

ULACIT
UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

MAESTRÍA EN DERECHO EMPRESARIAL

**EL DERECHO A LA INTIMIDAD DE LOS TRABAJADORES: EL CASO DEL
CORREO ELECTRÓNICO EN EL MINISTERIO DE HACIENDA**

Sustentante: Andrés Villalta Mata

Cédula de identidad: 1-1013-0235

Tutor: Alexander Godínez Vargas

**PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE
*MAESTRÍA EN DERECHO EMPRESARIAL***

Calificación: 95

**San José – Costa Rica
OCTUBRE 2004**

DECLARACIÓN JURADA

Yo, Andrés Villalta Mata, alumno de la Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), declaro bajo la fe de juramento y consciente de la responsabilidad penal de este acto, que soy el autor intelectual de la Tesis de Grado titulada: El Derecho a la Intimidad de los Trabajadores: El caso del Correo Electrónico en el Ministerio de Hacienda, por lo que libero a la ULACIT, de cualquier responsabilidad en caso de que mi declaración sea falsa.

Brindada en San José – Costa Rica en el día veintiséis del mes de octubre del año dos mil cuatro.

Firma del estudiante: Andrés Villalta Mata

Cédula de identidad: 1-1013-0235

ULACIT
UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

TRIBUNAL EXAMINADOR

Reunido para los efectos respectivos, el Tribunal examinador de la Escuela de Posgrados compuesto por:

Tutor: Alexander Godínez Vargas

Lector: Marianela Núñez Piedra

Presidente del Tribunal: Mauricio Vega Díaz

AGRADECIMIENTOS

A mi familia y a mi novia, por su apoyo, confianza y cariño; todo lo cual me permitió culminar esta etapa de mi vida académica. Al doctor Godínez y al licenciado Solano, por su invaluable colaboración.

DEDICATORIA

A la memoria de mi abuelo, quien reposa en los brazos de Dios. Gracias por ser un ejemplo de vida.

RESUMEN EJECUTIVO

El tema desarrollado en esta investigación se titula *“El Derecho a la Intimidad de los Trabajadores: El Caso del Correo Electrónico en el Ministerio de Hacienda”*; tópico que contiene una serie de aristas que tornan imperativo ahondar en varias ramas de las ciencias jurídicas.

El Derecho a la Intimidad, ha vuelto a los primeros planos con la introducción de las nuevas herramientas tecnológicas en los centros de labores, ya que éstas, además de su importancia para mejorar y acelerar las actividades, han sido utilizadas por el empleador para vigilar a sus trabajadores, muchas veces en detrimento del derecho antes mencionado.

Esta situación ha generado posiciones encontradas entre las partes integrantes de la relación laboral, que desencadenaron en inconvenientes que han llegado hasta el ámbito judicial, donde es claro el enfrentamiento entre el derecho a la intimidad –y dentro de éste el derecho al secreto de las comunicaciones- que ampara a los trabajadores, versus la facultad del empleador para salvaguardar su patrimonio y controlar la prestación de la actividad laboral, enfrentamiento que constituye el problema de fondo de la presente tesis, al plantear cual es el derecho que prevalece en este choque de intereses.

Para dar respuesta a dicha interrogante, analizamos una significativa cantidad de doctrina, legislación y jurisprudencia extranjera en la cual se ha ventilado esta problemática; a la vez que se circunscribe y materializa el tema en el Ministerio de Hacienda de nuestro país, a efecto de determinar si en esta institución del sector público, se encontraba rigiendo alguna disposición que regulara lo referente al *e-mail* y, en la eventualidad de que efectivamente existiera, constatar si la misma observaba los derechos constitucionales indicados.

Efectuado el examen de los elementos antes expuestos, logramos concluir que, inclusive en su lugar de trabajo, el empleado tiene el derecho al respeto de su intimidad y al secreto de las comunicaciones, dentro de las que se incluye correo electrónico, y que si bien es cierto el patrono en el ejercicio de su poder de dirección y control está facultado para fiscalizar el adecuado uso de esta herramienta, ello no lo legitima para imponerse del contenido de los mensajes que envían sus empleados, pudiendo únicamente tener conocimiento de aspectos no trascendentales de la comunicación, y ello con plena observancia al principio de proporcionalidad en sentido amplio.

Finalmente, luego de estudiar la Política sobre Uso de Internet que rige en el Ministerio de Hacienda, consideramos que la misma contempla los conceptos y garantías que amparan tanto nuestra Constitución Política, como los distintos instrumentos internacionales de derechos humanos. Sin embargo, ello no

implica que la disposición no pueda ser mejorada, por lo que sugerimos modificar algunos artículos de la misma, a efecto de corregir determinados aspectos que a nuestro parecer resultan ambiguos. Estas reformas, vendrían a proporcionar mayor seguridad jurídica tanto a la parte patronal como a los funcionarios del ente ministerial, lo que redundaría en una mejoría de las relaciones laborales. De igual manera, planteamos esquemáticamente un procedimiento para la emisión de futuras reformas, su comunicación a los empleados y, además, de revisiones periódicas para analizar los resultados alcanzados.

CAPÍTULO I	1
1.1.- INTRODUCCIÓN	2
1.2.- JUSTIFICACIÓN	6
1.3.- PLANTEAMIENTO DEL PROBLEMA	9
1.3.1.- FORMULACIÓN DEL PROBLEMA	9
1.3.2.- SISTEMATIZACIÓN	9
CAPÍTULO II	11
Marco Teórico	11
CAPÍTULO III	16
Marco Metodológico	16
3.1. – TIPO DE INVESTIGACIÓN	17
3.2.- MATRIZ DE DISEÑO DE INVESTIGACIÓN	18
3.3.- MATRIZ DE OPERALIZACIÓN DE VARIABLES	20
3.4.- SUJETOS Y FUENTES DE INFORMACIÓN	21
3.5.- ALCANCES Y LIMITACIONES DE LA INVESTIGACIÓN	22
CAPÍTULO IV	23
Análisis e Interpretación de Resultados	23
4.1.- SECCIÓN I. EL DERECHO A LA INTIMIDAD: NOCIONES GENERALES	24
4.1.1.- CONCEPTO	24
4.1.2.- DERECHOS Y DEBERES DEL TRABAJADOR Y DEL PATRONO	27
4.2.- SECCIÓN II. INSTRUMENTOS NORMATIVOS Y ANÁLISIS JUDICIAL	31
4.2.1.- CONSTITUCIÓN POLÍTICA	32
4.2.2.- TRATADOS INTERNACIONALES	33
4.2.3.- DERECHO COMPARADO	35
4.2.4.- JURISPRUDENCIA	39
4.3.- SECCIÓN III. EL SECRETO DE LAS COMUNICACIONES	45
4.3.1.- CUESTIONES DOCTRINARIAS Y EL PROBLEMA DE FONDO	47
4.3.2.- FUNDAMENTO CONSTITUCIONAL Y LEGAL	53
4.3.3.- EXCEPCIONES	55
4.3.4.- DELITOS	57
4.3.5.- JURISPRUDENCIA	62
4.3.6.- ANÁLISIS DE ALTERNATIVAS Y SOLUCIONES PROPUESTAS AL PATRONO	89
4.3.7.- EL DESPIDO POR LA UTILIZACIÓN PERSONAL DEL CORREO ELECTRÓNICO PROPIEDAD DE LA PARTE PATRONAL	95
4.4.- SECCIÓN IV. CUESTIONES INFORMÁTICAS	99
4.4.1.- FORMA EN QUE SE PUEDEN ACCEDER LOS CORREOS	99

4.4.2.- INSTRUMENTOS DE SEGURIDAD PARA IMPEDIR EL ACCESO	102
4.5.- SECCIÓN V. LOS FUNCIONARIOS PÚBLICOS Y EL DERECHO A LA INTIMIDAD	105
4.5.1.- USO DEL CORREO ELECTRÓNICO CON FINES PERSONALES	106
4.5.2.- ÉTICA DE LA FUNCIÓN PÚBLICA	108
4.6.- SECCIÓN VI. MECANISMOS DE CONTROL	110
4.6.1.- LÍMITES A LA FISCALIZACIÓN DE LOS SERVIDORES PÚBLICOS: LOS CONTRATOS DE TRABAJO	110
4.7.- SECCIÓN VII. ANÁLISIS DEL MANUAL DE NORMAS Y POLÍTICAS EN EL USO DE SERVICIOS DE CORREO Y ACCESO A INTERNET DEL MINISTERIO DE HACIENDA, EN CUANTO AL CORREO ELECTRÓNICO	112
4.7.1.- OBJETIVO	112
4.7.2.- ALCANCE	114
4.7.3.- USOS	114
4.7.4.- PROHIBICIONES	117
4.7.5.- MECANISMOS DE CONTROL	123
4.7.6.- SANCIONES	127
CAPÍTULO V	129
Conclusiones y Recomendaciones	129
5.1.- CONCLUSIÓN GENERAL	130
5.2.- RECOMENDACIONES	137

CAPÍTULO I

1.1.- INTRODUCCIÓN

El tópico de investigación que hemos seleccionado, se denomina “*EL DERECHO A LA INTIMIDAD DE LOS TRABAJADORES: EL CASO DEL CORREO ELECTRÓNICO EN EL MINISTERIO DE HACIENDA*”. Dicho tema, enmarca cuestiones que atañen tanto al Derecho Laboral como al Derecho Constitucional e, inclusive, a su homólogo Penal.

La implementación de la tecnología de avanzada en las instituciones, empresas y centros de labores en general, ha impulsado a la reorganización del trabajo en busca de incrementar la eficiencia técnica de las actividades, pero a la vez, está utilizándose como novedosa manera de vigilar la fuerza laboral, lo cual ha originado la aparición de nuevos problemas en este importante ámbito.

La presencia de estos equipos informáticos en los centros de trabajo, aumentan y mejoran las modalidades de control, ya sea con la finalidad de garantizar la productividad empresarial o institucional a través del cumplimiento por los trabajadores de sus obligaciones laborales, o bien, con respecto al personal que utiliza tecnologías de información y comunicación, a efecto de salvaguardar la seguridad de la organización ante intromisiones endógenas y/o exógenas.

Esta situación ha generado un interesante debate jurídico, referente al

derecho a la intimidad de los trabajadores en el seno de la relación laboral; sea la intromisión del poder patronal de dirección, control y vigilancia de la actividad productiva en la esfera privada del trabajador y, específicamente, en lo relativo al respeto de su intimidad y a la consideración debida a su dignidad en la utilización del correo electrónico.

Lo anterior, ha sido el motivo que nos ha llevado a estudiar el tema de marras, pretendiendo realizar un pequeño aporte a esta problemática mediante el presente estudio descriptivo-explicativo; ello con base tanto en lo que han manifestado la jurisprudencia y la doctrina extranjeras, como también en una serie de consideraciones y recomendaciones de carácter personal, toda vez que en Costa Rica el tema ha sido prácticamente inexplorado, dado lo novedoso del referido medio de comunicación electrónico.

A efecto de concretizar y circunscribir la temática, optamos por enfocar el tema hacia una institución del Sector Público, toda vez que al estar regidas por el principio de legalidad, dichas instituciones se ven en la obligación de publicar o dar acceso a los administrados de las normativas internas que rigen en ellas, contrario a lo que ocurre en la empresa privada, donde el patrono se muestra receloso o no anuente a brindar información.

En este orden de ideas escogimos el Ministerio de Hacienda, con la finalidad de establecer si en él existía o no, alguna normativa que regulara lo

concerniente al correo electrónico y, en el evento de que efectivamente existiera, verificar si la misma observaba los derechos constitucionales a la intimidad y al secreto de las comunicaciones que asisten a los trabajadores.

Este contexto, nos conduce a examinar el origen y la naturaleza jurídica del derecho a la intimidad, lo cual nos permitirá comprender su ubicación sistemática en el ordenamiento jurídico nacional. Las conclusiones de dicho supuesto, nos proporcionarán las bases para determinar si la propiedad de los medios permite a la parte patronal intervenir el *e-mail* de sus subordinados. Finalmente, los elementos de juicio que nos brinden las anteriores respuestas, nos permitirán establecer si la Política Sobre el Uso del Correo Electrónico del Ministerio de Hacienda observa las garantías constitucionales de los funcionarios.

La información a la que hacemos referencia en la presente investigación, se ha obtenido mediante la consulta bibliográfica y, sobre todo, a través de una ardua búsqueda vía internet, ya que dada la novedad del tópico existen pocos textos al respecto; lo cual se ve reflejado inclusive, en el hecho de que en Costa Rica únicamente contamos con un fallo de la Sala Segunda de la Corte Suprema de Justicia relativo al correo electrónico, contrario a lo acontecido en otras latitudes donde existen sendos pronunciamientos sobre el particular. Dicha información, ha sido sometida a un proceso metodológico que comprende la comparación, deducción y exégesis de los elementos de juicio extraídos a partir

de las fuentes antes citadas.

Este Trabajo de Investigación, está compuesto de cinco Capítulos con sus correspondientes Secciones.

El Capítulo Primero, lo dedicamos a plantear los aspectos formales que el estudio engloba, dentro de los que se contemplan la introducción, justificación, planteamiento y formulación del problema, así como también la sistematización.

La sustentación teórica de la investigación, en la que exponemos diversos enfoques, conceptos y antecedentes en general, imprescindibles para el correcto encuadre del estudio, la encontramos en el Capítulo Segundo referente al Marco Teórico.

En el Capítulo Tercero tenemos el Marco Metodológico, en el que se explica el tipo de estudio que efectuamos, sus alcances y limitaciones; así como también la problemática, objetivos y variables que presenta nuestro novedoso tópico.

Las disposiciones legales, los criterios jurisprudenciales, las vertientes doctrinarias, las cuestiones informáticas y el imperativo análisis de la Política sobre uso de internet emitida por el Ministerio de Hacienda, tiene lugar en el Capítulo Cuarto, en el que a lo largo del mismo se disgregan nuestras opiniones

según la temática tratada.

Finalmente, en el Capítulo Quinto efectuamos una conclusión general de los resultados obtenidos en nuestro trabajo, a la vez que se plantean una serie de proposiciones de *lege ferenda*, tendientes a reformar determinados aspectos de la Política de marras, las cuales en nuestro criterio, vendrían a apuntalar o mejorar en alguna medida el texto vigente; brindando de esta manera una modesta contribución a dicho Ministerio.

1.2.- JUSTIFICACIÓN

La introducción de la tecnología y del correo electrónico particularmente, en las diferentes instituciones, empresas y centros de trabajo en general, ha promovido la reorganización del trabajo con la finalidad de incrementar la eficiencia y eficacia de las labores.

No obstante, dicha situación también está utilizándose como una innovadora manera de controlar la actividad laboral, por lo que se han suscitado nuevos problemas que se han extendido inclusive al ámbito judicial, dada la incertidumbre jurídica que el uso de esta modalidad de correo causa a trabajadores y empleadores. Es claro entonces, que el devenir tecnológico ha cambiado en poco tiempo los medios que se empleaban normalmente en las comunicaciones, afectando a las partes que integran la relación laboral.

Así, la utilización de herramientas informáticas en los centros de trabajo, acrecientan y optimizan los tipos de control, ya sea a efecto de garantizar la productividad empresarial o institucional por medio del cumplimiento de las obligaciones laborales de los empleados, o bien, con relación al personal que utiliza tecnologías de información y comunicación, a fin de proteger la seguridad de la organización ante intrusiones internas y externas.

En este contexto se ha suscitado un atrayente problema jurídico, el cual responde a las nuevas realidades sociales que crean los procesos tecnológicos, y que se refiere al derecho a la intimidad de los trabajadores en el seno de la relación laboral; sea la actuación del poder patronal de dirección, control y vigilancia de la actividad productiva en la esfera privada del trabajador y, específicamente, en lo relativo al respeto de su intimidad y a la consideración debida a su dignidad en la utilización del correo electrónico.

Es así como precisamos dos posiciones totalmente adversas, en primer término, el derecho a la intimidad y el secreto de las comunicaciones de los empleados en cuanto a la utilización del correo electrónico y, en segunda instancia, el derecho que asiste al patrono para que los trabajadores utilicen dicho medio de comunicación con la diligencia debida para los fines que estrictamente se les proporcionó. El punto medular reside en establecer, si cuando el empleador procede a la apertura de los mensajes de la cuenta de correo electrónico de un trabajador, no siendo destinatario de los mismos,

incurre en una violación a los indicados derechos constitucionales; y en la eventualidad de que se pudiera saber el contenido de estos mensajes, cuál sería el límite a ese control. La complejidad del caso es precisamente lo que nos conducirá a intentar resolver el dilema desde la perspectiva de la ponderación de los derechos que están en juego.

En tal sentido, analizaremos si la Política sobre Correo Electrónico que actualmente se encuentra vigente en el Ministerio de Hacienda, a la luz de la legislación, doctrina, jurisprudencia y nuestra opinión, es respetuosa de los derechos constitucionales de los funcionarios.

Así las cosas, consideramos que el presente estudio permitirá, entre otros aspectos, brindar una interesante panorámica sobre este importante y poco explorado tema; materializando además los contenidos aprendidos mediante el análisis y propuesta de reforma a la Política vigente en el Ministerio de Hacienda, mismas que en nuestro criterio vendrían a depurar y mejorar la misma.

1.3.- PLANTEAMIENTO DEL PROBLEMA

1.3.1.- FORMULACIÓN DEL PROBLEMA

¿Prevalece el derecho a la intimidad personal e inviolabilidad de las comunicaciones que asiste a los empleados, o la facultad de control y dirección de la actividad laboral que tiene el patrono?

1.3.2.- SISTEMATIZACIÓN

El problema principal que formula nuestro estudio, inevitablemente hace surgir una serie de cuestionamientos con un mismo origen, cuyo planteamiento responde, precisamente, al contenido de la investigación misma. En esta tesitura, nosotros planteamos las siguientes interrogantes:

A.- Cobija el derecho a la intimidad las comunicaciones electrónicas de los trabajadores?

B.- La Propiedad del dominio a través del cual se envían los correos electrónicos, faculta al patrono para imponerse del contenido de las comunicaciones de sus empleados?

C.- La existencia de programas computacionales que proporcionan herramientas para controlar el correo electrónico, hace que por sí mismos su utilización sea legal?

D.- Existen en Costa Rica antecedentes jurisprudenciales donde se hayan ventilado aspectos concernientes a la intimidad en la utilización del correo electrónico?

E.- La Política Sobre el Uso del Correo Electrónico del Ministerio de Hacienda, es respetuosa de los derechos a la intimidad y al secreto de las comunicaciones de los funcionarios?

CAPÍTULO II

Marco Teórico

El derecho a la intimidad ha sido definido como un derivado de la dignidad de la persona, que conlleva la existencia de un espacio propio y reservado frente a la acción y conocimiento de los demás (Goñi, 2003). El ente procurador costarricense, ha señalado que implica el libre desarrollo de la vida interior de las personas, ajena a las relaciones que se mantienen con otros individuos; que permite conocerse como ser humano y que se funda en que el ámbito de la libertad interior es instrumento para el desarrollo de la personalidad (Procuraduría General de la República, 2003).

Asimismo y circunscribiéndonos a la esfera de trabajo, se ha dicho que el mencionado derecho ampara tanto la protección de las cuestiones pertenecientes a la vida no laboral del trabajador, como también determinadas injerencias de la vida laboral que podrían ser invasoras por sí mismas (Camas, 2003).

Dada la singular importancia que ostenta el derecho a la intimidad, numerosos instrumentos normativos se han ocupado de regular el mismo, tales como la Constitución Política, los Tratados Internacionales y las Leyes en general; ello tanto en nuestra tierra como en el extranjero. Así, en otros países -sobre todo en España-, encontramos varios e importantes criterios jurisprudenciales donde se analiza esta temática, verbigracia el fallo número 110/1984 del Tribunal Constitucional Español, en el cual afirmó el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluida del conocimiento ajeno y de las intromisiones de la tecnología, salvo autorización del interesado (Abad, 2003).

En el mismo orden de ideas y en una relación de género a especie, tenemos el Derecho al Secreto de las Comunicaciones, dentro de las cuales se engloba el correo electrónico. El propio numeral 24 de nuestra Carta Magna, se encarga de tutelar esta garantía fundamental frente a las injerencias de terceros, e incluso se ha llegado a afirmar por parte del Tribunal Constitucional de España, que no es dable distinguir el cause tecnológico de las mismas, toda vez que la normas hacen referencia a cualquier clase de comunicación privada (Villahermosa, 2003).

Sin embargo y en lo que se refiere específicamente al *e-mail*, multitud de empleadores observan como sus trabajadores gastan una importante parte de su tiempo laboral enviando y recibiendo todo tipo de mensajes por correo electrónico; razón por la cual surgen una serie de cuestionamientos con un origen común: ¿a quién pertenecen esos correos?, ¿se pueden considerar privados?, ¿puede el empresario acceder al contenido sustantivo de un e-mail? (Castañeda, 2000).

En este punto radica el problema de fondo que plantea nuestra investigación, consistente en establecer, al momento de generarse el choque de intereses entre la parte obrera y la patronal, si –como propugnamos nosotros– prevalece el derecho a la intimidad personal e inviolabilidad de las comunicaciones que asiste a los empleados o, por el contrario, se impone la potestad que tiene todo patrono a proteger los medios organizativos patrimoniales y a dirigir y controlar la actividad laboral de sus trabajadores.

La cuestión adquiere una mayor preponderancia, si analizamos los problemas que la utilización personal del *e-mail* puede provocar, principalmente los relacionados con inconvenientes de seguridad y ocasionadoras de daños a la empresa mediante virus, comportamientos de usurpación de personalidad, acoso sexual, pérdida de productividad y transmisión de datos confidenciales de la empresa (Rubio de Medina, 2003).

La jurisprudencia misma, no es coincidente al momento de analizar este tópico. Se han suscitado casos en los cuales los órganos jurisdiccionales consideran que a las compañías les asiste el derecho de examinar el correo de los trabajadores, puesto que el material informático es propiedad del empleador (Rubio de Medina, 2003); así como otros tantos en los que se ha estimado que el secreto de las comunicaciones está por encima de todo y la auditoría o examen de los correos personales del trabajador vulnera los preceptos constitucionales (Asociación de Internautas, 2003).

En el mismo contexto, la doctrina ha planteado al patrono una serie de alternativas, que procuran evitar los inconvenientes laborales en la utilización del correo electrónico, dentro de las que se encuentra el prever las circunstancias en el convenio colectivo o en el contrato de trabajo, así como también la posibilidad de que el empleador pueda controlar el nombre del destinatario pero no el contenido del mensaje (Rubio de Medina, 2003).

Sin embargo, cuando una falta cometida por el trabajador reviste gravedad, el empleador usualmente recurre al inmediato despido. No obstante, por la fuerza con que la acción de despido incide en la vida del trabajador, la jurisprudencia exige en estos supuestos la existencia de proporcionalidad y adecuación entre el hecho, la persona y la sanción, por lo que es necesario valorar de manera individual las circunstancias concurrentes en cada caso concreto, partiendo siempre de la teoría gradualista (Rubio de Medina, 2003.)

En tal sentido, abordamos las Normas y Políticas en el Uso de Servicios de Correo Electrónico y Acceso a Internet vigentes en el Ministerio de Hacienda (Ministerio de Hacienda, 2002), específicamente en lo que atañe al correo electrónico, con la finalidad de precisar si esta normativa, a la luz de la jurisprudencia, legislación y doctrina estudiada, cumple con los parámetros fundamentales para armonizar el derecho a la intimidad y el secreto a las comunicaciones que protege a las funcionarios con el derecho al control de la actividad laboral que asiste al patrono.

CAPÍTULO III

Marco Metodológico

3.1. – TIPO DE INVESTIGACIÓN

Consideramos que nuestro estudio presenta un carácter descriptivo-explicativo, toda vez que busca especificar y analizar el derecho a la intimidad de los trabajadores en el uso del correo electrónico; ello, evaluando sus características, la doctrina, los instrumentos normativos que lo garantizan y los principales criterios jurisprudenciales, tomando como base la información recolectada.

Lo anterior, con la finalidad de precisar si la Política sobre correo electrónico vigente en el Ministerio de Hacienda, es acorde y respetuosa de los derechos de los trabajadores. En tal sentido, examinaremos aspectos como la inviolabilidad de las comunicaciones, las cuestiones informáticas y los mecanismos de control, entre otros, los cuales están estrechamente relacionados con el contenido del indicado instrumento normativo.

De esta forma, por medio del conocimiento adquirido, vamos más allá de la simple descripción de conceptos, adoptando una posición unívoca y fundamentada en cuanto a la temática sometida a estudio, para finalmente sugerir la reforma de algunos numerales de la Política vigente.

