

II Congreso Mundial de Derecho Informático

ponencia

El uso legítimo del correo electrónico

(Sesión de conferencias sobre *Información y Libertades*)

Alejandra Castro Bonilla¹

¹ Asesora Legal de la UNED, Costa Rica. Licenciada en Derecho y Máster de la Universidad de Costa Rica. Especialista en Derechos de Autor, Ginebra. Doctoranda en Derecho Constitucional y egresada del Máster en Informática y Derecho de la Universidad Complutense de Madrid.

EL USO LEGÍTIMO DEL CORREO ELECTRÓNICO

Alejandra Castro Bonilla

I. ANTECEDENTES

El e-mail, correo electrónico o servicio de mensajería interpersonal, se ha convertido en una herramienta de comunicación eficaz dentro de las instituciones públicas y privadas y para el uso personal de los usuarios independientes. El correo electrónico ofrece una inmediatez en el envío de mensajes, sin necesidad de que el emisor y el receptor estén conectados simultáneamente. A esta transformación que ha sufrido la comunicación en la sociedad de la información, se refiere Fernández Esteban cuando dice: *“Los nuevos medios de comunicación electrónicos modifican radicalmente el intercambio de información que deja de ser dependiente del tipo de transporte para ser un proceso en el que la información se mueve a la velocidad de la luz. Las redes telemáticas permiten que mucha información que era previamente inaccesible y sin valor debido a que estaba en un lugar remoto, se convierta en útil y valiosa a través de la Red. Así, el acceso a bases de datos remotas y la transmisión de datos, sonidos e imágenes en tiempo real a cualquier parte del planeta, son ya hechos consumados. Del mismo modo, personas con las cuales se podía mantener una relación a distancia pueden ser ahora compañeros de trabajo que interactúan de un modo eficaz.”*²

El Libro Verde de la Convergencia de los Sectores de Telecomunicaciones, los Medios de Comunicación y las Tecnologías de la Información aprobado en Bruselas el 3 de diciembre de 1997³ así como otros documentos emitidos por la Unión Europea en los últimos años, consideran al correo electrónico como un servicio esencial para la transmisión de información y la conducción de señales por las redes por lo que incentivan el uso de este medio de comunicación en las nuevas relaciones humanas y laborales.

Efectivamente, el correo electrónico ha permitido la desaparición de las fronteras para el desarrollo de relaciones humanas y ha impulsado el comercio internacional facilitando el acceso a productos e información puestos a disposición de quien lo desee. Incluso la Administración Pública basa sus proyectos más novedosos de *E-government* en esta herramienta de comunicación. Estos cambios que ha introducido la tecnología han reformado al mundo jurídico que ha entrado en una nueva etapa de desafíos, sobre todo cuando están en juego los derechos fundamentales de los usuarios. El ordenamiento jurídico debe hacer frente a esos cambios introducidos en la sociedad de la información para proteger los intereses y derechos de los ciudadanos que vean sus derechos constitucionales afectados. Hasta la fecha, el derecho se ha escrito para la regulación del mundo predigital o analógico y ahora debe adecuarse a las nuevas tecnologías y su impacto en los derechos fundamentales con el advenimiento de la era de la digitalización.

² FERNÁNDEZ ESTEBAN (María Luisa). 1998. *Nuevas tecnologías, Internet y derechos fundamentales*. Editorial Mc Graw Hill, Madrid, p. XX

³ Libro Verde de la Convergencia de los Sectores de telecomunicaciones, los medios de comunicación y las tecnologías de la información aprobado en Bruselas el 3 de diciembre de 1997, visible en la página <http://www.info2000.csic.es/midas-net/docs/lvmedia/lvmedia.htm>

El derecho a la intimidad como pilar fundamental de la protección a la individualidad de la persona se ha visto vulnerado por el trasiego indiscriminado de datos que sobrepasa las fronteras y la soberanía de cada región, con una rapidez y facilidad sorprendentes. Igualmente, este derecho es hoy objeto de estudio ante el uso del correo electrónico en el tanto la interceptación de mensajes por ese medio puede significar una intromisión en la vida privada del usuario.

Internet introdujo una modalidad de tratamiento invisible de los datos⁴ que se ha acentuado a través del comercio electrónico. Todos los días miles de ciudadanos proporcionan sus datos personales (identificatorios de la personalidad y hasta crediticios) de forma expresa o tácita a empresas públicas y privadas a través de Internet, generalmente utilizando su dirección de correo digital. Eso provoca que –pese a la seguridad imperante– las empresas realicen ciertos tratamientos de datos que no son perceptibles al usuario, ya sea porque se presentan en principio como intrascendentes o bien porque se obtienen sin el consentimiento del usuario o a expensas de omisiones ilegítimas de información que afectan su autodeterminación informativa.⁵

En este estudio analizaremos esa vulnerabilidad de derechos de la persona ante el uso del correo electrónico, y aspectos entre los que se incluyen la intimidad en las comunicaciones privadas y la naturaleza pública o privada de este medio de comunicación; con el fin de proponer un acercamiento hacia un derecho que regule estas nuevas fronteras de la información en beneficio de la protección de los derechos fundamentales de los usuarios de Internet.

II. NATURALEZA JURÍDICA DEL CORREO ELECTRÓNICO

Como adelantamos, el correo electrónico es un nuevo medio de comunicación que permite la transmisión de datos, el flujo o distribución de material de toda índole, incluso protegido por el derecho de autor, transacciones económicas y correspondencia en general. Este servicio de Internet lo define Corripio diciendo que: “*El correo electrónico constituye un servicio de mensajería electrónica que tiene por objeto la comunicación no interactiva de texto, datos, imágenes o mensajes de voz entre un «originador» y los destinatarios designados y que se desarrolla en sistemas que utilizan equipos informáticos y enlaces de telecomunicaciones.*”⁶ Dependiendo de la perspectiva desde la cual se le analice, el correo electrónico posee una distinta naturaleza. En general, tiene una naturaleza múltiple que analizaremos en tres vertientes, retomando la clasificación inicial que hacía Corripio en la obra citada supra:

1. Como correspondencia o comunicación: El correo electrónico posee una idéntica naturaleza a la del correo tradicional, con la diferencia de que las comunicaciones (equivalentes del correo ordinario) se transmiten a través de la Red mediante tecnología digital. Por tanto, el secreto de las comunicaciones en el email se encuentra protegido igualmente dentro del art. 18.3 de la Constitución Política Española (CE) pues su equivalencia con el correo tradicional es evidente. Por ello en principio y como norma básica, el correo electrónico también es inviolable y no puede ser interceptado, abierto, manipulado, retenido o violentado de cualquier forma sin autorización

⁴ Por ocultarse los mismos al usuario, como por ejemplo los datos de conexión, los que identifican el IP (dirección personal de la computadora o protocolo de Internet).

⁵ Ver en este sentido el artículo: Alejandra Castro. *El Recurso de Habeas Data en la protección del derecho a la intimidad: el caso de España y la nueva legislación latinoamericana*

⁶ CORRIPIO GIL-DELGADO (María de los Reyes) 2000. *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*. Agencia de Protección de Datos. Madrid, p.68

judicial o con el consentimiento expreso del usuario de la cuenta. Si coincidimos en que la naturaleza del email es una comunicación, queda por lo tanto protegido por esta norma, aunque una redacción más precisa y acorde con las nuevas tecnologías, debería indicarlo expresamente.

La información que consta en torno al correo electrónico pertenece a la vida privada tanto si nos referimos al contenido de los mensajes como a la dirección IP que queda evidenciada en una transmisión y a la misma dirección electrónica (elemento identificatorio como el ID del correo electrónico⁷ así como el elemento que determina el servidor que proporciona el servicio⁸) todo lo cual va a constar como datos personales del usuario⁹, según lo veremos más adelante. Por tanto, tanto los datos recibidos como los datos enviados desde la cuenta de correo, constituyen elementos protegidos bajo el principio de inviolabilidad de las comunicaciones.

2. Como conjunto de datos: El correo electrónico es un conjunto de datos personales del usuario y como tal, su manipulación se encuentra supeditada a las normas relativas a la protección de datos personales.

