

LA PROBLEMÁTICA DEL CORREO ELECTRÓNICO EN LA EMPRESA

ALBERTO SOTO*

Consideraciones previas

El correo electrónico se ha transformado en un servicio muy eficiente para los usuarios particulares, y una herramienta estratégica para muchas empresas, tanto en el desarrollo de las estrategias de negocios con sus clientes, como para la administración y desarrollo del trabajo de uno de los recursos internos más valiosos que tiene: su personal.

Sólo será considerado el correo electrónico de una empresa, y específicamente en lo que hace a su uso por el personal de la misma.

Es evidente que este particular tema nos exige tratar de determinar todos los elementos componentes y sus inter y extra relaciones. ¿Por qué la necesidad de análisis de estas relaciones y de cada uno de sus elementos? Transcribiré parcialmente dos mails cursados en un grupo de trabajo (vía correo electrónico) donde estábamos tratando el tema uso del correo electrónico en una empresa, y la determinación de la responsabilidad ante la comisión de un acto ilícito:

* Profesor de Matemáticas y Cosmografía, Profesor de Física, Experto Universitario en Sistemas y Abogado. Actualmente es Gerente de Tecnología y Comunicaciones de Technisys S.A. Buenos Aires, Argentina.

Coincidió parcialmente con esta opinión de los medios comisivos, pero debemos recordar que en Argentina, como en muchos lugares del mundo, en materia penal no existe analogía, razón por la cual, si un delito no está tipificado, no es delito. Es muy distinto en el ámbito civil o comercial.

Además, debemos tener en cuenta el aspecto procesal, y dentro del mismo, las pruebas. En México, a un Juez de Primera Instancia, le pregunté sobre la responsabilidad en la emisión de correo electrónico, y me respondió rápidamente: es de la persona que tiene asignada la computadora. Le respondí que hay errores atribuibles a los vendedores de software, a los programas de computación, que implican a los que están sentados en una computadora personal en una red, sin ser los responsables de dichos errores.

Este segundo ejemplo es una de las respuestas al anterior:

Sobre lo que comenta respecto a la pregunta que le formuló a un Juez de Primera Instancia en México. Eso que dice es cierto. Hace aproximadamente 3 años en la Universidad de Guadalajara sucedió algo curioso: Una persona de otra Universidad ingresó al sistema red de la Rectoría General a través de la cuenta de un usuario localizado en un centro universitario. ¿Qué ocurrió? Lo siguiente: se envió un mensaje en son de broma a los usuarios registrados en la lista del rector general, cuando se estaba debatiendo la asignación de recursos extraordinarios a esta casa de estudios. Se localizó la fuente emisora del mensaje y lo primero que se hizo, fue rescindir la relación laboral del usuario, por “FALTAS DE PROBIDAD Y HONRADEZ”, contempladas en la Ley Federal del Trabajo. El trabajador se presentó ante la Junta de Conciliación y ganó la reinstalación. El motivo fue sencillo: NO PUEDE DETERMINARSE A CIENCIA CIERTA QUE LA PERSONA QUE ESTÁ CONECTADA SEA QUIEN ENVIÓ MENSAJES A TODOS LOS MIEMBROS DE LA RED, TODA VEZ QUE EL SISTEMA DE CONEXIÓN MOSTRABA FALLAS EN LOS SISTEMAS DE ACCESO A LA RED, ADEMÁS DE QUE LO CONTENIDO EN EL MENSAJE NO EQUIVALÍA A LO SEÑALADO EN EL AVISO DE RESCISIÓN. Más tarde volvió a ocurrir lo mismo y bueno, ahora sí, el Administrador de la Red en el Centro de Cómputo de Alto Rendimiento (CENCAR) localizó al intruso. Esta persona descubrió una falla que dejaba la puerta abierta para ingresar al sistema de la Universidad desde su computadora.

En este último ejemplo, hubo voluntad en cometer un ilícito, y además aprovechó una falla en el sistema: puerta abierta significa desde el punto de vista informático, una puerta que debería estar cerrada, tal como un port de comunicaciones, o un acceso a un programa que debería estar protegido con una clave de acceso y no lo está.

Como vemos por estos ejemplos anteriores y por otra buena cantidad que no es necesario insertar en este momento, tenemos la imperiosa necesidad de analizar todos los componentes involucrados, si en realidad no queremos cometer ciertos errores como los citados anteriormente.

El propósito principal es justamente intentar identificar a todos esos componentes, analizarlos y ver cómo podemos arribar a una conclusión que conjugue necesidades de uso, intereses, costos, impedimento de abuso en el uso, costo de los recursos involucrados, y las relaciones jurídicas necesarias en este complicado proceso, para que nos ayude a determinar el bien jurídico protegido y las responsabilidades ante hechos ilícitos que lesionen ese bien.

Por lo tanto, la visión será una combinación de tecnología informática y derecho aplicado, o al menos las sugerencias que tiendan a cubrir las faltas del mismo, que en algunos países están en este momento siendo analizadas, mientras que en otros no se le da la importancia que realmente requiere.