3.2.- MATRIZ DE DISEÑO DE INVESTIGACIÓN

TEMA	PROBLEMA	OBJETIVOS	
		GENERAL	ESPECÍFICOS
El Derecho a la Intimidad de los Trabajadores: El Caso del Correo Electrónico en el Ministerio de Hacienda	En el tópico del derecho a la intimidad y al secreto de las comunicaciones en la esfera laboral, particularmente en lo que se refiere al correo electrónico, al suscitarse el choque de intereses entre la parte obrera y la parte patronal, cuál derecho prevalece: El derecho a la intimidad personal e inviolabilidad de las comunicaciones que asiste a los empleados o, por el contrario, la potestad que tiene todo patrono a proteger los medios organizativos patrimoniales y a dirigir y controlar la actividad laboral de sus trabajadores?	<p><i>l. De Diagnóstico</i></p> <p>Analizar la posición del Ministerio de Hacienda con respecto al uso del correo electrónico de sus trabajadores, a la luz de la doctrina, de la jurisprudencia y del marco normativo que regula el derecho a la intimidad</p>	<p>1.-Analizar los alcances y limitaciones establecidos por la doctrina, referentes al uso del correo electrónico y su relación con el derecho a la intimidad</p> <p>2.-Determinar las disposiciones legislativas y los criterios jurisprudenciales que regulan el derecho a la intimidad con respecto al uso del correo electrónico</p> <p>3.-Evaluar las circunstancias en las que el empleo de instrumentos y/o medidas de control pueden vulnerar el derecho a la intimidad de los trabajadores al utilizar el correo electrónico</p>

TEMA	PROBLEMA	OBJETIVOS
		<p><i>II.- De</i> <u><i>Propuesta</i></u></p> <p>Armonizar la Política sobre Correo Electrónico vigente en el Ministerio de Hacienda, de acuerdo con la doctrina y la jurisprudencia moderna, analizadas en el texto de la investigación</p> <p>1.-Estructurar un procedimiento para materializar las reformas pertinentes, en la Política sobre Uso de Correo Electrónico vigente en el Ministerio de Hacienda</p> <p>2.-Implementar un procedimiento para comunicar a los funcionarios del Ministerio de Hacienda, las reformas operadas en la Política sobre Uso de Correo Electrónico</p> <p>3.-Establecer reuniones periódicas de revisión de la Política sobre Uso de Correo Electrónico, a efecto de medir los alcances de su vigencia y efectiva aplicación</p>

3.3.- MATRIZ DE OPERALIZACIÓN DE VARIABLES

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES	INSTRUMENTOS RECOLECCIÓN DE DATOS
Derecho a la intimidad	Conjunto de normas jurídicas que regulan y protegen la esfera privada del trabajador	Análisis jurídico del derecho a no tener intromisiones de terceros en la utilización del e-mail	Derecho Constitucional	-Análisis de legislación, doctrina y jurisprudencia - Observación
Doctrina	Conjunto de tesis y opiniones de los tratadistas y estudiosos del derecho que explican y fijan el sentido de las leyes o sugieren soluciones para cuestiones aún no legisladas	Estudio de los alcances y las limitaciones establecidas por la doctrina	Tesis y Opiniones	-Análisis de legislación, doctrina y jurisprudencia
Jurisprudencia	Conjunto de sentencias que determina un criterio acerca de un problema jurídico omitido u oscuro en los textos positivos o en otras fuentes del derecho	Examen de fallos reiterados de los Tribunales de Justicia	Conjunto de sentencias	-Análisis de legislación, doctrina y jurisprudencia

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	INDICADORES	INSTRUMENTOS RECOLECCIÓN DE DATOS
Disposiciones Legislativas	Regla de conducta obligatoria dictada por el Poder Legislativo, o por el Poder Ejecutivo cuando lo substituye o se arroga sus atribuciones	Análisis de las leyes emitidas por la Asamblea Legislativa en torno al derecho a la intimidad	Reglas coercitivas	-Legislación, doctrina y Jurisprudencia
Instrumentos y/o medidas de control	Medios para controlar la utilización del correo electrónico: comprobación, fiscalización, intervención	Grado de vulneración al derecho a la intimidad	Vigilancia	-Legislación, doctrina y Jurisprudencia

3.4.- SUJETOS Y FUENTES DE INFORMACIÓN

Las principales fuentes que utilizamos en el presente estudio las constituyen el internet, la jurisprudencia, los libros y doctrina en general, la bibliografía y la investigación de campo; a través de las cuales, recolectamos la información pertinente para la elaboración del trabajo de investigación.

3.5.- ALCANCES Y LIMITACIONES DE LA INVESTIGACIÓN

Pretendemos abordar el tópico del derecho a la intimidad de los trabajadores, en la utilización del correo electrónico propiedad del patrono. En tal sentido, el alcance de la investigación se circunscribe a analizar la doctrina, legislación y jurisprudencia existentes, definiendo y examinando los aspectos más trascendentales de las mismas, para posteriormente, constatar si la Política que rige en el Ministerio de Hacienda es respetuosa de los preceptos constitucionales y examinar la manera en la cual se ocupa de regular el tema del correo electrónico. Finalmente, se busca realizar un pequeño aporte al sugerir la introducción de algunos cambios, tanto de forma como de fondo, en la normativa vigente.

Las limitaciones encontradas en nuestra labor, podemos resumirlas en tres puntos: La prácticamente nula casuística existente en Costa Rica, la escasa legislación que puede resultar aplicable a los conflictos donde el correo electrónico tiene un papel preponderante y, finalmente, la poca cantidad de literatura sobre la temática, lo cual sin embargo no es de extrañar, ya que evidentemente se trata de un tópico novedoso que apenas empieza a ser explotado con la llegada de las tecnologías de información.

CAPÍTULO IV

Análisis e Interpretación de Resultados

4.1.- SECCIÓN I. EL DERECHO A LA INTIMIDAD: NOCIONES GENERALES

Cuando nos aprestamos a estudiar o evaluar una temática, siempre es necesario referirnos en primera instancia a las cuestiones más elementales, dado que ellas son las que, posteriormente, nos permitirán abordar los tópicos más complejos. Este análisis que va de los aspectos generales a los específicos, nos ayuda a tener una mayor visión y a desarrollar con claridad nuestras ideas. Por tal circunstancia, en esta sección nos avocaremos a reseñar sucintamente qué se entiende por el denominado derecho a la intimidad, así como también el lugar que ocupa en nuestra legislación y el desarrollo jurisprudencial que, tanto a nivel nacional como internacional, ha desencadenado.

En este orden de ideas, procederemos entonces a ilustrar los principales aspectos que los estudiosos del derecho han manifestado con relación al derecho a la intimidad.

4.1.1- CONCEPTO

La Real Academia Española (1992), define a la intimidad como *“la zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia”* (p.1182). Asimismo, se le ha conceptualizado como un derecho

derivado de la dignidad de la persona, que conlleva la existencia de un espacio propio y reservado frente a la acción y conocimiento de los demás (Camas, 2003).

Santos Cifuentes, citado por Cesario en su obra *Hábeas Data* (2001), se refiere al derecho a la intimidad como un derecho personalísimo, que posibilita al individuo sustraerse de la publicidad o de cualquier otro tipo de intromisiones a su vida privada.

En el mismo sentido, se ha dicho que el derecho a la intimidad supone la protección jurídica de la vida privada, lo que en el derecho anglosajón se conoce con el nombre de "*right of privacy*"; y se le ha concebido como aquel que tutela jurídicamente un espacio de autonomía individual integrada por los sentimientos, hábitos y costumbres, las relaciones de familia, cuestiones económicas, credo religioso, salud, y en general, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad, están reservadas al propio individuo (Cesario, 2001).

La Procuraduría General de la República (2003), también se ha referido a este derecho, manifestando que conlleva el libre desarrollo de la vida interior de las personas, ajena a las relaciones que se mantienen con otros individuos; que permite conocerse como ser humano y que se funda en que el ámbito de la libertad interior es instrumento para el desarrollo de la personalidad.

Además, se ha manifestado que la intimidad es la esfera personal de cada uno, en donde residen los valores humanos y personales, siendo un derecho fundamental para el desarrollo de la persona y de la familia además de ser un ámbito reservado a la curiosidad de los demás contra intromisiones e indiscreciones ajenas (Villahermosa, 2002).

En lo que atañe a la noción de “*vida privada*” en la relación laboral (que se asimila a estos efectos a la noción de privacidad, de raíz anglosajona), ampara tanto la protección de las cuestiones pertenecientes a la vida no laboral del trabajador, como también determinadas injerencias de la vida laboral que podrían ser invasoras *per se* (Camas, 2003).

Como puede observarse, algunos de los conceptos expuestos resultan ser más amplios que otros. Así, Camas (2003) se refiere a la intimidad como un derecho que se derivaba de la dignidad del individuo, el cual inclusive extiende su ámbito de aplicación a determinados asuntos que conciernen a la vida laboral de los empleados, criterio que no se aprecia en el resto de las definiciones apuntadas. En el mismo sentido, tanto el ente procurador (2003) como Villahermosa (2002) lo visualizan como un instrumento fundamental para el crecimiento de las personas. No obstante lo anterior, resulta evidente que los diversos autores coinciden plenamente en que la intimidad constituye el derecho a un espacio propio, íntimo y reservado contra intromisiones externas en la vida de las personas.

En resumen, es dable concluir que el derecho a la intimidad surge como un derecho personalísimo derivado de la dignidad humana, que ampara la vida privada protegiéndola de intromisiones de terceros, inclusive en el propio centro de labores, posibilitando a su vez, el desarrollo interior de las personas. Es claro entonces, que este razonamiento deviene aplicable en las relaciones entre el patrono y los trabajadores.

4.1.2.- DERECHOS Y DEBERES DEL TRABAJADOR Y DEL PATRONO

El análisis del deber de buena fe y del derecho al control de la actividad del trabajador, resulta imperativo al momento de estudiar la legalidad de las conductas, tanto del empleado como del patrono en la utilización y/o control del correo electrónico, por lo que seguidamente abordaremos los mismos.

i) Deber de buena fe

La doctrina lo describe como aquel principio que busca alcanzar una convivencia pacífica y próspera entre las personas de una comunidad, concretándose en la confianza de una actuación concreta de otro, en la lealtad de los tratos y en la fidelidad de la palabra dada (Rubio de Medina, 2003). Según señala Rubio de Medina (2003), la jurisprudencia española por su parte, ha ido perfilando poco a poco el amplísimo concepto de buena fe, así la Sala de

lo Social del Tribunal Superior de Justicia de Canarias, Tenerife, en su sentencia de fecha de 19 de enero del 2001, estimó que:

a) Por buena fe ha de entenderse obrar acorde con las reglas naturales y comunes recibidas de la honestidad y la rectitud, conforme a los criterios morales y socialmente imperantes

b) Que su finalidad está en proscribir aquellas actuaciones del trabajador intencionalmente dirigidas a inferir un daño material o moral al empleador, supuesto éste, en el que el fraude, la deslealtad o la conducta realizada con abuso de confianza no podrían buscar amparo bajo norma constitucional declarativa de derecho alguno

c) En este sentido, la facultad empresarial sancionadora debe amoldarse a la equidad, no subsumiendo mecánicamente los hechos en la norma, sino apreciando los factores concurrentes en el caso concreto

Según señala la autora antes citada, la jurisprudencia interpreta como incumplimiento de la buena fe contractual la utilización personal del correo electrónico de la empresa y ello con independencia de los perjuicios que la actitud del trabajador ocasiona a la organización. Sin embargo, es necesario señalar que este deber de buena fe es recíproco, es decir que no solo existe por parte del trabajador con respecto al patrono, sino que éste, a su vez, también

debe regirse por este principio en las relaciones con sus trabajadores.

La doctrina y los criterios jurisprudenciales, como veremos en detalle adelante, nos facilitan vislumbrar que, en ocasiones, no es el mero uso con carácter personal del correo electrónico por parte del trabajador lo que ha permitido justificar los despidos realizados por el patrono alegando vulneración de la buena fe contractual, sino el contenido de los mensajes, los cuales tenían como común denominador el carácter obsceno, despreciativo y/o humorístico (Rubio de Medina, 2003).

ii) Derecho al Control Patronal de la Actividad Realizada por el Trabajador

El empleado, en el ejercicio de sus labores, está obligado a cumplir una variedad de deberes laborales, los cuales se materializan con respecto al patrono en el poder de dirección y control de la actividad laboral.

Dentro del campo del posible control patronal en la utilización del *e-mail*, tenemos que tener en cuenta que éste será más intenso si partimos, de que en el ámbito laboral no cabe realizar actividades de carácter personal y que los medios de trabajo pertenecen a los empleadores.

No obstante lo anterior, la facultad del patrono para controlar la actividad del trabajador no es absoluta, como no lo es ninguno de los derechos, sino que

las medidas de vigilancia y control que pueda implementar –en el caso que nos ocupa acciones para controlar el uso del correo electrónico por parte del trabajador- deberá de establecerlas teniendo en consideración el respeto a la dignidad humana. En síntesis, la actividad de control de la parte patronal se encuentra limitada por el derecho a la dignidad del trabajador, el derecho al honor, a la intimidad personal, familiar, a la propia imagen y el derecho al secreto de las comunicaciones.

Por ello, en el tanto los medios tecnológicos permiten vigilar ciertas actividades de los trabajadores, el punto está en determinar si el empleador tiene derecho o no a utilizarlas para controlar la actividad de los trabajadores a su cargo. La jurisprudencia (Camas, 2003), como se verá más adelante, dado que el empleado tiene derecho a que se respete su dignidad, interpreta que las medidas de control se consideran correctas si:

- a) Nos encontramos ante una medida de control justificada
- b) Es una medida idónea para la finalidad pretendida
- c) Es necesaria en la medida que la prueba obtenida mediante el control impuesto por el empresario para despedir al trabajador sirva para probar la conducta irregular
- d) Es equilibrada o proporcionada

En todo caso, las medidas de control adoptadas por las empresas y las instituciones, tanto para controlar la utilización del correo electrónico como para

fiscalizar cualquier otro tipo de actividad, deberán ser comunicadas con carácter previo al trabajador e inclusive, como observa Thibault Aranda, y refiriéndose a las imágenes obtenidas por videocámaras, las imágenes habrán de conservarse solo el tiempo estrictamente necesario para cumplir la finalidad para la que se han recogido, así como facilitarse el acceso a las mismas de los trabajadores. Aunque, como se ha mencionado, este aspecto se refiere sólo a la conservación de películas tomadas con videocámaras, creemos que nada impide que se exija el mismo derecho para los mensajes enviados y/o recibidos a través de la cuenta de correo electrónico del trabajador que son conservados por el empresario (Rubio de Medina, 2003).

4.2.- SECCIÓN II. INSTRUMENTOS NORMATIVOS Y ANÁLISIS JUDICIAL

La intimidad en el uso del correo electrónico, de un dominio propiedad de una empresa o institución, supone adentrarse en un campo lleno de contradicciones, opiniones enfrentadas y posiciones diversas.

En este aparte, nos encargaremos de precisar los principales cuerpos legales en los que la intimidad encuentra resguardo. Ciertamente, son considerables las iniciativas tendientes a la regulación de este derecho, lo cual pone de manifiesto su importancia.

4.2.1.- CONSTITUCIÓN POLÍTICA

El derecho a la intimidad, el secreto a las comunicaciones, la inviolabilidad de los documentos privados y el derecho a la autodeterminación informativa, encuentran asidero constitucional en el artículo 24 de nuestra Carta Magna, mismo que establece lo siguiente:

Artículo 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para establecer asuntos sometidos a su conocimiento.

Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuanto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción (...) No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación (El subrayado es proveído)

De lo transcrito se extrae con claridad, que nuestro legislador consideró imprescindible dar protección de rango constitucional a los derechos fundamentales antes indicados, los cuales encuentran su razón de ser en la dignidad de las personas, la cual asegura a su vez, el respeto a la condición humana.

4.2.2.- TRATADOS INTERNACIONALES

La comunidad internacional también se ha preocupado por propugnar normas que tutelen el respeto al derecho a la intimidad. Es así como mediante instrumentos internacionales de derechos humanos, ha buscado dar sustento normativo a dicho derecho fundamental. A manera de ejemplo, a continuación exponemos brevemente parte del articulado que observa esta garantía:

i) Declaración Universal de Derechos Humanos

Artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias. (Naciones Unidas, 2004)

ii) Declaración Americana de los Derechos y Deberes del Hombre

Artículo 5: Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar (Inter-American Commission and Human Rights, 2004)

iii) Convención Americana Sobre Derechos Humanos

Artículo 11: Protección de la Honra y de la Dignidad (...) Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida

privada, la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. (Inter-American Commission and Human Rights, 2004)

iv) Pacto Internacional de Derechos Civiles y Políticos

Artículo 17.- Observación general sobre su aplicación

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques (Oficina del Alto Comisionado de las Naciones Unidas para Los Derechos Humanos, 2004)

v) Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales

Artículo 8. Derecho al respeto a la vida privada y familiar

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás (Ruidos.org., 2004)

Es claro que los cinco artículos transcritos, correspondientes a distintas disposiciones normativas internacionales, son coincidentes en salvaguardar la

vida privada de las personas y la privacidad de sus comunicaciones, señalando expresamente la existencia de protección jurídica contra cualquier tipo de injerencia arbitraria sobre las mismas.

Sin embargo, ello no significa que no existan diferencias entre dichas normas: mientras la Declaración Americana de los Derechos y Deberes del Hombre se refiere genéricamente a la protección de la vida privada y familiar de las personas, el resto de los instrumentos internacionales son más explícitos al tutelar expresamente la defensa contra las injerencias arbitrarias –abusivas o ilegales agregan algunos- en la vida privada, familiar, en el domicilio y en la correspondencia. El Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, incluso hace la atinada excepción de que salvo por previsión legal y en determinados supuestos, no puede darse intromisión alguna en la intimidad de lo ciudadanos; disposición que confirma la inexistencia de derechos absolutos.

4.2.3.- DERECHO COMPARADO

Con la finalidad de dar una mayor perspectiva, a continuación expondremos algunos fragmentos de distintos cuerpos normativos españoles (Rubio de Medina, 2003), en los cuales encuentra asidero el derecho a la intimidad.

i) Constitución Española de 1978

Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

ii) Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen

Artículo 1. Uno. El Derecho Fundamental al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, garantizado en el artículo 18 de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas(...)

Dos. (...)

Tres. El Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen es irrenunciable, inalienable e imprescriptible (...)

Artículo 7. Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:

...Dos. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o de cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción.

iii) Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores

Artículo 4. Derechos laborales. [...].

2. En la relación de trabajo, los trabajadores tienen derecho: [...]

e) Al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente a ofensas verbales o físicas de naturaleza sexual.

Artículo 18. Inviolabilidad de la persona del trabajador. Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

Artículo 20. Dirección y control de la actividad laboral.

3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

Como se desprende de las disposiciones normativas transcritas, la protección al derecho a la intimidad en el país ibérico es una constante; aunque lógicamente, existen algunas diferencias entre los artículos que lo amparan. De esta forma, encontramos que la garantía a la intimidad personal y familiar consagrada de manera genérica en el numeral 18 de la Constitución Española, es desarrollada un tanto más en la Ley Orgánica 1/1982, la cual le otorga el

carácter de irrenunciable, inalienable e imprescriptible, a la vez que señala una serie de conductas que considera intromisiones ilegítimas dentro del ámbito de protección del referido derecho, las que en nuestro criterio tienen fines ilustrativos y no un carácter taxativo.

Por su parte y siguiendo la misma línea de pensamiento, el Real Decreto Legislativo 1/1995 establece el respeto a la intimidad de los trabajadores. Para garantizar la inviolabilidad de la persona del trabajador, estipula que únicamente podrán efectuarse registros sobre el empleado cuando sean necesarios para proteger el patrimonio de la compañía y el de los demás trabajadores, dentro del lugar de labores y en horario de trabajo, debiéndose inclusive en estos casos y en todos aquellos en que se apliquen medidas de vigilancia y control, respetar al máximo la dignidad del trabajador; dejando patente los límites que tiene el poder de dirección empresarial.

Volviendo a la Constitución Española, es claro que expresamente garantiza el secreto de las comunicaciones, tema que trataremos en detalle más adelante, así como también que limita el uso de la informática para garantizar la intimidad de los individuos. Creemos que en esta última temática, el legislador tuvo un convencimiento visionario de las implicaciones de hecho y de derecho que la computación generaría en el futuro, máxime si tomamos en consideración que la norma data del año 1978, tiempo donde la informática no tenía ni por asomo el desarrollo del que goza hoy en día.

Recapitulando, podemos decir que constitucional y legalmente, la normativa española es clara al tutelar el derecho a la intimidad y el secreto de las comunicaciones, inclusive limitando explícitamente el uso de la informática para garantizar tales derechos, los cuales son calificados como inalienables, irrenunciables e imprescriptibles. No obstante, reconoce la facultad del patrono para que, en ejercicio del poder de dirección y control de la actividad laboral, adopte medidas para corroborar el cumplimiento de las obligaciones de los empleados, pero siempre en estricta observancia a las leyes y a la dignidad humana.

4.2.4.- JURISPRUDENCIA

Pese a que los Tribunales de Justicia costarricenses no se han ocupado con detenimiento de abordar el tema del derecho a la intimidad, en España, el Tribunal Constitucional ha incidido abiertamente en la configuración del mismo, tal y como puede extraerse de los fallos que de seguido pasamos a exponer (Abad, 2003):

i) En sentencia número 110/1984, afirmó el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluida del conocimiento ajeno y de las intromisiones de la tecnología, salvo autorización del interesado; es lo que se ha venido llamando derecho de autodeterminación informática.

Lo resuelto en este fallo, podemos relacionarlo con lo contemplado en el artículo 18 de la Carta Magna Española, en el sentido de que garantiza el derecho a la intimidad de los ciudadanos, ante intromisiones de agentes externos.

ii) En sentencia número 254/1993, estableció que el incremento de los medios técnicos de tratamiento de la información puede ocasionar la invasión de la esfera privada de los ciudadanos y, correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aún indirecto, que produzca este efecto, y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial del derecho.

Esta resolución, amplía lo expuesto en su homóloga anterior, en el sentido de que al poder la tecnología causar intromisiones en el ámbito reservado de las personas, el derecho a la intimidad debe acudir en resguardo de los ciudadanos para protegerlos, con independencia del medio por el cual se vea amenazada la esfera privada de éstos.

iii) En sentencia número 231/1998, Caso Paquirri, señaló que la intimidad personal es un derecho fundamental derivado de la dignidad de la persona, y que implica la existencia de un ámbito propio y reservado frente a la acción y

conocimiento de los demás, necesario –según las pautas de nuestra cultura– para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos y ligados a la existencia misma del individuo.

Este pronunciamiento introduce un nuevo elemento, el cual pudimos observar de similar manera, cuando nos ocupamos de definir el derecho a la intimidad: el afirmar el carácter personalísimo e inalienable de la intimidad de los individuos como un derivado de la dignidad humana. Asimismo, es congruente en reconocer el ámbito privado de cada persona ante el resto de sus semejantes.

iv) En la sentencia STC 90/2000 (Rubio de Medina, 2003) de 10 de abril, se interpreta que el derecho a la intimidad conlleva un ámbito propio y reservado frente a la acción y el conocimiento de tener una calidad mínima en la vida humana. Además, se señala que no es un derecho absoluto, sino que puede ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél vaya a experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho. Finalmente, asevera que el empresario, en el ejercicio de las facultades de control, puede establecer medidas que garanticen la buena marcha de la empresa, pero siempre deberá de adoptarlas respetando la dignidad del trabajador.

Este fallo nos aporta un aspecto de singular importancia, sea el indicar que el derecho a la intimidad no tiene un carácter absoluto, sino que puede ceder ante intereses constitucionalmente relevantes, siempre que para lograr el fin legítimo previsto se cumpla con los requisitos de necesidad, proporcionalidad y respeto al contenido esencial del derecho.

v) En sentencia número 98/2000 (Camas, 2003), declaró que el artículo 18.1 de la Constitución protege la intimidad personal y familiar del trabajador, tanto en aquellas parcelas incluidas en el marco de su vida privada, como en las que se incluye el entorno profesional. Ello al determinar que vulnera el derecho a la intimidad la instalación por la entidad Casinos de la Toja, S.A., en varios puestos de trabajo (el de cajero y el destinado a la ruleta rusa), de micrófonos de grabación de sonidos. El Tribunal Constitucional rechaza la argumentación de que el derecho a la intimidad sólo pueda ejercerse exclusivamente en el ámbito de la esfera privada del trabajador, que en el centro de trabajo quedaría delimitado por los lugares de descanso o esparcimiento, vestuarios, lavados o análogos, sino que por el contrario, extiende la protección a aquellos lugares en los que se desempeñan las tareas profesionales, donde también, por tanto, puede producirse una lesión del derecho fundamental, por ejemplo, mediante la grabación de las conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, en las que se aborden cuestiones ajenas a la relación laboral que se integran en lo que se denomina esfera propia de desenvolvimiento del individuo. La sentencia completa su razonamiento

argumentando que, para validar la disposición de medidas de vigilancia y control de la actividad laboral, se han de comprobar prioritariamente el cumplimiento del principio de proporcionalidad e intervención mínima que rige la modulación del derecho a la intimidad del trabajador por el poder de dirección empresarial, y que puede comprobarse a través de la existencia de varios elementos: que el control no se lleve a cabo de forma masiva e indiscriminada; que se hayan llevado a cabo subrepticamente; o la finalidad que persiguen con la consiguiente justificación, y por tanto, si las medidas de vigilancia resultan indispensables para la seguridad y buen desarrollo de la actividad productiva.

Como puede observarse, con el paso de los años la jurisprudencia fue generando nuevos e interesantes aportes al desarrollar el concepto de la intimidad. En este caso, se discierne que la Constitución Española tutela la intimidad del trabajador tanto en su vida particular como en su ambiente laboral; es decir, que aún en aquellos lugares en que el empleado realiza sus deberes profesionales se ve amparado por esta importante garantía. Además, coincide con el fallo STC 90/2000 analizado *supra*, en que las medidas de control empresarial deben cumplir con los principios de necesidad, proporcionalidad e intervención mínima.

vi) En las sentencias 207/1996 y 186/2000 (Camas, 2003), se estableció que la constitucionalidad de cualquier medida restrictiva del derecho a la intimidad y a la vida privada del trabajador, viene determinada por la estricta observancia del

principio de proporcionalidad, que implica cumplir con tres requisitos que son: el juicio de idoneidad, es decir, si la medida de vigilancia y control es susceptible de conseguir el objetivo propuesto; el juicio de necesidad de la medida, en el sentido de que no exista otra más respetuosa con la intimidad y dignidad del trabajador para conseguir el objetivo propuesto, y el juicio de proporcionalidad en sentido estricto, es decir, si la medida es ponderada y equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Coincidiendo con el comentario realizado a la sentencia anterior, estos pronunciamientos, vienen a abonar, ordenar, depurar y precisar lo expuesto por los fallos STC 90/2000 y 98/2000, en el tanto que señala que cualquier medida restrictiva de la intimidad del trabajador debe velar por la observancia del principio de proporcionalidad, el cual a su vez implica cumplir con tres subprincipios que se encuentran inmersos en él: idoneidad, necesidad y proporcionalidad en sentido estricto.

En síntesis, de las sentencias antes expuestas podemos extraer, a manera de conclusión, que la doctrina del Tribunal Constitucional Español está adaptando el artículo 18.1 de su Carta Magna, a las nuevas modalidades de control de la actividad laboral de los trabajadores que se están produciendo en el ámbito empresarial e institucional con la introducción de las nuevas tecnologías, y ello ante la falta de reformulación de la normativa ordinaria actualmente

existente en el espacio de los poderes patronales de vigilancia y control (Camas, 2003).