Con los datos obtenidos a través de una cuenta de correo se puede constituir el perfil de un usuario, quedando vulnerada con ello su intimidad, su vida privada. Por ejemplo, a simple vista una dirección puede evidenciar el nombre y apellidos del usuario, el lugar geográfico de origen, su lugar de trabajo e incluso aspectos más delicados como su inclinación política, religiosa o sexual, dependiendo del servidor que proporcione la dirección de correo. En el caso que el usuario haya proporcionado más datos de su vida privada en el momento de adquirir la cuenta, también desde su perfil se pueden determinar números de teléfono, dirección domiciliaria, gustos o incluso su profesión.

Dentro del conjunto de datos también la transmisión de mensajes electrónicos hace posible que pueda averiguarse la dirección IP del usuario (protocolo de Internet) que es en sí misma un dato personal, pues si se llega a descifrar la misma, se puede identificar la terminal del usuario (y en ocasiones con cierta destreza acceder a sus archivos) pero también la situación nominativa del titular. Todo esto pone en evidencia que el correo electrónico condensa una serie de datos del individuo, cuya manipulación (muchas veces invisible para el usuario) podría poner en vulnerabilidad su derecho a la autodeterminación informativa.

3. Como transmisor de material protegido por el derecho de autor: Finalmente, la naturaleza del correo electrónico puede ser analizada desde la perspectiva del derecho de autor, en el tanto sea un medio de comunicación por el que se transmitan obras literarias, científicas o artísticas.

Al permitir el trasiego de documentos en formato de texto, imagen o sonido, e incluso archivos multimediales, el correo electrónico se ha constituido en una herramienta de difusión de material protegido por el derecho de autor. De allí que pudiera ser un medio que ponga en flaqueza los

⁷ componente previo al símbolo “@”

⁸ componente posterior al símbolo “@” que muchas veces puede identificar desde una empresa hasta una zona geográfica.

⁹ Serían datos empresariales o públicos si el servicio es un correo electrónico laboral o de la Administración Pública, como lo analizaré en la tipología del email.

derechos de propiedad intelectual en la medida que el trasiego de material protegido a través de esta mensajería sea indiscriminado, ilegítimo y lesione el normal comercio de las obras.

El email efectivamente transporta material que ha sido digitalizado y por ende es de fácil transmisión, e imperceptible salvo para el emisor y los destinatarios, lo cual es uno de los problemas derivados de las nuevas tecnologías. El contenido mismo del mensaje de correo (aún si no se transmite una obra literaria, artística o científica) sería susceptible de protección en calidad de derechos de autor del titular de la cuenta, por cuanto si posee una naturaleza similar a la del correo ordinario o cartas¹⁰, la obra estaría protegida por ser precisamente una carta personal pero en formato digital. Para ello, deberá ser siempre original, que no implique un mero mensaje informativo y que contenga las características de identificación de la personalidad.

Sobre la protección del contenido de los correos electrónicos a partir de la propiedad intelectual, dice Asensio: *“Ahora bien, la protección por la propiedad intelectual del contenido de los mensajes de correo electrónico resultará limitada, en particular tratándose de breves mensajes de texto. No sólo por las restricciones de los artículos 31 y siguientes LPI, sobre todo respecto al contenido informativo de los mensajes (arts. 33 y 35 LPI), y del artículo 51 sobre la transmisión de los derechos del autor asalariado, sino fundamentalmente porque en la medida en que estos mensajes de texto son con frecuencia obras muy sencillas se reduce la posibilidad de que presenten el necesario carácter original, éste sí estará presente con frecuencia cuando se trate sobre ciencia, política, cultura o sectores muy especializados, pero normalmente quedarán al margen de la tutela específica de la propiedad intelectual, entro otros, los mensajes referidos en términos comunes a asuntos habituales, cuestiones técnicas simples o cartas comerciales...”*¹¹

Debemos anotar, sin embargo, que en su mayoría los correos electrónicos son simples mensajes con redacción suscita que permiten la interacción de un modo muy similar a las conversaciones simultáneas, pero en formato escrito, por lo que pocas veces constituirán material semejante a un epistolario digital.

III. TRATAMIENTO DEL CORREO ELECTRÓNICO SEGÚN SU TIPOLOGÍA

A partir de la naturaleza compuesta descrita en el apartado anterior, debo referirme a la tipología de correos electrónicos que existen, en virtud de la cual se ha desatado una polémica en torno a la legalidad de la interceptación del correo y la propiedad de los mensajes que se transmiten por este medio de comunicación. Efectivamente la tipología define características disímiles para cada cuenta de correo, por lo cual, deben regir normas jurídicas distintas pero flexibles, justas y proporcionadas.

1. Correo electrónico privado: Como ya explicamos, en principio el correo electrónico es un medio de comunicación privado protegido como una correspondencia inviolable de conformidad con el artículo 18.3 de la CE.

¹⁰ Recordemos que el artículo 10.1.a) del TRLPI español, cita a los epistolarios como obra amparada a los derechos de autor.

¹¹ DE MIGUEL ASENSIO (Pedro). *Derecho privado de Internet*. Editorial Civitas. Madrid 2001. 222-223p.

El correo electrónico más típico en este sentido es aquel que el usuario posee de forma gratuita como un servicio proporcionado por algún *host* de la Red o un proveedor de servicios, e incluso existen direcciones de correo que se ofrecen previo pago de una cuota, lo cual es menos común, en virtud de la facilidad de acceder gratuitamente a una cuenta personal.

En estos casos, los usuarios del servicio quedan supeditados a las normas de seguridad y de uso de la cuenta que aceptan en el momento de realizar la suscripción al servidor que les proporciona el servicio. Este correo es de uso estrictamente personal y por ende no puede ser manipulado, interceptado, intervenido o alterado de alguna forma si no se posee una autorización judicial, pues corresponde legítimamente a una naturaleza idéntica a la del correo tradicional y por ende se encuentra protegido por el secreto de las comunicaciones y por el derecho a la intimidad.

El nuevo derecho de acceso a Internet¹², que es el derecho que tiene todo individuo a recibir los servicios disponibles en Internet como servicios universales, obliga a hacer asequible los servicios de Internet (y por ende de correo electrónico) a todos los ciudadanos del mundo sin distinción de situación política, social, económica, sexual, laboral o geográfica.

En este sentido, no se pueden imponer al usuario trabas o limitaciones para poseer una cuenta de correo electrónico que le permita utilizar este servicio de mensajería de forma gratuita y sin poner en peligro su derecho a la intimidad y a la privacidad de las comunicaciones.

La propiedad de los mensajes que se transmiten por este medio es del titular de la cuenta de correo (del usuario que recibe el servicio) y no del servidor que ofrece el servicio (pues es un simple administrador técnico, una vez que proporciona la facilidad de acceso) y que por consiguiente se encuentra obligado a adoptar las medidas necesarias para proteger al usuario tanto en la manipulación de sus datos, como en lo que respecta a medidas para evitar que su correspondencia sea violentada por un tercero no autorizado. El usuario por su parte, queda obligado a adoptar sus propias precauciones como el resguardo de la clave, *password* o *pin* que se le concede para el acceso exclusivo a su cuenta y a utilizar el servicio según las condiciones que acepte en el contrato de suscripción. La intimidad personal protegida de esta forma, coincide con lo dispuesto en el artículo 2.2 de la LEY ORGÁNICA 1/1982 DEL 5 DE MAYO de España, cuyo objetivo es el resguardo de este derecho fundamental que debe extenderse a los datos e información de la persona constantes en su cuenta de correo o bien en el material que trasiega a través de su dirección electrónica.

El Código Penal español en su artículo 197.1 dice en lo que interesa que: *“El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, será castigado con penas de prisión de 1 a 4 años y multa de doce a 24 meses.”*

El artículo 197.4 del mismo Código Penal, agrava la conducta anterior si los hechos los realiza el encargado o responsable de fichero, soporte informático, electrónico o telemático; por lo que las

¹² Derecho que podría calificarse como de *cuarta generación* en la tipología de los derechos fundamentales, por corresponder a un derecho de la nueva sociedad de la información.

actuaciones del administrador del correo deben estar estrictamente amparadas a medidas de resguardo de los datos del usuario, y todo acuerdo en contrario evidentemente sería inconstitucional y leonino. Por tanto, la protección evidencia la voluntad del legislador de proteger la intimidad de las comunicaciones por email privado contra el descubrimiento y revelación de secretos. El correo, así entendido, debe verse tanto como una correspondencia inviolable como también un domicilio personal (digital) pues por sus características es posible mediante las medidas técnicas pertinentes que cualquier sujeto mal intencionado pueda conocer la dirección IP del usuario o los datos para su ubicación geográfica.

