

# Las facultades de control del empleador y las nuevas tecnologías

por Julio Armando Grisolia y Ricardo Diego Hierrezuelo

## 1) Introducción.

Como lógica consecuencia del poder de dirección del empleador, que conforma una de las facultades jerárquicas que el ordenamiento jurídico le atribuye, surge la facultad de control, ya que si tiene el poder de emitir directivas al trabajador necesariamente debe tener la *posibilidad de controlar la debida ejecución de las órdenes impartidas*.

La doctrina reconoce tres tipos de controles: 1) Control sobre la prestación del trabajo —verificando la producción y el modo de efectuarlo— y sobre la asistencia y puntualidad del trabajador —por ejemplo, mediante registros y tarjetas-reloj— ; 2) Controles de salida con el fin de evitar la sustracción de mercaderías o materias primas, y 3) Control médico, que se manifiesta en una cantidad determinada de posibilidades.

Las tecnologías y herramientas englobadas bajo el título “nuevas tecnologías” ya no son un fenómeno novedoso: se han estado incorporando al espacio organizacional de la empresa y a nuestras vidas desde hace años.

Podría decirse -incluso- que el hecho de seguir refiriéndose a ellas (al *e-mail*, a *internet*, a la mensajería instantánea, a los *weblogs*, a las cámaras webs, al uso de la informática en general, etc) como “nuevas tecnologías”, no hace más que reafirmar que quien utiliza tal expresión, aunque pueda estar perfectamente adaptado a su utilización y funcionamiento, pertenece a una “generación anterior”; sea esta la llamada “*generación X*” (los nacidos en los años 70); la “*generación Y*” (nacidos en los años ochenta), o a generaciones anteriores, predecesoras de aquella a la que pertenecen las personas jóvenes que incorporaron esas “nuevas tecnologías” desde la cuna, y para quienes el uso de un *i-phone*, el manejo de un *mouse*, el envío de un *e-mail* o recurrir a *wikipedia* buscando información, no representan “algo nuevo” que deben incorporar a su modo de vida. Esta nueva generación, que terminará de imponer -más temprano que tarde- un nuevo paradigma, son los denominados “nativos digitales”; también denominados *iGeneration* (por *iPod* o *iPhone*) o *millennials*, por vivir su desarrollo más intenso junto con la llegada del tercer milenio, caracterizados por haber naturalizado procesos de lectoescritura instantánea y participativa regidos por una gramática novedosa que reformula los idiomas y las reglas sintácticas, y los fusiona en una *melange* entre la taquigrafía (por ejemplo: “*px tq*” = “porque te quiero”) y el pictograma (baste citar el ya clásico smiley “☺”, que ha evolucionado hacia formas mucho más sofisticadas, gracias al llamado *lenguaje chat* o *lenguaje SMS*) de fácil comprensión (una suerte de esperanto recargado).

La legislación debe adaptarse a los cambios que se presentan, porque -de lo contrario- quedará desactualizada. No olvidemos que a medida que esos jóvenes ingresen a los claustros universitarios y a la vida adulta (laboral, política, judicial, social, económica, familiar, etc) irán remodelando la realidad a una forma distinta de la actual. Pensemos en los futuros jueces laborales o legisladores surgidos de esa generación, para quienes el envío de un mail (o de otro tipo de información) desde el ámbito laboral, desde una herramienta propia o provista por el empleador, no sea una falta siquiera leve, sino algo natural que no merece reproche alguno.

El derecho laboral y la jurisprudencia vienen haciendo esfuerzos para adaptarse a esa realidad, aunque en algunos casos se pierda la noción de la dimensión del fenómeno.