Del análisis de la legislación, doctrina y jurisprudencia expuestas en este capítulo, en nuestro criterio, el ordenamiento jurídico costarricense tutela una amplia defensa del derecho a la intimidad, incluyéndose dentro de éste cualquier tipo de atentado sin que importe el modo, forma, o medio empleado, por lo que obviamente incluye la protección al correo electrónico.

4.3.- SECCIÓN III. EL SECRETO DE LAS COMUNICACIONES

El humano por su propia naturaleza, es un ser que necesita vivir en comunidad con sus iguales. Dentro de una sociedad, existen medios a través de los cuales las personas se comunican entre sí, a efecto de satisfacer sus necesidades más elementales. La carta, el telégrafo, la telefonía y más recientemente el correo electrónico, son algunos de los instrumentos que se han venido utilizando para tal fin. Dada la trascendencia que una comunicación privada reviste, desde hace muchas décadas alrededor del orbe los órganos encargados de legislar han considerado necesario tutelar, incluso a nivel constitucional, el secreto de las comunicaciones privadas.

Los procesos tecnológicos crean nuevas realidades sociales que muchas

veces generan problemas jurídicos. El correo electrónico está provocando muchos conflictos en las empresas e instituciones, los cuales se han extendido inclusive al ámbito judicial, dada la incertidumbre jurídica que el uso de esta modalidad de correo causa a trabajadores y empleadores. En ese sentido, el desarrollo tecnológico ha cambiado en poco tiempo los medios que se utilizan normalmente en las comunicaciones, afectando a las partes que integran la relación laboral.

Ahora bien, es importante tener en consideración que una cosa es acceder a las direcciones de internet, las cuales, en la mayoría de los casos tienen un contenido público que puede visitar cualquier persona, y otra muy distinta abrir los mensajes de correo electrónico con la finalidad de comprobar si su contenido tiene o no que ver con el trabajo desempeñado por el empleado. Así, es menester vincular el derecho a la intimidad con el derecho al secretismo en las comunicaciones (Rubio de Medina, 2003).

Tal y como se indicó con anterioridad en este trabajo, el artículo 24 de nuestra Carta Magna protege el derecho fundamental al secreto de las comunicaciones, como una manifestación de la intimidad de las personas, el cual no obstante, como se verá *infra*, no guarda un carácter irrestricto.

4.3.1.- CUESTIONES DOCTRINARIAS Y EL PROBLEMA DE FONDO

El derecho al secreto de las comunicaciones, es un facultad subjetiva que es inmediatamente exigible frente a los poderes públicos y privados. Se trata de un derecho de defensa frente a injerencias de terceros, que se concreta en la imposibilidad de interceptar una comunicación si no es a través del cause previsto en la Constitución, y en nuestro caso, por remisión, en las leyes especiales, como por ejemplo la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, número 8204. Como se verá más adelante, tanto el numeral 24 de la Constitución Política costarricense como el artículo 18 de su homóloga española, ambos citados con anterioridad, protegen el secreto de las comunicaciones.

Sin embargo, muchos empleadores observan como sus funcionarios gastan gran parte de su tiempo de trabajo enviando y recibiendo todo tipo de mensajes por *e-mail*. Es una realidad que cada día, gran parte de los cientos de millones de usuarios del correo electrónico de todo el mundo, envían y reciben correos desde sus puestos de trabajo.

En esta tesitura, nacen una amplia cantidad de inquietudes con un origen común: ¿de quién son estos correos?, ¿quién ostenta la titularidad de los mismos?, ¿se pueden considerar privados?, ¿puede aplicarse a los *e-mail* la

protección de inviolabilidad existente para las llamadas telefónicas o la correspondencia postal? ¿está justificado que, con la excusa del ámbito laboral, el empresario, aún con las garantías que se construyan, pueda acceder al contenido sustantivo de un correo electrónico? ¿Puede un trabajador, amparado en el secreto de las comunicaciones y en el delito tipificado en el Código Penal mandar cuantos correos quiera, toda vez que le protege este derecho fundamental?

Por un lado se contempla el problema del tiempo que un empleado utiliza en elaborar y enviar correos particulares, así como también el que puede hacer perder a sus compañeros de trabajo; es decir, el factor tiempo como un costo real para el patrono. De otro lado, y derivado del primero, surge la duda de la legitimación de la empresa o institución para controlar, leer, etc., el correo de los empleados, que se supone privado.

No obstante, hay quienes opinan que parece erróneo el afán por ampararse en el derecho a la intimidad del trabajador para negarse a estos registros, ya que en las relaciones laborales con esta garantía no se pretende proteger *prima facie* el derecho a la intimidad, por lo que el uso profesional del correo electrónico ha de quedar fuera de toda actividad propia de la intimidad del trabajador (Abad, 2003).

Comparar el *e-mail* con las llamadas telefónicas personales realizadas en

el centro de labores, es un ejemplo que nos puede aportar perspectiva. El hecho de que cualquier empleado use el teléfono del trabajo para realizar alguna llamada personal, suele ser una práctica normalmente admitida por la parte patronal. Sin embargo, los problemas acontecen cuando algún empleado dedica gran parte de su tiempo a hablar por teléfono. Al patrono le preocupa tanto el costo de las llamadas, como el tiempo perdido en realizarlas. Por ello muchas empresas e instituciones advierten a sus empleados de que la información acerca de todas las llamadas que realizan queda registrada (número de abonado al que se llama, duración de la llamada, número de llamadas realizadas y/o recibidas, etc).

Así, si algún empleado hace un mal uso del correo, se le puede avisar, amonestar, sancionar o incluso ser despedido (si incurre en causas que justifiquen la procedencia del mismo), pero salvo casos excepcionalísimos ningún empleador cortaría el teléfono. De igual manera, tampoco se podría, sin autorización expresa e intervención de terceros, intervenir un teléfono para saber de qué hablan sus empleados, mientras que ambas soluciones sí han sido propuestas para acabar con los problemas que plantea el correo electrónico (Castañeda, 2000).

Es así como manejamos dos posiciones antagónicas, por una parte el secreto de las comunicaciones en cuanto a la utilización del correo electrónico de los empleados, pero también y estrechamente relacionado, el derecho del

empresario para que los trabajadores lo usen con la debida diligencia. La cuestión radica en determinar, si cuando el empresario procede a la apertura de los mensajes de la cuenta de correo electrónico enviados por un trabajador, no siendo destinatario de los mismos, incurre en una violación al secreto de las comunicaciones; y si se pudiera conocer el contenido de estos mensajes, donde se encuentra el límite a ese control. Nosotros somos partidarios de proteger el secreto de las comunicaciones suscitadas vía correo electrónico, aunque no con un carácter absoluto, ya que como se expone más adelante, consideramos que el patrono podría enterarse de aspectos no trascendentales de la comunicación, para resguardar sus intereses.

En España, en el momento en que se empezaron a ventilar casos sobre esta materia en los estrados judiciales, podríamos decir que los pronunciamientos favorecían, de una u otra forma, los intereses del empresario. En este sentido, se equiparaba el *e-mail* a la "*taquilla*" del trabajador y consecuentemente, era posible su registro para comprobar la probable mal utilización del mismo, siempre que se hiciera con determinadas protecciones y garantías. Sin embargo, a raíz de una sentencia del Tribunal Supremo francés, junto con un primer pronunciamiento y acercamiento de su homólogo español, se empezó a cambiar la línea jurisprudencial y tutelar en mayor medida el secreto de las comunicaciones hasta lograr el reconocimiento que hoy goza. Es evidente la necesidad de buscar un punto intermedio, pero encontrarlo muchas veces, es casi utópico, especialmente por la cantidad de situaciones diversas y

derechos afectados, todos de suprema importancia, que es preciso proteger.

Cuando hablamos del "*secreto del correo electrónico en la empresa*" no nos referimos a una actividad única. Algo tan sencillo como mandar un *e-mail* tiene una complejidad interna que es merecedora de explicación, para luego introducirnos en las posibles responsabilidades jurídicas. No es lo mismo mandar un correo electrónico con un dominio propio de la empresa en la que el trabajador presta sus servicios, que hacerlo desde uno de los tantos servicios gratuitos de correo que pululan en la red de redes.

En el primer supuesto, el empleado está comprometiendo el nombre y prestigio de la entidad que defiende, mientras que en el segundo solo se compromete él mismo. En general, si el trabajador tiene una dirección de correo electrónico cuyo nombre de dominio se parezca, o sea idéntica a la de la empresa o entidad a la que presta sus servicios y ha hecho un mal uso de el, tiene un ámbito de gravedad más amplio que aquel que ha usado un correo gratuito (tipo *hotmail*). En primer término, en el supuesto inicial el trabajador está usando más infraestructura empresarial que en el segundo: la contratación de un dominio de Internet es algo que no es gratuito, por el contrario en el segundo caso si lo es. En segundo lugar, el nombre de la empresa aparece en el primer caso, no así en el segundo. La consecuencia es clara: el trabajador puede incluso contratar productos con cargo a la empresa con fines ilegítimos o al menos no apropiados, lo que constituye otro elemento más a ponderar para

determinar la trascendencia de los hechos (Villahermosa, 2002).

De la misma forma, cuando nos referimos a la acción de "*espiar*" el contenido del *e-mail* de un trabajador, no puede ser lo mismo adentrarnos en datos poco reveladores de la intimidad personal, como puede ser el destinatario del mensaje, o el "*subject*", donde solo se suelen dar datos generales, que en el cuerpo del mensaje. Para comprobar si un correo es idóneo dentro del objeto social del patrono, bastaría, en la mayoría de las ocasiones, con mirar el destinatario o el asunto del correo. Obviamente, la entrada en el cuerpo del mensaje es alcanzar un límite que no se debería sobrepasar, toda vez que lo contrario, podría suponer una vulneración de los Derechos antes explicados, sobre todo si no se hacen con las garantías suficientes. Asimismo, no es igual mandar un *e-mail* personal al día que hacerlo con una alta frecuencia.

En este orden de ideas, es claro que el costo para la organización es realmente mínimo: el empresario no pierde dinero -en términos de uso de la infraestructura empresarial- por el envío de uno o de cuatrocientos correos. Desde la instauración de la tarifa plana -e incluso sin que estuviera ésta-, y más teniendo en cuenta las sucesivas conexiones de banda ancha que priman en las actuales estructuras empresariales, mandar un correo tiene un "*costo cero*" para el patrono. Obviamente, hablar en términos de falta de productividad del trabajador es hablar de la falta de horas que ha dejado de dedicárselas a la entidad, y esto si tiene relación directa con el número de correos electrónicos, o

la longitud de los mismos.

La complejidad del asunto nos llevará a intentar resolver el problema desde la perspectiva de la ponderación de los derechos que están en juego.

Junto a esto, tal y como veremos *infra*, el estado de la técnica hace que hoy en día, programas de cifrado sean totalmente accesibles para las personas. Utilizando complejos algoritmos de encriptación, prácticamente cualquier persona, haciendo un par de "*clicks*", puede tornar, literalmente, inaccesible cualquier contenido del *e-mail* que quiera cifrar. Cabe preguntarse si el trabajador tiene derecho a usar este software o no. Actualmente, ni en España ni en Costa Rica hay jurisprudencia que contemple este extremo (Villahermosa, 2002).

4.3.2.- FUNDAMENTO CONSTITUCIONAL Y LEGAL

El derecho al secreto de las comunicaciones hace referencia a cualquier clase de comunicación privada. El propio Tribunal Constitucional Español, ha establecido que el precepto constitucional garantiza la inviolabilidad de las comunicaciones de manera vinculante, sin distinguir el cause tecnológico de las mismas (Novatica, 2001). El citado órgano jurisdiccional ha relativizado el concepto de comunicación al establecer que, sea cual sea el ámbito objetivo de

dicho concepto, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceras personas ajenas a la comunicación misma. En tal sentido, la garantía del derecho fundamental no depende en forma alguna de la propiedad del medio a través del cual se produce la comunicación, sino que es absolutamente independiente de la titularidad del soporte. El secreto ampara el mensaje, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado (Novatica, 2001).

El precepto consagrado en el numeral 24 de nuestra Carta Magna de “*se garantiza el secreto de las comunicaciones*”, amén de lo expuesto y en atención al aforismo jurídico de que no deben hacerse distinciones donde la ley no las hace, incluye cualquier acto comunicativo privado, con independencia del medio empleado. De esta manera, la protección que lleva a cabo el texto constitucional ampara la protección de las comunicaciones a través del correo electrónico. La Constitución, al reconocer y proteger el secreto de las comunicaciones está consagrando implícitamente la libertad de las mismas; libertad que se erige así como el bien constitucional protegido.

En esta tesitura y refiriéndose específicamente al *e-mail*, en España se ha señalado que, a la luz de la interpretación del artículo 18.3 de la Constitución, de los fallos de los Tribunales Ordinarios y del estudio de la legislación, resulta evidente que el correo electrónico es un medio de comunicación amparado por

el derecho fundamental al secreto en las comunicaciones por tratarse de un “*canal cerrado*”, que genera claras expectativas de secreto, ya que para acceder al mensaje, se precisan una serie de acciones conscientes dirigidas a su apertura -por el destinatario- o interceptación -por terceros- (Novatica, 2001).

Se ha dicho a este respecto, que el derecho puede conculcarse tanto por la interceptación en sentido estricto, (que suponga aprehensión física del soporte del mensaje –con conocimiento o no del mismo- o captación de otra forma del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo). Además, están quienes afirman que no solo cubre el contenido de la comunicación, sino también en su caso, otros aspectos de la misma, como la identidad subjetiva de los interlocutores o de los corresponsales (Jaén, 2002).

4.3.3.- EXCEPCIONES

Pese a la importancia que revisten las comunicaciones, dentro de las cuales encontramos el correo electrónico, su protección debe tener un límite, toda vez que no puede haber derechos absolutos. Las normas jurídicas, son precisamente las que establecen los casos en los que, a efecto de tutelar un bien jurídico de mayor valor o trascendencia, es posible levantar esa barrera constitucional.

La única intervención legítima de las comunicaciones, ha de ser la autorizada por resolución judicial de autoridad competente; pronunciamiento que, en todo caso, ha de ser específica, fundamentada, razonada y que, en cuanto supone una injerencia sustancial en el ámbito personal, ha de otorgarse conforme al principio de legalidad y al principio de proporcionalidad (Villahermosa, 2002).

En tal sentido, en Costa Rica la ley número 8204, Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, resulta ser la normativa que contempla los supuestos en que dichas intervenciones son procedentes, veamos:

Artículo 9.- Autorización de las intervenciones. Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas o digitales, cuando involucre el esclarecimiento de los siguientes delitos: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas...

Como puede extraerse de lo antes transcripto, la ley establece un listado de los delitos en cuya fase de investigación es factible, previa resolución debidamente motivada por una autoridad jurisdiccional penal, autorizar la intervención de cualquier clase de comunicación. Dicho listado resulta ser,

como se dijo, *numerus clausus*, es decir que única y exclusivamente en esas circunstancias y en los ilícitos que se enumeran, es posible ordenar la referida intervención, sin que sea posible ampliar la misma o realizar interpretaciones extensivas de la norma.

Resulta interesante hacer énfasis en la protección que nuestro legislador otorga al secreto de las comunicaciones. Nótese que aún y cuando se establecen circunstancias en las cuales es posible obviar este derecho, inmediatamente se fija un límite, cual es el indicar taxativamente los ilícitos en los que una eventual intervención resulta procedente, muestra inequívoca de la seguridad jurídica que nuestro ordenamiento brinda a los ciudadanos.

4.3.4.- DELITOS

En su definición más elemental, un delito es un hecho típico, antijurídico y culpable. La unión de estos tres elementos hace que una conducta determinada se considere un ilícito penal, ya que si sólo concurren uno o dos de ellos, el delito no se configura. Nuestro legislador ha considerado que ciertos comportamientos que atentan contra el derecho a la intimidad y el secreto de las comunicaciones que ampara a todos los habitantes de La República, deben ser elevados a la categoría de delitos, desarrollando de esta manera el precepto establecido en el artículo 24 de la Constitución Política. Es así como el Código

Penal costarricense establece en el Título Sexto los Delitos contra el Ámbito de la Intimidad, y dentro de éste a su vez, los que resguardan el secreto de las comunicaciones, tales como la violación de correspondencia, la violación de comunicaciones electrónicas, la sustracción, desvío o supresión de correspondencia, y el uso indebido de correspondencia, principalmente. De seguido, mostraremos un pequeño resumen de los delitos mencionados, buscando dejar de manifiesto sus principales elementos.

i) Violación de Correspondencia

Este ilícito se encuentra tipificado en el artículo 196 del Código Penal, y reza así:

Artículo 196: Será reprimido, con prisión de uno a tres años, quien abra o se imponga del contenido de una comunicación destinada a otra persona, cualquiera que sea el medio utilizado

El bien jurídico tutelado a través de este numeral, resulta ser la esfera de la intimidad. La doctrina sobre los valores de la personalidad, trata la inviolabilidad de la correspondencia como una derivación del derecho a la intimidad, en la que no se requiere que el contenido de la correspondencia constituya un secreto, ya que lo que se tutela es la posibilidad de que se incluyan secretos en ella. Así, el tipo penal es estructurado como de peligro abstracto, prueba de lo cual es que para la consumación del delito, no se necesita que el que abra la correspondencia se imponga de su contenido (Llobet

y Rivero, 1997).

ii) Violación de comunicaciones electrónicas

Se encuentra contenido en el artículo 196 bis, el bien jurídico que tutela es la esfera de la intimidad y literalmente expresa lo que a continuación se indica:

Artículo 196 bis: Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos de otros o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

Las novedades tecnológicas que han sido introducidas en los últimos años, han generado una serie de innovadoras técnicas que permiten quebrantar el derecho a la intimidad, de una manera distinta a la que estábamos acostumbrados. El desarrollo de la informática ciertamente ha creado un mayor peligro al secreto de las comunicaciones.

El derecho, como ciencia social que es, responde a los fenómenos que se van dando en una colectividad, por lo que continuamente debe estarse actualizando a las necesidades de un mundo cambiante. Este artículo es un fiel

reflejo de la situación descrita: fue adicionado mediante la ley número 8148 de 24 de octubre de 2001, buscando adecuar nuestra legislación penal al discurrir tecnológico. Resulta ser, en nuestro criterio, una norma similar a su antecesora, pero que contempla específicamente la represión a las nuevas maneras de violentar la intimidad de los ciudadanos por medios tecnológicos. Sobre este particular, es rescatable el esfuerzo realizado en pos de modernizar nuestra legislación. Así, en este numeral específicamente, es donde encuentran resguardo las comunicaciones por medio del correo electrónico.

iii) Sustracción, desvío o supresión de correspondencia

Esta disposición legal la encontramos contenida en el numeral 197, en los términos que de seguido se exponen:

Artículo 197: Será reprimido, con prisión de uno a tres años, quien se apodere de una carta o de otro documento privado, aunque no esté cerrado, o al que suprima o desvíe de su destino una correspondencia que no le esté dirigida

Al igual que en los anteriores artículos, el bien jurídico tutelado es la esfera de la intimidad. El concepto de apoderamiento que se usa en este delito tiene un sentido amplio. Según Creus, citado por Llobet et al. (1997), apoderarse equivale a:

introducir o hacer permanecer el objeto en la propia tenencia; quedan comprendidos, por tanto, el acto de apoderamiento propio de las figuras de hurto y robo, en el que el agente desapodera al

legítimo tenedor para constituir su propia tenencia sobre la cosa, como el acto de quien se hace entregar el objeto por medios ardidosos o engañosos, o de quien teniendo legítimamente el objeto con una finalidad determinada, se queda con él, o de quien habiéndolo recibido erróneamente lo guarda para sí...(p.351).

El objeto material de este ilícito resulta ser más amplio que el de violación de correspondencia, ya que no establece supuestos taxativamente, sino que lo extiende a cualquier documento que tenga carácter privado.

iv) Uso indebido de correspondencia

El uso indebido de correspondencia, encuentra su lugar en el artículo 210 del Código sustantivo:

Artículo 201: "Será reprimido con prisión de seis meses a un año, el que usare indebidamente en cualquier forma, cartas, papeles, grabaciones, despachos telegráficos, telefónicos, cablegráficos o de otra naturaleza que hubieren sido sustraídos o reproducidos.

En primera instancia, debemos apuntar que usar implica hacer servir una cosa para algo. El artículo protege no sólo la correspondencia, puesto que se enumeran los papeles y las grabaciones, mismos que podrían no reunir el carácter de correspondencia. Lo que importa es que el documento o grabación haya sido sustraído o reproducido. Así, ha sido sustraído el documento o grabación del que se ha apoderado ilegítimamente un sujeto, quien puede ser el que usa indebidamente el documento, o un tercero que con conocimiento de que

se trata de un documento sustraído lo usa. Ha sido reproducido el documento o grabación, con respecto al cual se ha sacado sin autorización una copia (Llobet et al., 1997).

4.3.5.- JURISPRUDENCIA

En este apartado, nos disponemos a apreciar una importante cantidad de resoluciones extranjeras que dirimen conflictos atinentes al secreto del correo electrónico; así como también el reciente y único fallo de los órganos jurisdiccionales costarricenses que logramos ubicar sobre el particular, mismo que analizaremos en detalle. En esta tesitura, encontraremos pronunciamientos que apoyan la existencia del secreto, así como también fallos que niegan la aplicabilidad del mismo en los centros de trabajo.

i) Caso Deutsche Bank

El hecho de utilizar el correo electrónico de la empresa, para fines que no sean exclusivamente profesionales, puede tener consecuencias negativas para los trabajadores.

En el caso de un empleado de la institución bancaria Deutsche Bank, la Sala de lo Social del Tribunal Superior de Justicia de Catalunya (TSJC),

revocando a su vez una Sentencia anterior de un Juzgado de lo Social de Barcelona, el 14 de noviembre del 2000 falló que es procedente el despido de un trabajador que en el transcurso de cinco semanas envió 140 correos electrónicos ajenos a la actividad profesional de su empresa, por transgresión de la buena fe contractual. Valga mencionar que el contenido de dichos mensajes era de carácter sexista, humorístico y, en algunos casos, obsceno (Gimeno, 2000).

Dicha sentencia, refleja la interrogante que se planteó con anterioridad en este estudio, sea el ponderar los intereses de las partes de la relación laboral, es decir, sobre si debe pesar más el derecho a la intimidad de los empleados o la necesidad de las empresas o instituciones de ejercer un control sobre el correo electrónico de éstos.

Dentro de los hechos probados de la resolución *supracitada*, se estableció que el trabajador utilizaba el correo electrónico para fines personales en horario laboral, aún cuando la compañía había establecido directrices claras contrarias a esa práctica. Según la sentencia del Tribunal, *"...concurre así un acreditado incumplimiento laboral del trabajador sancionado..."*, ya que su actitud *"...supone la pérdida de tiempo de trabajo efectivo, tanto del trabajador al confeccionar y enviar los mensajes como de sus compañeros al recibirlos y leerlos..."* (Gimeno, 2000). Inclusive, algunos de los empleados que participaron de la conducta del demandante –el trabajador despedido- fueron amonestados o

sancionados.

Es así como en este caso, el órgano jurisdiccional admite y justifica la necesidad de llevar a cabo una revisión del correo electrónico por parte de la empresa respecto a los empleados *"...a efectos de precisar la incuestionable naturaleza de los mensajes judicialmente apreciados"* (Gimeno, 2000). Se ha de decir que en este caso -en el cual no se invocó una eventual violación del derecho a la intimidad ni del derecho fundamental al secreto de las comunicaciones del trabajador-, los magistrados se limitaron a constatar que la conducta del empleado, consistente en utilizar el correo electrónico en gran número de ocasiones para fines ajenos a sus labores, supone una infracción del deber de lealtad profesional que justifica la decisión empresarial de extinguir el contrato de trabajo. La resolución comentada no entra a valorar, por tanto, la lesión que al derecho a la intimidad o al secreto de las comunicaciones puede haber supuesto el conocimiento por la empresa del contenido de los mensajes enviados.

En el mismo sentido, algunos juristas expertos estimaron que el despido del Deutsche Bank era procedente, y que a las compañías les asiste ese derecho a examinar el correo de los empleados, máxime en el caso de que hubiera una prohibición expresa de hacer un uso particular del mismo (Castañeda, 2000).

Sin embargo, no todos están de acuerdo. La intromisión de las empresas en la correspondencia electrónica de sus empleados, indudablemente ha generado un fuerte debate social. A raíz del fallo recaído en esta sumaria del Deutsche Bank, la denominada Asociación de Internautas, a finales del mes de noviembre del año dos mil, comunicó que la *“Primera Campaña por la Intimidad de las Comunicaciones Electrónicas en el Trabajo”*, rindió sus primeros resultados, toda vez que más de dos mil personas han instalado en sus sistemas de correo electrónico herramientas de cifrado; mientras otras seis mil mostraban su repulsión hacia el Deutsche Bank por violar comunicaciones privadas. Es así como dicha Asociación ha contabilizado un total de seis mil descargas del Programa Ignorer para protestar por el despido del empleado del Deutsche Bank, después de que esta entidad controlara sus comunicaciones (Redacción Asociación de Internautas, 2000).

En el mismo sentido, dentro de los objetivos de la referida Campaña, se encontraban la especificación de medidas que protegieran de manera efectiva el derecho a la intimidad e inviolabilidad de las comunicaciones en los correos electrónicos, así como también pautas de seguridad tendientes a impedir la lectura de los mensajes. La Asociación de Internautas, que se proponía además informar acerca del uso y aplicación de herramientas que permiten el cifrado de las comunicaciones, ha atendido alrededor de dos mil internautas interesados en esquivar el *“espionaje”* de sus correos.

Podemos notar aquí, las posiciones antagónicas surgidas a raíz de este conflicto, elemento constante en el resto de los casos.

Así, se considera que el procedimiento de control iniciado por el empresario, podría resultar legítimo cuando existiesen indicios razonables para ello; que se procediese al conocimiento del número de mensajes y los horarios de la jornada de trabajo durante los que se han enviado para determinar si la actuación del trabajador reviste la gravedad suficiente para constituir un incumplimiento contractual, pero, por la presencia de los derechos de privacidad del trabajador, sin inmiscuirse en su contenido, salvo permiso expreso del propio trabajador (Camas, 2003); posición con la que nos encontramos de acuerdo dado que protege el patrimonio de la parte empresarial, sin violentar los derechos constitucionales de los empleados.

ii) Caso Nikon France

La Nikon France, es una empresa que en el año 1995 despidió a uno de sus trabajadores, alegando falta grave por usar gran parte de su tiempo laboral para asuntos personales.