2. Correo electrónico laboral: Si la normativa penal vigente es así de clara como lo expuse en el punto anterior en cuanto a la inviolabilidad del contenido del correo electrónico, en principio no se podrían establecer excepciones que (más allá de la autorización judicial) permitan la interceptación del correo electrónico, pues no podríamos imponer limitaciones donde la ley no las indica expresamente.

Sin embargo, la naturaleza del correo electrónico laboral propone una nueva interpretación en la medida que se considera que su titular (trabajador o servidor público) no es el dueño de la cuenta sino que lo es el patrono que proporciona la misma para fines exclusivamente laborales y por ende las normas deben tender en este caso a proteger los intereses de una persona jurídica como nuevo titular de la cuenta de correo, que la asigna a un funcionario o trabajador para su uso y administración en nombre del cargo que desempeña y para fines estrictamente laborales.

Muchos autores priman la protección del derecho del trabajador a la intimidad dentro del correo electrónico sobre el derecho de los empresarios. Sin embargo debe evaluarse en este caso que hoy en día todo ciudadano tiene amplias posibilidades de poseer una cuenta personal y gratuita de correo electrónico en uno de los múltiples sitios de la Red que proporcionan tal servicio, tales como Yahoo, Hotmail, Terra, AOL, etc. Si el trabajador puede acceder por su cuenta a ese servicio, no existe razón alguna por la cual deba utilizar las cuentas de correo asignadas en su trabajo para fines personales, pues están en juego intereses de la empresa tales como el tiempo invertido por el trabajador para atender asuntos personales, el uso del equipo de la empresa, la imagen de la empresa, la vulnerabilidad de la seguridad de las comunicaciones de la empresa, eventuales daños al patrimonio empresarial o institucional, etc. Por tanto, quienes defienden este argumento consideran que si el ciudadano tiene acceso gratuito a cuentas de correo en Internet, la cuenta de correo que proporciona la empresa no tiene porqué ser utilizada para fines personales o privados. Incluso se autoriza dentro de esta perspectiva, el control patronal sobre el contenido del correo, pues se interpreta que la cuenta no pertenece al usuario sino al patrono.

El almacenamiento informático es cada vez más una realidad tanto en el sector público como en el sector privado. Igualmente, el trasiego de documentos laborales por medio del correo electrónico ha contribuido a que las funciones profesionales y administrativas ordinarias se agilicen y ha logrado conservar un contacto más expedito entre los trabajadores y entre éstos y los usuarios de sus servicios independientemente de la naturaleza de empresa de la que se trata.

El correo electrónico laboral lo constituye aquella cuenta proporcionada por el patrono privado o bien por la Administración Pública a sus trabajadores o servidores públicos (según corresponda), generándose así dos sub-categorías de correo que son:

a.) El correo proporcionado por patrono privado: En la empresa privada existe un porcentaje importante de trabajadores que laboran con cuentas de correo electrónico proporcionadas por sus patronos o empresas para el ejercicio de sus funciones.

En este sentido, el trabajador posee una cuenta que si bien puede contener su nombre para identificación del usuario y la identificación de su persona con los actos que gestiona a través de su cuenta, también contiene un elemento que distingue a la empresa y por medio del cual quedan fusionadas todas sus actuaciones con esa empresa que le otorga la cuenta. Por ello, cada actuación que realice el usuario, indefectiblemente será una actuación que un tercero que reciba un mensaje por esa vía, identificará con la empresa que aparece en la dirección digital.

Si el trabajador utiliza el correo para asuntos personales, como por ejemplo para enviar chistes, mensajes religiosos, noticias, enlaces de Internet o cualquier otra actuación ajena a su trabajo, está utilizando para asuntos personales una mensajería laboral que no le pertenece y sobre todo está sobreutilizando los bienes de la entidad para la que labora y ejerciendo acciones sobre las que no ha sido autorizado por el servidor que le facilita la herramienta de comunicación.

Precisamente por ello resulta imprescindible que de previo a conceder una cuenta de correo electrónico, la empresa advierta al trabajador las condiciones de uso de ese servicio, y que proporcione las medidas pertinentes para que las restricciones del uso del email laboral estén siempre al alcance de los trabajadores, ya sea a través del portal de acceso o exhibido en sitios públicos en el lugar de trabajo. En todo caso siempre será necesaria una comunicación personal al trabajador en el momento de asignarle la clave de ingreso al buzón asignado. Este es sin duda un corolario del derecho a estar informado de los extremos del contrato laboral que afectan al trabajador, información que además debe contener la advertencia de las posibles consecuencias en caso de incumplimiento de las condiciones del servicio.

Igualmente, si el trabajador utiliza el email laboral para fines personales durante el ejercicio de sus funciones (en horas laborales) o bien con los medios empresariales (conexión empresarial a la red, ordenador de la empresa, electricidad a cargo de la empresa, etc.) la situación es aún más compleja pues deja en evidencia que no está destinando su tiempo al trabajo -según lo exige su contrato laboral-, que está abusando de los bienes patrimoniales de la empresa utilizándolos para uso privado no autorizado.

En este sentido, el patrono puede vigilar el uso que se le dé al correo electrónico sin previo aviso y sin intervención judicial, pues se trata de sus cuentas de correo, de sus activos empresariales, de sus documentos laborales; siempre bajo el respeto de la autoridad jerárquica que rige en cada institución, y bajo el entendido de que el trabajador fue debidamente advertido que no estaba autorizado a ejercer ningún uso personal o privado de la cuenta de correo asignada. Sobre este punto, es importante resaltar que en el caso de asignación de una cuenta de correo laboral (privado o de la Administración Pública) se debe informar al trabajador de las limitaciones sobre el uso de tal herramienta, en lo que respecta a lo dictado por el artículo 52 del TRLPI.

El Estatuto de los Trabajadores señala en su artículo 20.3 el derecho del empresario de adoptar medidas de vigilancia y control patronal sobre las actividades de su empresa y de los trabajadores, en aras de asegurar el cumplimiento de deberes laborales, situación que a mi juicio justifica claramente el monitoreo del correo laboral, sin que exista roce de constitucionalidad

alguna con el derecho a la inviolabilidad de las comunicaciones; pues en este caso no se trata de una comunicación personal sino de un instrumento más de trabajo. Si esto es así, la intervención de las cuentas de correo de origen laboral quedaría justificada en virtud de este principio de control patronal pero sobre todo porque la cuenta le pertenece no al trabajador sino a la empresa.

En mi opinión personal, dado que todo usuario de Internet puede poseer una cuenta privada de correo electrónico, y por la finalidad que poseen los correos laborales y la inversión que realiza la empresa en la asignación de las cuentas indicadas, considero que la cuenta de correo del trabajador es propiedad de la empresa y se debe utilizar atendiendo exclusivamente a sus fines laborales.

Lo anterior, no impide que los sindicatos puedan utilizar este medio de comunicación de forma legítima para comunicarse con sus afiliados, y en este caso el patrono no puede alterar el contenido de tal comunicado ni interceptarlo, por imperar la libertad sindical en este asunto y porque se trata de utilizar un medio de comunicación para intereses que indirectamente también tienen estrecha relación con el trabajo en donde interactúan patronos, trabajadores y sindicatos.

En este sentido se debe distinguir entre el mensaje que se envía desde el correo electrónico laboral del que se recibe en esa misma dirección. El que se envía es responsabilidad exclusiva del trabajador usuario de la cuenta, pero el que se recibe es exclusiva responsabilidad del emisor externo, exigiéndosele al trabajador el mínimo deber de diligencia en la manipulación de ese mensaje, de modo que en ningún modo dañe al patrono, como sería la recepción de un archivo contaminado con un virus, de material que afecte derechos fundamentales del usuario o de terceros, recepción de obras protegidas por el derecho de autor o de software ilegal o que atente contra la seguridad general de la empresa, etc..