Componentes tecnológicos

Para que un servicio de correo electrónico funcione adecuadamente, debe contener los siguientes componentes que paso a describir.

Una computadora, la mayoría de las veces dedicada, a la que se denomina servidor de correo electrónico. Esta computadora (hardware) debe contener dos programas (software), uno de base (sistema operativo) y otro de aplicación, que brinda todo lo nece-

sario para gestionar el correo electrónico. El ejemplo de software de base: Linux, o Windows NT. Ejemplo de software de aplicación: Squirrel o MS EXchange.

Una red de comunicaciones interna (red de área local), donde estén integradas las estaciones de trabajo (computadoras personales, generalmente). Cada una de estas estaciones de trabajo deben a su vez contener un sistema operativo, y varios de aplicación, tales como el programa de correo electrónico que “conversará” con el servidor de correo. Ejemplo de este programa: Outlook Express y también Mozilla. Comúnmente se lo denomina “cliente”. Y hasta aquí encontramos lo que en un sistema de información se denomina una arquitectura “cliente-servidor”.

En cada estación de trabajo además pueden, aunque quizás deberíamos decir deben, existir otros programas de aplicación, tales como un procesador de textos, una planilla de cálculo, un utilitario para presentaciones, por decir los más comunes. Con ellos podremos trabajar con los agregados (attach) a los correos electrónicos, tanto para preparar los que enviamos, como para poder procesar los que recibamos.

La empresa debe contar con por lo menos un Administrador de Correo Electrónico, según la envergadura de la misma, que haya recibido la capacitación correspondiente. Es quien, según directivas recibidas de su gerente, dará el alta, las bajas y las modificaciones de los usuarios de dicho sistema de correo, y además se encargará de la resolución de toda la problemática que se presente en la operación. Un ejemplo: debe controlar el espacio en disco de ese servidor de correo, y en particular el espacio en disco que está ocupando cada usuario en lo que se denomina normalmente su “casilla de mail”, además de la seguridad de ese sistema de correo.

También es necesario un vínculo de comunicaciones, que ligue a la empresa con Internet. Este vínculo puede ser o no permanente. Para que funcione adecuadamente debe contar con un dispositivo electrónico (ruteador) que debe “entenderse” con otro similar que está en el otro extremo de ese vínculo, en el proveedor de Internet.

La seguridad informática de acceso, y también de egreso, se logra a través de otro computador que tiene un programa, conocido con el nombre de Firewall, cortafuegos o pared de fuego.

Otros componentes necesarios, que podrían estar en la empresa o ser brindados como servicios por el proveedor de Internet, son los servidores de dominio. Se utilizan dos computadoras, una que hace de servidor primario y otra de servidor secundario, siendo este último respaldo del primero. Éstos se ocupan de realizar la administración de dominios y una traducción entre números de una dirección denominada IP (Internet Protocol), conformada por cuatro particiones (vg.: 192.168.21.33) y nombres de dominio (vg.: www.empresa.com.ar), para que los veamos como tales. Es decir que yo escribo un mail para pepito@empresadepepito.com y los servidores de dominios “traducirán” ese nombre en una dirección IP como la citada (numérica) y comenzará a buscar en la red esa dirección IP; cuando la encuentre, el servidor de dominios de la empresa de Pepito, hará la traducción inversa de número IP en nombre de dominio.

Todo esto si la empresa cuenta con una sola ubicación física. Para el caso de varias sucursales, las posibilidades de ingeniería informática para configurar una solución son muchas, así que no la complicaremos más allá de este punto.

Componentes legales

El ítem tecnológico es más fácil de determinar. ¿Cómo determino los componentes legales?

Solamente analizando el uso del correo electrónico, y verificando las posibilidades de hechos ilícitos, de derechos lesionados, de graduación de daños provocados, de determinación de competencia, de responsabilidades, de medios probatorios, y sobre estos últimos cuáles son y cómo obtenerlos.

Todo ello en cada uno de los componentes tecnológicos citados en el párrafo anterior, el que a su vez se halla plagado de irregularidades técnicas cuyo origen radica en imprudencia, negligencia o impericia; responsabilidades no determinadas entre proveedor de hardware o software o servicios, de fallas cuya resolución técnica es solucionada en minutos, horas o días, y cuyas consecuencias legales no pueden ser analizadas a la luz de legislación inexistente.

Personalmente estoy suscrito a varios servicios de correo electrónico que hacen a la seguridad de la información (virus, criptografía, información general, etc.), algunos con frecuencia diaria.

He realizado un análisis de uno de ellos, que tiene frecuencia de información diaria, cuyo objetivo es informar fallas de seguridad informática, sin importar color o marcas.

Expone la falla, quien la investigó, cuál es la vulnerabilidad descubierta, cuál es el producto involucrado citando la marca, la versión, la fecha y todo detalle técnico que es necesario para entender de qué se está hablando, informando a su vez la existencia o no de solución para el problema presentado, y en caso de existir cómo es o dónde debe buscarse la misma.