En la sentencia que resolvió el asunto, el Tribunal Supremo francés calificó la apertura del correo electrónico de los trabajadores por parte de los empleadores de violación de privacidad, al dictaminar que "*...un empresario no*

puede tener conocimiento de los mensajes personales enviados por un trabajador y recibidos por éste a través de un útil informático puesto a su disposición para su trabajo..." sin violar el secreto de correspondencia. Este fallo reviste singular importancia toda vez que equipara el correo electrónico a otros tipos de correspondencia, y su lectura o apertura se considera una violación aunque el patrón *"haya prohibido la utilización no profesional del ordenador"*, y va más lejos al contemplar que *"el trabajador tiene derecho, incluso en su tiempo y lugar de trabajo, al respeto a su intimidad y su vida privada"* (Redacción de Baquía, 2001).

Asimismo, la resolución supera el criterio que regía en los primeros pronunciamientos de los órganos jurisdiccionales sobre este tema en el viejo continente, al considerar que el trabajador, aún en su puesto de labores, se ve asistido por el derecho a la intimidad, como un ámbito propio y reservado necesario para su desarrollo personal y profesional.

iii) Caso Netcom

Netcom es una compañía que, ante la gran avalancha de correo basura y publicidad no deseada (*spam*) que recibían en la empresa, *de motu proprio* instaló un sistema de filtrado informático automatizado. Dicho programa escaneaba el correo de todos los empleados y eliminaba los mensajes cuyas palabras clave habían sido prefijadas.

No obstante, las protestas de los empleados surgieron prácticamente de inmediato. Un programa de este tipo –se asevera- no debería haberse instalado sin el consentimiento de los funcionarios, pero sobre todo sin previo aviso de su instalación, ya que era muy sencillo programarlo para que, además de controlar el correo basura, pudieran detectar qué empleados enviaban mensajes de contenido privado o no adecuado según los criterios de la empresa, conocer a los que usaban el correo sobre todo para fines no profesionales y tomar medidas contra ellos (Castañeda, 2000).

En este caso, se analiza la necesidad de que el patrono comunique previamente a sus empleados, la instalación de programas informáticos que actúan sobre los correos electrónicos de todo el personal. Independientemente de la legalidad o no de este tipo de elementos computacionales, el funcionario debe tener la posibilidad de, al menos conocer, que puede ser objeto de vigilancia al utilizar el *e-mail* proporcionado por la empresa para el desarrollo de sus actividades, en atención al debido proceso y a la seguridad jurídica que lo resguarda.

iv) Caso Lanata

El fallo recaído en esta sumaria tramitada en la República Argentina, ayudó a definir al debate sobre la privacidad del *e-mail*, al establecer que:

... el correo-e posee características de protección de la privacidad

más acentuadas que la vía postal a la que estamos acostumbrados, ya que para su funcionamiento se requiere un proveedor de acceso al servicio, el nombre del usuario y una clave de acceso. Sentadas estas bases, nada se opone -continúa la sentencia- para definir el medio de comunicación electrónico, como un verdadero correo en versión actualizada. En tal sentido, la correspondencia y todo lo que por su conducto pueda ser transmitido o recibido, goza de la misma protección, al menos, que la del correo convencional... (Castañeda, 2000).

Esta sentencia, constituye también un paso trascendental en el resguardo del carácter secreto que ostentan las comunicaciones dirigidas vía correo electrónico, toda vez que se les equipara al correo tradicional, mostrando un acertado acoplamiento de los juzgadores a los tiempos modernos. Inclusive, nótese que deja entrever la posibilidad de que, en atención a sus características, la comunicación dirigida por *e-mail* tenga una mayor privacidad.

v) Posición en Reino Unido, Alemania y Francia

El gobierno británico en octubre del año dos mil, autorizó a las empresas a tener “*acceso rutinario*” a los *e-mail* y llamadas telefónicas de sus empleados, siempre que fuera para comprobar si eran o no relativas a cuestiones de trabajo (Castañeda, 2000).

En contraposición a la ley inglesa, el gobierno alemán está estudiando una legislación que prohibiría a las compañías leer el correo electrónico privado enviado desde el lugar de trabajo. Alemania tiene una legislación rígida y muy respetuosa con la privacidad y los sindicatos han instado al gobierno a actualizar

la protección en la era de Internet. Esta situación se conocía, varias semanas después de que el gobierno británico quitara las trabas que obligaban a las compañías a obtener el consentimiento de los empleados antes de hacer un seguimiento de sus comunicaciones (Castañeda, 2000).

Francia parece seguir un concepto similar al alemán. En Sentencia del Tribunal Correccional de París, se condenó a tres altos cargos de la Escuela Superior de Física y Química Industrial de la capital francesa por violación del secreto de correspondencia electrónica al interceptar mensajes de un estudiante. Según dicha resolución, el correo electrónico *"es como uno convencional, una correspondencia privada protegida por el derecho al secreto de las comunicaciones postales"* (Castañeda, 2003). Similar criterio había sido externado por el Tribunal Supremo francés en el caso de la Nikon France, según observamos líneas atrás.

Así, la posición del Tribunal Correccional de París, resulta prácticamente idéntica a la esgrimida por la jurisprudencia Argentina, según logramos verificar *supra*, toda vez que equipara el correo electrónico con el convencional, sin realizar distinciones de ningún tipo y mostrando también, su adaptación a las realidades de la sociedad y del mundo jurídico.

vi) Posición Española

El uso del correo electrónico en las empresas y las decisiones judiciales que se suscitan a consecuencia de ello, son en España hasta el momento dispares; toda vez que existen dos bloques: el modelo anglosajón -con EE.UU. a la cabeza- en el que en el capítulo de las comunicaciones se limitan los derechos constitucionales al momento de la transmisión; y, por el contrario, el sistema continental, que abarca más allá y encuadra el soporte físico de transmisión (Castañeda, 2003).

Así las cosas, las decisiones judiciales en España referidas a la capacidad empresarial para acceder a los correos electrónicos toman dos rumbos. Un primer sector, se inclina por considerar que, ya que el material informático es propiedad del empleador, el derecho fundamental al secreto de las comunicaciones -artículo 18.3 de la Constitución Española- no ampara las comunicaciones "*inter-privatus*", puesto que la compañía tiene por ley -artículo 20.3 del Estatuto de los Trabajadores (ET)- asignadas las competencias de vigilancia sobre la actividad laboral de sus empleados y el uso de medios empresariales. A modo de ejemplo, los Tribunales Superiores de Justicia de Cataluña (5-7-2000), del País Vasco (31-10-2000), Galicia (4-10-2001) y Madrid (4-12-2001), e inclusive el ya reseñado caso del Deutsche Bank.

La parte empresarial justifica su actuación al amparo del artículo 18 y/o

del artículo 20 LET, aduciendo proteger el patrimonio empresarial o la productividad de los empleados. En general además, la doctrina de la buena fe es utilizada, tanto en el orden interno como en el ámbito internacional, para delimitar el deber de respetar la privacidad de los trabajadores (Camas, 2003).

No obstante, la implantación de las tecnologías de la información y la comunicación; específicamente la introducción de Internet en el centro de trabajo con relación al respeto a la vida privada y la intimidad, tiene un alcance totalmente diferente al que pueda suponer la vigilancia del empresario llevada a cabo por escuchas telefónicas, video-vigilancia, grabadoras, detectives privados, o registro físico de las taquillas del trabajador; con las nuevas tecnologías la vigilancia se produce no a través de elementos ajenos al propio instrumento de trabajo del empleado (a no ser por ejemplo que el trabajador sea un teleoperador), sino que dicha vigilancia se lleva a cabo utilizando las propias herramientas de trabajo de aquél.

En el otro lado de la balanza está la doctrina, que las mismas fuentes judiciales apuntan como mayoritaria, en la que el secreto de las comunicaciones está por encima de todo y la auditoria o examen de los correos personales del trabajador vulnera los preceptos constitucionales (Asociación de Internautas, 2003), posición que en los últimos tiempos se ha venido imponiendo, tal y como lo ejemplifican las sentencias que de seguido exponemos:

a) Según la STC 114/1984 de 29 de noviembre, el derecho fundamental al secreto de las comunicaciones *“consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas”*, y añade que *“la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados, el derecho posee eficacia “erga omnes”) ajenos a la comunicación misma”* (Camas, 2003). Así, la presencia de un elemento ajeno a aquellos entre los que media el proceso de comunicación, es indispensable para que se configure el ilícito. Queda entendido, según se expuso con anterioridad, que una de las consecuencias que conlleva la violación del secreto a las comunicaciones viene regulada desde el punto de vista penal.

b) La sentencia de la Audiencia Provincial de Barcelona de 31 de julio de 1998, establece que *“la titularidad del aparato telefónico no autoriza la intromisión en las conversaciones que con él se realicen, pues lo protegido es el secreto de las comunicaciones, no solamente las del titular de aparato”* (Novatica, 2001). La tesis de que la propiedad de las líneas por parte de la compañía permite interceptar la comunicación que se realiza a través de ellas, no es acogida por los Tribunales. En otras palabras, los juzgadores no aceptan que el empresario sea un tercero calificado que, al poseer los mecanismos por medio de los cuales se realizan las comunicaciones, pueda acceder a éstas sin vulnerar su secreto.

c) En la STSJ de Cataluña (Sala de lo Social) de 5 de julio del 2000 (A.S. 3452), dos trabajadores habían mantenido de forma reiterada –durante aproximadamente un mes y medio- conversaciones entre sí por correo electrónico cuyo contenido era obsceno y despreciativo en relación a dos compañeras, pese a que en la empresa se había anunciado a los empleados, que no estaba autorizado el uso de los medios informáticos para asuntos ajenos a la empresa. En determinada ocasión una de la indicadas funcionarias, al utilizar el ordenador de uno de los trabajadores en cuestión para enviar el correo solicitado por un cliente, leyó un *e-mail* en el que la trabajadora creyó que se hacía referencia a ella y a su esposo con términos vejatorios. Denunciados los hechos, la empresa encargó una auditoria interna sobre el uso del correo electrónico por parte de los trabajadores acusados (previo consentimiento de éstos), misma que confirmó las actuaciones denunciadas y que fue a la postre la razón por la cual se despidió a los trabajadores debido al quebrantamiento de los deberes de fidelidad y lealtad implícitos en toda relación laboral, al haber incumplido las normas de la empresa sobre el uso del correo electrónico así como el código de ética. Los empleados cesados, al admitir con su consentimiento la auditoría de sus correos legitimaban la actuación empresarial, aunque cabe considerar si el acto de la trabajadora al abrir el correo del compañero de trabajo y leerlo para comunicar posteriormente a la empresa lo que había encontrado, se considera una prueba obtenida en lesión del derecho fundamental al secreto de las comunicaciones, lo que por tanto, no hubiera podido surtir ningún efecto (Camas, 2003).

d) La Sentencia del Tribunal de Primera Instancia de las Comunidades Europeas (Sala Tercera) de 18 de octubre de 2001, X contra Banco Central Europeo, que resuelve el caso en que el BCE despide a un trabajador, basándose en el artículo 4.1a) de sus Estatutos (*“Los empleados del BCE han de cumplir sus obligaciones en conciencia y sin tener en cuenta sus intereses personales. Deberán guardar una actitud conforme con sus funciones y con la condición de institución comunitaria del BCE”*), así como al amparo de una circular interna sobre la utilización por el personal de Internet y del correo electrónico, en la que se establece que *“el BCE pone a disposición de sus empleados accesos a Internet en interés del servicio”* (3.1). La imputación realizada al trabajador consistía en el acoso a que había sometido a otro funcionario de la empresa, utilizando para ello el correo electrónico, y la obtención a través de Internet, de documentos de carácter pornográfico y político y su envío posterior a terceras personas por *e-mail*. Ante el argumento del demandante de que la Circular del BCE carece de efectos, el TPICE manifiesta que la regla del artículo 3.1 de la Circular interna es una expresión del principio de que el material de trabajo que el empleador entrega al trabajador debe utilizarse, en general y sin perjuicio de excepciones específicas, para la ejecución de las tareas profesionales del asalariado (ap. 121). Pues bien, añade el TPICE, que este principio *“sólo constituye, por su parte, una aplicación de aquél, plasmado en el artículo 4, letra a), de las condiciones de contratación, según el cual los empleados deben cumplir sus obligaciones de manera concienzuda y desinteresada, que constituye, a su vez, la mera expresión del principio de que los contratos de*

trabajo deben cumplirse de buena fe". En conclusión, para el TPICE, independientemente de la legalidad del artículo 3.1, existe la obligación del empleado del BCE de utilizar los instrumentos de trabajo de los que dispone, en principio, sólo con fines profesionales (Camas, 2003).

e) En la STSJ de la Comunidad Valenciana 9.11.2000, se señaló que era fácil concluir que el bien jurídico protegido en el artículo 18.3 de la Constitución y en definitiva el derecho fundamental del actor a la libertad de comunicación y su secreto, resultó infringido en el doble aspecto reseñado por la doctrina constitucional de referencia -la comunicación fue interceptada y se conoció antijurídicamente su contenido por terceros ajenos a la comunicación misma- (Rubio de Medina, 2003).

En tal sentido, de los anteriores criterios jurisprudenciales puede deducirse que, ante el conflicto entre los derechos fundamentales de los trabajadores y los poderes del empresario, el Tribunal Constitucional fija una regla de preferencia condicionada a favor de los primeros, que se imponen a los segundos siempre que se ejerciten de buena fe, y en el tanto, del propio objeto del contrato no se derive necesariamente la restricción del derecho fundamental. No obstante lo anterior, es preciso aclarar que cada caso reviste una serie de particularidades que lo distinguen de los demás, por lo que resulta imperativo que cada uno se analice de manera separada, teniendo como punto de referencia el secreto de las comunicaciones establecido en la Constitución;

derecho que, como ya hemos manifestado, garantiza la impenetrabilidad de las comunicaciones por terceras personas, y ello con independencia de quien sea el titular del medio utilizado para efectuar la comunicación.

De esta manera, se pone de manifiesto la existencia de un conflicto entre las facultades empresariales y los derechos a la intimidad, vida privada y comunicaciones de los trabajadores en una esfera especial: las tecnologías de la información hacen fluidas las fronteras entre la vida privada y la vida profesional. De hecho, como se ha postulado desde determinados foros europeos, ante la capacidad de comunicación y de relación que ofrecen el correo electrónico e internet, y que acaban configurando un espacio de la vida privada del trabajador en el seno de la empresa, se vienen haciendo propuestas en el sentido de que se clarifiquen las lógicas de los trabajadores y los empleadores: los primeros tomando conciencia, como mayormente así ocurre, que sus instrumentos forman parte del lugar de trabajo y han de ser utilizados en aras al cumplimiento de su prestación laboral, y por parte de los empleadores, que Internet (como lo que ocurre con el teléfono) puede ser usado para fines personales, excepto de forma abusiva; en este sentido, ya se han lanzado algunas propuestas en las que se promueve una interpretación que consiste en una presunción de utilización profesional de Internet pero también posibilidad de utilización razonable y delimitada, siendo esta utilización la que podrá fundar el control empresarial (Camas, 2003).

vii) Costa Rica: Caso Baxter Productos Médicos Limitada

Como lo explicamos con anterioridad, este caso resulta ser el único que ha examinado –según los resultados de nuestra búsqueda- aspectos relacionados al correo electrónico en Costa Rica, por lo que sin lugar a dudas reviste singular importancia, tal y como lo veremos a continuación.

Se trata de un proceso ordinario laboral que se estableció ante el Juzgado de Trabajo de Cartago, por parte de Paola Melissa Baboza Quirós contra Baxter Productos Médicos Limitada –empresa que la había despedido-, a efecto de que en sentencia se condenara a dicha compañía a pagarle extremos laborales.

A este respecto, la demandada alegó que la señora Barboza Quirós fue despedida por cometer falta grave a sus obligaciones contractuales, sobre todo a la ética y probidad con que debía cumplir y conducirse en su trabajo.

La empresa había facilitado a la trabajadora un computador con acceso a internet y correo electrónico, entre otras facilidades, para que efectuara sus labores. En este sentido, para trabajar en la máquina y por ende para usar el correo electrónico -el cual tenía como parte de la dirección el nombre de la empresa (paolabarboza@baxter.com) necesariamente debía utilizar su password personal.

Baxter Productos Médicos Limitada se percató de que la empleada había enviado por medio del correo electrónico de la compañía, una serie de chistes de contenido morboso e inmoral a un amigo ajeno a la empresa, contraviniendo las directrices y advertencias que sobre el particular regían en la institución, lo cual en criterio de la misma, constituyó un uso distinto e indebido del correo electrónico de la compañía, abandono de trabajo y un daño a la imagen de la empresa puesto que su buen nombre se veía dañado, pero sobre todo un quebranto de la buena conducta desde el punto de vista ético y moral, dado el contenido de dichos correos, por lo que consideró violentado el inciso h) del artículo 81 de Código de Trabajo, el cual en lo que interesa dice que es causa que faculta al patrono para dar por terminado el Contrato de Trabajo *“...cuando el trabajador se niegue en igual forma a acatar, en perjuicio del patrono, las normas que éste o sus representantes en la dirección de los trabajos le indique con claridad para obtener la mayor eficacia y rendimiento en las labores que se están ejecutando”* (Código de Trabajo, Ley No. 2 de 2 de agosto de 1943). Además estimó infringidos los numerales 18 y 19 del Código de rito, referidos a la buena fe que debe regir el contrato de trabajo.

Por su parte, la señora Barboza Quirós en su demanda señaló, fundamentalmente, que ella no envió dicho correo, que no sabía de qué manera lograron utilizar el mismo, pero que obviamente se trataba de una persona con bastante conocimiento en materia de informática.

En primera instancia, el Juzgado de Trabajo declaró sin lugar en todos sus extremos la acción. No obstante, al conocer en apelación el fallo, el Tribunal de Trabajo de Cartago revocó la sentencia apelada y declaró con lugar la demanda laboral interpuesta. En cuanto al uso distinto e indebido del correo electrónico, señaló:

La demandada, en la carta de despido, le indica que, al utilizar ese canal, en esa forma, le está dando a los recursos tecnológicos de la empresa, un uso distinto e indebido a los que están destinados. Lo anterior es una de las prohibiciones establecidas en el artículo 72 inciso d) del Código de Trabajo, que indica: d) "Usar los útiles y herramientas suministradas por el patrono, para objeto distinto de aquél a que están normalmente destinados;", sin embargo la sanción a esta falta la establece el artículo 81 inciso i) ibídem: i) Cuando el trabajador, después de que el patrono lo aperciba por una vez, incurra en las causales previstas por los incisos a), b),c),d) del artículo 72". No basta, entonces, que el trabajador cometa la falta del artículo 71 inciso d), sino que, para que sea procedente el despido sin responsabilidad patronal, previamente tiene que existir un apercibimiento, caso contrario no se puede aplicar el numeral 81. En el subjuicio, la parte demandada no ha demostrado que, haya apercibido a la actora, mínimo una vez, por la utilización del correo electrónico con fines netamente personales; un apercibimiento no es una circular, ya que aquél debe ser personalizado y preventivo, y no como en este caso, donde si bien es cierto, las autoridades administrativas de la empresa mandaban a sus empleados notas, correos o circulares, como quiera llamarse, sobre el uso que se le debía dar al correo electrónico de Baxter y qué no debía hacerse, ello no son apercibimientos (tipo sanción), para la actora en los términos que señala el numeral 81 inciso i) del Código de Trabajo. Por lo anterior no es posible jurídicamente apoyarse en esa falta para despedir sin responsabilidad patronal a la trabajadora. Ese fundamento jurídico debe descartarse, por no haberse cumplido con lo que dispone la ley para ese caso concreto. El subrayado es nuestro. (Tribunal de Trabajo de Cartago, Voto 120-03 de las 14:50 horas del 30 de mayo del 2003)

En relación al abandono de trabajo, por el envío del correo, consideró que:

Señaló la parte patronal, en la carta de despido, que la actora “hizo abandono del trabajo o de sus funciones”, para enviar el correo. Sobre esta causal nos dice el Dr. Carlos Carro, en su libro “Las justas causas del despido en el Código de Trabajo y jurisprudencia de Costa Rica”, pág. 53-55, que “El abandono de labores, típicamente, se produce cuando el trabajador se aleja del establecimiento donde presta sus labores; pero, también, el abandono puede darse en el lugar de trabajo y, en esas circunstancias, se produce cuando el trabajador deja de realizar las labores que le corresponden y con las que debe cumplir. En consecuencia el abandono de trabajo, se entiende como la dejación, durante la jornada de trabajo, de las labores objeto del contrato, sin que medie alguna causa, que lo justifique. Se traduce en una conducta maliciosa y culpable; pues conlleva siempre la clara intención de abandonar las tareas, que se están realizando; pudiendo consistir, también, en una pasividad negligente”. En el presente caso, es posible que la actora incurriera en esa falta, se desconoce si al momento en que envió el correo, estaba o no en algún receso programado o autorizado, pero de todos modos, el patrono no acreditó que cumpliera con lo que dispone y manda el inciso i) del artículo 81, sea el apercibimiento previo. No consta en autos, que dentro de los últimos tres meses de la relación laboral, a la actora se le hubiere apercibido por escrito, de ese tipo de abandono, que lo tipifica el artículo 72 inciso a) del Código de Trabajo. En este caso el demandado no puede ampararse en ese motivo para un despido sin responsabilidad patronal, en otras palabras ello no es causal de despido en esas condiciones... . El subrayado es nuestro. (Tribunal de Trabajo de Cartago, Voto 120-03 de las 14:50 horas del 30 de mayo del 2003)

Finalmente, respecto al daño o riesgo de daño a la imagen de la empresa por el envío del correo electrónico, el *A quem*, señaló:

Por último, alegó el patrono, con la falta de la actora, un daño a su imagen. Si analizamos al tipo de personas que dicho correo se envió, se concluye que ningún perjuicio o daño de la imagen de Baxter se produjo, ni siquiera un peligro para ello. El mismo se envió al señor Adrian Chaverri Coto, persona, que aunque es ajena

a la empresa, tenía un ligamen o relación sentimental con la actora, por lo que si recibió ese texto, él sabía quien lo enviaba y en qué carácter; las otras personas que, tuvieron acceso a el, fue un grupo de personeros de la misma empresa, círculo muy reducido, ya que el mismo testigo Eddie Vasquez Rivera, sobre este punto indicó: “En fecha 25 de marzo la actora hace envío del correo al destinatario achaverri, ese correo entra a la lista de correos, que se llama CR-Cartago. Sistem, del cual formo parte porque soy empleado del Departamento de Sistemas. También, forma parte mi jefe, quien es Miguel Jiménez, Gerente de Sistemas. Este mismo día a las 3:33 de la tarde, Miguel Jiménez, dirige el mensaje a la Gerente de Recursos Humanos, al Gerente de Calidad, Departamento al que pertenece Paola Barboza, y al Gerente General de la compañía, finalmente aparece el jefe del Departamento de Calidad, alertando a los supervisores...”. De lo anterior se concluye, que el conocimiento que todas esas jefaturas tuvieron de ese correo, enviado por Paola a Adrian Chaverri, fue porque el testigo Eddie Vasquez y su jefe Miguel Jiménez, formaban parte del Departamento de Sistemas, y al entrar el texto a la lista de correos, ellos pudieron accederlo, luego Miguel Jiménez lo envía a los jefes de la empresa indicados. Este Tribunal se pregunta: ¿Cómo se afectó la buena imagen de Baxter? . De estos hechos no se puede deducir lo anterior. Tampoco la demandada ha demostrado, que el envío de ese correo, le ocasionó un perjuicio económico, por la utilización de ese medio, además en la carta de despido no se hace mención a ello, ni siquiera al contestarse la demanda.... El subrayado es nuestro. (Tribunal de Trabajo de Cartago, Voto 120-03 de las 14:50 horas del 30 de mayo del 2003)

Tras lo cual concluyó, exponiendo que:

Por todo ello, este Tribunal considera, que aunque está demostrado que la actora cometió una falta, la misma no reviste la gravedad que el patrono le da, y el despido sin responsabilidad patronal es desproporcionado al hecho cometido. Si nos atenemos a la carta de despido, previamente tenía que haber apercibimientos escritos, los que no existen, y la falta no es de tal magnitud que pueda encuadrarse en el inciso l) del artículo 81 del Código de Trabajo, además al despedírsele no se le imputó eso ni en esa forma, en conclusión el despido fue incausado, porque no se siguieron los procedimientos que establece el artículo 81 inciso i) del Código de Trabajo, para sancionar la falta de la trabajadora...

El subrayado es nuestro. (Tribunal de Trabajo de Cartago, Voto 120-03 de las 14:50 horas del 30 de mayo del 2003)

Visto lo anterior, la empresa recurrió el fallo ante la Sala Segunda de la Corte Suprema de Justicia, la cual resolvió en definitiva el caso. En votación dividida (tres votos contra dos), la Sala confirmó el fallo de Segunda Instancia, en el sentido de que pese a la existencia de la falta, la misma no revestía la gravedad que la empresa le confirió, en razón de las circunstancias en que la misma ocurrió, por lo que el despido era improcedente y desproporcionado en relación al hecho cometido.

Los Magistrados hicieron notar además, que el despido está regido por un principio fundamental, cual es el de la causalidad, el que en su modalidad objetiva, implica la necesaria existencia de una relación de causa a efecto entre los hechos invocados como sustento del rompimiento de la relación y el acto jurídico de despido, y que precisamente en atención al referido principio, la parte patronal no puede en el proceso laboral sustituir o ampliar los hechos expuestos en la carta de despido, toda vez que deben protegerse los principios de debido proceso, igualdad y de la defensa del trabajador, puesto que la causal plasmada en la carta de despido será la base de discusión dentro del proceso judicial. Así las cosas, en este caso el único hecho invocado como sustento del cese fue el envío por la trabajadora de un correo electrónico, sin que sea dable, como intentó la demandada, ampliar las causas del despido dentro del proceso.