A ambas partes se les exige un uso diligente del servicio. Si el emisor remite su mensaje a la empresa, por ejemplo, se le podrían limitar los *spams* o mensajes masivos o bien aquellos que pudiesen implicar algún peligro para la entidad. El trabajador que recibe mensajes externos debe tomar también ciertas previsiones en resguardo de los bienes de la empresa, como revisar que el mensaje no contenga virus y evitar la expansión o distribución de mensajes que no tengan relación con las actividades de la empresa y que por el contrario distraigan de sus labores a los demás trabajadores. Tal es el caso de los mensajes bien intencionados como pensamientos de amistad, que tienen gran difusión en la red, pero que en el fondo muchas veces sirven para generar a favor de empresas invisibles para el usuario, bancos de datos con las direcciones de quienes se inscriban en la cadena de emisiones.

En la discusión de si el email es privado o empresarial surge el DERECHO AL USO SOCIAL como el derecho al uso del email, en una campaña elaborada por los sindicatos, la revista *Kriptopolis* y por algunos miembros del propio Parlamento quienes alegan que no se puede poner restricciones al correo electrónico laboral, por que el trabajador ostente el derecho al uso social de una herramienta que proporcionan las nuevas tecnologías.

Sin embargo, considero el correo electrónico como una herramienta puesta al servicio del trabajador para el uso controlado y limitado a su trabajo. Un uso privado del mismo implica mala fe y abuso de confianza pues se debe tener presente que al trabajador no se le está negando el derecho al uso social, pues perfectamente puede acceder a una cuenta de correo privada que no tenga relación con la empresa.

Si el trabajador utiliza el correo que se le asigna en su lugar de trabajo, el nombre de la empresa será relacionado con el contenido de sus mensajes, lo cual podría perjudicar la imagen y el comercio de la organización, coadyuva a que pueda existir mayor facilidad de fuga de datos empresariales y aumenta la posibilidad de importar virus que afecten los bienes del empresario.

El trabajador, además, debe obediencia, discreción, responsabilidad y buena fe en su trabajo a favor de quien lo contrate, por lo que si es expresamente advertido de las condiciones del uso legítimo del correo electrónico, no puede alegar violación a la intimidad en caso de ser monitoreado, ni utilizar el correo para fines distintos a los que encomiende el contrato laboral.

Valga indicar que ese derecho del empresario de resguardar sus intereses se empieza a reconocer en la jurisprudencia. Recientemente el Tribunal Superior de Catalunya dictaminó procedente un despido de un trabajador que en horas laborales utilizaba el correo electrónico para la distribución de mensajes ajenos a la actividad de la empresa. El mismo Tribunal declaró procedente el despido de un trabajador que en horas laborales jugaba al Solitario en su ordenador.

Contrario a esta postura, la justicia francesa recientemente determinó que las cuentas de correo electrónico laborales están amparadas por el secreto de correspondencia. Por ello, el Tribunal Correccional de París condenó a tres jefes de la Escuela Superior de Física y Química Industrial (ESPI) de París por violar el secreto de las comunicaciones de un Kuwaití, Tareg Al Baho, a quien se le intervino el correo electrónico por sospecharse que lo utilizaba para fines privados.¹³ El afectado recibió una indemnización por 10.000 francos, pero hay que indicar que en este caso, nunca se le informó al afectado de la posibilidad que existía de intervenir su correo y del destino exclusivo que debía darle a la cuenta.

b.) El correo proporcionado por la Administración Pública: En el caso de la Administración Pública, también se conceden cuentas de correo a los funcionarios o servidores públicos, con la particularidad que las cuentas identifican al usuario con el Gobierno Central o descentralizado de un Estado. Son cuentas asignadas a los **funcionarios públicos**, para que ejerzan sus funciones ordinarias y para permitir la comunicación entre los servidores públicos, las instituciones estatales y los ciudadanos.

Aquí no solo existe en la dirección un elemento identificatorio de la institución pública sino que existe además una imagen pública de Estado que debe resguardarse tras las actuaciones que se realicen por medio de esa cuenta de correo, lo que hace más sensible el trasiego de datos (de interés público en su mayoría y exceptuando aquellos relativos al expediente personal del estudiante) y la manipulación de este servicio.

Además, los documentos que emiten no son simple mensajería, sino que en la medida que cumplan los requisitos de un documento público, el contenido de los mensajes adquiere una importancia aún mayor, y por ende la publicidad de los mismos también. Si el archivo fue emitido por un empleado público competente, en el ejercicio de sus funciones, contiene los requisitos de un documento público y fue emitido con los medios que facilita la Administración, el archivo es por tanto un documento público aún si es electrónico o digital (no en soporte

¹³ Ver detalle en www.jurídica.com/cgi-bin/noticias_public/mostrar_doc.pl?iddoc=112

material) y por tanto es válido y eficaz. El *Libro verde sobre la información del sector público en la sociedad de la información. Un recurso clave para Europa*. [COM (1998) 585]¹⁴, habla de un “gobierno electrónico” dentro de la Unión Europea, por lo que impulsan decididamente el uso de las nuevas tecnologías en la Administración Pública, dentro de las que se incluye el correo electrónico.

Hay aquí dos asuntos que interesan: el acceso de la Administración para el ejercicio del control de la acción administrativa a través del correo electrónico, y la publicidad que deben tener los documentos que emita la Administración de cara al administrado, aunque dichos documentos consten en los archivos de una cuenta de correo.

El derecho de acceso está relacionado al derecho que ostentan los ciudadanos de participar en su gobierno, controlando, criticando y velando por el buen funcionamiento de sus instituciones. Por tanto, no existiría motivo alguno que limite ese derecho de acceso a los documentos públicos que constan archivados o que se trasieguen por correo electrónico, sobre todo si éste es en sí mismo una base de datos, como vimos en su naturaleza jurídica.

Sin embargo, si bien ese acceso es libre, debe ser controlado. Al efecto, deben establecerse responsabilidades de administración y manipulación del correo administrativo pues el acceso solo debe ser autorizado con ciertas medidas de seguridad básicamente para evitar la alteración del contenido de los documentos o irrupciones en los sistemas informáticos del Estado o sus archivos. Por ende, a tales instrumentos solo accedería personal legítimo que los administren en virtud de una investidura de servidores públicos.

El principio de transparencia exige efectivamente que la Administración ponga a disposición de los ciudadanos todos los documentos que emite, incluso si son digitales y salvo que afecte la seguridad y defensa del Estado; pues el derecho de la información administrativa, el derecho de acceso a los archivos y los registros no declarados *Secreto de Estado* no pueden ser limitados en las nuevas comunicaciones generadas por Internet. Por lo tanto, las comunicaciones electrónicas de la Administración son públicas y no privadas, por lo que no rige en esta tipología el principio de intimidad de las comunicaciones al no haber sujeto pasivo sobre el cual resguardar tal intimidad, pues el Estado es un ente público.

No obstante lo anterior, existe un principio que se ha esgrimido en la nueva sociedad de la información. Se trata del *principio de la seguridad digital*, del que hablaré más adelante, en virtud del cual es legítimo establecer restricciones de acceso a esos documentos (en principio públicos) para evitar un daño ulterior a los bienes e intereses del Estado. Por ello, podríamos decir que el acceso a estos documentos puede ser indirecto a la luz de este principio, pero jamás ese acceso puede prohibirse, ni siquiera a la luz de la intimidad de un servidor público, quien está obligado a no tramitar asuntos personales a través de su cuenta de correo laboral/administrativo.

Tanto en el correo laboral de empresa como en el administrativo, debe procurarse la protección de los documentos que resguarden el secreto profesional tutelado en el art. 199.2 del Código Penal Español. En este sentido, debe considerarse que la norma sobre el secreto profesional trata de secretos precisamente, no de documentos de trámite público. Se protege el derecho de

¹⁴ Visible en la siguiente dirección: <http://www.info2000.csic.es/midas-net/docs/lvisp/lvisp.htm>

intimidad de los clientes o de los administrados, pero no cubre este aspecto el acceso a todo documento público ordinario que se tramite por email. Por ejemplo, es lícito considerar privados dentro de la Administración Pública, documentos sobre los datos personales de funcionarios que consten en una Oficina de Recursos Humanos o trámites legales en proceso de investigación que pudiesen poner en entredicho un secreto de sumario o investigación.