En el análisis de información de un año de publicación, he encontrado “agujeros” de seguridad, por ejemplo, en productos de una conocidísima corporación, con juicios por monopolio en EEUU de América, y por la misma causa otros que se están iniciando en Europa. Muchísimos de esos agujeros de seguridad, unidos a la complejidad de configuración de sus productos, han llevado a determinar la imputación de responsabilidades a quienes no la tenían. Y con mi doble experiencia de informático y abogado, veo otras tantas fallas técnicas que se suman a la falta de legislación o fallas en la misma. Y solamente estamos hablando sobre una pequeña parte de la seguridad de la información referida a correo electrónico, y no hemos tocado temas como contratos electrónicos, validación de certificados digitales, tipificación de delitos informáticos, competencias en comercio electrónico, marcas y dominios, spam, hackers, derechos de autor en el ciberespacio, privacidad de los datos, regu-

lación de actividades de prestadores de servicio de Internet, leyes sobre teletrabajo, regulación o no de contenidos de Internet, protección de menores y dignidad humana en la red, validez de la identificación biométrica, ...y dejemos por ahora aquí.

Es decir, los componentes legales, son pocos, o no existen. Sí, hay jurisprudencia que puede ser tomada en cuenta, y que citaré más adelante.

Más difícil aún en sistemas como el nuestro, provenientes del Derecho Romano, donde un acto no tipificado no es delito.

El Correo electrónico y el Derecho a la intimidad y/o Derecho a la privacidad

Vemos la etimología, según el Diccionario de la Real Academia Española:

Intimidad.

1. f. Amistad íntima.

1. f. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.

Privacidad.

2. f. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión

La diferencia que hace la Real Academia Española es importante: la intimidad está referida a “espiritualidad íntima” mientras que la privacidad a la “vida privada”.

Sin embargo, veremos que muchos juristas utilizan estos términos básicamente como sinónimos, causando una verdadera confusión al respecto.

Otros, toman al término privacidad, más relacionado al aspecto de protección legal que tienen que tener los datos de una persona.

Davara Rodríguez define privacidad como

término al que podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona —su titular— y que en ellos se pueden analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad.

Adhiero a este concepto. Desde el punto de vista informático, hablamos de datos y de información. Un dato es un elemento que por sí solo no tiene relevancia, pero que junto con otros datos, me brinda información. Es decir que si tengo varios datos y los proceso adecuadamente, obtendré información. Veamos un ejemplo: Tengo en una empresa una base de datos de personal, si tomo cada uno de los siguientes datos por separado —nombre, apellido, número de legajo, domicilio particular, domicilio de un familiar cercano, teléfono particular, teléfono de un familiar cercano, puesto de trabajo, haber mensual, cantidad de hijos, color de ojos, número de calzado, religión, sexo, peso, deporte preferido, etc, etc.—, no tengo absolutamente nada, pero si los veo a todos ya juntos, realmente tengo información bastante completa de la vida de un empleado. Y sí que tiene relevancia.

En Derecho Informático decimos justamente que el bien jurídico protegido es la Información.

Luego, ¿qué es el derecho a la intimidad? Es el derecho que tiene la persona o grupos de personas a que su vida íntima, su espiritualidad sea respetada. Es decir, que no exista intromisión ni divulgación de la información.

¿Y qué es el derecho a la privacidad? Es el derecho que tiene la persona o grupo de personas de protección sobre cierto ámbito,

también respecto de sus actos, que se traducen en información sobre él o ellos.

Pese a la confusión de estos términos, sugiero utilizar el de privacidad, como más ajustado jurídicamente a nuestro objeto de estudio.

Hablemos entonces de privacidad de la información dentro de un ámbito. Dentro de los distintos ámbitos nos topamos con el ámbito laboral, y dentro del mismo con un sistema de información y dentro de ese sistema de información, con el correo electrónico.

Ahora, el correo electrónico es provisto y pagado por la empresa, a fin de su utilización por parte del personal de la misma, y como toda herramienta de la empresa, para el cumplimiento de los objetivos de la misma.

Para el cumplimiento de esos objetivos, toda empresa debe tener normas escritas para ser cumplidas por su personal, y existe obligatoriedad de su cumplimiento. Esta normativa es el marco de acuerdo entre empleado y empleador, y rige sus relaciones. Muchas de ellas están de acuerdo con normativas de orden superior, tales como las leyes laborales. Pero también con leyes como la de Protección de Datos Personales, y este punto de cruce o de zonas oscuras o con poca luz, es el ámbito donde deberemos movernos.

Ahora bien, partimos de la siguiente concepción: el correo electrónico, no difiere del correo epistolar. ¿Por qué ese punto de partida? Porque tanto la jurisprudencia como la legislación, están tendiendo a su equiparación y a realizar un tratamiento similar.

En Argentina, la Resolución de fecha 4 de marzo 1999, emitida por la Cámara de Apelaciones Criminal y Correccional, Sala 6, en los autos “Edgardo Martolio c/Jorge Lanata s/querella”, equiparó el correo electrónico a la correspondencia epistolar y lo amparó con su garantía constitucional.