Finalmente la Sala, aceptando como se dijo, que otro de los reproches de la demandada consistió en que el correo era en sí mismo vulgar, ofensivo y contrario a los valores de la compañía; y, por eso mismo, gravemente perjudicial de la buena imagen de Baxter pues, aunque se enviara con intención personal, inmediatamente se ligaba a la empresa al contenido enviado; aún así, en cuanto a la magnitud y gravedad de estas últimas circunstancias, estimó que seguían siendo válidos y aplicables los razonamientos del *A quem*. Al respecto, manifestó que ha de tenerse en cuenta lo siguiente:

Sobre el contenido del correo se deben distinguir dos planos bien diferentes. Como verá, el envío del correo electrónico no es necesariamente vulgar, aunque sí lo son los chistes en él transcritos. Por lo demás, la actora no sirvió de otra cosa que no fuera de simple faja de transmisión de ese texto. Sin agregar comentario alguno. El cual, tras recibirlo de previo e internamente en su buzón, aparte de un amigo externo a la empresa, a nadie más lo envió, al menos personal e intencionalmente. Aún así, existe duda razonable que su amigo lo hubiera recibido o enterado de su contenido. Aparte, no existe certeza de que la actora intencionalmente lo propalara a lo interno de la empresa. Como se verá, antes de su envío, la actora lo había recibido, al parecer de parte de un empleado de la empresa; y, después de ella, fueron dos personas, con autoridad dentro de la compañía, quienes se encargaron de reproducirlo. Precisamente por medio del correo electrónico de "Baxter".

(...)

*Lo cual le resta gravedad a la falta, no solo por la escasa magnitud del hecho, habida cuenta el círculo reducido de personas que lo recibieron, a lo interno de la empresa, como razonó el Ad quem, sino además, por la imposibilidad de saber, con absoluta certeza, no solo si realmente fue recibido por un tercero, ajeno a la compañía, sino también que, en relación a su recibo en el Departamento de Sistemas de la empresa, existiera realmente el elemento moral, vale decir intencional, en el comportamiento de la actora. Al no ser de recibo los agravios invocados en esta tercera instancia, el fallo dictado por el Tribunal de Trabajo de Cartago debe confirmarse. **POR TANTO: Se confirma el fallo recurrido.** El subrayado es nuestro. (Sala Segunda de la Corte Suprema de*

Justicia, Resolución 2003-00797 de las 15:00 horas del 18 de diciembre del 2003)

Así las cosas, podemos concluir que en las tres instancias jurisdiccionales, se tuvo como hecho probado que la trabajadora Barboza Quirós, efectivamente había enviado a un amigo, por medio del correo electrónico de la empresa, una serie de chistes pasados de tono que reñían con la moral, la probidad y las buenas costumbres, contraviniendo abiertamente las disposiciones de la compañía que prohibían este tipo de conductas.

No obstante lo anterior, el punto medular del asunto, resulta ser que tanto el Tribunal de Trabajo como la propia Sala Segunda de la Corte, estimaron que si bien era cierto que a los recursos tecnológicos empresariales se les había dado un uso indebido, no lo era menos que para que fuera procedente el despido sin responsabilidad patronal, debía existir un apercibimiento previo, el cual no se dió en este caso. En tal sentido, aunque quedó demostrado que la actora cometió una falta, la misma no tenía la gravedad que la empresa le otorgó, por lo que el despido resultaba desproporcionado en relación al hecho cometido, posición con la que nos manifestamos de acuerdo y que según la doctrina y la jurisprudencia estudiada, podemos tener como mayoritaria.

Pese a que lo reseñado fue el voto de mayoría, estimamos conveniente, a efecto de mostrar una vez más las posiciones encontradas que suscita este tema y que fueron la base para el desarrollo de esta investigación, lo consignado

en el voto salvado de los Magistrados Villanueva y Van der Laet.

Dichos juzgadores, tuvieron como acreditado que la señora Barboza Quirós utilizó la cuenta de correo electrónico que le había facilitado su empleadora para enviar chistes pasados de tono tanto a personas de la propia empresa como ajenas a ella, lo que, en su criterio, constituye una falta grave al contrato de trabajo, ya que, por un lado, implica un abandono de labores; por otro, una utilización inadecuada de una herramienta de trabajo para fines personales; y, finalmente, una violación a las buenas costumbres que deben imperar en el ambiente laboral. Así las cosas, consideraron que no era necesario el apercibimiento previo que echaron de menos los otros integrantes del Tribunal, ya que, al darse las faltas mencionadas en forma simultánea, tienen la virtud de verse agravadas. Profundizando en estos extremos señalaron lo que de seguido se transcribe:

Lo anterior porque el correo electrónico implica un costo para el empleador, aumenta la posibilidad de los contagios mediante virus, implica pérdida de tiempo de trabajo tanto para el que envía como para el que recibe el mensaje, se corre el riesgo de que se sature el casillero de mensajes, etc. La utilización, no expresamente autorizada, de los medios informáticos y de comunicación de la empresa con fines estrictamente personales constituye un incumplimiento de los deberes laborales y una vulneración de la buena fe contractual, lo que es suficiente para que quien incurra en ella pueda ser sancionado incluso con el despido. Dicha utilización y su ocasional sanción nada tienen que ver ni con el derecho a la intimidad personal ni con el derecho a la protección de datos de carácter personal, ni consecuentemente con los espacios de privacidad que puedan existir en la empresa, ya que ésta es, por su propia naturaleza y por definición legal, "una unidad productiva con organización específica", es decir, los medios, instrumentos y

herramientas puestos por la dirección a disposición de los trabajadores lo son en orden a la producción de bienes y servicios y no para su uso particular y personal. Es verdad que en ocasiones el uso indebido de los citados medios obedece a situaciones de tolerancia y benevolencia de las empresas, que en cualquier caso deberían ser revisadas. En este sentido, el empleado no tiene una expectativa razonable de intimidad en la comunicación del correo electrónico, hecha voluntariamente sobre un sistema de correo provisto por la compañía. El patrono tiene la potestad, dentro de sus poderes de dirección, de fiscalizar el uso que sus empleados hagan de las herramientas de trabajo que se ponen a su disposición, dentro de las cuales se encuentra el correo electrónico. En este sentido, el derecho a la intimidad personal e inviolabilidad de las comunicaciones cede frente la potestad que tiene todo empresario a proteger sus medios organizativos patrimoniales y a dirigir y controlar la actividad laboral de sus trabajadores. El subrayado es nuestro. (Sala Segunda de la Corte Suprema de Justicia, Resolución 2003-00797 de las 15:00 horas del 18 de diciembre del 2003)

En la misma línea, en España mediante STSJ 5.2.2002 se estimó que la correspondencia enviada desde el trabajo por *e-mail*, no ostenta carácter privado al ser emitida con instrumentos que pertenecen a la empresa, por lo que no cabe la invocación al derecho a la intimidad del trabajador. De igual manera, la STSJ 25.2.2000 considera que el artículo 18 ET “*autoriza al registro en la terminal del ordenador que utiliza el trabajador, pues el ordenador a estos efectos puede asimilarse a la taquilla, ya que no podemos olvidar que dicho ordenador es un instrumento de trabajo propiedad de la empresa y que no debe ser utilizado para otros fines distintos y diferentes que la realización de la actividad laboral, por lo que no cabe hablar de documentos personales incorporados al mismo.*” (Rubio de Medina, 2003). Esta posición, como puede observarse, se basa en la propiedad de los instrumentos de trabajo.

Pese a que respetamos en un todo el pensamiento de los Magistrados Villanueva y Van der Laat, así como también los pronunciamientos españoles indicados, nosotros consideramos que, aún en su centro de labores, el trabajador tiene derecho al respeto de su intimidad y al secreto de las comunicaciones, dentro de las cuales se incluye obviamente el correo electrónico, y que si bien el patrono en el ejercicio de su poder de dirección y control está legitimado para fiscalizar el adecuado uso de esta herramienta, ello no lo faculta para imponerse del contenido de los mensajes que envían sus empleados. Contrario a lo externado por los distinguidos funcionarios judiciales, nosotros creemos que al suscitarse este choque de intereses entre la parte obrera y la patronal, debe protegerse al extremo más débil de la relación laboral, así como también y principalmente, que los preceptos constitucionales del derecho a la intimidad y al secreto a las comunicaciones, se encuentran por encima de los intereses de los patronos.

Valga mencionar además que, el fallo que hemos reseñado, no entra a analizar la manera en que Baxter Productos Médicos Limitada se entera del contenido del correo enviado. La empresa alega que al momento de remitirlo, la trabajadora por error accedió a alguna de las listas que era del Departamento de Sistemas y que, de esa manera, lograron descubrir la falta acusada. Los juzgadores asumen como cierto este punto, fundamentalmente porque en teoría, dado que la computadora tenía *password*, únicamente el funcionario respectivo tenía acceso a la misma. Sin embargo, la trabajadora obviamente lo niega, e

incluso se apoya en el testimonio de la persona a la cual supuestamente le remitió los chistes, quien a su vez indicó en la oportunidad procesal correspondiente, que él nunca recibió dicho mensaje electrónico.

Creemos que resulta interesante sembrar aquí la inquietud, pese a que la sentencia no entró a analizar este aspecto, puesto que en nuestro criterio eventualmente podríamos estar en presencia de prueba obtenida por medios ilícitos y por ende nula. Inclusive, podría plantearse la posibilidad de que alguna otra persona con acceso a la red, hubiera enviado el mensaje, lo cual no es imposible según lo veremos más adelante.

4.3.6.- ANÁLISIS DE ALTERNATIVAS Y SOLUCIONES PROPUESTAS AL PATRONO

A fin de evitar que, en la medida de lo posible, se produzcan violaciones de los derechos a la intimidad y del secreto de las comunicaciones en cuanto a la apertura del correo electrónico, el patrono, en ejercicio del poder de dirección y control que le asiste, tiene varias opciones:

i) Algunas soluciones apuntan a la posibilidad de que el empleador pueda controlar el nombre del destinatario pero no el contenido del mensaje. Con esto, el patrono podría ejercer el poder empresarial (o institucional en su caso), de

una manera proporcionada, al vigilar la adecuada utilización del *e-mail*, sea para fines meramente laborales, a la vez que respeta el secreto a las comunicaciones de sus trabajadores.

En esta tesitura, Rubio de Medina (2003) señala que en su opinión, está permitido el despido por detectarse un uso abusivo del correo electrónico transmitiendo o recibiendo mensajes de índole no profesional, simplemente controlando quienes son los destinatarios de tales mensajes, siempre que:

- a) El trabajador tenga conocimiento de la actividad controladora del empresario
- b) No se conozca el contenido de los mensajes de carácter personal
- c) De estar reguladas las infracciones que pudiera cometer el trabajador, que la conducta del mismo se califique como muy grave y se encuentre sancionada con la máxima sanción aplicable, en el despido se respeten las formalidades aplicables en la empresa
- d) Las pruebas se extraigan del ordenador del trabajador siguiendo las garantías indicadas en el artículo 18 ET o de la copia de seguridad propiedad de la empresa, siempre que esta actitud no suponga la violación del derecho al secreto de las comunicaciones

ii) Otra posibilidad es prever estas circunstancias en el convenio colectivo o en el contrato de trabajo. A este respecto, Del Var Arnal (Rubio de Medina, 2003) menciona la posibilidad de negociar acuerdos entre patronos y empleados para

delimitar el espacio de intimidad personal del trabajador en el uso del correo electrónico y erradicar la inseguridad jurídica en el Centro de Trabajo.

Por este medio, nos parece que los representantes de los trabajadores podrían negociar que se les faculte para utilizar razonablemente el *e-mail*, así como las circunstancias en las cuales el empleador tendría oportunidad de vigilar el ejercicio de la actividad laboral, brindando seguridad jurídica a los trabajadores y a los patronos.

También hay quienes señalan que se podrá optar por incluir en el contrato de trabajo cláusulas en las que el trabajador consienta, de manera expresa, el acceso del empresario a su cuenta de correo electrónico, aunque Sempre Navarro y San Martín Mazzucconi (Rubio de Medina, 2003) ya han señalado que parte de la doctrina niega la validez de estas cláusulas contractuales por encubrir una renuncia absoluta a los derechos del trabajador –con lo cual nos encontramos de acuerdo dado que el trabajador se ve imposibilitado de negociar u oponerse, al ser una típica cláusula de adhesión-; pero lo cierto es que, hasta el momento, no existe ninguna línea jurisprudencial con la suficiente fuerza como para apoyar una u otra opción.

iii) En defecto y/o como complemento del punto anterior, la parte patronal puede utilizar el poder de dirección y control, y prohibir de manera expresa la utilización del correo electrónico para fines particulares, o bien añadiendo esto a una

cláusula del contrato de trabajo o bien mediante la emisión de circulares, políticas, manuales, protocolos de funcionamiento, códigos de ética aplicables a la empresa, etc.

Como hemos podido constatar a lo largo de este estudio, cuando nos referimos al correo electrónico, el límite para diferenciar entre los aspectos personales y los privados es sumamente tenue. Por esta razón es recomendable, dentro de lo posible, que quede constancia para los trabajadores de forma categórica que el uso del correo electrónico en el trabajo sólo se consienta para fines profesionales, quedando prohibidos los usos particulares del mismo; dado que esta postura es la más adecuada con la finalidad de evitar los complejos problemas que se plantearían si el patrono da su consentimiento a que el trabajador utilice de forma privada el correo electrónico propiedad de la empresa o institución, dado que a los mensajes privados no podría acceder el empresario en el uso de sus facultades de control y la cuestión está en ¿cómo diferenciar un mensaje personal de otro profesional? (Rubio de Medina, 2003).

Es imperativo que en los convenios colectivos que se negocien para ser aplicables a las empresas o entidades, se especifique la graduación de las faltas y la tipificación de las sanciones por la incorrecta utilización del correo electrónico, dado que el mero uso esporádico de dicho correo para fines particulares, no justificaría, en ningún caso, la sanción por despido alegando vulneración de la buena fe contractual, salvo que de tales conductas

esporádicas se deriven daños considerables para la empresa, tales como infectar los ordenadores de la misma de virus que acceden a los sistemas informáticos por la apertura de mensajes de carácter personal.

iv) La doctrina se ha cuestionado si se asimilan al consentimiento expreso del trabajador, los mensajes en la pantalla de la computadora, en los que el patrono hace saber a sus trabajadores la existencia de controles en el material informático puesto a su disposición para fines profesionales. Para Barcelón Cobedo, si el trabajador pulsa la tecla de *ok* de un mensaje que aparece en su pantalla advirtiéndole de que su contenido puede ser fiscalizado por la empresa, como único medio para poder activar el equipo y trabajar con el ordenador, este acto no deberá de entenderse como equivalente a dar su consentimiento expreso al control empresarial; aunque la jurisprudencia si considera válido este consentimiento tácito, al respecto Sempere Navarro y San Martín Mazzucconi citan las SSTSJ Madrid 30.10.2001 y 4.12.2001; coincidiendo estos autores en la importancia que tienen las corrientes que estiman que no cabe asociar el consentimiento tácito con un consentimiento expreso sobre la base del criterio restrictivo que mantiene el Tribunal Constitucional en la limitación de los derechos fundamentales (Rubio de Medina, 2003).

En todo caso, es necesario que el trabajador tenga conocimiento, con carácter previo al registro, que la revisión de su correo, o de los documentos de su ordenador puede producirse, para evitar que se genere la obtención de una

prueba violando sus derechos fundamentales, la cual tendrá la consideración de nula.

v) En ausencia de regulación del uso del correo electrónico en el seno de la empresa -o institución agregamos nosotros-, Thibault Aranda (Rubio de Medina, 2003) propone dos posibles soluciones: los meros controles de futuro en evitación de males mayores, los cuales podrán realizarse previa información al trabajador de las condiciones de uso del correo electrónico y de las circunstancias de los controles respetando los derechos anteriormente expuestos; y, en segundo lugar, estima que cuando se detecte el uso irregular de la cuenta de correo asignada al trabajador, la revisión habrá de efectuarse mediante la aplicación analógica del artículo 18 ET, siguiendo las garantías exigidas en la citada disposición.

vi) Por otra parte, algunos defensores del uso del correo electrónico para asuntos personales, consideran que con ello se está ahorrando a la empresa el tiempo que el trabajador debería emplear para realizar ciertas gestiones (ir al banco, presentar la declaración de Hacienda, realizar una consulta médica, etc.).

En efecto, internet y el correo electrónico constituyen novedosas herramientas para efectuar gestiones, diligencias y transacciones personales en cuestión de minutos, sin que el trabajador deba pedir permiso a su jefe para llevarlas a cabo. No obstante, la otra cara de la moneda nos hace ver el tiempo

que el mismo trabajador pierde al enviar y recibir correos, lo cual redundaría en un perjuicio económico para el empleador al ver reducida su capacidad productiva.

Ciertamente, como indica la jurisprudencia, en todos estos casos habrá que aplicar el principio de proporcionalidad y valorar si el bien que se pretende defender justifica una intromisión en un derecho tan fundamental como es el derecho a la intimidad personal y uno de sus instrumentos, el secreto de las comunicaciones. Nos hallamos entonces ante un conflicto de derechos sobre el que será necesaria su ponderación en el caso a valorar.

4.3.7.- EL DESPIDO POR LA UTILIZACIÓN PERSONAL DEL CORREO ELECTRÓNICO PROPIEDAD DE LA PARTE PATRONAL

Por la fuerza con la que el despido incide en la vida del trabajador -e inclusive de su propia familia-, cese de los ingresos del mismo, y por ser la sanción más grave que se puede imponer en el campo laboral, la jurisprudencia española, especialmente en las Sentencias SSTS 2.11.1987, 26.11.1987 y 5.3.1987, exige en estos supuestos la existencia de proporcionalidad y adecuación entre el hecho, la persona y la sanción, por lo que es preciso valorar de manera individual las circunstancias concurrentes en cada caso concreto, con la finalidad de solucionar el conflicto cuestionado en específico. El despido disciplinario solo tiene razón de ser si partimos de los principios de la teoría

gradualista (Rubio de Medina, 2003), ya que el mismo sólo cabrá imponerlo en último término, ante comportamientos del trabajador que se califiquen como conductas extremadamente graves. Precisamente por esta circunstancia, algunos autores como Fernández Rodríguez opinan que siendo el uso del correo electrónico una actuación que supone una pérdida irrisoria de tiempo de trabajo para la empresa, es excesivo, partiendo del principio de proporcionalidad, sancionarla con el despido del empleado (Rubio de Medina, 2003).

Por otra parte, según la jurisprudencia española (Rubio de Medina, 2003), nos encontramos ante conductas que son causa de despido disciplinario en los siguientes casos:

i) Cuando se realice el despido por haber utilizado el trabajador los medios informáticos con que cuenta la empresa, en gran número de ocasiones, para fines ajenos a los laborales y ello con independencia del costo económico que esta conducta ha provocado en el empresario, siendo un accionar contrario a las reglas de la buena fe y de diligencia laboral con la finalidad de garantizar los derechos a la intimidad del trabajador (STSJ Cataluña 14.11.2000)

ii) Cuando la empresa alega como causa del despido disciplinario que el trabajador ha transgredido la buena fe contractual por la utilización desviada de los instrumentos facilitados por la empresa, como es el correo electrónico y la navegación por internet para fines ligados a la actividad productiva en horario

laboral y sin autorización de la compañía, supone transgresión a tal principio y abuso de la confianza depositada en él, supuesto analizado por la STSJ Galicia 4.10.2001 (Rubio de Medina, 2003).

En este extremo, resulta imprescindible calificar la conducta del trabajador, toda vez que la utilización del *e-mail* con carácter personal no es fundamento sólido para que se produzca, por sí mismo, el despido del empleado, sino que deberá ser una infracción reglada, grave, culpable y sancionable (Rubio de Medina, 2003).

iii) Con independencia de que la conducta venga reglada como causa de despido o no en el convenio colectivo que sea aplicable a la empresa, lo evidente es que, como ha observado Cardona Rubert, nos hallamos ante una infracción de carácter genérico, encuadrable dentro de los incumplimientos contractuales que pueden exigirse al trabajador en virtud del principio de buena fe contractual.

iv) Respecto a la característica de gravedad imputable a la conducta del trabajador, se deberá tener en cuenta si incurrir en un uso esporádico del correo electrónico es causa de despido disciplinario o no. Habrá que estarse a la graduación de las faltas (leves, graves y muy graves) que se establezcan en el convenio colectivo que, en cada caso, resulte aplicable a la empresa. En caso que el convenio no recoja estos extremos, o no exista, lo habitual es aplicar

criterios de ponderación en función de la regla de proporcionalidad, bastando, en nuestra opinión, la emisión y/o recepción de un solo correo para producir el despido si sus consecuencias son perjudiciales a la empresa –piénsese por ejemplo en los daños que la propagación de un virus que ha llegado al sistema de la empresa mediante un mensaje electrónico de un trabajador puede causar en el sistema de la empresa-.

v) Algunos autores, requieren, además, para que se pueda producir el despido del trabajador, al menos que se genere un requisito adicional que posibilite que el empresario pueda llevar adelante el despido disciplinario: la culpabilidad. Es la opinión de García Viña, para quien cuando se produce cualquier despido por vulneración de la buena fe empresarial por parte del trabajador, además de encontrarnos ante una conducta que se tendrá que incluir dentro de los supuestos indicados en el artículo 54.2 ET, deberá ser un comportamiento culpable del trabajador, teniendo en cuenta, además, que el requisito de culpabilidad se ve sensiblemente atenuado cuando la empresa con su conducta maliciosa y olvidadiza de la exigencia de buena fe, sirvió de motivación a la conducta del trabajador. Sería el caso de que la empresa consintiera el uso del correo electrónico de manera personal por sus trabajadores y no realiza ningún tipo de observación acerca de la prohibición con la finalidad de acumular pruebas que permitan despedir, por razones disciplinarias, al trabajador.

Esta exigencia de culpabilidad, es avalada por la STSJ de Galicia

19.9.1998, en la cual se externó que no basta con incurrir en conductas tipificadas como faltas, sino que es necesaria una conducta grave y culpable, debiendo la sanción guardar la imprescindible proporcionalidad con la gravedad de la falta (Rubio de Medina, 2003).

4.4.- SECCIÓN IV. CUESTIONES INFORMÁTICAS

4.4.1.- FORMA EN QUE SE PUEDEN ACCEDER LOS CORREOS

i) Estructura de red corporativa

Las estructuras de redes empresariales o de entidades estatales suelen ser bastante complejas, según veremos en el esquema que de seguido se detalla.

Los ordenadores "*clientes*" se conectan mediante la red entre ellos, y obtienen las aplicaciones necesarias de servidores de ficheros, se enlazan a internet mediante un *router*, usan servicios *web* por medio del servidor y se protegen con diversos *firewalls*. Sin embargo, todo esto está controlado desde la posición del administrador, que es una persona con privilegios exclusivos para el mantenimiento de toda la red. La consecuencia es que un ordenador cliente envía el correo electrónico desde su máquina y pasa al servidor, para enlazar,

mediante el *router*, con la red de redes (Villahermosa, 2002).

El administrador es consciente, o puede ser consciente, del contenido del correo en todo momento: es lo mismo que el correo no se haya mandado, o que se encuentre en el servidor. No cabe duda que el administrador es la persona que tiene mas facilidades -además de formación técnica- para que esto se produzca. Además, los correos mandados siempre dejan rastros, en forma de archivos "*logs*" que se pueden encontrar en los ordenadores clientes y en el servidor.

La intimidad en este supuesto también puede verse vulnerada, dados los amplios poderes que puede tener esta figura denominada administrador –los cuales incluso son prácticamente desconocidos por los trabajadores - a la que no se le ha dado la suficiente importancia. Sobre este particular, no se han encontrado referencias jurisprudenciales que aborden la problemática. Se considera no obstante, que puede no haber vulneración si el administrador hace un trabajo equitativo y los datos a los que accede son estrictamente necesarios para la consecución de su trabajo (Villahermosa, 2002).

ii) Soluciones que vulneran la intimidad

Así como existen programas que protegen la intimidad de un usuario en la utilización del correo electrónico, también hay aplicaciones informáticas que la

violentan. Programas como "*spector*" por ejemplo, producen de manera automática decenas de "*snapshots*" (imágenes) del computador del trabajador para "*vislumbrar*" cómo trabaja. En este tanto, es claro que permite la lectura de los correos desde la empresa, pero no sólo eso, sino que prácticamente cualquier cosa queda al descubierto.

Resulta curioso comprobar como la licencia de uso de este software queda constreñida a que el adquiriente avise a todas las personas, que van a ser "*observadas*" mientras trabajan, siendo el producto número uno en ventas de su tipo en Estados Unidos (Villahermosa, 2002). Es así como las compañías estadounidenses, son las que con mayor frecuencia acuden a esta clase de programas computacionales, a fin de velar por la adecuada utilización de los recursos que ponen a disposición de los trabajadores. Según los estudios realizados, hasta un cincuenta y cinco por ciento de las empresas tienen instalados sistemas de rastreo del *e-mail*, capaces de interceptar y eliminar mensajes que contengan determinadas palabras o expresiones "*prohibidas* "; verbigracia marcas competidoras, términos sexistas u obscenos, etc.

Según lo expuesto, una vez más se manifiesta el choque entre los intereses de las empresas –e instituciones- y el derecho al secreto de las comunicaciones de los empleados a su cargo, siendo éste último derecho como ya hemos señalado, el que consideramos debe prevalecer.

4.4.2.- INSTRUMENTOS DE SEGURIDAD PARA IMPEDIR EL ACCESO

i) Cifrado

La función inmediata del cifrado, es el suministro del servicio de confidencialidad, sea de los datos o del flujo de tráfico, pero además es una pieza fundamental para el logro de otros varios servicios.

Resulta interesante señalar como prácticamente toda la problemática que se plantea, podría verse reducida a la nada si el trabajador en cuestión usara herramientas de encriptación (cifrado), para que resultara imposible la lectura de los correos electrónicos que él envía. Con los algoritmos que se usan hoy en día (hasta 512 bits), resultaría virtualmente imposible acceder a un determinado tipo de información con el simple uso de un software, como PGP - <http://www.pgp.com>- (Villahermosa, 2002).

ii) Firma electrónica y certificados digitales

Este mecanismo conlleva dos etapas: en primera instancia, la firma del mensaje y, posteriormente, la verificación de la misma. La firma electrónica se consigue a partir del propio mensaje, o una transformación precisa del mismo, a firmar, de modo que si éste cambia también lo hace la firma, y de una información privada sólo conocida por el signatario (Villahermosa, 2002).