Dentro de los límites a ese derecho de acceso, existen las informaciones que afecten la intimidad de la persona, pero es la intimidad de un administrado cuya información conste en el contenido de un email y no la de un funcionario público a la que se refiere tal principio; pues insisto en que el funcionario está inhibido de tramitar asuntos personales por su cuenta de correo proporcionada por la Administración Pública.

III. LA SEGURIDAD DIGITAL Y EL CORREO ELECTRÓNICO:

La seguridad digital surge como un principio de la nueva sociedad de la información¹⁵ que permite el resguardo preventivo de los bienes propiedad de los agentes que intervienen en los medios de comunicación, y que puedan verse vulnerados con los avances tecnológicos. La seguridad digital puede proteger la información que se resguarda en formato digital [ya sea en línea (en la Web) o en ordenadores públicos o privados] mediante mecanismos técnicos y normas de seguridad empresariales o institucionales que protejan los bienes y la información sensible o en trámite.

En el caso de los empleados estatales, éstos son depositarios de bienes públicos, llamados a ejercer todas las acciones de control y supervisión de aquellos bienes adquiridos con recursos del Estado. Es parte del deber de diligencia y sana administración, proteger la información sensible, proteger los recursos y tomar toda previsión posible que evite eventuales responsabilidades administrativas, civiles o penales, o bien pérdidas que representen un perjuicio económico para el Estado. Igualmente, en el caso de los trabajadores de empresa privada, dentro de su contrato laboral están llamados a proteger los bienes de la empresa en la que trabajan, por lo que adoptar medidas para proteger la información que en ambos casos se manipula por el correo electrónico o evitar accesos no autorizados en virtud de un uso no diligente de sus claves o revelación de las mismas a terceros; resulta una obligación inherente a su condición de empleados.

Los derechos que se protegen con la seguridad digital se conocen con el carácter de *sui generis*, pues la doctrina constitucionalista no ha logrado consolidar la naturaleza de los mismos, aunque coinciden en la necesidad de su protección en virtud de los bienes jurídicos que resguardan. En lo personal, y sin que ello sea objeto de este ensayo, considero la seguridad digital como un derecho humano de cuarta generación y por ende con el rango de derecho fundamental.

En las últimas décadas juristas e informáticos se han unido para elaborar un marco de protección al movimiento que ha venido desarrollando la tecnología en nuestras sociedades. Por tanto, el acceso de los ciudadanos a los archivos y registros administrativos si bien es lícito y está protegido como parte del derecho a la información, ese derecho encuentra su límite si el acceso a la información afecta la seguridad y defensa del Estado, la averiguación de los delitos y la

¹⁵ La seguridad digital también es un derecho fundamental de la nueva sociedad de la información y por ende constituye parte de los derechos de *cuarta generación*.

intimidad de las personas; o bien si se utiliza el derecho de forma abusiva para la manipulación, destrucción o uso ilegítimo de los bienes protegidos.

Las medidas de seguridad digital suelen variar dependiendo del servidor del que se trate. Por lo general, son normas de índole técnica y algunas que deben adoptar los usuarios según se obligan en las condiciones generales de acceso a los portales que proporcionan sus servicios. No es tema de este ensayo la seguridad digital, sobre la que me dedicaré en otro momento, pero valga citarla como un código deontológico que poco a poco ha adquirido más fuerza por su naturaleza cambiante según las exigencias diarias del servicio, y por ser la que mejor se adecua al régimen de convivencia en la era digital. Incluso, valgo considerar la seguridad digital como un derecho fundamental de los miembros de la sociedad virtual.

IV. PRERROGATIVA DE ACCESO TECNICO

En cuanto al acceso a las cuentas de correo electrónico, existen ciertos sujetos que por su condición profesional o técnica tienen acceso privilegiado al contenido de los email de los usuarios, y son los que administran el servicio en cada *host*.

En el caso de los correos electrónicos proporcionados en el ámbito laboral o de la Administración Pública, en principio dichos accesos no tendrían mayores controversias si se delimitan responsabilidades por abusos e indemnizaciones cuando se afecte a la institución, a la empresa o a terceros. Sin embargo, la prerrogativa de acceso debe estar centralizada y debidamente autorizada para evitar alteraciones de documentos o daños en los bienes informáticos de la Administración.

Por otro lado, en el caso de los *host* privados, el que un sujeto desconocido y ajeno a nuestro entorno e incluso desarrollando su actividad en otra jurisdicción o geografía, pueda tener acceso tanto a mis datos personales (y manipularlos de forma no autorizada) e incluso acceder al contenido de mis correos, resulta evidentemente más gravoso no solo por la dificultad del usuario de acceder al administrador sino porque en este caso sí se trata de asuntos relativos a la inviolabilidad de la correspondencia privada.

En este sentido, el Administrador de Correo es capaz de conocer, interceptar, y manipular los correos aún sin que el usuario lo sepa. De allí que el Código Penal Español en su artículo 197.4 agrave el delito de violación de la correspondencia constante en un correo electrónico si los hechos los realiza el encargado o responsable de fichero, soporte informático, electrónico o telemático.

En los *newsgroups* o en los foros de discusión se presenta una situación similar en donde hay un moderador también adscrito al personal técnico del proveedor de servicios, que controla las intervenciones de los usuarios e incluso sin previo aviso puede intervenir censurando o expulsando a un miembro por su criterio o ejerciendo acciones contra su dirección de correo electrónico; lo que ya en sí mismo podría consistir en un roce directo al derecho de libertad de expresión.

Pero en tanto no se creen mecanismos técnicos que puedan impedir totalmente esta situación, los servidores deben contar con medidas de control de su personal y adoptar un código de conducta

que los distinga como “sitios seguros en la Red”; mientras que el usuario debe acudir a los proveedores de servicios que ofrezcan las mayores garantías de seguridad y resguardo de los derechos fundamentales de los usuarios.

V. DERECHOS SUCEPTIBLES DE VULNERACIÓN CON EL USO DEL CORREO ELECTRONICO

Sanz de las Heras define el ACE (Abuso en Correo Electrónico) como las distintas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios.¹⁶ Cada uno de esos abusos, puede llegar a constituirse en un limitador pasivo o por omisión del derecho de acceso a Internet por miedo a que la dirección de correo electrónico u otros datos sensibles que distingan al usuario o puedan eventualmente ser utilizados maliciosamente en su perjuicio, sean capturados y manipulados sin la autorización o control debidos; lo que los hace sumamente trascendentes en esta materia y revela la necesidad de protegerles.

1. Protección de datos personales: El artículo 18.1 CE garantiza el derecho a la intimidad personal y familiar. Esta norma cobija por tanto también ese derecho en lo que respecta al uso del correo electrónico, como ya indiqué en apartados anteriores. Por su parte el artículo 18.4 CE dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar, por lo que se evidencia la intención del legislador de proteger la intimidad del individuo ante los nuevos avances de la informática y las redes de comunicación.

Ya había advertido que el correo electrónico puede permitir la elaboración de perfiles personales del usuario y por ende provocar que su intimidad quede vulnerada. Esos perfiles indican desde el lugar de trabajo, el nombre y apellido del usuario y el país de residencia, sólo dentro de la dirección de correo. Además, por medio de *cookies* es posible adicionar otros datos complementarios para la elaboración de un perfil sensible, tales como edad, raza, religión, cuenta de crédito, número de teléfono, dirección postal y dirección domiciliaria, por citar algunos ejemplos. El email es en sí mismo un domicilio electrónico y por ende deben cuidarse sus datos que son identificatorios del sujeto y su situación geográfica y otros aspectos que definen su personalidad. Hay que recordar que existen mecanismos que nos permiten configurar nuestro navegador para no dejar constancia de nuestra dirección de correo electrónico en los sitios Web a los que ingresamos, pues ello podría contribuir a proporcionar aún más información sobre nuestras actividades, gustos y tendencias.

El correo electrónico también transmite la dirección IP que identifica a la persona y todo lo que su ordenador resguarde o la institución en la que labora resguarde, situación que hace más evidente la necesidad de que la persona que manipule una cuenta de correo lo haga con la mayor diligencia posible, sobre todo en el caso del correo laboral o administrativo en donde se es responsable tanto a nivel personal como solidariamente con la empresa.