Pero en algunos países, la excepción a tal protección amplia, está dada por la distinción que realizan respecto del correo electrónico generado a partir de una relación laboral.

Sintéticamente, se está avanzando en este camino: la equiparación del correo electrónico al correo epistolar, y por ende a darle la misma protección respecto de su privacidad.

Legislación y jurisprudencia sobre el uso del correo electrónico en la empresa

Una carta en papel no produce ni introduce virus en ningún lado, y nadie envía muchas cartas por correo a muchos destinatarios porque cuesta mucho dinero; con estos sencillos ejemplos empezamos a ver la diferencia de consideración dentro del ámbito laboral.

Es decir, cuando no hay normas internas y comienza a producirse falta de control y entran o se propagan virus, con el consiguiente perjuicio para la empresa, cuando se saturan las redes por el envío masivo de mails con agregados muy “pesados” (que son de envergadura respecto de su tamaño), cuando el contenido del mail se convierte en un ilícito (agravios, injurias, revelación de datos personales), es donde tenemos que ver qué dicen las leyes laborales y las que podemos aplicar respecto del correo electrónico en la empresa.

Veremos algunas de esas leyes, citando la de protección de datos personales, y luego varios ejemplos donde el Juez interviniente o la Cámara de Apelaciones, realizan citas de legislación laboral o jurisprudencia sobre esta temática.

Transcribo el Art. 1 de la Ley de Hábeas Data de la Argentina:

Artículo 1º- Objeto. La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos

de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

El Art 2. de la misma Ley nos será de mucha ayuda en nuestro análisis:

Artículo 2º- Definiciones. A los fines de la presente ley se entiende por:

- Datos personales. Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- Datos sensibles. Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o política e información referente a la salud o a la vida sexual.
- Archivo, registro, base o banco de datos. Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
- Tratamiento de datos. Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
- Responsable de archivo, registro, base o banco de datos. Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
- Datos informatizados. Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- Titular de datos. Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.
- Usuario de datos. Toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros, o bancos de datos propios o a través de conexión con los mismos.
- Disociación de datos. Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

La información que protege esta norma o similares aprobadas en distintos países, puede estar contenida en un correo electrónico, es más, quizás sea introducida voluntariamente en un mensaje electrónico, con el objetivo de causar perjuicio a alguien.

Además, el servidor de correo es en sí mismo, un contenedor de una base de datos que contiene ese tipo de datos, según el párrafo tercero del Art. 2 precitado. También es una fuente de obtención de pruebas para el caso de que las necesitemos. Es muy probable que no sean borrados los mensajes, pero lo más importante, son los registros históricos en éste y en otros servidores de ese sistema de información. Pero, ¿por cuánto tiempo estarán esos registros históricos? ¿Está especificado en la norma interna de la empresa?

Es decir, estaríamos en presencia de un ilícito. ¿Cómo lo investigamos, cómo lo probamos? ¿Quien emitió el correo electrónico, desde donde, lo hizo utilizando una cuenta de un tercero, lo hizo el Administrador del Correo, que tiene acceso y posibilidades técnicas de hacerlo? Tendremos que revisar los componentes tecnológicos que citáramos al principio. Recuerden el primer ejemplo que dimos.

Para ello, tendremos que conformar un equipo multidisciplinario, trabajar muy rápido antes de que los registros informáticos sean borrados (esto porque no hay obligación de que se guarde esta información), y rezar mucho... porque la falta de legislación es la principal causal de no encontrar las pruebas correspondientes,

amén de la complejidad tecnológica, que con buenos profesionales, puede ser superada.

¿Qué pasa con los componentes legales? ¿Tenemos leyes que nos permitan realizar esta investigación? ¿Tenemos una ley que haya obligado a las empresas a guardar información por un determinado tiempo, que nos permita la obtención de pruebas?

¿Existe en la empresa en cuestión, una normativa donde todos los empleados hayan tomado conocimiento del uso del correo electrónico?

Aquí, si tomamos el último ítem, tendremos la punta del ovillo. Son muchísimas las empresas que no tienen ninguna norma respecto del uso del correo electrónico. Si no existe, no podremos exigirle a empleador o a empleado alguno, respecto de lo más básico, qué es la norma interna. Hay jurisprudencia en muchos países, veremos algunos ejemplos en Argentina:

SUMARIO DESPIDO CON CAUSA. Uso indebido de correo electrónico por parte del trabajador.