El segundo proceso se obtiene aplicando a la firma a comprobar una información pública, que aunque es una función matemática de la citada información privada, es computacionalmente imposible de obtener de ésta última. Finalmente, el resultado de este proceso se coteja con el mensaje, o la transformación citada del mismo (Villahermosa, 2002).

Sin embargo, para brindar entera seguridad jurídica a este mecanismo, se necesita hacer intervenir en la comunicación una tercera parte confiable entre los sistemas terminales, la cual garantiza que las claves usadas en la firma digital son efectivamente de aquél que se dice su propietario. Este tercero de confianza se denomina "*Autoridad de Certificación*".

El uso de la firma electrónica, conjuntamente con certificados digitales expedidos por autoridades de certificación competentes, consiguen un alto grado de autenticación en los mensajes de correo electrónico. Recordemos que "*La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y los documentos que la incorporen serán admisibles como prueba en juicio, valorándose éstos, según los criterios de apreciación establecidos en las normas procesales*" (Villahermosa, 2002).

En el seno de una empresa o entidad, perfectamente puede estar asentado el uso de esta tecnología. No obstante, en el ámbito que nos interesa en este momento, debemos contemplarlo como un elemento de prueba a la hora de identificar al emisor de mensajes. Los programas-cliente de correo actuales o las cuentas *web-mail*, ya proporcionan suficiente información al respecto para averiguar el destino, uso, fecha, y muchos otros detalles como para razonar la debida o indebida utilización de una persona de los medios informáticos de su centro de labores, sin la necesidad de usar mecanismos como el que estamos contemplando ahora mismo. Aunque por supuesto, ello provocaría un refuerzo casi inapelable sobre la autoría del envío de los *e-mail*. De nuevo, no tenemos constancia de pronunciamientos sobre el caso planteado, y es que, a pesar de su gratuidad, se trata de técnicas bastante desconocidas para un usuario medio de la red de redes (Villahermosa, 2002).

En nuestra Asamblea Legislativa, actualmente se encuentra un Proyecto de Ley sobre este tópico, denominado "*Ley de Firma Digital y Certificados Digitales*", expediente número 14276, el cual tiene como objetivo regular el uso y el reconocimiento jurídico de la firma digital, otorgándole la misma validez y eficacia jurídica que el uso de la firma manuscrita u otra análoga que conlleve manifestación de voluntad, así como autorizar al Estado para su utilización. Un resumen de los principales contenidos del Proyecto citado, se anexa al presente trabajo.

4.5.- SECCIÓN V. LOS FUNCIONARIOS PÚBLICOS Y EL DERECHO A LA INTIMIDAD

El derecho a la intimidad protege a todos los trabajadores, independientemente de si laboran en el sector privado o si se desempeñan dentro de la Administración Pública. Es válido decir, que así como en el ámbito privado el patrono goza de un poder de vigilancia y control sobre la organización productiva, que le permite verificar el efectivo cumplimiento por parte del trabajador de sus obligaciones y deberes labores, en el sector público la Administración ostenta facultades de fiscalización sobre los funcionarios, que le posibilitan verificar la diligencia del empleado en su trabajo y el uso que le da a los bienes de la institución, toda vez que los mismos ostenta el carácter de públicos, con las implicaciones legales que ello conlleva.

Pretendemos en este apartado, determinar hasta que punto el derecho a la intimidad que asiste a los funcionarios públicos, puede evitar actuaciones de la Administración que pretendan impedir el uso indebido por parte de los trabajadores de los bienes y servicios a que tengan acceso, como medio para atender las funciones propias de su cargo. Ello, toda vez que resulta imprescindible un balance entre los derechos del funcionario y el control interno.

4.5.1.- USO DEL CORREO ELECTRÓNICO CON FINES PERSONALES

La utilización del correo electrónico en una empresa o institución, especialmente cuando se distorsiona su uso de fines profesionales a particulares, puede desencadenar en una serie de problemas que, en ocasiones, pueden ligarse a conductas reprochables en el campo penal y/o laboral. Rubio de Medina (2003), señala algunas de estas conductas que trastornan la fluidez de las relaciones laborales:

- i) Las relacionadas con problemas de seguridad y ocasionadoras de daños patrimoniales en la empresa, al infectarse el sistema informático de la misma, mediante virus que han llegado desde el exterior por la apertura por parte del trabajador de *e-mail* de índole personal
- ii) Los comportamientos que conllevan la usurpación de la personalidad, como cuando un trabajador se hace pasar por otro, anomalía que puede evitarse adoptando técnicas de encriptado, es decir, mediante la implantación de la firma electrónica entre los trabajadores de la empresa
- iii) Los comportamientos que son causa de problemas de acoso moral *-mobbing-* o acoso sexual, dado que se pueden utilizar los mensajes de correo electrónico para intimidar a los superiores, a los subordinados o a los compañeros de trabajo

iv) Las actuaciones que conlleven acciones discriminatorias, lo que podría ocurrir cuando un empresario favorece la discriminación entre los trabajadores al transmitir órdenes genéricas de manera particular a una cuenta individual de correo y no al resto del personal

v) Cuando se produce la pérdida de productividad de la empresa al descender el rendimiento laboral de los trabajadores, los cuales destinan parte de su jornada laboral a enviar y/o contestar los mensajes electrónicos

vi) Los comportamientos que conllevan la transmisión de datos confidenciales de la empresa a los competidores, mediante el envío de información confidencial por correo electrónico

vii) El incremento de los costos económicos de la empresa en la factura telefónica –si no se tiene implantada la tarifa plana-, o en el material consumible (gran consumo de papel, disquetes, CD-Rom y similares) al utilizarse para imprimir y/o grabar los contenidos de los mensajes y/o ficheros adjuntos, etc.

Los problemas que ocasionan estos comportamientos en el seno de la empresa, institución, o centro de trabajo, es que mientras que para la protección de datos personales y la regulación del fenómeno de internet han existido y existen normas que tratan de reglamentar los abusos, no ocurre lo mismo cuando tratamos de analizar el tema del correo electrónico desde el punto de

vista laboral, donde lo más llamativo es, precisamente, la ausencia de una normativa que, al día de hoy, es muy necesaria.

En tal sentido, es de suma importancia concretar cuando el patrono que despide a uno de sus trabajadores alegando vulneración de la buena fe contractual por la utilización personal del correo electrónico, está actuando conforme a derecho y cuando no.

4.5.2.- ÉTICA DE LA FUNCIÓN PÚBLICA

Los bienes de la Administración Pública, deben ser utilizados por los funcionarios públicos para los fines para los cuales les son asignados, es decir los de carácter laboral, de forma tal que no se sirvan de los mismos para obtener un aprovechamiento personal.

La Procuraduría General de la República ha dejado de manifiesto la importancia de la ética pública. En el Estado Social de Derecho, el Gobierno debe velar porque las decisiones políticas y administrativas favorezcan al interés general y, por ende, beneficien a toda la colectividad. Toda conducta contraria a la ética pública, impide concretizar los fines y funciones del Estado Social de Derecho, por lo que salta a la vista la importancia de que los funcionarios públicos actúen conforme lo impone la ética de la función pública.

La ética se funda en valores y en tal medida debe propiciar que el comportamiento de los servidores públicos se oriente en el sentido de la realización eficaz y eficiente del servicio y en el uso de los recursos del Estado en cumplir sus fines, sin desviaciones que signifiquen traspaso de recursos públicos a fines particulares ajenos al servicio. Los valores imponen una determinada forma de conducta al funcionario público. Por ello, valores como probidad, lealtad, responsabilidad, eficiencia y honestidad son fuente de obligaciones y deberes para el funcionario; así, deber de confidencialidad, de imparcialidad, de objetividad en el desempeño del cargo.

Asimismo, la Procuraduría (Dictamen C-003-2003 de 14 de enero de 2003) ha manifestado que *“...la violación de normas morales o jurídicas, con el objeto de obtener una ventaja material es contraria a la función pública y lesiona el interés general. Se está ante esta hipótesis siempre que el funcionario actúe en función de ventajas personales (...) En general, todo aquel cuyo comportamiento se aparta de los deberes formales de un cargo público en busca de la satisfacción del interés privado, estaría violentando los deberes de la función pública...”*.

Podemos concluir válidamente, que la Administración debe velar porque los funcionarios utilicen debidamente los bienes del Estado que les fueron confiados para desempeñar su cargo, así como también por fiscalizar que no difieran la utilización del tiempo laboral para la realización de actividades

personales. Ello, toda vez que conductas de esta naturaleza atentan contra la eficacia y la eficiencia de la gestión pública, principios fundamentales de la organización administrativa y consecuentemente de los funcionarios públicos.

4.6.- SECCIÓN VI. MECANISMOS DE CONTROL

Como adelantáramos líneas atrás, la Administración Pública tiene la obligación de tutelar el correcto y adecuado uso de los bienes y servicios de su propiedad, por lo que a fin de no ver mermada la productividad de sus funcionarios, debe establecer mecanismos que le permitan vigilar la debida diligencia en las labores que los mismos realizan.

4.6.1.- LÍMITES A LA FISCALIZACIÓN DE LOS SERVIDORES PÚBLICOS: LOS CONTRATOS DE TRABAJO

Como hemos podido observar, en varios escenarios se cuestiona la legitimación del empleador para vigilar los hábitos de sus funcionarios, para supervisar sus usos de navegación o la utilización del correo electrónico. Ha quedado claro que la propiedad de las computadoras es de los patronos, y que el tiempo empleado en el *e-mail* “*pertenece*” también a la parte patronal. Sin embargo, no se contempla como garantía el hecho de que el empleador tenga

una autonomía ilimitada sobre los equipos o sus recursos humanos; o sea, que el contrato laboral que ampara ese derecho del empresario a disponer o a controlar esos recursos no es absoluto.

En este sentido, estimamos improcedentes -y por ende nulas- las cláusulas que se incluyan en los contratos de trabajo, con el propósito de que el empleado explícitamente brinde su consentimiento para que el patrono accese a su cuenta de correo electrónico, toda vez que las mismas pretenden burlar el derecho del trabajador a su intimidad y al secreto de las comunicaciones que le asiste, sin que tenga posibilidad alguna de oponerse, dado el carácter leonino de la disposición.

En aras de proteger el derecho del patrono de controlar los recursos que pone a disposición de los empleados para realizar la actividad laboral, no puede vulnerarse su homólogo a la intimidad, que se encuentra protegido en la Constitución y por ende es de mayor rango. La posible solución, como lo hemos comentado, habrá de armonizar necesariamente ambos derechos, ya que permitir el acceso ilimitado al correo electrónico del trabajador, pasaría por encima del derecho de éste al secreto de las comunicaciones, que se establece como una garantía formal a la comunicación libre, al margen de quién ostente la titularidad de la empresa.

4.7.- SECCIÓN VII. ANÁLISIS DEL MANUAL DE NORMAS Y POLÍTICAS EN EL USO DE SERVICIOS DE CORREO Y ACCESO A INTERNET DEL MINISTERIO DE HACIENDA, EN CUANTO AL CORREO ELECTRÓNICO

El principio de legalidad en materia administrativa, se encuentra establecido en el numeral 11 de la Ley General de la Administración Pública. Dicho artículo, exige que los órganos del Estado actúen apegados al ordenamiento jurídico, no pudiendo ir más allá de lo que las normas les permiten. Es así como toda acción de la Administración Pública debe estar amparada a una disposición normativa.

En esta tesitura, a efecto de regular el uso del correo electrónico y el acceso a internet, tanto el Ministerio de Hacienda como otras instituciones públicas se vieron en la obligación de dictar, previamente, un instrumento que le brindara eficacia y validez a sus actuaciones; y en el caso que nos ocupa resultan ser las Políticas de Uso de Internet y Correo Electrónico. Procederemos entonces en el presente capítulo, a analizar la referida Política vigente en el Ministerio de Hacienda, pero única y exclusivamente desde la perspectiva del correo electrónico, por ser éste nuestro campo de investigación.

4.7.1.- OBJETIVO

Según consta en el texto bajo estudio, desde el año 1999 la Dirección

General de Informática del Ministerio de Hacienda, estableció las “*Políticas de Uso de Internet y Correo Electrónico*”, mismas que en su oportunidad fueron puestas en conocimiento de la totalidad de los funcionarios del ente y que contienen normas para lograr una adecuada y responsable utilización del *e-mail*.

En este punto, debemos hacer énfasis en que desde el momento de la instauración del servicio de correo electrónico, los jefes del Ministerio de Hacienda observaron que la nueva herramienta laboral pese a sus muchas ventajas presentaba un eventual inconveniente, sea que sus empleados desviarán la utilización del mismo a su ámbito personal. Ante esa necesidad y plenamente conscientes de que la Administración Pública se rige por el principio de legalidad, atinadamente decidieron redactar un texto que regulara el funcionamiento del *e-mail*, a fin de garantizarse su eficaz y correcto uso en las funciones cotidianas, el buen funcionamiento de los sistemas y por ende responder cabalmente a los fines institucionales. Asimismo, la Política fue comunicada a todos los funcionarios, con la finalidad de cumplir con el debido proceso.

Es así como el objetivo fundamental de la Política es regular el uso de los servicios de correo electrónico y el acceso a Internet, para lo cual emite una serie de lineamientos que son de acatamiento obligatorio para todo el personal del Ministerio que utilice los recursos de la red.

4.7.2.- ALCANCE

La Política es clara al establecer que todos los usuarios deben estar enterados y conscientes de los deberes que, al utilizar los servicios de la red, han adquirido. Por ello, considera necesario adoptar las medidas que correspondan a efecto de respetar la normativa. En ese sentido, todos los usuarios de la red están sujetos a los términos de la Política, así como a externar un comportamiento acorde a los principios morales y éticos que deben privar al momento de utilizar los recursos del Ministerio, sea fondos públicos.

El uso de la red y los recursos de información del Ministerio, están disponibles para fortalecer el flujo de información interna, la investigación en materia tributaria, administrativa, educativa, y apoyar en cualquier otra clase de tarea encomendada para el mejor rendimiento en sus labores. Es por ello que el uso inapropiado de la red, tal y como se dirá *infra*, es sancionado con la eliminación del acceso a estos recursos y puede conllevar a la aplicación de las sanciones disciplinarias respectivas, sin perjuicio de las consecuencias administrativas y judiciales que eventualmente pudieran resultar aplicables.

4.7.3.- USOS

El documento que analizamos, señala que es responsabilidad de todos

los funcionarios del Ministerio de Hacienda, cumplir con las normas y procedimientos estipulados para tener acceso a los servicios de correo electrónico e internet. En este sentido, enumera lo que se considera usos aceptables y usos inaceptables en la utilización de tales herramientas.

i) Usos Aceptables

Como usos aceptables de la red (Ministerio de Hacienda, 2002), indica los que conciernen a los siguientes aspectos:

- a) Comunicación entre investigadores, economistas y personas relacionadas con las labores desempeñadas en el ámbito nacional y extranjero, siempre y cuando exista un intercambio mutuo y en condiciones recíprocas
- b) Comunicación e intercambio con la comunidad académica, universitaria u otras instituciones con el fin de tener acceso a los últimos avances relacionados con la especialidad o tareas desempeñadas
- c) Anuncios o servicios nuevos para el uso de los usuarios en general, pero no para publicidad de tipo comercial o personal alguno
- d) Comunicación entre instituciones o empresas privadas siempre y cuando

estén vinculadas con las tareas encomendadas

- e) Actividades de capacitación por medios virtuales o en línea

Pese a que se enuncian una serie de conductas, consideramos que este listado no es *numeros clausus*, por lo cual es posible encontrar otras circunstancias en las que la utilización del *e-mail* puede considerarse aceptable, verbigracia evacuar consultas de los administrados, lo cual no contravendría en nada el instrumento normativo.

ii) Usos inaceptables

En la misma línea seguida en el punto anterior, la Política consigna una serie de utilizaciones consideradas inadmisibles, tanto del correo como de internet, mismas que de seguido se detallan (Ministerio de Hacienda, 2002):

- a) Cualquier actividad que sea lucrativa o comercial de carácter individual, privado, o para negocio particular
- b) Acceso a lugares obscenos, que distribuyan libremente material pornográfico, o bien materiales ofensivos en perjuicio de terceros
- c) Acceso a lugares recreativos, deportes, música, chistes, entre otros

- d) Utilización de los servicios de correo para envío de información personal, chistes, pensamientos y cualquier otra información que no sea de carácter laboral

Al igual que en el anterior apartado, estimamos que el listado transcrito no es cerrado, sino que más bien pretende ejemplificar conductas impropias con la finalidad de hacer más digerible el contenido de la norma para los empleados.

4.7.4.- PROHIBICIONES

La Política plantea, taxativamente, una serie de conductas que considera inadecuadas en la utilización del instrumento de trabajo (*e-mail*), razón por la cual determina la prohibición de ejecutarlas. Seguidamente, veremos cada una de ellas (Ministerio de Hacienda, 2002) e iremos comentando brevemente las mismas.

- a) La transmisión de materiales en violación de cualquier regulación, queda prohibida. Esto incluye, pero no se limita, a materiales con derechos de propiedad intelectual, materiales que legalmente se consideren amenazantes u obscenos. Lo anterior en cumplimiento con el Decreto N° 29915-MP Prohibiciones Material Pornográfico-Equipo Electrónico-Reglamento Autónomo de Servicio-Dirección General de Servicio Civil.

Se restringe la transmisión de todo tipo de material que atenta contra el ordenamiento jurídico. La restricción se esgrime de manera genérica, pero también muestra a manera de ejemplo, dos actuaciones que vulneran el precepto, tales como la transmisión de materiales con derechos de propiedad intelectual y materiales obscenos. Además, incorpora la normativa que brinda sustento legal a la medida adoptada.

- b) Queda prohibido el envío de información en forma masiva a todo el Ministerio o Grupos de usuarios, por lo cual se restringe su uso en forma automática.

Esta limitación obedece a la necesidad de dar un adecuado uso a la red, a fin de optimizar su rendimiento y por ende, de los sistemas, internet y otros servicios disponibles. Obviamente existen casos especiales en los cuales, al contar con la debida autorización del órgano competente, es posible enviar mensajes colectivos de carácter estrictamente laboral.

Debido al alto nivel de seguridad con el que se debe de contar en el Ministerio, las claves de acceso al servidor de WEB y correo electrónico deberán de ser estrictamente confidenciales y personales. Además de censurar la visita de páginas en la red dedicadas a áreas que no sean de interés investigativo, capacitación, económico, legal, o del área de competencia, o bien que simplemente se haga mal uso de los recursos para acceder información no

relacionada con el área de trabajo.

Como hemos mencionado en cantidad de oportunidades, el servicio de correo es un instrumento de trabajo. En tal sentido, únicamente debe ser utilizado para cuestiones que tengan relación con el cargo que se desempeña. Las manifestaciones que un funcionario realice, al provenir de un dominio que pertenece al Ministerio, implican que se externan en representación de la institución; de ahí la importancia de guardar estricto secreto en las claves de acceso correspondientes.

- c) Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas del Ministerio.

Este punto también pretende reafirmar que el correo debe ser utilizado exclusivamente para fines laborales, sin que de ninguna forma pueda ser empleado en cuestiones contrarias a la moral o al orden público, sea dentro o fuera del centro de trabajo.

- d) Utilizar los recursos del Ministerio para ganar acceso no autorizado a redes y sistemas remotos.

Los instrumentos que el Ministerio de Hacienda y los demás entes y órganos del Estado ponen a disposición de los trabajadores, no deben ser utilizados para acceder a lugares no autorizados para los usuarios del sistema.

- e) Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas.

Atentar contra los bienes de la institución, que guardan el carácter de públicos, implica un accionar contrario a las disposiciones del Estatuto de Servicio Civil y del propio Código de Trabajo, lo cual inclusive puede considerarse como una causal de suspensión o despido.

- f) Monopolizar los recursos en perjuicio de los otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones voluminosas, uso de recursos de impresión no autorizado.

Tal y como se señaló con anterioridad, se prohíbe el envío de mensajes masivos, las famosas “*cadenas*”, o cualquier otro proceso contrario a la finalidad del servicio de correo, a efecto de que la red no sufra problemas y lograr un correcto uso de los sistemas.

- g) Utilizar los servicios de red para enviar archivos que sean confidenciales.

Existen archivos que por la naturaleza del asunto sobre el que versan, no deben ser del conocimiento de individuos ajenos a la institución, por lo que se estima improcedente el envío de esta clase de documentos a agentes externos a la institución, independientemente de la finalidad con la cual vayan a ser utilizados.

- h) La exhibición de material pornográfico en cualquier lugar de la institución utilizando el equipo de cómputo y/o los servicios de comunicación de la institución, asimismo el uso de equipo electrónico del Estado para observar o reproducir pornografía. El incurrir en el incumplimiento de esta normativa acarrea una falta grave que será sancionada según las regulaciones vigentes.

En la misma tesitura de anteriores comentarios, al ser una práctica ajena a la moral, las buenas costumbres y los objetivos para los cuales el Ministerio dota de la herramienta de correo a sus funcionarios, no resulta permitida la transmisión de cualquier tipo de material pornográfico. La contravención a esta norma, explícitamente es considerada como falta grave con las sanciones que ello implica.

- i) Envío de mensajes masivamente a todos los usuarios de la red o segmentos, iniciación y facilitaciones de cadenas y creación de procesos de discusión y contestación.

Todos los usuarios son responsables de lograr y brindar un adecuado uso de la red, para lo cual ésta debe evitar congestionarse. Este tipo de mensajes masivos o las populares cadenas, por el tamaño de los archivos y la gran cantidad de personas a las cuales se dirige, atenta contra el funcionamiento de la red, por lo que se impide su divulgación.

- j) Envío de correos en donde se solicitan ayudas a personas o grupo de personas, este tipo de mensajes únicamente serán permitidos si son canalizados por medio de Centro Virtual de Conocimiento Hacendario.

Pese a que podría considerarse que una disposición de esta envergadura atenta contra un fin social loable, lo cierto del caso es que este tipo de correos también ocupan un espacio bastante considerable en la red, lo cual puede ocasionar problemas en la entrada y salida de los mensajes y en la rapidez con que el servidor actúe. Nótese que, sin embargo, la posibilidad no se cierra totalmente, sino que procura orden, puesto que esta clase de comunicaciones pueden ser canalizadas a través del Centro Virtual de Conocimiento Hacendario, órgano que dirimirá la procedencia o no de la gestión. Sin demérito de lo anterior, es menester indicar que muchas veces tales correos son falsos, lo cual podría inclusive conllevar un perjuicio económico para los propios usuarios.

4.7.5.- MECANISMOS DE CONTROL

De la misma manera en que el empresario tiene la facultad de vigilancia y control como presupuesto ineluctable de la organización productiva, la Administración Pública debe velar por el grado de dedicación que el funcionario brinde a su trabajo, así como también sobre las herramientas que se le facilitan para el desarrollo de sus labores. El servicio de correo no puede ser una excepción a este precepto. El Ministerio de Hacienda ha evaluado la necesidad de establecer mecanismos que le permitan tutelar el efectivo cumplimiento de estas situaciones, las cuales pasamos a detallar sucintamente (Ministerio de Hacienda, 2002):

a) La administración de la red, de la Dirección General de Informática, no ejerce control sobre el contenido de la información que pase por la red, o de quien la utilice, quedando bajo la responsabilidad del funcionario que la accese o la utilice. No obstante lo anterior, la administración pondrá en funcionamiento herramientas de control que posibilitan analizar y detectar usos indebidos, por lo anterior se advierte que el contenido de la información es monitoreada y sujeta a controles y reportes sobre el uso.

En esta norma es posible visualizar el respeto que la Política guarda a los derechos constitucionales de intimidad e inviolabilidad de las comunicaciones. Es así como se regula que la Dirección General de Informática no se encuentra

facultada para imponerse del contenido de los mensajes que pasen por la red, dejando en manos del respectivo funcionario la responsabilidad en caso de accederla o utilizarla. No obstante, la disposición no deja portillos abiertos, puesto que advierte la existencia de controles que permiten a la Administración de la Red analizar y detectar usos indebidos, sin violentar el secreto de la comunicación.

b) La administración de la red de la Dirección General de Informática, no da garantías de ningún tipo, sea expresa o implícitamente, para el servicio que provee, por lo que no existirá ninguna responsabilidad por cualquier daño que el usuario sufra causado por negligencia propia o los errores u omisiones de sus usuarios.

Es claro que las herramientas de trabajo que las instituciones públicas ponen al servicio de sus empleados para las actividades laborales cotidianas, son un simple medio para que el funcionario pueda realizar su actividad de una manera más rápida, eficiente y eficaz, sin que ello implique obligación alguna de la Administración de proveerle estos elementos. En tal sentido, toda clase de perjuicio que el usuario sufra por cualquier causa en la utilización del correo electrónico, no implica responsabilidad alguna de la Administración de la Red ni de la institución.

c) Los mensajes que se envíen vía Internet, serán de completa responsabilidad

del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ninguna otra institución.

Pese a que los mensajes electrónicos se envían del dominio perteneciente al Ministerio de Hacienda, y que éstos mensajes se consideren efectuados en nombre de la institución, al existir un deber de utilizarlos únicamente en cuestiones de índole laboral, el usuario será el responsable de las comunicaciones que dirija bajo su total y exclusiva responsabilidad, debiendo ajustarse al raciocinio y a las buenas costumbres. Tales mensajes deben canalizarse para fines laborales, y nunca para afectar intereses de personas físicas o jurídicas.

d) La Dirección General de Informática, tiene la autoridad para controlar y negar el acceso a cualquier funcionario que viole las políticas o interfiera con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.

La Dirección General de Informática del Ministerio, resulta ser en razón del ámbito de competencia, la encargada de vigilar el estricto acatamiento de la Política. En esta función, se encuentra habilitada para tomar medidas de control y negar el acceso al servicio de correo a todo aquel empleado que infrinja las

disposiciones normativas o violente los derechos de sus compañeros. No obstante, este poder no es irrestricto, toda vez que tiene la obligación de notificar a los afectados las decisiones que se adopten y dar un adecuado razonamiento sobre las mismas.

e) La Dirección General de Informática, utilizará herramientas de monitoreo del uso de los recursos, por lo cual podrá establecer controles de acceso a sitio y de envío de información masivamente por la red.