Los datos que se trasiegan con el uso del correo pueden manipularse sin nuestro consentimiento para establecer los perfiles de la personalidad que indiquen nuestra tendencia política, sexual,

¹⁶ Ver en este sentido SANZ DE LAS HERAS (Jesús). *Abusos en el correo electrónico*. En <http://www.ucm.es/info/dinforma/activi/libro/9.html>

religiosa, etc. y a partir de la participación en grupos de noticias, foros de discusión, *mailing list* o *chats*, establecer una descripción precisa de nuestra personalidad. Esa información podría utilizarse para fines propagandísticos, publicitarios o bien para fines políticos que incluso podrían poner en peligro la integridad personal o moral del usuario.

La dirección de correo es la forma más común de registrar la identidad de una persona en Internet. Se debe ser precavido del tipo de dato que se suministra y a quién se le indica. Por ello es tan importante el manejo adecuado y diligente de nuestra información y la conciencia de la vulnerabilidad en la que ésta se encuentra en la Red. La DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, señala en su considerando 47: *“Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio; (...)”*

Es clara la preocupación en la Unión Europea del resguardo de la intimidad en la manipulación de los datos relativos al uso del correo electrónico, aunque también existe la conciencia que muchas veces el email no deja mucho margen a la anonimidad salvo en el uso de *nicks* y la previsión de no indicar datos personales cuando el usuario se dé de alta en un servicio.

El comportamiento del consumidor puede ser observado por el proveedor que puede acumular información personal e ir registrando detalles sobre los servidores Web a los que accede un usuario, en qué páginas se detiene más tiempo y qué temas busca de manera habitual. El usuario no siempre es consciente del destino de sus datos, o la travesía que éstos deben tomar para llegar al lugar de destino, e incluso le es imposible controlar que sus datos sean siempre utilizados para los fines por los cuales fueron recabados.

Para ello, es recomendable utilizar servidores Web que brinden altos niveles de seguridad (generalmente aquellos con navegadores más recientes o que hagan constar explícitamente en su portal las medidas de seguridad sobre protección de datos personales), y utilizar mecanismos como la firma digital (que cada vez se irá incorporando para evitar la usurpación de identidad) o la criptografía; que consiste en el uso de algoritmos para cifrar la información, protegiendo los datos de quien no posea la clave de descifrado respectiva. Este método, actualmente utilizado para proteger la información contenida en un correo electrónico, permite que sea imposible intervenir y cifrar los mensajes que se envían por email. Como otra medida se puede requerir la disociación de datos (con respecto a la identidad) ante el navegador o servidor que nos brinde tal servicio para el resguardo de los datos personales.

2. Privacidad de las comunicaciones: El correo es protegido en su carácter de comunicación personal o privada por el secreto de las comunicaciones, por lo que en principio su contenido es inviolable y no puede ser incautado o abierto sin que medie intervención judicial, tal como se

aplica al correo tradicional y con las excepciones indicadas para el correo laboral y administrativo.

La RECOMENDACIÓN 3/97 SOBRE ANONIMATO EN INTERNET ADOPTADA POR EL GRUPO DE TRABAJO EL 3 DE DICIEMBRE DE 1997 indica claramente que la intimidad queda vulnerada ante la falta de seguridad en las comunicaciones, por lo que debemos entender que dicha intimidad debe ser resguardada siempre en el correo electrónico privado.

Existe tipificado en el ordenamiento jurídico español, el delito autónomo de indiscreción, según el artículo 197.3 del Código Penal Español, que condena la revelación de datos captados por correo electrónico, entre otros medios de comunicación. Esta norma, permite establecer como delictiva la conducta de la interceptación del email y la información que allí se trasiega. El secreto de la comunicación ampara tanto el contenido del mensaje como la identificación de su entorno, que revele cualquier aspecto de la intimidad del sujeto o del contenido de los mensajes que transmite. Al no haber garantía total de la identidad del emisor y del receptor, ni garantía de confidencialidad en el intercambio de la información, hay riesgos de que la información pueda ser accesada por un tercero, que exista suplantación de la identidad del emisor o receptor y por ende violación de la comunicación.

Se protege por tanto la vida privada en las comunicaciones y no los documentos públicos que existan en ellas. El correo electrónico dentro de la Administración Pública es por tanto público y de acceso libre salvo en lo que respecta a medidas de seguridad que resguarden su contenido para evitar su alteración.

3. No hay garantía de que los mensajes lleguen íntegramente: Sobre la integridad del mensaje desde el momento que se envía hasta cuando llegue a su destino, valga indicar la definición ofrecida por Corripio que al efecto señala: *“La integridad se entiende como la fiabilidad del contenido del mensaje o documento, de forma que la información transmitida sea un fiel reflejo del dato que representa en realidad. La definición de integridad debe comprender los términos de exacta, autorizada y completa y se dirige a asegurar que los datos recibidos se corresponden exactamente con los enviados por un emisor autorizado.”*¹⁷

Efectivamente, la integridad se exige en esta materia como un principio de seguridad del envío de la comunicación y comprende tanto la identidad entre el contenido emitido y el recibido. Es necesario que las partes tengan esa garantía de quien ofrezca el servicio de mensajería electrónica, del mismo modo que en el correo tradicional se le exigía a la oficina postal la certeza de que los envíos llegasen a su destino tal y como fueron remitidos.

4. No se garantiza al remitente que el mensaje llegó a su destino: No existe un medio seguro que determine si el mensaje llegó al destinatario, salvo en casos que haya existido algún problema de comunicación o que la dirección haya sido digitada de forma errónea, el administrador de correo de forma automática notificará al usuario de tal anomalía. Sin embargo, actualmente se parte de la premisa de que todo mensaje enviado fue recibido por el destinatario de forma inequívoca, pese a que tal circunstancia es difícil de certificar con plena certeza. La

¹⁷ CORRIPIO GIL-DELGADO (María de los Reyes) 2000. *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*. Agencia de Protección de Datos. Madrid, p.123

garantía de no rehusabilidad tanto por parte de quien envía como de quien recibe el mensaje, solo podría garantizarse con sistemas de cifrado como la criptografía y la firma electrónica. Pero no hay que ser fatalistas: ¿cuántas veces en el correo tradicional una carta se desvió de su destino? Internet no es una herramienta infalible pero tampoco es desechable. Por el contrario, pese a esta y otras desventajas que poco a poco se están perfeccionando, es hoy en día el medio de comunicación más económico y eficaz.

5. No se garantiza la identidad del remitente o del receptor: La identidad de las partes es necesaria en el envío de toda correspondencia, con el fin de determinar la responsabilidad del envío del material. Tal como lo señala el considerando 47 de la DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, el responsable del envío de un mensaje electrónico es el emisor y no el servidor del sitio. De allí la importancia en la utilización personal y exclusiva de una cuenta a favor de un único usuario, con el fin de tener la certeza de que la identidad de la mensajería le corresponde a un único emisor y que el destino de un mensaje a una cuenta a su vez corresponde a un único receptor, razón por la cual el uso de la clave de acceso o password, se considera secreto, individual y personal.

“La autenticidad del mensaje consiste en la correcta atribución de la identidad del emisor. La despersonalización del mensaje telemático originada por la naturaleza del propio medio electrónico impone la necesidad de asegurar la identificación de las partes que se comunican entre sí. La autenticación debe permitir determinar que aquel que se conecta a la red se corresponde al número indicado. (...) Entre los protocolos de identificación destacan: kerberos, PGP y PEM (en Internet) y EDI.”¹⁸

El uso de una estafeta de otro usuario implica el uso de un canal de comunicación no autorizado, lo cual ciertamente es posible y muy común, pero debe ser restringido totalmente dentro de las normas de la sana comunicación electrónica. Podría incluso considerarse en esta nueva materia como una especie de fraude de transmisión, el remitir un mensaje electrónico usurpando una cuenta de correo asignada a otro usuario, sea mediante la usurpación de identidad o por interceptación de la cuenta.