Recepción y reenvío de e-mails con contenido pornográfico

S. 72/03 - "V.R.I c/Vestiditos SA s/despido" - JUZGADO NACIONAL DE PRIMERA

INSTANCIA EN LO LABORAL N° 24 - 27/05/2003

Juzgo como suficientemente acreditado que la reclamante utilizó repetida y constantemente su horario y herramienta de trabajo (sistema de correo electrónico de la accionada) pese a las indicaciones que en contrario le fueran reiteradamente impartidas, para recepcionar y reenviar el tan particular y en diversos aspectos objetable material literario y gráfico y perturbando al normal funcionamiento de la accionada y personal de la misma en la medida que éste se veía diariamente convertido en pasivo destinatario de las manifestaciones de su estrafalario sentido del humor, para calificar con suma benevolencia al contenido de aquellos mensajes (mails) por medio de los cuales la actora canalizaba una personalidad que no dudo en tipificar —en el aspecto que nos ocupa— como diametralmente opuesta a los linea-

mientos previstos por el ordenamiento legal de aplicación en lo que hace a las conductas que deben observar las partes integrantes de una relación laboral como aquella que mantuvieran los actuales litigantes (Art. 63 y concordantes de la LCT).

Ley 20744-)" (LCT = Ley de Contrato de Trabajo, aclaración del autor del artículo)

Establecida, como se ha destacado, la intervención protagónica de la actora en los sucesos de marras, el proceder disolutorio adoptado en el evento por la principal aparece como ajustado a derecho toda vez que si bien no escapa al suscripto la circunstancia de conllevar quizás la disposición resolutoria un acentuado rigorismo dado que, ante la ausencia de antecedentes sancionatorios de la dependiente podrían haberse utilizado, antes de la cesantía, las penalidades correctoras de menor alcance contempladas por el ordenamiento respectivo, no es menos cierto que las características que revistiera el tan reiterado proceder de la actual reclamante así como el contenido y trascendencia del material por aquella difundido, provee a mi entender de una justa causa al acto rescisorio adoptado por la principal.

Es un fallo importante, donde hubo despido directo, sin preavisos tal como lo prevé la legislación aludida.

Otro fallo es el de la Sala X de la Cámara Nacional de Apelaciones del Trabajo confirmó el despido de una empleada de YPF por enviar correos electrónicos personales en horario laboral. No obstante admitió el reconocimiento a un premio de "bonificación adeudada por cumplimiento de objetivos totales año 1999".

"Así lo resolvió el tribunal integrado por Julio César Simón, Gregorio Corach y Héctor J. Scotti en los autos "G. D. M. del R. c/ Y.P.F. Yacimientos Petrolíferos Fiscales S.A. s/ despido" arribados al tribunal luego del recurso interpuesto por la actora contra la sentencia de primera instancia que le fue adversa.

En la misiva rescisoria —señaló el tribunal— se advierten imputados diversos incumplimientos a la Srta. García, mas cabe poner de manifiesto que, con acreditar uno o alguno de ellos se entenderá ajustada a derecho la disolución del vínculo siempre

—claro está— que resulte suficientemente injurioso a la luz de lo normado por el art. 242 LCT. “Con que resulte probado que la actora dedicó cierta cantidad de tiempo durante su jornada de labor en trabajos que ninguna relación tenían con sus funciones y utilizaba para ello los medios de comunicación de la compañía (por ejemplo e-mails) existiría sin duda una violación al deber de diligencia y buena fe que generaría pérdida de confianza...”, advirtió el tribunal.

No obstante los camaristas expresaron, como lo solicitó la demandante que debía analizarse el contenido de los e-mails porque la “pérdida de confianza”, como factor subjetivo que justifica la ruptura del contrato, debe derivar de un hecho objetivo que, injuriante por sí mismo, se vea agravado por la pérdida de confianza que tal hecho trae aparejada.

La demandante expresó haber sido sometida a una “extorsionante actitud” porque, en su lugar de trabajo ingresaron a los archivos de su computadora ante escribano público, quien labró un acta según la cual la actora prestó conformidad para que se accediera a su casilla personal de correo electrónico informando su contraseña personal o password, alegando insinceridad de las declaraciones del acta de comprobación de hechos.

Pero como no redarguyó de falsedad lo manifestado por el oficial en cuanto a su consentimiento —destacaron los vocales— cabe entender que el mismo existió sin ningún signo de violencia moral, tal como surge de lo expuesto por el escribano.

En consecuencia, al analizarse el contenido de los mails afirmó el tribunal que, de acuerdo al horario de envío y recepción de los mismos, no es cierto que el “ejercicio intelectual” a que alude la actora en su descargo fuera realizado después de hora.

Asimismo, en el informe psicológico que presenta la accionante se advierte que dedicó sus horas libres dentro del trabajo (sin descuidar sus obligaciones) a otro proyecto independiente del tema petrolero junto a algunos compañeros en ocasión de la compra de

YPF por Repsol en que pasó de trabajar 14 horas por día a tener sólo dos horas de ocupación real.

Remarcó el tribunal que el hecho de utilizar las herramientas de trabajo para fines personales —y durante el tiempo de trabajo— contraría deberes del trabajador contemplados en nuestro ordenamiento, tales como el de realizar el trabajo; el de diligencia en especial con dedicación adecuada a las características de su empleo y a los medios instrumentales que se le provean; las directivas genéricas de buena fe, colaboración y solidaridad como así también el deber de fidelidad.