No obstante lo expuesto, la introducción de esta nueva tecnología en comunicación e informática (TIC) que el empleador pone al servicio de la empresa para acelerar la realización del trabajo y es utilizada por los trabajadores, plantea serios cuestionamientos a la hora de determinar cuáles son los controles que aquél puede realizar para constatar que no sean utilizadas para fines extralaborales. Aquí entran en colisión dos derechos fundamentales: el derecho de controlar la prestación de trabajo con que cuenta el empleador, por un lado, y el derecho a la intimidad del trabajador, por el otro. Sostiene Trillo Párraga que con relación al uso que el trabajador da a las TIC aparece una colisión de derechos fundamentales entre la libertad de empresa y el derecho a la intimidad personal. El empresario no utiliza los medios de vigilancia para fiscalizar el correcto cumplimiento de la prestación laboral, sino para controlar un posible uso desviado de las TIC a disposición del trabajador. Sin embargo dicho control, aunque sea indirectamente, guarda relación con el adecuado cumplimiento de la deuda laboral contraída por el trabajador desde el momento en que el uso –por ejemplo de internet para fines distintos de los estrictamente laborales- implica una merma de la jornada de trabajo o una disminución del rendimiento del trabajador<sup>1</sup>.

Raso Delgue señala que las posibilidades de control del empleador sobre el trabajador han sido potenciadas por las nuevas tecnologías aplicadas a viejos o a nuevos sistemas de monitoreo. Entre los instrumentos de control más conocidos, podemos enumerar cámaras filmadoras, cámaras fotográficas, micrófonos, teléfonos celulares y localizadores GPS del personal (como pulseras); además de GPS en los vehículos, registro de huellas digitales o de las manos, sistemas cerrados de televisión, software para medir presión arterial mientras se trabaja en la computadora, pantallazos desde la computadora para vigilar al que la utiliza, etc.

Este autor, siguiendo a Spiwak Lew recuerda la opinión del grupo de trabajo sobre la protección de datos (art. 29 de la directiva CE 95/46) que ha señalado que toda actividad de control debe justificarse en base a los siguientes requisitos: a) necesidad: el empleador debe demostrar que la vigilancia es absolutamente necesaria para un objetivo específico (vgr., cámaras en el Metro de Madrid para evitar ataques terroristas en áreas consideradas sensibles); b) finalidad: los datos deben recogerse con fines determinados, explícitos y legítimos y no ser tratados posteriormente de manera incompatible con dichos fines; c) transparencia: el empleador debe indicar en forma clara y abierta con qué elementos realizará su control; d) legitimidad: el tratamiento de datos de un trabajador no puede perjudicar los derechos fundamentales de los trabajadores, como el derecho a la intimidad; e) proporcionalidad: los datos personales deben ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben; deberían evitarse sistemas de vigilancia automática y continua; f) exactitud y conservación de datos: los datos almacenados por el empleador, por ejemplo, no deben guardarse más tiempo del necesario; g) seguridad: el empleador debe utilizar medidas técnicas y organizativas adecuadas para proteger los datos personales<sup>2</sup>.

## **2) Los controles visuales y auditivos.**

El avance tecnológico ha producido la aparición de nuevos sistemas de controles de la actividad laboral de los trabajadores; en algunos casos puede resultar cuestionable su instrumentación. Ellos son los controles visuales y auditivos, procedimientos industriales que se utilizan para controlar la actividad de los trabajadores, sobre los cuales no existen normas expresas como en otras legislaciones que regulen su implementación.

---

<sup>1</sup> Trillo Párraga, Franciso J. “Las nuevas tecnologías de la información y comunicación en las relaciones laborales”, en Colección Temas de Derecho Laboral, Correo Electrónico e Internet en el ámbito laboral, Errepar, Buenos Aires, 2009, págs. 41/43.

<sup>2</sup> Raso Delgue, Juan. “El impacto de las nuevas tecnologías en la intimidad y privacidad del trabajador”, en Colección Temas de Derecho Laboral, Correo Electrónico e Internet en el ámbito laboral, Errepar, Buenos Aires, 2009, págs. 55/94.

Con relación a los controles visuales, que generalmente consisten en la implementación de cámara de video en distintos sectores de establecimiento, la permisión de este medio de control (sin que ello afecte la dignidad del trabajador ni viole su derecho a la intimidad) dependerá de diversos factores relacionados con la actividad desarrollada por la empresa, los elementos con los cuales se trabajan y el sector donde se instale el sistema de control. Por ejemplo, resulta lógico que se implementen sistemas de control en el sector cajas o tesorería de bancos y en las góndolas de los supermercados. Estela Ferreirós recuerda una empresa en la cual las cámaras visoras enfocaban durante toda la jornada a los trabajadores, estuvieran donde estuviesen, e incluía una vista constante de las puertas de los baños, en las cuales se había hecho una especie de ventanita para ver las caras de quienes ocupaban los sanitarios. Tal situación dio lugar a un reclamo judicial que tramitara por ante el Tribunal de Trabajo n. 2 de San Isidro; en el fallo con primer voto de la Dra. Morey, se resolvió que había existido una conducta antisocial cayendo en el abuso del derecho y correspondiendo a los trabajadores la reparación del perjuicio sufrido, y ordenando el retiro de las máquinas.