Hay sistemas de cifrado o de autenticación en correo electrónico como los PGP o las normas PEM, que evitan la irrupción en el contenido del correo o suplantación de personalidad y cuya adopción es recomendable siempre que sea posible. Las medidas y restricciones de manipulación, almacenamiento, cambio periódico y escogencia oportuna de una clave personal de acceso, que a su vez sea difícil de cifrar por parte de terceros, deben ser medidas obligatorias por necesidad de seguridad jurídica tanto del titular de la cuenta como de quien recibe el mensaje respectivo.

5. Difusión de contenido inadecuado: Es evidente que la difusión de contenido inadecuado o ilegítimo a través del correo electrónico, puede afectar sensiblemente los derechos de los receptores así como los de terceros.

¹⁸ CORRIPIO GIL-DELGADO (María de los Reyes) 2000. *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*. Agencia de Protección de Datos. Madrid, p.122

Dentro del contenido que puede considerarse inadecuado, podemos citar los mensajes ajenos al ámbito laboral en los correos proporcionados por empresas privadas o por la Administración Pública; mientras que existen correos que tanto dentro del correo electrónico privado como dentro del laboral se consideran inadecuados por ir contra el ordenamiento jurídico o bien por afectar el servicio, tales como la apología del terrorismo, apología de la xenofobia, la pornografía infantil, etc.:

6. Envío masivo de publicidad no solicitada por email o correos no solicitados: Con la palabra inglesa *Spam* o *spamming* se designa la actividad de enviar a varias direcciones de correo electrónico, mensajes publicitarios no consentidos o no solicitados que en principio no deben permitirse. Tampoco es lícito brindar servicios al usuario condicionando su aceptación a la recepción indiscriminada de correos publicitarios.

El envío masivo de publicidad o de correos no solicitados, puede causar inconvenientes técnicos y humanos. Esta actividad puede estar destinada a bloquear un servicio de correo específico, saturando las líneas, la capacidad de la memoria del servidor o el espacio de disco del usuario o servidor. Igualmente, el envío masivo de correos suele causar molestias al usuario pues la recepción de estos mensajes quitan tiempo a sus actividades ordinarias e incluso podrían afectar su sensibilidad en caso de que se trate de mensajes de corte religioso, ideológico o similares. Las empresas que envían spams deben identificar el contenido de sus mensajes en el *subject*, asunto o casilla destinada al tema del correo, e informar sobre la posibilidad de la exclusión voluntaria en cada envío, de manera que el receptor pueda optar a que se le excluya de la lista (también de un *mailign list*) o bien no abrir un mensaje que ya ha identificado como publicitario. Sin embargo, es una actividad que de prohibirse podría afectar sensiblemente a las PYMES que han encontrado en este medio una forma económica de ofrecer sus servicios.

Las formas más fáciles de conocer el email sin el consentimiento del usuario son, sin ánimo de ser taxativa, las siguientes:

- ✍ Listas de distribución o grupos de noticias
- ✍ Captura de direcciones en directorios
- ✍ Captura de direcciones en correos masivos
- ✍ Venta, alquiler o intercambio de direcciones entre proveedores
- ✍ Entrega de dirección de correo por parte de los programas navegadores, al conectar a los servidores Web
- ✍ Recepción de mensajes de correo requiriendo contestación a una dirección determinada y pidiendo la máxima difusión de los mismos
- ✍ Participación en cadenas de mensajería

Ante esto es importante informarse con el servidor en el cual estamos adscritos o donde utilizamos cierto servicio en donde se deba aportar nuestros datos, las políticas con respecto al alquiler, préstamo y venta de nuestros datos, con el fin de tener la opción de decidir si me inscribo o no en un servidor que no garantiza mi intimidad en todas sus posibilidades.

7. Listas de distribución o mailing lists: Las listas de distribución sirven para formar grupos de personas con intereses coincidentes en torno a ciertos temas o afinidades, quienes reciben información simultánea a través de los correos electrónicos registrados ante un administrador de

la lista. Estas personas utilizan estas listas para intercambiar mensajes o información respecto de los temas que los agrupan, a través de sus direcciones de correo. El mensaje se envía a la lista y de inmediato y de forma simultánea se distribuye a todos sus miembros. Esos mensajes pueden incluso llegar a terceros, si alguno de los miembros de la lista redirecciona el mensaje a otros usuarios o a otras listas a las que esté adscrito.

La misma lista de distribución es un correo electrónico con respecto a su formato y funcionamiento por lo que suele ser fácil de identificar. Igualmente, el usuario debe tener la opción permanente de darse de baja de la lista para evitar seguir recibiendo mensajes de la misma. Una modalidad de lista de distribución también son los Grupos de noticias (News, Newsgroups, Netnews o Usenet) pues muchas veces se accede a ellos a través del correo electrónico o bien se ingresa directamente a un portal, en cuyo caso la dirección de correo no tiene trascendencia.

Se trata de una especie de foros de discusión organizados en torno a temas como la informática, negocios, sociedad/amistad, profesionales y otros; en donde se exhibe cada manifestación de los usuarios para generar la discusión. Existen grupos moderados en los que los mensajes se le envían a un determinado sujeto que los clasifica e incluso puede eliminarlos ejerciendo una especie de censura previa, y los grupos que no poseen moderador, en donde las opiniones se envían directamente a la lista de usuarios o foro de discusión.

Mediante los grupos de noticias se facilita el *profiling* o elaboración de perfiles personales de los usuarios pues deja en clara evidencia las tendencias y preferencias de quien accede a ellos e incluso sus opiniones personales y datos que son por lo general clasificados como sensibles. A su vez, estos grupos no son aptos para preservar el secreto de las comunicaciones pues permiten visualizar incluso en tiempo real, tanto los datos como las opiniones del sujeto que accede a ellos.

Los comentarios, opiniones, críticas, documentos o archivos que el usuario aporte a estos grupos, foros de discusión o bien en *chats*, son accesibles para cualquier interesado y por tanto de carácter público pues en principio no existe ninguna restricción para ingresar en ellos. El usuario debe no sólo estar consciente de ese hecho, sino que también debe ser advertido por el servidor que brinde el servicio con el fin de proteger sus derechos fundamentales, sobre todo tomando en consideración que muchas de las opiniones escritas, no conllevan connotaciones de entonación que podrían dispensar de una mala interpretación de lo que se exprese, o bien no conocen de susceptibilidades propias del lugar de origen o de la perspectiva de los receptores; y por tanto deben tomarse mayores precauciones en esas expresiones que además suelen ser espontáneas.

Un uso ilegítimo de la dirección electrónica en este ámbito se constituye también cuando se gestionan bases de datos con direcciones de correo cuya manipulación no ha sido autorizada por los usuarios. Existen empresas que intercambian listas de correo con fines publicitarios y sin el consentimiento de los dueños de las cuentas electrónicas, por lo que esta situación también debe controlarse y ser autorizada expresamente por el usuario.

8. Comercio electrónico: Las telecomunicaciones han introducido nuevas técnicas de comercio (compra y venta de bienes y servicios en línea). En el ámbito internacional ya se han emitido normas genéricas que pretenden la regularización de estas actividades, tales como la Ley Modelo

sobre el Comercio Electrónico¹⁹, el Contrato Tipo de la Comisión Europea²⁰ y la Iniciativa Europea de Comercio Electrónico²¹; entre otras. Los contratos electrónicos son los que se acuerdan y celebran a través de medios electrónicos o telemáticos, por lo que el correo electrónico es el sistema utilizado mayoritariamente para consolidar este tipo de transacciones. Hay quienes afirman también que los contratos electrónicos son sólo los tramitados por el Electronic Data Interchange (EDI), o sea con la transmisión electrónica y cifrada de datos comerciales y administrativos de ordenador a ordenador.

El comercio electrónico (transacción comercial en línea) que sea realizado por correo electrónico puede ser vulnerable para el usuario si no hay garantía de seguridad en el resguardo de la identidad, número de tarjeta de crédito y demás datos personales, se deben tomar otras medidas de seguridad que nos brinden el respaldo suficiente para realizar los negocios que deseamos en este medio. No se trata de ser alarmista, pues igual riesgo corre el comprador que asiste a una tienda y proporciona su tarjeta de crédito para el pago. Internet sigue siendo un sitio seguro para realizar negociaciones y compras, en general, si se realizan a través de sitios confiables y tomando las precauciones debidas; como corresponde en toda transacción comercial sea o no electrónica.