Más allá de que la actora haya obtenido las mejores calificaciones y fuera considerada una excelente empleada a juzgar por los resultados de su trabajo, no cabe soslayar que el empleador la contrató por tiempo y no por rendimiento y que ella distrajo parte de ese tiempo en tareas ajenas y utilizó en forma impropia un medio de comunicación que le brindaba la accionada el correo electrónico, que no está destinado al esparcimiento ni puede utilizarse para realizar solapadamente tareas paralelas sino que es provisto evidentemente para facilitar el cumplimiento del objeto de contrato y, en última instancia, para alguna comunicación personal urgente, concluyeron los magistrados.

En los dos casos anteriores, no hubo violación de la privacidad del empleado, ahora veremos otro ejemplo en Argentina.

SUMARIO

CORREO ELECTRÓNICO. Ingreso a la casilla de e-mail del imputado sin orden de juez competente. Violación al derecho a la intimidad.

Nulidad del acto

C. 19418 - "Grimberg, Alfredo H. s/ sobreseimiento" - CNCRIM Y CORREC DE LA CAPITAL FEDERAL - SALA I - 11/02/2003

El correo electrónico es sin lugar a dudas correspondencia privada que está protegida por la Constitución Nacional y otros tratados sobre derechos humanos incorporados a ella.

El reconocimiento de la libertad de intimidad, y el consecuente derecho a la vida privada, configuran un valor que está estrechamente relacionado con la dignidad del ser humano en función de la idea política dominante en las sociedades en vísperas del siglo XIX. La violación de estas garantías básicas conllevan la nulidad de las actuaciones que dependen de esos actos procesales, más allá de la distinción que la doctrina ha hecho sobre prohibición de prueba y prohibición de valoración de la prueba.

La única forma en que se puede ingresar al ámbito privado es por orden de juez competente, mediante auto fundado, ya que esa es la autoridad a la que se refiere la Constitución Nacional. El hecho de que anónimamente se haya hecho llegar la correspondencia del correo electrónico de la parte imputada, lleva sin duda a la invalidez de dicho acto que es la base de toda posible acusación.

Los fundamentos hacen referencia a leyes de jerarquía suprema tales como la Constitución Nacional, y además a tratados internacionales sobre Derechos Humanos, que en Argentina por la Reforma Constitucional de 1994, muchos de ellos tienen rango constitucional.

Otro fallo: CORREO ELECTRÓNICO. E-Mail. Naturaleza. Valor Probatorio. Protección Jurídica. PRUEBA ANTICIPADA: Allanamiento de computadoras de la demandada para determinar la existencia de correos electrónicos por aquélla remitidos o recibidos. Correspondencia entre comerciantes . Expte. 39749 - "G., D. E. c/C. SA s/ diligencia preliminar" - JUZGADO COMERCIAL N° 18 - Sec. N° 36 - 23/10/2001.

La Corte ha considerado a la inviolabilidad del domicilio y de la correspondencia en términos sustancialmente entrañables, calificándolos como un derecho "básico" o "fundamental" de la persona humana.

No se advierten motivos para que —aún sin existencia de legislación específica— el denominado "correo electrónico" escape a dicha protección, tanto más si así fue admitido jurisprudencialmente en el ámbito del derecho penal, donde la analogía está prohibida (CNCrim. y Correc., Sala VI, marzo 4-999, "Lanata, Jorge").

Sin perjuicio de lo expuesto, el caso en examen debe resolverse considerando que se trata en el caso de mensajes atinentes a una contratación mercantil.

La exhibición de la correspondencia entre comerciantes con motivo de una negociación debe asimilarse a la parcial de los libros de comercio, que es admitida por la legislación mercantil en caso de pleito pendiente, o como medida preliminar, pues reposa en el principio de la comunidad de los asientos.

Sin embargo, se ha dicho que ello no autoriza a efectuar esa exhibición en forma compulsiva, ya que la negativa trae aparejada la sanción prevista por el art. 56, es decir, el litigio será resuelto en función de los libros de su adversario.

Siendo así, la medida requerida aparece violatoria del principio de igualdad procesal que este Juez debe preservar (art. 34, inc. 5° c) del Código Procesal).

Dos fallos de tribunales españoles dejaron sin efecto despidos por uso indebido de e-mail laborales. En tanto que un pronunciamiento avaló la privacidad y el derecho a la intimidad, el otro consideró que la potestad del empleador del despido fue extrema ya que al empleado se lo pudo haber sancionado. Los fallos completos pueden obtenerse en: <http://www.diariojudicial.com/mail-noticia.asp?ID=14331>.

En 1996, un juez federal de Filadelfia, EE.UU., rechazó una demanda presentada por un hombre que había sido despedido por mandar un e-mail "cáustico"; no todos coinciden en que las comunicaciones establecidas a través del correo electrónico laboral no son privadas. Michael Smyth, el empleado en cuestión, enjuició a la empresa para la que trabajaba, argumentando que los comentarios que se habían traído a cuento para despedirlo eran claramente "confidenciales".