Como lo hemos comentado en otras secciones, hoy en día existen programas que permiten al empleador vigilar la correcta utilización de los bienes públicos. Dichos programas facilitan, sin imponerse del contenido de la información que consta en la comunicación electrónica, establecer controles en el envío y recepción de mensajes que salgan e ingresen en la red; lo cual posibilita ejercer medidas de control sin violentar derechos fundamentales de los individuos, siempre con miras a cumplir con los fines institucionales.

f) La Dirección General de Informática enviará reporte del uso del servicio de correo o Internet a las Jefaturas respectivas, para que tomen medidas tendientes a mejorar su utilización.

Como medida de vigilancia, la Dirección General de Informática periódicamente debe enviar un reporte a las diversas Jefaturas, sobre el manejo

que los funcionarios a su cargo han observado en el empleo del servicio de correo. Esta regla tiene como finalidad que los jefes ejerzan el control interno, en la utilización que sus subalternos le han brindado al correo electrónico, pretendiendo velar por el buen funcionamiento de la Institución, a fin de que el trabajo se realice de manera eficiente al maximizar los recursos disponibles.

4.7.6.- SANCIONES

La Dirección General de Informática, es el órgano competente para determinar la aplicación de la suspensión de acceso al servicio de *e-mail*, ello en atención al grado de contravención a la Política vigente. Dichas sanciones son aplicables de manera inmediata y reflejan una gradualidad al momento de aplicar la suspensión del servicio, dado que se plantean de la siguiente manera (Ministerio de Hacienda, 2002):

- a) Incumplimiento por primera vez de las normas y lineamientos establecidos, se suspende el servicio por quince días naturales

- b) Incumplimiento de las normas y lineamientos por segunda vez, se suspende el servicio por un mes calendario

- c) Tercera vez de incumplimiento, se suspende el servicio por dos meses o

suspensión permanente

De igual manera, el cuerpo normativo objeto de estudio, señala que la acción de suspensión no impide que se establezcan procedimientos administrativos, a efecto de aplicar sanciones disciplinarias por el uso indebido del equipo electrónico y las telecomunicaciones en la institución, es decir, que las acciones no son excluyentes la una de la otra.

CAPÍTULO V

Conclusiones y Recomendaciones

5.1.- CONCLUSIÓN GENERAL

En los centros de trabajo, el correo electrónico se ha convertido en un instrumento que incrementa la eficiencia de las labores, pero, a su vez, ha suscitado una importante cantidad de problemas en el ámbito jurídico, empresarial, institucional e inclusive judicial. El choque de intereses entre el poder de control y dirección del patrono en relación con su actividad productiva y el derecho a la intimidad de los trabajadores, ha sido una constante.

Este derecho a la intimidad de los empleados y de todas las personas en general, es sumamente reconocido; se le concibe como de un carácter personalísimo, necesario para el desarrollo del individuo, de injerencia y aplicación, inclusive, en la vida laboral. No obstante, dicho derecho no es absoluto, dado que en las relaciones de trabajo deben observarse ciertos principios básicos para lograr una convivencia armónica entre las partes que configuran la relación laboral. En tal sentido, si bien es cierto el patrono puede implementar medidas de vigilancia y control, no lo es menos que éstas estarán limitadas por la dignidad, el derecho a la intimidad, y el secreto de las comunicaciones de sus subordinados.

Varios cuerpos normativos tutelan el derecho a la intimidad: textos constitucionales, tratados internacionales y leyes, constituyen tan sólo algunos de los más representativos. Sin embargo, es la jurisprudencia quien realiza el

aporte más importante. En una temática tan novedosa como la que nos ocupa, la línea jurisprudencial se encarga de definir, aclarar y profundizar en el contenido de los conceptos, aplicando la letra muerta a los casos concretos, y diseñando de esta manera los alcances que hoy día se le otorgan a este derecho fundamental.

Como un derivado del derecho a la intimidad, surge su homólogo a las comunicaciones, regulado de igual forma en el artículo 24 de nuestra Carta Magna, y que dicho sea, ampara cualquier clase de comunicación sin discriminación de tipo alguno. El supuesto de que un patrono se imponga arbitrariamente del contenido de los mensajes de correo electrónico de sus empleados, con la idea de corroborar si tiene que ver con el trabajo que desempeña, nos hace ligar el derecho a la intimidad con el derecho al secretismo en las comunicaciones, ya que la garantía no depende en forma alguna de la propiedad del canal que se utilice.

Ninguna comunicación, y en nuestro caso específico el *e-mail*, puede ser interceptada por un tercero ajeno a la misma, sino es por medio del camino y en las circunstancias previstas en la Constitución Política, mismo que es desarrollado en ocasiones por las leyes especiales. En nuestro país la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, resulta ser la que, de manera taxativa, señala los casos en que es factible intervenir un comunicado.

No obstante lo anterior, multitud de patronos miran como sus funcionarios consumen una buena cantidad de su tiempo laboral, enviando y recibiendo correos electrónicos que no tienen que ver con las actividades empresariales o institucionales y que pueden desencadenar en una serie de problemas relacionados con seguridad, daños patrimoniales, pérdida de productividad y usurpación de personalidad, entre otros. En tal sentido, se suscitan dos posiciones abiertamente contrarias: el secreto de las comunicaciones de los trabajadores versus la facultad de control y dirección del patrono.

En este conflicto, aunque es sumamente difícil, se debe tratar de encontrar un punto intermedio, el cual permita a la parte patronal ejercer sus facultades de vigilancia sin vulnerar los derechos constitucionales de los funcionarios. Nosotros estimamos que una solución viable, es que el patrono pueda –cuando existan indicios razonables para ello– conocer la cantidad de mensajes y el horario de la jornada de trabajo en que se han enviado, para determinar si la actuación del empleado reviste gravedad. Inclusive, consideramos que la parte patronal podría observar aspectos “*poco trascendentales*” del *e-mail*, como por ejemplo el destinatario y el sujeto, pero no el contenido del mismo (salvo permiso expreso del trabajador), lográndose un balance favorable para ambas partes de la relación laboral. No obstante lo anterior, debemos aclarar que es imperativo que las medidas de control que vayan ser establecidas sean comunicadas previamente a los funcionarios, en atención al debido proceso y al principio de seguridad jurídica.

Asimismo, consideramos inválidas las cláusulas que se incluyan en los contratos de trabajo, tendientes a que el trabajador consienta el acceso del patrono a su correo electrónico, pues encubren una afrenta al principio de irrenunciabilidad de derechos.

La inobservancia a la impenetrabilidad de las comunicaciones, puede tener sendas repercusiones en el campo laboral, civil y penal. En lo que atañe a este último, nuestro Código Penal tutela una serie de delitos contra el ámbito de la intimidad, dentro de los cuales se encuentra el de Violación de Comunicaciones Electrónicas, en el que encontraría adecuación típica una eventual intromisión en el contenido de un correo electrónico.

Pese a no hallar fallos donde se ventilaran delitos similares al expuesto, sí analizamos pronunciamientos extranjeros en materia laboral referente a intromisiones ilegítimas del patrono en el correo electrónico de sus subordinados, siendo el apoyo y respeto al secreto de las comunicaciones el criterio predominante, por encima pero no excluyendo las facultades patronales de control y fiscalización.

En Costa Rica, únicamente tenemos noticia de una sentencia judicial en la cual se trató el tema del correo electrónico, la cual, sin embargo, abre una brecha que muy probablemente seguirán los posteriores conflictos referentes a este tópico. En dicho pronunciamiento, es fácil observar el conflicto planteado

en este trabajo, sea por un lado, el derecho a la intimidad del trabajador en sus diferentes expresiones y, por otra parte, la facultad de control del patrono en el ejercicio de su actividad; todo ello visible en la ajustada votación de los señores Magistrados de tres votos contra dos.

Así, consideramos que en dicho caso se estimó acertadamente que, pese a la existencia de la falta, la misma no revestía la gravedad que la empresa le confirió, en razón de las circunstancias en que la misma aconteció, por lo que el despido resultaba desproporcionado en relación al hecho cometido; lo que constituye una franca aplicación de la teoría gradualista. En este orden de ideas, es imprescindible en cada hecho concreto calificar la conducta del trabajador, ya que la utilización del correo electrónico con fines personales no es motivo suficiente para que genere, por sí mismo, el despido del empleado, sino que debe ser una infracción reglada, grave, culpable y sancionable.

Sin embargo, es claro que la sentencia no analizó la forma en que la compañía se impuso del contenido del *e-mail* enviado por el empleado. A este respecto, observamos que en las redes corporativas todo está controlado desde la posición del *webmaster*, figura que es o puede ser consciente del contenido del correo en todo momento, lo que se le facilita además por su formación técnica. Por tanto, al administrador de la red debe prestársele especial atención a efecto de que no incurra en violaciones al derecho a la intimidad y, más específicamente, al secreto de las comunicaciones.

En esta tesitura, es notoria la existencia de aplicaciones informáticas que violentan la intimidad del usuario en la utilización del correo electrónico, así como también de programas que la protegen. En el primer supuesto, hay sistemas que permiten vislumbrar mediante imágenes la forma en que el empleado labora, e inclusive leer y rastrear los correos que ingresan al servidor de la empresa. Por el contrario, existen herramientas de cifrado que suministran confidencialidad a la comunicación electrónica, además de mecanismos como la firma electrónica y los certificados digitales, que confieren un alto grado de autenticación a los mensajes; situación esta última sobre la cual existe un Proyecto de Ley en nuestra Asamblea Legislativa.

Por otro lado, en lo que se refiere específicamente al Sector Público, es claro y congruente con todo lo expuesto, que la Administración ostenta facultades de fiscalización sobre los funcionarios, que le posibilitan verificar la diligencia del trabajador en sus labores y el uso que le da a los bienes de la institución -los cuales ostentan el carácter de públicos-, así como constatar que no se difiera la utilización del tiempo laboral para la realización de actividades de índole personal. Lo anterior, dado que conductas de esta naturaleza atentan contra la eficacia y la eficiencia de la gestión pública, principios fundamentales de la organización administrativa.

El aparato estatal debe apegarse al principio de legalidad, tutelado en el artículo 11 de la Ley General de la Administración Pública, lo que implica que

debe actuar sometido al ordenamiento jurídico, no pudiendo realizar más actos que aquellos que le estén expresamente autorizados. Es por ello, que ante la imperiosa necesidad de regular la utilización del *e-mail*, tanto el Ministerio de Hacienda como otras instituciones públicas, se vieron en la obligación de dictar un instrumento que le brindara validez y eficacia a sus actuaciones, siendo en el caso de dicho Ministerio la Política de Uso de Internet y Correo Electrónico.

La Política en cuestión, se encarga de regular principalmente lo referente al objetivo, alcance, utilización, prohibiciones, mecanismos de control y correspondientes sanciones, a que los funcionarios de la institución se ven sometidos al utilizar el servicio de correo electrónico. Asimismo, dicho instrumento normativo respeta la vasta cantidad de conceptos y garantías que hemos expuesto y que han quedado diseminadas a lo largo de nuestra investigación.

En tal sentido, debemos destacar tres aspectos: en primera instancia, que la disposición fue comunicada a los funcionarios de la entidad previamente a su aplicación y vigencia, cumpliendo con el debido proceso y brindando seguridad jurídica a los empleados; en segundo término, que expresamente se consigna que la administración de la red no ejerce control sobre el contenido de la información que pase por dicha red, quedando ésta bajo la responsabilidad del funcionario que la utilice, aunque advierte a su vez de la existencia de controles para detectar usos indebidos, es decir que la actividad fiscalizadora se realiza

sin violentar el secreto de la comunicación. Finalmente, rescatamos la gradualidad en la imposición de las sanciones, sin ser excluyentes de eventuales responsabilidades en ámbitos distintos del administrativo.

5.2.- RECOMENDACIONES

Tal y como se señaló en el Capítulo III, nosotros estimamos conveniente reformar algunos de los numerales de la actual Política Sobre Correo Electrónico del Ministerio de Hacienda, con la finalidad de solventar aspectos ambiguos de la misma. Las referidas modificaciones brindarían mayor seguridad jurídica tanto a la parte patronal como a los funcionarios del ente ministerial, lo que redundaría en una mejoría de las relaciones laborales.

De igual manera, planteamos de manera esquemática, un procedimiento para la emisión de eventuales reformas, comunicación de las mismas a los empleados y revisiones periódicas para analizar los resultados alcanzados.

i) Reformas

a) En el acápite 4.2 Usos Aceptables, punto primero, consideramos que debe incluirse la palabra público, a efecto de cubrir la totalidad de las actividades y no limitarlas a las de índole privado, ya que perfectamente un órgano del Estado

puede verse beneficiado de una práctica comercial, y ello igualmente va en perjuicio del buen funcionamiento de la red. Además, consideramos importante incluir de manera expresa que el listado no es de carácter taxativo, para posteriormente no tener problemas de adecuación típica con conductas que se encuentran fuera del listado. En tal sentido, proponemos la siguiente redacción:

“Queda prohibido el uso de los recursos de internet y correo en los siguientes aspectos:

- e) Cualquier actividad que sea lucrativa o comercial de carácter individual, privado, público, o para negocio particular (...)*

El anterior listado no es de carácter taxativo, por lo también será considerado como uso inaceptable cualquier otra conducta que atente contra la moral, el orden público, los intereses institucionales, credos religiosos y la buena marcha de los sistemas informáticos.”

b) En el apartado 5.1 Administración de la red, punto primero, estimamos conveniente para una mayor claridad y tutela, estipular que las medidas de monitoreo y control se ejercen tomando en consideración los derechos constitucionales de los empleados. Así, planteamos la siguiente redacción:

“a) La administración de la red, de la Dirección General de Informática, no

ejerce control sobre el contenido de la información que pase por la red, o de quien la utilice, quedando bajo la responsabilidad del funcionario que la accese o la utilice. No obstante lo anterior, la administración pondrá en funcionamiento herramientas de control que posibilitan analizar y detectar usos indebidos, por lo anterior se advierte que el contenido de la información es monitoreada y sujeta a controles y reportes sobre el uso; lo cual no obstante se realiza observando las garantías constitucionales de los funcionarios.”

c) En el acápite 5.2 Prohibiciones, creemos conveniente incluir en el punto cuarto, dos conductas que no se encuentran expresamente contempladas, como son la usurpación de la personalidad y las acciones que conlleven acciones discriminatorias; así como también dejar constancia de que la lista que se describe no es de carácter taxativo. En tal sentido, estimamos conveniente que la disposición se redacte en los términos siguientes:

“d) Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, usurpar la personalidad, realizar actuaciones que conlleven acciones discriminatorias, o interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas del Ministerio (...)

El anterior listado no es de carácter taxativo, por lo también será considerado como prohibida cualquier otra conducta que atente contra la moral, el orden

público, los intereses institucionales, credos religiosos y la buena marcha de los sistemas informáticos.”

d) En el apartado 6. Sanciones Aplicables, creemos prudente realizar modificaciones en los puntos uno y dos, con la finalidad de integrar a las normas que las sanciones contempladas no son excluyentes de responsabilidades de otro tipo; además de precisar las disposiciones cuyo incumplimiento acarrea la suspensión del servicio de correo, a efecto de evitar eventuales problemas de tipicidad. En esta tesitura, planteamos el cambio de la siguiente manera:

“a) La Dirección General de Informática determinará la aplicación de la suspensión de acceso a los servicios, en atención al tipo de contravención al presente documento, las cuales serán cumplidas inmediatamente, sin perjuicio de eventuales responsabilidades civiles y/o penales

b) El incumplimiento de las disposiciones establecidas en los puntos 4.2 Usos Inaceptables y 5.2 Prohibiciones, podrá acarrear la suspensión del servicio de la siguiente forma (...)”

ii) Procedimiento para la emisión de reformas

a) En primer término, la modificación pretendida debe ser analizada y revisada por el área legal del Ministerio, en un plazo no mayor a los 15 días hábiles

después de recibida.

- b) Posteriormente, el documento debe ser examinado por los jefes del Ministerio y por los personeros de los grupos sociales organizados de mayor representatividad; ello en un término que no exceda los 15 días hábiles.
- c) El área legal en coordinación con un representante del señor Ministro, procede al estudio e incorporación de las observaciones que correspondan.
- d) Las reformas operadas a la Política deben ser emitidas.
- e) Finalmente las reformas, atendiendo al principio de seguridad jurídica, deben ser Publicadas en el Periódico Oficial La Gaceta.

iii) Procedimiento para la Comunicación de las Reformas a los Funcionarios

- a) El área legal debe coordinar con el Departamento de Recursos Humanos, a efecto de notificar a los funcionarios las modificaciones operadas a la Política.
- b) El Jefe de cada área notificará personalmente y mediante listados a sus subalternos, quienes estamparán su rúbrica dándose por enterados. Las listas indicadas serán remitidas al Departamento de Recursos Humanos para su guarda y custodia.
- c) Los artículos reformados, o la Política íntegra conteniendo las modificaciones realizadas, debe exhibirse en lugares visibles del Ministerio.
- d) En caso de que algún empleado, sin razón fundada, se negara a firmar la constancia de notificación, se procederá a suspenderle el servicio de correo

electrónico.

iv) Revisiones de la Política

a) Deben establecerse reuniones trimestrales entre el área legal, el Departamento de Recursos Humanos, un representante de los grupos organizados y un representante del Ministro, para evaluar el impacto (beneficios, perjuicios, reacciones) que han generado las reformas efectuadas a la Política, así como también para analizar la casuística que se vaya presentando.

b) Asimismo, pero con una periodicidad semestral, es imperativo efectuar reuniones para analizar la vigencia de la Política de acuerdo a las condiciones del entorno, con el fin de determinar si el documento normativo deviene aplicable o, por contrario, necesita nuevos cambios para adaptarlo a las necesidades Ministeriales y a la legislación actual.

BIBLIOGRAFÍA

A) LIBROS

Cesario R. (2001). *Hábeas Data*. Buenos Aires: Editorial Universidad.

Fayos A. (2000). *Derecho a la Intimidad y Medios de Comunicación*. Madrid: Centro de Estudios Políticos y Constitucionales.

Godínez A. – Compilador –. *Límites al Derecho a la Intimidad de los Trabajadores*. San José: Poder Judicial.

Hernández R., Fernández C. y Baptista P. (2003). *Metodología de la Investigación*. México: Editorial Mc Graw Hill.

Méndez C. (2001). *Metodología. Diseño y desarrollo del proceso de investigación*. México: Editorial Mc Graw Hill.

Pierini A., Lorences V. y Tornabene M. (2002). *Hábeas Data*. Buenos Aires: Editorial Universidad.

Rubio de Medina M. (2003). *El Despido por Utilización Personal del Correo Electrónico*. Barcelona: Editorial Bosh.

B) REVISTAS

Chirino A. (1991). *Informática y Derecho a la Intimidad, Perspectivas de Política Criminal. Revista Judicial, Año XVI, No. 53, 133-173.*

C) DICCIONARIOS

Cabanellas G. (2000). *Diccionario Jurídico Elemental.* Argentina: Editorial Eliasta.

Real Academia Española (1992). *Diccionario de la Lengua Española.* Madrid: Editorial Espasa Calpe.

D) CONSTITUCIÓN POLÍTICA

Constitución Política de la República de Costa Rica de 7 de noviembre de 1949.

E) TRATADOS INTERNACIONALES

Convención Americana Sobre Derechos Humanos. Ley No. 4534 de 23 de febrero de 1970.

Convenio Europeo para la Protección de los Derechos Humanos y Libertades

Fundamentales, de 4 de noviembre de 1950. Ratificado por España con fecha 26 de septiembre de 1979, y publicado en el Boletín Judicial del Estado de 10 de octubre de 1979. Recuperado el 2 de septiembre de 2004, de http://www.ruidos.org/Normas/Conv_europeo_dchos_hum.htm

Declaración Americana de los Derechos y Deberes del Hombre. Aprobada en la Novena Conferencia Internacional Americana Bogotá, Colombia, 1948. Recuperado el 2 de septiembre de 2004, de <http://www.oas.org/SP/PROG/pg19-23.htm>

Declaración Universal de Derechos Humanos. Adoptada y proclamada por la Resolución de la Asamblea General 217 A (iii) del 10 de diciembre de 1948. Recuperado el 2 de septiembre de 2004, de <http://www.un.org/spanish/aboutun/hrights.htm>

Pacto Internacional de Derechos Civiles y Políticos. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. Recuperado el 2 de septiembre de 2004, de http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm

F) CÓDIGOS

Código Penal, Ley No. 4573 de 8 de noviembre de 1971.

Código de Trabajo, Ley No. 2 de 26 de agosto de 1943.

G) LEYES

Ley General de la Administración Pública, Ley No. 6227 de 2 de mayo de 1978.

Ley Sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso No Autorizado, Legitimación de Capitales y Actividades Conexas. Ley No. 8204 de 26 de diciembre del 2001.

H) POLÍTICAS

Ministerio de Hacienda (2002). *Política de Uso de Internet y Correo Electrónico.*

I) DICTÁMENES

Procuraduría General de la República (2003). *Dictamen C-003-2003 de 14 de enero de 2003.*

J) INTERNET

Abad L. *La Lucha por la Intimidación en Internet.* Recuperado el 4 de agosto de

2003, de <http://ucm.es/info/cyberlaw/actual/9/leg04-09-01.htm>

Asociación de Internautas. *El Uso del Correo Electrónico Particular en Horas Laborales Divide a los Jueces*. Recuperado el 4 de agosto de 2003, de <http://www.internautas.org./article.php?sid=654>

Asociación de Internautas (2000). *Primeros Resultados de la Campaña a favor de la Inviolabilidad de los E-mails*. Recuperado el 11 de agosto de 2003, de <http://www.internautas.org/NOTICIAS/DIC00/08.htm>

Baquía (2001). *Protección Suprema para el Correo de los Empleados Franceses*. Recuperado el 4 de agosto de 2003, de <http://www.baquia.com/com//20011004/not00005.html>

Camas F. (2003). *La Intimidación y la Esfera Privada del Trabajador ante las Nuevas Modalidades de Control y Vigilancia de la Actividad Laboral*. Recuperado el 4 de agosto de 2003, de <http://www.uned-terrassa.es/agenda/Camas.doc>

Castañeda J. (2000). *¿Puedes Abrirme el Correo?*. Recuperado el 11 de agosto de 2003, de <http://www.baquia.com/com/20001221/art00032.print.html>

Gimeno A. (2000). *Despido Procedente por E-Mail*. Recuperado el 11 de

agosto de 2003, de <http://www.internautas.org/NOTICIAS/NOV00/27C.htm>

Jaén M. – Compilador – (2002). *Revista Electrónica de Ciencia Penal y Criminología*. Recuperado el 11 de agosto de 2003, disponible en <http://www.criminet.ugr.es/recpc.com>

Novatica (2001). *Proposición de Ley Sobre Uso del Correo Electrónico en la Empresa*. Recuperado el 11 de agosto de 2003, de <http://www.ati.es/novatica/2001/151/docs151.pdf>

Villahermosa A. (2002). *Apuntes Sobre El Correo Electrónico en la Empresa*. Recuperado el 4 de agosto del 2003, de <http://www.delitosinformaticos.com/ciberderechos/usocorreo2.shtml>

K) RESOLUCIONES JUDICIALES COSTARRICENSES

Sala Constitucional. *Acción de Inconstitucionalidad No. 1174-V-92, Voto No. 3308-94, de las 14:57 horas del 5 de julio de 1994.*

Sala Segunda de la Corte Suprema de Justicia. *Resolución 2003-00797 de las 15:00 horas del 18 de diciembre del 2003, Recurso de Casación interpuesto por O.B.C.*

ANEXOS

MANUAL DE POLÍTICAS

NORMAS Y POLÍTICAS EN EL USO DE SERVICIOS DE CORREO Y ACCESO A INTERNET

CÓDIGO PL-03

Setiembre del 2002

1. OBJETIVO

Desde al año 1999, la Dirección General de Informática estableció las “Políticas de uso de Internet y Correo Electrónico”, las cuales fueron comunicadas a todos los funcionarios del Ministerio y que contienen políticas y normas de uso del servicio de correo e Internet .

El objetivo de la política es la de regular el uso de los servicios de correo y el acceso a Internet, para lo cual emite los siguientes lineamientos que son de cumplimiento obligatorio para todo el personal que utilice los recursos de la red.

2. ALCANCE

La Dirección General de Informática considera indispensable regular el uso de los servicios de correo y el acceso a Internet, para lo cual emite los siguientes lineamientos, que son de cumplimiento obligatorio para todo el personal que utilice los recursos de la red.

Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y reglamentos que han adquirido para el uso del correo y el acceso a Internet, tomando todas las medidas que correspondan para que éstos normas se respeten y se cumplan, ya que Internet es una ventana al mundo y debe ser cuidadoso su manejo. Para facilitar el uso, se incluye en este texto un enfoque al comportamiento que las organizaciones y los individuos deben tomar y adaptar para su apropiado uso. Los usuarios deben estar consientes de que no importa quien les brinde el acceso a Internet, se tienen regulaciones acerca del uso, del correo electrónico y los archivos, acerca de lo que es correcto colocar y enviar, y cómo presentarlo.

El uso de la red y recursos de información del Ministerio, están disponibles para fortalecer el flujo de información interna, la investigación en materia tributaria, administrativa, educativa y apoyar a las diferentes tareas encomendadas para mejoramiento de nuestras labores. Todos los usuarios de la red están sujetos a esta política y a los términos de este manual, y a una actuación con altos principios morales y éticos al utilizar los recursos del Ministerio, el uso inapropiado de la red será sancionado con la eliminación del acceso a estos recursos y puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

La utilización de los recursos de red y de información, a través de las facilidades que provee la Dirección de Informática, está abierta a todas las dependencias del Ministerio que lo justifiquen y a otras personas a las que el Ministerio desee extender los privilegios de acceso, dadas las condiciones de disponibilidad de recursos y servicios.

El uso de los recursos deberá tomar en cuenta que se guarden las medidas de seguridad que garanticen la integridad de los sistemas de cómputo, ya instalados y su accesabilidad por otros, para hacer el trabajo eficiente y productivo.

3. ABREVIATURAS Y DEFINICIONES

INTERNET: Internet es una gran comunidad de computadoras conectadas entre sí, por medio de líneas de comunicaciones especiales, la cual oscila entre 30 millones de usuarios permanentes o esporádicos y se extiende a lo largo de 170 países, agrupando una gran cantidad de asociaciones y empresas.

