

Fuga de información



Rafael H. Gamboa B.

Control de herramientas informáticas y responsabilidad legal

De un tiempo para acá el entorno empresarial ha cambiado muchísimo. Hasta hace unos pocos años, la comunicación se hacía mediante cartas en papel, documentos ^[1], y la información era almacenada, de manera física, en grandes espacios, con los consecuentes riesgos de estos procedimientos.

Tratos previos, ofertas, aceptaciones, contratos, otrosíes, pólizas y la contabilidad, entre otros, engrosaban los archivadores, los cuales en su gestión presentaban fallas en el acceso y en su seguridad.

Con el advenimiento de la tecnología, movilidad e interconectividad, así como de la desmaterialización de la información, los procesos se volvieron mucho más rápidos y eficientes, pero a la vez, el volumen de la información creció exponencialmente por la velocidad en las comunicaciones, generando que su control, sea cada vez más difícil.

Las organizaciones enfrentan el dilema sobre cómo controlar la información que

les es valiosa, sin que en el camino se vulneren los derechos constitucionales que tienen sus empleados. Adicionalmente, cómo pueden prevenir conductas que redunden en una responsabilidad de la empresa.

Aspectos como las solicitudes particulares, órdenes judiciales, la privacidad e intimidad de los empleados en el uso de las herramientas electrónicas, llevan a las organizaciones a adoptar medidas que, respetando el ordenamiento, garanticen que no se van a ver perjudicadas las empresas, por acción u omisión de su recurso humano.

Información y herramientas

En el presente escrito cuando nos referimos a “información”, nos estamos refiriendo a todo aquello que refleja, bien sea visual o audiblemente, el desarrollo de la empresa.

Secretos industriales, negociaciones con proveedores y empleados, “políticas” internas de la empresa, cámaras de seguridad, rastreo y seguimiento de actividad laboral entre otras, son algunas de las informaciones, que pueden afectar a la

organización, desde el punto de vista comercial, así como de su propia imagen.

Es usual que las empresas entreguen a sus empleados, tarjetas de acceso, portátiles, dispositivos inteligentes, USBs, acceso a internet, cuenta de correo electrónico, para el mejor desempeño de sus funciones, el problema surge cuando estas herramientas entregadas se usan para fines personales, ajenos a su actividad laboral.

En este punto, la pregunta es ¿cómo se hace para saber que las herramientas están siendo correctamente utilizadas? ¿Quién controla esto? La respuesta, es el Departamento de IT, toda vez que serán ellos los encargados de atender los requerimientos de la gerencia, para supervisar el correcto uso.

Lo anterior nos lleva a concluir que en la actualidad un área bien importante de una organización, es la de IT. Así mismo, que el área más “peligrosa” de una organización es la de IT. Y, por consiguiente, surge el interrogante sobre ¿quién controla al área de IT? ... ¡Nadie!

La citada “peligrosidad” del área de IT, más que generar temores, representa una oportunidad para las organizaciones, de tener no sólo excelentes profesionales, sino además personas leales, pulcras y transparentes en su actuar.

A través de sistemas informáticos, cada vez es más fácil saber si un empleado está haciendo su trabajo y qué tan productivo es. Las tarjetas de acceso o los celulares o dispositivos equipados con GPSs, nos muestran el desplazamiento del empleado junto con la hora, día y permanencia en cada lugar.

El acceso a la red de la empresa o a Internet provisto por la organización, empleando el equipo de la oficina, el portátil suministrado o aún un dispositivo propio, puede indicar de una manera clara y exacta los sitios y duración de las visitas que realiza el empleado, sean relacionados o no con su trabajo, tales como correos electrónicos personales, redes sociales, casinos en línea entre otros.

Está establecido, mediante acuerdo entre la empresa y el empleado, que la cuenta de correo electrónico de la organización, además de la red y el acceso a internet anteriormente mencionado, deben ser exclusivamente usados con fines laborales, pero ¿cómo hace la empresa para saber que se está cumpliendo lo establecido, sin vulnerar los derechos que tiene el empleado? O peor aún, ¿cómo sabe una empresa que su empleado no está utilizando herramientas electrónicas para cometer ilícitos o sacar información valiosa de la empresa?

Alojamiento de pornografía infantil, de material protegido por los derechos de autor, uso de infraestructura computacional para realizar ataques o actividades ilícitas o simple fuga de información valiosa, pueden repercutir en gravísimas consecuencias para la organización, más aún, si ésta no adoptó las medidas necesarias para evitar que sucedieran las conductas anteriormente mencionadas.