Con respecto a los controles auditivos, es necesario analizar cada situación en particular, ya que atenta contra la privacidad del trabajador la introducción de micrófonos o la intervención del teléfono asignado. Sin embargo, muchas veces el escuchar la conversación del personal con un cliente es necesario para controlar la prestación del servicio, como sucede con la función de *telemarketer*, cuyas tareas consisten justamente en la venta telefónica de distintos productos. En esos casos, se torna necesario establecer un sistema que permita distinguir entre llamadas personales y laborales, pudiendo escuchar el supervisor sólo estas últimas.

La OIT ha señalado que a nivel internacional se han desarrollado diversos mecanismos de control de la actividad laboral de los trabajadores por razones de seguridad, salud laboral y para asegurar la calidad del servicio. En Estados Unidos, hay algunos sectores como el bancario, de telecomunicaciones y de seguros en los cuales un 80% de los trabajadores son observados por vía telefónica o por medios informáticos. En Japón está en aumento la vigilancia mediante cámaras en fábricas y comercios. No obstante ello, el informe de la OIT señala que la tendencia hacia una mayor protección de la vida privada de los trabajadores está ganando terreno en todo el mundo, sobre la base de una encuesta en diecinueve países industrializados. En Italia, Noruega y Suecia los abusos cometidos en el lugar de trabajo han provocado la imposición de restricciones específicas a la vigilancia de los trabajadores por equipos de video y audio. En Austria, Bélgica, Alemania, Holanda y Suecia, el uso de medios técnicos para supervisar el comportamiento y rendimiento de los trabajadores requiere el acuerdo o la consulta previa con el trabajador. En Francia, la alarma suscitada por las investigaciones realizadas por las empresas durante el proceso de selección de personal llevó a reformar el código de trabajo a fin de proteger el ámbito privado de los aspirantes a un empleo<sup>3</sup>.

### **3) Control sobre la utilización de internet y del chat.**

En las últimas décadas el derecho del trabajo ha sido testigo de cómo el desarrollo de las llamadas “nuevas tecnologías” ha modificado lo que históricamente se entendía por lugar de trabajo, y del dilema que ello plantea en cuanto a la protección de la personalidad moral del trabajador frente a los nuevos métodos de monitoreo laboral.

Los avances producidos en la informática y la aparición de internet llevaron a los empleadores a proveer a los trabajadores de este sistema con el fin de acelerar la búsqueda de información y conectarse con otros trabajadores y clientes ubicados en cualquier lugar del planeta. Con este novedoso sistema las distancias se han acortado considerablemente y las comunicaciones se realizan en forma inmediata, permitiendo a los intercomunicadores no sólo comunicarse vía chat, sino también pasarse los archivos y la información necesaria en cuestión de segundos.

---

<sup>3</sup> Conf. “¡Cuidado, un ojo electrónico lo vigila!”, *Rev. Trabajo*, OIT, nro. 10, 1994-22, cit. por LIVELLARA, Carlos A., *Ley de Contrato de Trabajo...*, cit., p. 853.

Sin embargo, las posibilidades que brinda este sistema son numerosas, razón por la cual es factible que el trabajador lo utilice durante la jornada de trabajo, no para la prestación de servicios, sino en beneficio personal, con lo cual distrae tiempo de trabajo para fines propios.

Lo mismo sucede con el *messenger* u otro sistema de chateo que implemente la empresa para la comunicación interna o externa. En este último, le permitirá al trabajador conectarse con los clientes, pero también es frecuente que lo utilice como forma de dialogar con amigos, familiares u otras personas. Incluso cuando el sistema sólo permite el chateo con otros trabajadores de la empresa, es habitual que los trabajadores alternen en sus diálogos cuestiones relacionadas con el trabajo con inquietudes o problemas personales.