En otros casos, por cometer errores en el envío, ha sucedido lo siguiente: "Paul Chung acababa de ser contratado por el Carlyle Group, una empresa estadounidense especializada en inversiones en producción de insumos militares. El joven ejecutivo se había incorporado a la firma para trabajar en las oficinas de la empresa en Seúl, Corea del Sur, y llevaba escasas semanas allí cuando envió el fatídico e-mail que finalmente le costó el empleo. El viernes de la

semana pasada, Chung, de 24 años, se vio obligado a renunciar al Carlyle Group por haber alardeado sus experiencias sexuales y su tendencia al despilfarro por e-mail. El mensaje fue enviado por Chung a través de la red de la compañía a un grupo de 11 amigos que trabajan en una de las oficinas de Merrill Lynch, en Nueva York, Estados Unidos, donde él había trabajado antes de viajar a Corea. Desafortunadamente para Chung, el e-mail fue remitido a miles de personas vinculadas al mundillo financiero de Wall Street, y terminó en la casilla de correo electrónico de varios de sus jefes. La reacción fue inmediata: o renunciaba o lo despedían”.

En el diario *La Nación* de Buenos Aires del viernes 22 de octubre de 1999 en el suplemento *The Wall Street Journal Americas*, sección 2 página 7, también de un artículo a página entera, extraemos lo siguiente:

... a diferencia de las llamadas telefónicas, los mensajes electrónicos a menudo pueden desenterrarse meses o años después de haber sido enviados, y pueden utilizarse como pruebas en casos de litigios contra las compañías o sus empleados.

El título de un artículo a dos páginas del diario *Clarín* del miércoles 8 de diciembre de 1999, en el suplemento *Informática*, página 12: “Internet en el ámbito laboral, un debate que recién comienza: SONRÍA, ESTAMOS REVISANDO SU E-MAIL”.

En este último artículo se mencionan las causas de ese espionaje, citando tres principales: mensajes ofensivos, divulgación de secretos y caídas del sistema.

En Francia, se ha determinado que las cuentas de correo electrónico en el ámbito laboral están amparadas por el secreto de la correspondencia epistolar.

En el caso Tareg Al Baho, Ministere Public / Francoise V, Merc F et Hans H el Tribunal Correccional de Paris condenó a los demandados por violación del secreto de la correspondencia. Los demandados eran directivos de la Escuela Superior de Física y

Química Industrial de París, que interceptaron el correo electrónico del demandante, porque sospechaban que el mismo utilizaba dicho sistema con fines personales.

El Tribunal de Trabajo de Bruselas en mayo del 2002, basándose en el Art. 8 del Convenio Europeo de Derechos Humanos, resolvió que el envío de correo electrónico personal desde la empresa pertenece a la vida privada del trabajador, considerando que el análisis del número de mensaje, su tamaño y su carácter privado, eran datos suficientes para proceder a su sanción, sin necesidad de intervenir el mismo tomando conocimiento de su contenido. El empleador lo había despedido por falta grave, previo acceso a su correo electrónico.

Este último fallo indica a las claras no es necesario “mirar contenidos” para controlar el correo electrónico, sino que pueden utilizarse otras pautas y ejercer un control total sobre los recursos de la empresa.

Normas internas

Antes de realizar alguna conclusión, quiero regresar a este tema, al que considero de fundamental importancia.

La norma interna sobre el uso del correo electrónico en la empresa, debe contener como mínimo lo siguiente:

- ♦ Información sobre la importancia de utilizar una herramienta provista por la empresa, y el significado del nombre de la empresa en el correo electrónico, y la responsabilidad que se asume en el uso de esa herramienta, sea el mail utilizado laboral o personalmente.
- ♦ La explicación anterior debe abarcar los aspectos legales de la responsabilidad civil y penal ante la comisión de ilícitos, y el alcance que le compete al empleado y al empleador.

- ♦ Debe explicitar lo permitido y lo prohibido, conteniendo ejemplos claros.
- ♦ Debe explicitar la funcionalidad del sistema de correo electrónico, con identificación de cargos y nombre de los responsables.
- ♦ Debe asegurar el respeto a la privacidad, pero que el personal tenga conocimiento que se recurrirá a la justicia de ser necesario, y se podrá obtener la orden respectiva.
- ♦ Debe guardarse información que permita la identificación del autor de un ilícito, adecuándose a la legislación vigente en su país, respecto de la forma y los tiempos.
- ♦ La norma debe ser comunicada a la totalidad del personal, en forma fehaciente.

Es una lista muy corta la anterior, pero de gran contenido. Su confección lleva muchas hojas y mucho tiempo, pero es imprescindible contar con ella, para lograr cumplir con los objetivos de la empresa, respetando la privacidad del empleado.

Conclusiones

Evidentemente nos encontramos ante un escenario complejo, donde insisto, nuestra mejor estrategia debe ser el exhaustivo análisis.