Dentro de una investigación o de una instancia judicial, el investigador o el juez, analizará la diligencia con que actuó la empresa para evitar el tema investigado. Si se prueba que no adoptó medida alguna, será considerada su actitud como negligente, pudiéndosele encontrar responsable.

¿Puede o debe la organización adoptar medidas para evitar ser responsable por actividades de sus empleados en el uso de las herramientas electrónicas? La respuesta es un contundente SÍ.

Pronunciamientos jurisprudenciales en Colombia

En Colombia hay pronunciamientos judiciales donde el juez ha analizado la actitud que ha tenido el empleador frente a sus empleados, así como de terceros frente a la información de la empresa, en el uso de las herramientas electrónicas.

A continuación se mencionan los casos más significativos en los escenarios en donde se incluye la norma aplicable, el caso en concreto, la decisión adoptada y los comentarios del caso.

Solicitud vía derecho de petición de información por parte de particulares.

La Norma:

“ARTICULO 23. De la Constitución Nacional. Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales.”

El Caso:

Un particular, sin vinculación alguna de la empresa, vía derecho de petición consagrado en el artículo 23 de la Constitución Nacional, solicita información que reposa en el los archivos de la empresa.

Comentario:

Aunque originalmente la norma consagrada en el artículo 23 de la Constitución Nacional era para destinación de los funcionarios del Estado, vía jurisprudencia constitucional, se estableció que los particulares, están sometidos a la norma citada, siempre y cuando la no entrega de la información pueda acarrear una vulneración a cualquier derecho constitucional.

Debe analizarse la solicitud y sobre todo el potencial riesgo que haya con la entrega de la solicitada información.

Acceso no autorizado a una cuenta de correo.

La Norma:

“ARTÍCULO 195 del Código Penal. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirllo, incurrirá en multa.”^{[2]»^[3]}

El Caso:

Exempleado, con base en el artículo 195 del Código Penal, vigente para ese momento, denuncia penalmente al Administrador del correo de la empresa y al Vicepresidente de tecnología, ya que “abusivamente” ingresaron a su cuenta de correo de la empresa, la cual estaba protegida con una “medida de seguridad” (contraseña).

La decisión:

El 28 de octubre de 2004, la Fiscalía 57 local delegada ante los Jueces Penales Municipales, precluyó la investigación

por no haber acto “abusivo”, no haberse violado medida de seguridad.

Comentario:

Efectivamente, entre el empleado y la empresa había un acuerdo y términos de uso en donde se establecía expresamente que el correo electrónico era para fines de la empresa y que el empleado no podía esperar privacidad.

Por otro lado, la fiscalía no encontró que se hubiere vulnerado medida de seguridad, ya que el administrador al ser “superusuario”, no tenía necesidad de conocer o usar la contraseña de quien denunciaba.

Acceso no autorizado a imágenes alojadas en portátil de la empresa.

La Norma:

Intimidad y Buen Nombre. *“Artículo 15 de la Constitución Nacional. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.”*

Honra. *“Artículo 21 de la Constitución Nacional. Se garantiza el derecho a la honra. La ley señalará la forma de su protección.”*

El Caso:

Empleada, había almacenado imágenes de contenido sexual en el portátil que le había sido entregado por parte del empleador. La empleada le prestó el portátil

a un compañero de trabajo, el cual informó al empleador de las imágenes. El empleador enterado de la situación, le solicita a la empleada su renuncia y ésta interpone una acción de tutela en contra de la empresa.

La decisión:

El 24 de mayo de 2007, la Corte Constitucional, protegió la intimidad, honra, buen nombre así como la autodeterminación sobre la imagen de la empleada y ordenó a la empresa la destrucción de las imágenes.

Comentario:

La Corte fundó su decisión en que, no obstante existir un acuerdo de destinar el equipo exclusivamente a aspectos laborales, las imágenes encontradas estaban en una carpeta denominada “mis imágenes”, lo que implicaba el deseo de tener privacidad.

Requerimiento judicial de copia de correos electrónicos del servidor de una empresa.

La Norma:

Intimidad e Inviolabilidad de correspondencia. *“Artículo 15 de la Constitución Nacional. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*

...La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley...”

El Caso:

Dentro de un trámite arbitral se solicitó como prueba la copia de los correos electrónicos tomados del servidor de la empresa. El Tribunal de Arbitramento decretó la prueba, ante lo cual, los empleados de la empresa de donde se tomarían los correos electrónicos, interpusieron tutela en contra del Tribunal de Arbitramento.

La decisión:

El 4 de septiembre de 2007, la Sala Civil de la Corte Suprema de Justicia, no tuteló los derechos reclamados, toda vez que no se vulnera la intimidad o la inviolabilidad de la correspondencia cuando existe un mandato legal.