También, con la finalidad de mantener conectado a los trabajadores y permitir intercambiar información, es común que la empresa les asigne una casilla de *e-mail*, la cual, al igual que en los anteriores supuestos, puede ser utilizada por el dependiente para ambos fines (laborales y personales).

En principio, la utilización de los elementos proporcionados por la empresa para fines personales constituye un incumplimiento contractual, susceptible de ser sancionado por el empleador. Pero para ello deberá respetar los límites del ejercicio de las facultades disciplinarias, debiendo aplicar sanciones proporcionales a la falta cometida. Así, por ejemplo, si toleró la utilización del *messenger* para fines personales y nunca lo sancionó, no puede sin más despedir al trabajador sin antes utilizar algún otro tipo de medida disciplinaria (moral y suspensión) que permita hacer ver al trabajador que esa conducta no será consentida por la patronal.

Pero una cosa es el control sobre la utilización irracional de los medios que la empresa le provee para la realización del trabajo, y otra distinta es la posibilidad del empleador de controlar el contenido de los *e-mails* que el trabajador envía desde su casilla.

#### **4) Uso del correo electrónico**

Se entiende por correo electrónico toda correspondencia, mensaje, archivo, dato u otra información electrónica que se transmite entre computadoras. La protección del *e-mail* abarca su creación, transmisión y almacenamiento (conf. res. 333/01 del 10/9/2000, Secretaría de Comunicaciones). Sobre este tema no debe perderse de vista que en el ámbito laboral coexisten, por un lado, el derecho del empleador a ejercer cualquier industria lícita y, por otro, los derechos que como ser humano corresponden a todo trabajador. Por ello, cualquier abordaje debe efectuarse intentando armonizar los derechos de unos y otros, y para ello resultan de suma utilidad los principios generales del derecho del trabajo.

Como criterio general es aceptado que cuanto mayor sea el grado de intromisión a la hora de efectuar los controles de diligencia y probidad de sus dependientes por parte del empleador, más difícil resultará su legitimación.

Un grado de intromisión moderado es aceptado por la doctrina y la jurisprudencia mayoritarias, es decir, la elección del medio de monitoreo eficaz pero menos invasivo entre las alternativas posibles, evitando así los controles subrepticios, ocultos o sin conocimiento fehaciente del dependiente y que estén referidos exclusivamente a aspectos relacionados con el trabajo.

Un caso singular y de actualidad es el de la protección de la intimidad del trabajador frente a los accesos del empleador, sin su consentimiento, al contenido de las casillas de correo electrónico (*e-mail*), donde el trabajador recibe y remite correspondencia en el ámbito laboral.

Resulta claro que cuando el empleador pone a disposición de sus trabajadores computadoras con capacidad de comunicación externa, lo hace con la intención de mejorar sus resultados empresarios, y no con la finalidad de proveerle al dependiente una herramienta para uso personal en horario de trabajo.

Sin embargo, existe una utilización generalizada de este tipo de herramientas para usos personales, como sucede también con otros medios tecnológicos puestos a disposición del dependiente y cuya utilización para fines personales no ha suscitado tanto debate.

Probablemente ello se deba a que el correo electrónico o *e-mail*, pese a que no puede ser asimilable completamente a la correspondencia tradicional, guarda evidentes similitudes con ella, que habilitarían a considerar si la auditoría empresaria sobre la correspondencia electrónica remitida o enviada por los trabajadores constituye o no una invasión a su esfera de privacidad.

Los fundamentos que se han esbozados para justificar el control empresarial sobre el uso del correo electrónico son: a) Mensajes ofensivos: los empleados pueden usar el *e-mail* para transmitir insultos o injurias hacia otras empresas o particulares. Una actitud como ésta podría generarle una querrela, no sólo a la persona que envía el *e-mail*, sino también a la empresa en la que trabaja, b) Divulgación de secretos: cualquier empleado, desde su lugar de trabajo, sin levantarse de la silla y sin llevarse ninguna carpeta, podría enviar información confidencial de la empresa. c) Caída del sistema: el uso indebido e incontrolado del acceso puede generar inconvenientes en el sistema informático. Los programas *shareware* y *freeware* que se bajan de internet y los *e-mails* que se reciben pueden contener virus que afecten gravemente a las computadoras. También se podría congestionar el acceso a la web, debido al uso indiscriminado de los accesos y de la información que se transfiere. d) Falta de productividad: ocasionada por el uso irregular y excesivo del correo electrónico<sup>4</sup>.

