personales o a datos sensibles. Resulta clave poner en práctica una política clara y adecuadamente comunicada, y mantener la proporcionalidad de la medida y la observancia de garantías para el empleado.

En un momento de impresionantes avances tecnológicos el entorno presenta un desafío significativo en la forma de equilibrar la necesidad legítima del empleador de gestión del fraude corporativo, y el derecho del empleado a la privacidad. No obstante, no tenemos dudas de que un empleador que cumpla con todos los preceptos recomendados en este artículo incrementará notoriamente las chances de poder desarrollar una prueba sólida ante la comisión de un fraude, y que esta evidencia sea ponderada positivamente en un proceso judicial.