Comentario:

Este caso es un claro ejemplo que cuando existe una orden judicial, ésta debe ser acatada. En la misma decisión, se ordenó además, hacer un filtro, para que los correos electrónicos tuvieran relación con los temas del proceso judicial.

Correos electrónicos aportados a un proceso sin autorización judicial.

La Norma:

Intimidad. *“Artículo 15 de la Constitución Nacional. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas...”*

Debido Proceso. *“Artículo 29 de la Constitución Nacional. El debido proceso se*

aplicará a toda clase de actuaciones judiciales y administrativas...”

Acceso afectivo a la Administración de Justicia. *“Artículo 229 de la Constitución Nacional. Se garantiza el derecho de toda persona para acceder a la administración de justicia. La ley indicará en qué casos podrá hacerlo sin la representación de abogado.”*

El Caso:

Dentro de un proceso de divorcio, la mujer aportó en un interrogatorio de parte, correos electrónicos tomados del computador y de la cuenta que compartía la pareja. Ante tal situación, el perjudicado interpuso acción de tutela en contra del Juez para que desestimaran los correos aportados.

La decisión:

El 18 de septiembre de 2008, la Corte Constitucional protegió la intimidad, el debido proceso y el efectivo acceso a la administración de justicia, por correos obtenidos sin autorización judicial.

Comentario:

Al haberse aportado correos electrónicos sin que hubiere medido una orden judicial, ningún juez puede tenerlos en cuenta. Lo anterior no obsta para que de manera oficiosa, el juez decreta pruebas encaminadas a descubrir la verdad y generar convencimiento, para proferir una sentencia.

Desarrollos internacionales

A nivel internacional ya es pacífica la jurisprudencia y la ley que, como consecuencia de las múltiples condenas a las empresas, previo acuerdo con los empleados y con “conocimiento consenti-

do”, impongan los mecanismos que estimen pertinentes para proteger la propia información de la empresa, así como de eventuales responsabilidades en el ámbito, penal, civil y comercial.

En resumen, en países como los Estados Unidos, respecto de las herramientas electrónicas entregadas al empleado por la empresa, existe un principio que los empleados no pueden esperar la más mínima privacidad o confidencialidad y en caso de sospecha de alguna actividad, que perjudique o pueda perjudicar a la empresa, se aplica la política de “cero tolerancia”.

Conclusiones

Actualmente en Colombia, ante la ausencia de orden judicial, la Jurisprudencia constitucional es unánime en proteger la intimidad y confidencialidad de los empleados, así medie acuerdo entre las partes de no existir tales derechos.

La anterior situación va a tener necesariamente que cambiar, toda vez que como ocurrió en otras latitudes, la empresa debe protegerse y hacer cumplir la ley, lo cual sólo se puede garantizar de una manera eficiente y diligente, mediante la aplicación y empleo de herramientas tecnológicas de control.

Finalmente, la gran disyuntiva del empresario colombiano es, no supervisar

para evitar condenas vía tutela, o supervisar y someterse a una condena adversa. En el primer escenario el empresario expone sus más importantes activos por la posibilidad de fuga y una eventual responsabilidad de la empresa; y en el segundo escenario, correrá la posibilidad de fuga, de responsabilidades y si es demandado vía tutela, la orden del juez será cesar en la actividad vulneradora de los derechos constitucionales.

¿Cuál escoge usted?

Notas al pie de Página

^[1] El Código General del Proceso, en estudio en el Congreso, define en su artículo 243, las distintas clases de documentos así: “Artículo 243.- Distintas clases de documentos. Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.”

^[2] Este artículo fue modificado el artículo 25 de la ley 1288 de 2009 (declarada inexecutable el 16 de noviembre de 2010), el cual fue derogado por el artículo 4 de la ley 1273 de 2009.

^[3] Una norma similar es la que se encuentra vigente en el artículo 269 A del Código Penal

Rafael Hernando Gamboa Bernate. Abogado, Pontificia Universidad Javeriana de Bogotá. Master en leyes (LL.M.) en Tecnologías de la Información y Privacidad de The John Marshall Law School Chicago. Master en leyes (LL.M.) en Propiedad Intelectual de The John Marshall Law School Chicago. Ha sido Profesor de posgrado en las universidades de los Andes, UPB Bucaramanga, UPB Medellín, Antioquia, Javeriana Bogotá, Externado, El Rosario, La Sabana, Sergio Arboleda. Trabajó con el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá; con Caracol y RCN Televisión. Actualmente es miembro de la oficina de Abogados Bernate & Gamboa Abogados.