En nuestro país se han presentado distintos proyectos de ley en uno y otro sentido, esto es, dando preeminencia a las facultades de control del empleador por sobre el derecho a intimidad, o viceversa.

La jurisprudencia uruguaya ha privilegiado los derechos de empresa por sobre los derechos a la intimidad y privacidad del trabajador. Los derechos del empleador se sustentan, en opinión de los tribunales, en dos ideas básicas: a) la propiedad de las máquinas y servidores y b) la disciplina que debe mantenerse en el lugar de trabajo.

En cambio, en el derecho comparado prevalece la postura que prohíbe al empleador el acceso e interceptación de los correos electrónicos.

Lo expuesto permite señalar existen intereses contrapuestos que deben ser adecuadamente merituados a la hora de evaluar los casos concretos. Por un lado, habrá que considerar las prerrogativas de los empleadores encaminadas a vigilar el comportamiento de su personal, que se traduce en el empleo de los medios pertinentes, para constatar el uso efectuado por el trabajador del correo electrónico puesto a su servicio con fines laborales. Pero también habrá que tener en cuenta el derecho a la intimidad de los empleados, y que por aquella vía no se vulnere la reserva y privacidad de su correspondencia particular. Por ello, para dilucidar los casos habrá que analizar las conductas de las partes, dentro de los carriles de la buena fe contractual (arts. 62, 63 y concs., LCT) y de la razonabilidad, buscando de conciliar los reales intereses de ambos, evitando conductas discriminatorias y abusivas.

Al efecto, resulta aconsejable que la empresa notifique al empleado la prohibición o limitación de la utilización del correo electrónico para cuestiones particulares, y que se reserva la facultad de controlar tal uso por los medios técnicos a su alcance. Y luego, al implementar el contralor, se deberá evitar molestias o invasiones innecesarias a la intimidad del trabajador.

### **5) La reforma de la ley 26.388.**

La ley 26.388 (sancionada el 4/6/2008, promulgada de hecho el 24/6/2008; y publicada en el BO del 25/6/2008) modificó el Código Penal (art. 153) e incorporó el art. 153 bis, reguló en materia de “delitos informáticos”, normativa que repercute en nuestra disciplina, aunque sin resolver concretamente el problema de fondo, cual es, quien detenta la titularidad del “correo electrónico”. Se trata de una norma que modifica algunos artículos del Código Penal e incorpora otros, introduciendo profundas reformas en cuanto a los alcances de las nuevas tecnologías en el mundo

---

<sup>4</sup> OVIEDO, María Natalia, *Control empresarial sobre los e-mails de los dependientes*, Hammurabi-SADL, Buenos Aires, 2004, p. 73.

del derecho. Es una norma positiva pues tiende a la equiparación, acercando la legislación a la realidad del mundo cotidiano.

Incorpora como últimos párrafos del artículo 77 del Código Penal, incorporando al concepto de “documento”, “firma”, “suscripción”, “instrumento privado” y “certificado”, las versiones digitales correspondientes. Así dispone que: *“El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente”.*

Se sustituye el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: *“Violación de Secretos y de la Privacidad”*, renueva el texto del artículo 153 del Código Penal, estableciendo penas de prisión de quince (15) días a seis (6) meses para el que *“...abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena”.*

La disposición se complementa con la incorporación del art. 153 bis al Código Penal, que dispone penas de prisión de entre quince días y seis meses -si no resultare un delito más severamente penado- para las personas que, a sabiendas, accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido (la pena es mayor – de un mes a un año de prisión- cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros).