Sin embargo, hay que advertir sobre la necesidad de adoptar medidas de seguridad pues aquí se adquieren nuestros datos y a la vez se puede vincular nuestra identidad con el tipo de bienes y servicios que se obtienen. Esa información puede ser alquilada o vendida por el proveedor a compañías que se dediquen a publicidad o bien para controlar a la persona. Se recomienda usar el dinero electrónico (*digital cash* o *electronic wallet*) en virtud del cual se resguarda la identidad del comprador y procurar nuevamente el acceso a sitios que brinden toda la seguridad necesaria para las transacciones que se requieran; pues recordemos que el comercio electrónico muchas veces implica la transferencia electrónica de fondos.

9. Conversación electrónica (*chatting* o *IRC*): Permite la comunicación simultánea entre varios usuarios, que utilizan su identidad real, seudónimo o *nickname*. Para que la identidad no sea obtenida o violada la comunicación (pues se puede grabar texto, voz e imagen), es recomendable dejar en blanco los espacios donde solicitan datos personales en la inscripción del servicio. El IRC (Internet Relay Chat) permite el diálogo simultáneo entre usuarios conectados a la misma red UNDERNET que utilizan seudónimos, apodos o *nicks* (*nicknames*). Estos sistemas permiten tener conversaciones públicas o privadas a través de ciertos comandos que facilitan dividir en pantallas las conversaciones que elijan los usuarios.

V. NUEVA VALORACIÓN DEL EMAIL EN EL DERECHO POSITIVO

Debemos enfrentarnos a la realidad que exige esta nueva dinámica y proponer en lugar de rígidas ordenanzas legales, un sistema normativo conciliatorio que no perjudique a ninguno de los

¹⁹ Aprobada por la Asamblea General de las Naciones Unidas el 30 de enero de 1997, a propuesta de la Comisión de las Naciones Unidas para el Comercio Internacional (UNCITRAL); UN doc. SG 51, Sup. 17, A/51/17.

²⁰ Recomendación del 19 de octubre de 1994, sobre los aspectos jurídicos del intercambio electrónico de datos (DOCE L 338/98 del 28 de diciembre de 1994).

²¹ Aprobada por el Consejo Económico y Social del 29 de octubre de 1997 (DOCE C 19/72 del 21 de enero de 1998)

involucrados en este proceso, pero que regule y oriente de forma armoniosa y justa sus relaciones personales, laborales, comerciales, etc..

El Estado unitario no puede regularlo todo y la correulación entre naciones o regiones resulta insuficiente. Las medidas deben ser universales, acordes con el ámbito de actuación de las nuevas tecnologías y específicamente de la plataforma de Internet donde se desarrolla el correo electrónico. La experiencia nos ha indicado que la autorregulación (por la que abogan empresarios y Estados con tendencia a privar la protección de la economía sobre los derechos de los usuarios), genera excesos y relaciones leoninas. Es preferible optar por un ordenamiento no de índole coaccionador sino más bien deontológico, que permita una cierta flexibilidad para el buen funcionamiento de la Red sin que ese funcionamiento resulte en detrimento de los derechos fundamentales de cualquier sujeto que interactúe en este medio, bien sea usuario o proveedor de servicios.

En este marco, es importante tomar conciencia de que no todos los servicios de correo electrónico poseen una idéntica naturaleza. Las comunicaciones en el mundo digital son divergentes según el ámbito en el que puedan utilizarse. El email, al ser una herramienta de comunicación, puede pertenecer tanto a una persona natural como a una persona jurídica, y en este caso, ser un instrumento laboral que debe utilizarse diligentemente en ese margen. Basta con determinar la titularidad de la cuenta de correo, en lo que respecta al uso legítimo del mismo, y definir en cada caso el régimen de utilización adecuado a través de convenios colectivos, reglamentos internos de trabajo o mediante una legislación específica que reconozca esa naturaleza disímil de los diversos medios de comunicación. Si la cuenta de correo electrónico pertenece a la empresa, su control o acceso no podría implicar una violación a las comunicaciones privadas del trabajador y por ende no sería constitutivo de ningún supuesto delictivo contra la confidencialidad. Como medio de empresa, el email puede ser utilizado para actividades propias del trabajo, actividades sindicales pero no para asuntos personales que deberán tramitarse por medio de una cuenta de correo que no identifique al usuario con la empresa.

Permitir que el trabajador utilice el email empresarial para asuntos personales podría incidir en un daño directo a la imagen de la empresa o bien provocar una afectación patrimonial pues aumenta el riesgo ante un uso no diligente, de introducir virus o software ilegal en la empresa.

No obstante, en el tanto el uso del email de empresa ha sido desde su inicio una herramienta de uso personal del trabajador, en cambio que se propone en este ensayo implica en primer lugar la instauración de una cultura de reconocimiento de la fragilidad de la seguridad digital de la empresa y de su imagen pública, por lo que la práctica consentida deberá variarse bajo esa premisa. De ahí que considere necesario la adopción de un convenio bilateral, pues no bastaría la simple comunicación al empleado de las prohibiciones de uso del correo, sino que deberán establecerse reglas de utilización definidas conjuntamente por medio de la participación de los agentes que intervienen en el contrato laboral.

Todo ello es parte de una cultura nueva que nos exige la convivencia en la sociedad de la información, que nos exige tomar conciencia de ciertos riesgos que afectarían los derechos de los intervinientes en la sociedad global pero además, que nos llama a evitar como juristas imponer obstáculos desmedidos a la circulación de información y a la agilidad de las comunicaciones en la red.

RESUMEN

El ensayo pretende dar una nueva visión del uso legítimo que debe regir para el correo electrónico de conformidad con las diversas tipologías que existen con respecto a este medio de comunicación, al cual debe valorársele de conformidad con su diversa naturaleza jurídica.

El email privado es de uso estrictamente personal y por ende no puede ser manipulado, interceptado, intervenido o alterado de alguna forma si no se posee una autorización judicial, pues corresponde legítimamente a una naturaleza idéntica a la del correo tradicional y por ende se encuentra protegido por el secreto de las comunicaciones y por el derecho a la intimidad. El correo, así entendido, debe verse tanto como una correspondencia inviolable como también un domicilio personal (digital) pues por sus características es posible mediante las medidas técnicas pertinentes que cualquier sujeto mal intencionado pueda conocer la dirección IP del usuario o los datos para su ubicación geográfica.

El correo proporcionado por el patrono o por la administración pública, pertenece a ésta y lo delega como una herramienta de trabajo a sus servidores pero no como una dirección privada. Permitir que el trabajador utilice el email empresarial para asuntos personales podría incidir en un daño directo a la imagen de la empresa o bien provocar una afectación patrimonial pues aumenta el riesgo ante un uso no diligente, de introducir virus o software ilegal en la empresa, de poner en entredicho la imagen empresarial o simplemente desviar los recursos de la empresa a otros fines.

Se analizan también diversas actuaciones relacionadas al uso del correo electrónico que deben ser realizadas con diligencia y bajo códigos deontológicos que impidan la vulnerabilidad de los derechos fundamentales de los usuarios.

ABSTRACT

We try to give a new vision of the legitimate use that must prevail for the electronic mail in accordance with the different kinds that exist with respect to this mass media. Email must be value in accordance with its diverse legal nature.

The private email is of strictly personal use and therefore it cannot be manipulated, be intercepted, be taken part or altered by any way; unless by a judicial authorization. This is because email corresponds legitimately to an identical nature of the traditional mail and therefore is protected by the secret of the communications and the right to privacy. The mail, thus understood, must be seen as much as an inviolable correspondence as also a personal (digital) address. By its characteristics is possible by means of a pertinent technical procedure that anyone can know the users IP direction or his personal data.

The mail provided by the employer or the Public Administration belongs to this one who delegates it to its workers like a tool of work but not like a private direction. To allow that the worker uses the enterprise email for personal issue, could produce a direct damage to the image of the company or cause a patrimonial affectation because it increases the risk of a non-diligent use, introduction of virus or illegal software in the company, to harm the enterprise image or just to turn aside the resources of the company to other aims.

Diverse performances related to the use of the electronic mail are also analyzed in the essay. Email must be managed with diligence and under a legal ethic to prevent the vulnerability of the fundamental rights.