Aquí, nos encontramos nuevamente con la biblioteca dividida más o menos en partes iguales: una parte aludiendo a que la empresa es dueña de los recursos involucrados, que su alto costo está destinado a cumplir con los objetivos de la misma, y no a satisfacer las necesidades o gustos personales de sus empleados, con quienes se ha celebrado un contrato de trabajo claro, con un salario estipulado para realizar una tarea también estipulada. Que este contrato está siendo violado por el empleado y que la empresa tiene el derecho de accionar contra el mismo.

Por otra parte, el resto de la biblioteca, si bien reconoce parte de lo anterior, no es partidaria de analizar el costo involucrado, sino los derechos individuales del trabajador, como su privacidad, la falta de fundamento de la empresa a revisar, por ejemplo el correo electrónico del mismo.

Creo que de nuestro análisis, obtenemos los siguientes datos:

- Existe una importante inversión por parte de la empresa para montar eficientemente los servicios que hemos citado, no sólo en recursos informáticos, sino en recursos humanos y la capacitación correspondiente para mantener el correcto funcionamiento del sistema.
- Pero en la mayoría de las empresas no hay normas claras, y hasta no existen en muchos de esos casos, que informen a sus empleados sobre el uso de esos recursos.
- Es normal que el personal de la empresa, con independencia de su cargo o puesto, permanezca en la misma un lapso diario importante, que en muchos casos va más allá del estipulado, y en la mayoría, al menos hoy en día, sin percibir horas extras. Esta larga permanencia horaria, y las negativas o los rostros “feos” de los respectivos jefes cuando deben pedir permiso para realizar trámites, hacen que se vean perjudicados en no poder realizar esos necesarios, a veces imprescindibles trámites personales.
- La evolución histórica de la relación empleado-empleador, nos muestra que de la rigurosidad en la antigüedad, hemos ido pasando por mejoras que se han convertido en sustanciales y son derecho adquirido por el empleado. Y considero que el uso del correo electrónico es uno de ellos.
- Esto siempre que se haga uso y no abuso.
- Existen medios modernos que permiten medir ese “uso o abuso”, sin necesidad de ver el contenido de los correo electrónico.

cos, no sólo en la cantidad emitida, sino recibida y también respecto de su magnitud.

Es cierto que los recursos para ese servicio fueron aportados por la empresa, y también es cierto que el personal requiere del uso del mismo para satisfacer necesidades de orden particular, desde su puesto de trabajo. Además es probable que ese uso sea más barato para la empresa que el costo de que el mismo se retire para realizar dicho trámite. También es cierto que el uso se transforma en abuso.

En mi opinión, y no soy original en ello, es que debemos optar por una posición intermedia. Recordemos el proceso de cualquier norma, pensándolo en la forma más simple posible: existe una necesidad en la población, el legislador trata de cubrirla emitiendo la norma pertinente, es promulgada y luego de transcurrido el tiempo establecido, se presume conocida, entra en vigencia, y cuando es violada, se sanciona su incumplimiento.

Con el uso del correo electrónico debería suceder lo mismo dentro de la empresa:

- En primer lugar, al implementarse los servicios, no sólo de correo electrónico, sino todos los involucrados en el sistema informático, simultáneamente deben ser implementadas las normas correspondientes. Existen varias metodologías en seguridad de la información, y todas coinciden que en debe haber una directiva general denominada Política de Seguridad de la Información, debajo de ellas directivas particulares y detalladas que se denominan Normas y Procedimientos de Seguridad de la Información. Es en las Normas y Procedimientos donde deben estar contenidas las directivas sobre el uso del Correo Electrónico.
- Esas normas deben contemplar no sólo la protección de la inversión y el cumplimiento de los objetivos de la empresa, sino también el hecho de que el uso debido de dichos recursos por

parte del personal, hacen también al cumplimiento de esos objetivos.

- Debe existir un circuito fehaciente de toma de conocimiento de esas normas por parte del personal de la empresa.
- Debe existir un proceso de capacitación en el uso de los recursos de la empresa, aunque también podría llamarse de concientización, de forma tal de prevenir inconvenientes futuros, tanto a la empresa como al personal.
- El personal debe asumir la responsabilidad que le cabe y ejercer sus derechos, conociendo sus capacidades y limitaciones.
- No debe violarse la privacidad del personal, observando el correo electrónico, pero deben tomarse las medidas técnicas de resguardo de información, para que en caso de una conducta ilícita, pueda realizarse la investigación correspondiente a fin de determinar la responsabilidad y posibilitar la obtención de las pruebas necesarias.

Sintéticamente, creo que la legislación sobre correo electrónico, debe obligar a que exista la reglamentación interna de las empresas, dado que es garantía para la misma y para su personal.

Hay muchas empresas que tienen esas normas, pero el espíritu no es el conveniente para mantener este equilibrio. Esta metodología intenta evitar a las empresas los grandes costos incrementales en los recursos involucrados, y que el personal de la misma satisfaga sus necesidades que de otra forma no podría hacerlo. De esta forma ambos podrán, o al menos intentar, cumplir con sus respectivos objetivos.