La ley 26.388 también modifica otros artículos del Código Penal (arts. 155, 157, 157 bis, 173, 183, 184, 197, 255, y deroga los 78 bis y 117 bis), aunque si bien se trata de modificaciones provechosas, inciden sólo tangencialmente en nuestra disciplina en general, al estar referidas a punir conductas como el hackeo en diversas versiones, la propagación y daños causados por los virus informáticos, la intromisión en bancos de datos personales, la comercialización de programas adulterados, etc).

Si bien del nuevo texto legal no parece excluirse la posibilidad de monitoreo de las cuentas corporativas de los empleados, ya que se trata de herramientas de trabajo, cuentan de todos modos con una expectativa de privacidad, por lo que la empresa que pretenda efectuar controles debe previamente aplicar e informar su política general a todos los empleados.

A tal efecto, y ante el vacío en la legislación laboral, parece aconsejable recurrir a acuerdos entre las partes que autorice la práctica, a fin de evitar posibles consecuencias penales (indicar quienes son los autorizados para la requisa, la forma que se realizará, y cualquier elemento complementario que asegure que esta tarea no sea considerada una trasgresión del tipo penal contemplado en el art. 153).

Recordemos que dicho artículo establece penas de prisión para el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido, o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado, o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. Y agrega además que igual castigo corresponderá

a quien indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido, estableciendo un agravante si el autor además comunicare a otro o publicare el contenido de la comunicación, o si el hecho lo cometiere un funcionario público que abusare de sus funciones.

Las reformas introducidas también se proyectan sobre las compañías que prestan servicios de Internet y telefonía móvil, fijando la política con el personal que tienen acceso a las cuentas de e-mail y a los SMS de los clientes. Asimismo, cabe señalar que la ley 26.388 determina que puede estar sujeto a sanciones el empleado que injurie a otro miembro de la empresa a través del correo electrónico laboral, como así también a aquel que trafique obras indebidas (software o imágenes, entre otras), realice hackeos o envíe material pornográfico.

También contiene normativa tendiente a la protección de datos personales, al incorporar el artículo 157 bis al Código Penal, que reprime con "hasta dos años de prisión al que ilegítimamente accediera un banco de datos personales", equiparando a nuestro país a la mayoría de las legislaciones del primer mundo que ya han desarrollado normativa en el tema, como Estados Unidos, Unión Europea, y la mayor parte de los demás países de Europa, en especial Austria, Noruega y Dinamarca, que son amplias a la hora de definir la noción de "datos personales" al definirla como "toda información susceptible de ser puesta en relación con personas determinadas o determinables", y se refiere tanto a persona física como jurídica en los dos primeros casos, mientras que en Dinamarca sólo admite la protección de los individuos.

Cabe reiterar que el derecho a la intimidad o privacidad es uno de los derechos fundamentales que tiene el individuo, que tiene consagración constitucional en el art. 19 se contempla que "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados"<sup>5</sup>.

Sin embargo, reiteramos, esta normativa no resuelve el problema de quien detenta la titularidad del correo electrónico corporativo, y esto puede traer ahora problemas de tipo penal, porque si se entiende que la titularidad del mismo pertenece al trabajador, la intromisión del empleador en el correo del trabajador sin la autorización del mismo podría constituir un ilícito penal.

Por ello, y sin perjuicio de los acuerdos a los que puedan arribar las partes (incluso podría ser materia de negociación colectiva), o lo que dispongan al respecto los reglamentos de empresa, se torna necesario una regulación legal que determine hasta donde llega el derecho a la privacidad del trabajador y donde empieza el derecho del empleador de efectuar el control sobre la utilización que aquél le esté dando a las herramientas que se le pongan a su alcance.

**Julio Armando Grisolia**  
Vicepresidente ARTRA

**Ricardo Diego Hierrezuelo**  
Abogado egresado de la Facultad de Derecho y Ciencias Sociales de la UBA,  
Doctor en Derecho del Trabajo, Previsión Social y Derechos Humanos

---

<sup>5</sup> Grisolia, Julio Armando, La violación de la correspondencia electrónica en la ley 26.388", en Colección Temas de Derecho Laboral, Correo Electrónico e Internet en el ámbito laboral, Errepar, Buenos Aires, 2009, págs. 181/198.