WORLD WIDE WEB: También llamado WWW o simplemente "el web", este servicio de Internet es el más ampliamente difundido. De hecho muchas personas

piensan en el web e Internet como un sinónimo, y no se dan cuenta que "el web" es una entidad que corre en el Internet. La característica más importante de los documentos WWW es que están enlazados con otros documentos por medio de hipertexto. El hipertexto permite enlazar documentos con sólo hacer un click con el ratón.

WEB BROWSER: Un browser es un programa que provee una interfase para acceder y ver archivos en Internet. Antes de que existieran los browsers, se necesitaba saber una serie de complicados comandos para ver los recursos en el Internet. Los browsers básicamente hicieron el Internet más amigable y fácil de usar.

FILE TRANSFER PROTOCOL(FTP): FTP es un servicio heredado del Internet, pero todavía es ampliamente utilizado para hacer algunos tipos de información disponibles. Básicamente FTP es un protocolo de Internet usado para transferir información y/o documentos de una computadora a otra.

CORREO ELECTRÓNICO: El correo electrónico E-mail es una forma grandiosa de comunicarse por una red o por el Internet. El correo electrónico puede existir en una red de cualquier tamaño. Después del Web, posiblemente el correo electrónico sea el servicio de mayor uso en el Internet.

INTRANET: Una Intranet, es una red que utiliza tecnología de Internet aplicada a una red interna con la diferencia que el contenido sólo está disponible internamente, en la red de área local.

4. RESPONSABILIDAD

Es responsabilidad de todo funcionario del Ministerio de Hacienda., cumplir con las normas y procedimientos establecidos en este documento para acceso a los servicios de correo y de Internet

4.1 Usos Aceptables

Los servicios de correo electrónico y accesos a Internet se disponen para los siguientes tópicos :

- Comunicación entre investigadores, economistas y personas relacionadas con las labores desempeñadas en el ámbito nacional y extranjero, siempre y cuando exista un intercambio mutuo y en condiciones recíprocas.
- Comunicación e intercambio con la comunidad académica, universitaria u otras instituciones con el fin de tener acceso a los últimos avances relacionados con la especialidad o tareas desempeñadas
- Anuncios o servicios nuevos para el uso de los usuarios en general, pero no para publicidad de tipo comercial o personal alguno.
- Comunicación entre instituciones o empresas privadas siempre y cuando estén vinculadas con las tareas encomendadas.

- Actividades de capacitación por medio virtuales o en línea.

4.2 Usos Inaceptables

Queda prohibido el uso de los recursos de Internet y correo en los siguientes aspectos :

- Cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular.
- Acceso a lugares obscenos, que distribuyan libremente material pornográfico, o bien materiales ofensivos en perjuicio de terceros.
- Acceso a lugares recreativos, deporte, música, chistes, entre otros.
- Utilización de los servicios de correo para envío de información personal, chistes, pensamientos y cualquier otra información que no sea de carácter laboral.

5. CONTROL DEL USO DEL SERVICIO

5.1 Administración de la red.

- La administración de la red, de la Dirección General de Informática, no ejerce control sobre el contenido de la información que pase por la red, o de quien la utilice, quedando bajo la responsabilidad del funcionario que la accese o la utilice. No obstante lo anterior, la administración pondrá en funcionamiento herramientas de control que posibilitan analizar y detectar usos indebidos, por lo anterior se advierte que el contenido de la información es monitoreada y sujeta a controles y reportes sobre el uso.
- La administración de la red de la Dirección General de Informática, no da garantías de ningún tipo, sea expresa o implícitamente, para el servicio que provee, por lo que no existirá ninguna responsabilidad por cualquier daño que el usuario sufra causado por negligencia propia o los errores u omisiones de sus usuarios.
- Cualquiera que acceda a otras redes nacionales o internacionales por medio del nodo del Ministerio debe acatar las reglas que rijan las mismas.
- Corre por cuenta o riesgo del usuario cualquier información obtenida por medio del servicio de comunicaciones del nodo de Internet .
- Los mensajes que se envíen vía Internet, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, así como de ninguna otra institución.
- La Dirección General de Informática, tiene la autoridad para controlar y negar el acceso a cualquier funcionario que viole las políticas o interfiera con los derechos de otros usuarios. También tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.
- La Dirección General de Informática, utilizará herramientas de monitoreo del uso de los

recursos, por lo cual podrá establecer controles de acceso a sitio y de envío de información masivamente por la red.

- La Dirección General de Informática enviará reporte del uso del servicio de correo o Internet a las Jefaturas respectivas, para que tomen medidas tendientes a mejorar su utilización .
- La demanda de servicios puede ocasionalmente exceder la disponibilidad, por lo que serán establecidas las prioridades, dando la más alta prioridad a las actividades consideradas más esenciales para llevar a cabo la misión del Ministerio.
- El administrador de la red monitorea en forma automática los sitios visitados por los funcionarios, por lo cual se advierte que se aplicaran las sanciones establecidas por el acceso indebido.

5.2 Prohibiciones:

- La transmisión de materiales en violación de cualquier regulación, queda prohibida. Esto incluye, pero no se limita, a materiales con derechos de propiedad intelectual, materiales que legalmente se consideren amenazantes u obscenos. Lo anterior en cumplimiento con el Decreto N° 29915-MP Prohibiciones Material Pornográfico-Equipo Electrónico-Reglamento Autónomo de Servicio-Dirección General de Servicio Civil .
- Queda prohibido el envío de información en forma masiva a todo el Ministerio o Grupos de usuarios, por lo cual se restringe su uso en forma automática.
- Debido al alto nivel de seguridad con el que se debe de contar en el Ministerio, las claves de acceso al servidor de WEB y correo electrónico deberán de ser estrictamente confidenciales y personales. Además de censurar la visita de páginas en la red dedicadas a áreas que no sean de interés investigativo, capacitación, económico, legal, o del área de competencia, o bien que simplemente se haga mal uso de los recursos para acceder información no relacionada con el área de trabajo.
- Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar, insultar o acosar a otras personas, interferir con el trabajo de los demás provocando un ambiente de trabajo no deseable dentro del contexto de las políticas del Ministerio.
- Utilizar los recursos del Ministerio para ganar acceso no autorizado a redes y sistemas remotos.
- Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas.
- Monopolizar los recursos en perjuicio de los otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones voluminosas, uso de recursos de impresión no autorizado.
- Poner información en la red que infrinja los derechos de los demás.
- Utilizar los servicios de red para juegos a través del servicio de Internet o Intranet.
- Utilizar los servicios de red para ver publicaciones de deportes.

- Utilizar los servicios de red para ver publicaciones de pornografía.
- Utilizar los servicios de red para enviar archivos que sean confidenciales.
- La exhibición de material pornográfico en cualquier lugar de la institución utilizando el equipo de cómputo y/o los servicios de comunicación de la institución, asimismo el uso de equipo electrónico del Estado para observar o reproducir pornografía. El incurrir en el incumplimiento de esta normativa. acarrea una falta grave que será sancionada según las regulaciones vigentes.
- Envío de mensajes masivamente a todos los usuarios de la red o segmentos, iniciación y facilitaciones de cadenas y creación de procesos de discusión y contestación.
- Envío de correos en donde se solicitan ayudas a personas o grupo de personas, este tipo de mensajes únicamente serán permitidos si son canalizados por medio de Centro Virtual de Conocimiento Hacendario.

5.3 Uso del Correo electrónico

- **PRIVACIDAD DE CORREO:** Todos los usuarios tienen derecho a la privacidad del correo electrónico, cuando éste es usado para fines de trabajo, teniendo en mente que el uso del correo es para efectuar labores, en la especialidad que tenga dicha persona.
- **SEGURIDAD DE CORREO:** En caso que otra persona quiera contactar a una persona que no lo ha solicitado, debe notificar el hecho a la D.GI., dado que todos los usuarios deben estar conscientes de que existe material y servicios que pueden ser ofensivos a grupos o personas.
- **LIBERTAD DE EXPRESIÓN:** La red está abierta a la expresión libre de ideas y puntos de vista, que tengan relación con las actividades de cada individuo en el Ministerio; no obstante lo anterior, queda prohibido el envío de correos masivos y discusiones por medio de envío de correo .

5.4 Para regular el uso se establecen los siguientes lineamientos que son de acatamiento obligatorio:

a- Lectura de Correo

- Leer el correo frecuentemente, al menos una vez al día .
- Es obligatorio la utilización de carpetas personales para almacenar la información del correo que ingresa y que desea conservar.
- Si no tiene tiempo de contestar los mensajes completamente, envíe un breve mensaje de forma tal, que la persona que le envió el mensaje sepa que usted lo recibió.
- Elimine mensajes innecesarios.
- Mantenga los mensajes relacionados en carpetas aparte dentro de las carpetas personales.
- Seleccione la opción de eliminar mensajes cuando sale de Exchange o Outlook.

b- Envío de Correo

- Intente enviar mensajes bien formateados. Las personas que reciben mucho correo

pueden no leer un mensaje mal formateado. No utilice letras en MAYÚSCULA, esto es considerado como gritar.

- No utilice tabuladores ya que mucho software administrador de correo no entiende este tipo de caracteres, lo que puede acarrear basura en el mensaje original.
- Utilice el campo asunto dentro del mensaje.
- No utilice las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante. Es innecesario, la mayoría de las veces provoca mucho tráfico en la red.
- Recuerde que los lectores del mensaje no pueden ver su cara o escuchar su voz, todas las expresiones deben ser palabras o signos de puntuación. Evite ser sarcástico y utilice comillas cuando sea necesario.
- No envíe mensajes a gente que no conoce, a menos que exista una razón de peso de por medio.
- No envíe mensajes ofensivos, abusivos, etc.
- No envíe mensajes a todo el personal del Ministerio o dependencia, a menos que sea un asunto oficial que involucre a toda la institución. Se advierte que esta prohibido el envío de mensajes masivos que no estén debidamente autorizados o que se trate de asuntos oficiales.
- Antes de enviar el mensaje revise el texto que lo compone y los destinatarios. Esto con el fin de corregir errores de ortografía, forma o fondo.
- Cada buzón de correo tiene un máximo de 8 MB de espacio disponible, tomando en cuenta los mensajes ubicados en las diferentes carpetas de la casilla de correo (bandeja de entrada, elementos enviados, elementos eliminados y cualquier otra carpeta creada en su buzón), una vez que este espacio es consumido, no será posible enviar un mensaje hasta que libere el espacio del buzón.

c- Autofirmas

- Su firma debe ser breve e informativa (no mayor de tres líneas), pueden utilizarse aspectos intelectuales.
- Nunca incluya su dirección de correo en la firma, ya que ésta fue incluida en la parte superior del mensaje.
- La idea de una autofirma es útil, pero debe usarse solamente cuando es necesario. Usualmente es mejor firmar los mensajes con un conjunto de palabras amistosas.

d- Reenvío de Mensajes

- Cuando se reenvía un mensaje, incluya el mensaje original, para que la o las personas, hacia las que va el mensaje, conozcan de que se está hablando en un momento dado.
- En muchas ocasiones se utiliza un mensaje para entremezclar una respuesta, eliminando las partes que son irrelevantes. Es altamente recomendable incluir el mensaje original, tal y como fue recibido.

- Su correo marca el mensaje original por medio del signo mayor ">" o bien por medio de otro color de letra.

e- Cadenas de Mensajes

- No envíe ni sea parte de una cadena de mensajes, esto es considerado ilegal y puede acarrear la desactivación de la casilla, aunque no haya sido usted la persona que comenzó con la cadena.

f- Listas de Correos

- Queda prohibido el envío de mensajes con adjuntos a grupos de usuarios de la institución, únicamente podrán realizarlo los funcionarios debidamente autorizados.
- Si se siente ofendido por un mensaje no lo responda inmediatamente, envíe el mensaje hacia el administrador de correo, con el fin de tomar las acciones respectivas.
- No haga que un tema de discusión se convierta en otro tópico. Si así lo desea comience con otro mensaje.
- No se suscriba a listas de amigos por Internet, esto provoca que gran cantidad de mensajes lleguen a su casilla de correo provocando saturación.

g- Tamaño de los mensajes

- El tamaño de los mensajes adjuntos no debe exceder de los 500 KB, este tamaño puede ser chequeado por medio de las propiedades de cada archivo, desde el Explorador de Windows o seleccione el archivo y presione ALT+ENTER para ver el tamaño.
- Si el adjunto excede los 500 KB, debe ser compactado, para ello el Centro de Atención de Usuarios, ofrecerá las instrucciones del caso por medio de una carpeta pública, en el cual se ubicará el software necesario, así como un manual con instrucciones básicas de uso.
- Si el mensaje aún compactado excede este tamaño puede enviar el mensaje; una vez que el mensaje sea enviado, el mismo debe ser eliminado de la casilla de enviados, ya sea borrando el mensaje del todo o bien pasándolo a las carpetas personales.

h- Antivirus

- Desconfíe de todos los mensajes que vengan de Internet pues pueden estar infectados con virus, por lo cual las opciones dentro del antivirus deben de activarse de tal forma que se chequeen todos los archivos aún los que se encuentren compactados y que la acción que debe de seguirse, sea la de eliminar el virus automáticamente.
- Si el mensaje que se detecta tiene un virus que no puede ser removido, entonces el mensaje no debe ser salvado o abierto y debe ser eliminado por completo.
- Se debe chequear, en forma constante, la máquina para evitar virus al momento de enviar documentos adjuntos
- Cada usuario es responsable por los adjuntos que envía, se tomarán las medidas

respectivas en caso de que un mensaje sea enviado con virus, es responsabilidad de cada funcionario tomar las medidas para evitar el contagio.

- El chequeo diario de virus en el correo se hará para todas las casillas en el servidor de correo, tratando de limpiar todo mensaje contagiado, si el mensaje tiene virus y no puede ser eliminado el mensaje será borrado del correo.

i- Vigencia de los mensajes

- Los mensajes tendrán una vigencia de 30 días, desde la fecha de entrega o recepción de los mismos. Todos los mensajes anteriores a un mes serán eliminados en forma automática, permanentemente del servidor de correo.
- Si desea mantener un mensaje, en forma permanente, se debe almacenar en una carpeta personal, en la maquina del usuario.

J- Envío de correo Institucional o por dependencia.

- El envío de mensajes a todo el personal del Ministerio o dependencia se autoriza únicamente para asuntos oficiales.
- Queda prohibido el envío de mensajes masivos, que no estén debidamente autorizados o que no se trate de mensajes oficiales.
- Para evitar el abuso y exceso de tráfico en la red, lo cual representa un costo de la entrega del mensaje y que es compartido entre el que lo manda y quien lo recibe, se prohíbe el envío de correo por grupo de usuarios y para lo cual se restringe el uso, estableciendo los siguientes procedimientos:
 - ⇒ Únicamente están autorizados para el envío de correos a todo el personal del Ministerio y de la dependencia a su cargo, las autoridades superiores, gerenciales (Ministro, Viceministros, Oficial Mayor, Directores de Programa y Subprograma), los funcionarios debidamente autorizados por las autoridades superiores gerenciales y los servicios de información corporativas, entre ellos Centro Virtual de Conocimiento CEVCOH, CENTEC, CALL CENTER y GRUPO ANTIRIVUS
 - ⇒ Se establece como medio oficial de comunicación a todo el Ministerio, el Centro Virtual de Conocimiento Hacendario, el cual se encargará de divulgar los comunicados de carácter institucional , lo que realizará por medio del boletín emitido diariamente.
 - ⇒ Se establece que todo el material por divulgar, en forma institucional, debe de ser enviado mediante correo electrónico a la dirección cevcoh.hacienda.go.cr, la publicación del mismo se realizará en la mañana o en la tarde, estableciendo el siguiente horario para la recepción de la información: antes de las 12 :00 p.m., el material se publicará en el Boletín de la tarde y antes de las 5 :00 p.m., el material se publicará en el boletín de la mañana.
 - ⇒ EL CECVOH únicamente publicará aquel material cuyo contenido de los mensajes cumpla con la característica de ser mensajes oficiales y de carácter laboral

- ⇒ Tratándose de correo por dependencia tendrán acceso de envío los niveles directivos y gerenciales de cada Área, a saber: Ministro, Viceministros, Directores de Programa o Subprograma.
- ⇒ Para que los niveles de jefatura o funcionarios puedan enviar correo a todo el Ministerio o dependencia, deberán ser autorizados mediante el envío de una nota o correo electrónico, autorizado por el Ministro, Viceministros, Directores de Programa o Subprograma, con atención Ing. Roger Corazari; Jefe de Comunicaciones y Redes .
- ⇒ Las personas autorizadas serán responsables por el contenido de los mensajes a efecto que cumplan la característica de ser mensajes oficiales y de carácter laboral.

K-El correo electrónico es privado e individual.

- A menos que se utilice un dispositivo de encriptación (hardware o software), se debe asumir que el correo en el Internet no es seguro. Nunca ponga en un mensaje de correo información que no ponga en un sobre.
- Respete los derechos de autor en el material que reproduzca. Casi todos los países incluido el nuestro, tienen leyes para los derechos de autor.
- Si está respondiendo a un mensaje no cambie la redacción. Si el mensaje era personal y usted los está mandando a un grupo, debería pedir permiso primero. Podría acortar el mensaje y resaltar las partes relevantes, pero asegúrese de dar las atribuciones pertinentes.
- Nunca mande cartas en cadena por medio de correo electrónico. Las cartas en cadena son prohibidas en el Internet. Los privilegios que tenga en la red serán revocados y posiblemente hasta se sancione. Se debe notificar al Administrador de Correo de la D.G.I si alguna vez recibe una carta en cadena.
- Una buena regla es: sea conservador en lo que mande y liberal en lo que reciba. No debería mandar mensajes "calientes" (llamados "flames") aunque sea provocado. No se sorprenda si recibe "flames" y es prudente no responderlas.
- En general, es una buena idea, por lo menos revisar todos los subjects antes de responder un mensaje. Así mismo asegúrese que los mensajes que responda vayan dirigidos a usted.
- Sea cuidadoso cuando direcciona su correo. Hay algunas direcciones que pueden ir a un grupo, pero la dirección parece la de una persona. Sepa a quién le manda el correo.
- No mande correo no solicitado, preguntando por información a personas cuyos nombres aparecen en RFC (Request for Comments) o en un campo de lista de correo.
- Recuerde que las personas con las que se comunica, están localizadas a través del mundo. Si manda un mensaje del cual quiere una respuesta inmediata, la persona que lo recibe podría estar en su casa durmiendo cuando llegue el mensaje. Déle la oportunidad de despertarse, llegar a su trabajo, e ingresar a la red antes de asumir que el correo no llegó o que no les importa.
- Verifique todas las direcciones antes de iniciar un discurso largo o personal. También es

una buena práctica incluir la palabra "Long" en el encabezado del asunto, para que la persona a la que envía el mensaje sepa que le va a tomar tiempo leerlo y responderlo. Más de 100 líneas es considerado "grande".

- Sepa a quien contactar por ayuda. Usualmente tendrá recursos cerca y a la mano. Además sepa a quien recurrir si recibe algo cuestionable o ilegal. Para ayuda en estos casos puede recurrir a la D.G.I.
- Escriba usando mayúsculas y minúsculas. En el Internet escribir sólo en mayúsculas es sinónimo de insulto.
- Use símbolos para enfatizar algo. Ejemplo: use asteriscos (*) para "ponerle" negrilla a una palabra o frase, use guión menor (_) para subrayado. Ejemplo: Esto *es* lo que quiero decir, _La guerra y la Paz_ es mi libro favorito.
- Limite el largo de las líneas a 65 caracteres y termine la línea con un retorno <ENTER>
- Los mensajes de correo deben tener un asunto que refleje el contenido del mensaje.
- Las expectativas para comportarse por medio de e-mail, dependen en las relaciones con una persona y el contenido de la comunicación. Las normas aprendidas en un ambiente de e-mail particular, no necesariamente aplican en general a los mensajes a través del Internet. Sea cuidadoso con los vulgarismos o acrónimos locales.
- El costo de la entrega del mensaje es compartido entre el que lo manda y quien lo recibe. Esta es una razón económica fundamental por la cual el correo no solicitado no es bienvenido (y prohibido en muchas formas).

6. SANCIONES APLICABLES.

- La Dirección General de Informática determinará la aplicación de la suspensión de acceso a los servicios, en atención al tipo de contravención al presente documento, las que serán cumplidas inmediatamente.
- El incumplimiento de las normas establecidas podrán acarrear la suspensión de servicio de la siguiente forma:
 - ⇒ Incumplimiento por primera vez de las normas y lineamientos establecidos, se suspenderá el servicio por quince días naturales.
 - ⇒ Incumplimiento de las normas y lineamientos por segunda vez, se suspenderá el servicio por un mes calendario
 - ⇒ Tercera vez de incumplimiento, se suspenderá el servicio por dos meses o suspensión permanente.
- Asimismo se establece que la acción de suspensión no impide que se establezcan procedimientos administrativos, para aplicar sanciones disciplinarias por el uso indebido del equipo electrónico y las telecomunicaciones en la institución.

A manera de ejemplo se incluyen algunas normas que regulan el uso adecuado de los servicios tecnológicos que dispone la institución:

- a) Capítulo IX de Prohibiciones, Artículo 23 del Reglamento Autónomo de Servicio y

Organización de la Dirección General de Servicio Civil, Decreto N° 25813-MP, publicado en La Gaceta N° 36 del jueves 20 de febrero de 1997,

“...inciso s) La exhibición de material pornográfico en cualquier lugar de la institución utilizando el equipo de cómputo y/o los servicios de comunicación de la institución, asimismo el uso de equipo electrónico del Estado para observar o reproducir pornografía. El incurrir en el incumplimiento de esta normativa. acarrea una falta grave que será sancionada según las regulaciones vigentes.....”

b) Ley 8131 de Administración Financiera de la República Presupuestos Públicos

Artículo 111 Delito Informático. “ Cometerán delito informático, sancionando con prisión de 1 a 3 años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:

-Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido

-Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.

-Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.

-Utilizar las facilidades del sistema para beneficio propio o de terceros...”

c- Reglamento Autónomo de Servicios – Ministerio de Hacienda

Artículo 115 “Respecto del servidor(a) que incurra en las causales que se dirán, sin perjuicio de cualquier otra prevista en las leyes y reglamentos de orden estatutario, laborales y en este reglamento, podrá acordarse la gestión de despido para que pueda ser removido de su puesto sin responsabilidad para el Estado.

Son causas justas las siguientes...

-Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos, diseñados para las operaciones de cualquiera de las dependencias del Ministerio, con cualquier propósito.

-Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos del Ministerio, para que otra persona los use.”

7. REQUERIMIENTOS PARA OBTENER SERVICIOS

Para que el personal del Ministerio pueda hacer uso del servicio de Internet e Intranet, es necesario que cumplan con los requerimientos siguientes:

7.1 Solicitud del Servicio.

La Dirección o Jefatura interesada deberá enviar la solicitud a la Dirección General de Informática, mediante el procedimiento establecido para tal efecto, se indica que es responsabilidad de cada jefatura el velar por el cumplimiento las normas establecidas. Asimismo es responsabilidad de la misma, notificar a la Dirección General de Informática, los cambios o movimientos del personal que autoriza, ya sea por traslados a otra dependencia , despido, renuncia entre otros.

7.2 Requisitos mínimos de hardware y software.

HARDWARE

Para que un computador tenga acceso a Internet/Intranet, será necesario que cuente con lo siguiente:

- CPU Intel Pentium III
- 64 MB de RAM
- 50 MB de espacio libre en disco.
- Video SVGA con soporte de 256 colores
- Multimedia (opcional)
- Tarjeta de red Ethernet 10/100 Base-T, interfase RJ-45
- Esta conectado en red con acceso a la Dirección General de Informática.
- UPS más infraestructura eléctrica adecuada.

SOFTWARE

Se deberá contar con el siguiente software instalado:

- Windows 98 o superior
- Internet Explorer, ú otros browser de WWW.

De no contarse con un browser, se le proporcionará uno de parte de la Dirección General de Informática

En caso que no contar con tarjeta de red y conexión a la red de Dirección General de Informática, se deberá realizar una solicitud, requiriendo la asignación de la dirección IP del usuario, indicando lo siguiente:

- Dependencia y nombre completo del solicitante.
- Justificación del servicio.
- Con el visto bueno de la Dirección, o del jefe inmediato superior.
- Ubicación exacta de la PC para poder determinar la cantidad de cable.

Posteriormente el equipo será evaluado por un técnico de la DGI, el cual hará un dictamen técnico del equipo por conectarse.

Es esencial para los usuarios reconocer su responsabilidad respecto del acceso a los servicios de correo y acceso a la red interna o por medio de Internet. Cada usuario es el responsable final de sus acciones cuando accede a los servicios disponibles.

RESUMEN DEL PROYECTO DE LEY DENOMINADO
LEY DE FIRMA DIGITAL Y CERTIFICADOS DIGITALES

EXPEDIENTE N° 14276

Principales aspectos de interés que contempla el proyecto:

Objetivo: Regular el uso y el reconocimiento jurídico de la Firma Digital, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, así como el autorizar al estado para su utilización. (Art. 1)

Diferencia entre los términos digital y electrónico: Digital se refiere a cualquier información codificada en dígitos, la cual resulta ser más precisa que el término electrónico, referente al medio físico de procesamiento, al almacenamiento o transmisión, el cual es uno de los medios para generar, transmitir y almacenar información digital. (Art. 3)

Firma digital: Es el conjunto de datos, anexos a otros datos o datos asociados funcionalmente, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. (Art. 2)

Firma digital avanzada: La Firma Digital Avanzada, siempre que esté basada en un certificado digital reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma digital, el mismo valor jurídico que la firma manuscrita en relación con los

consignados en papel. (Art. 5)

Uso de la firma y los documentos electrónicos por el Estado: Se autoriza a los Poderes Legislativo, Ejecutivo y Judicial, al Tribunal Supremo de Elecciones, Contraloría General de la república, Defensoría de los Habitantes, así como a todas las instituciones públicas descentralizadas, y **entes públicos no estatales** para la utilización de la Firma Digital avanzada y los documentos electrónicos firmados digitalmente en sus relaciones internas, entre ellos y con los particulares, de conformidad con las previsiones de esta Ley y su reglamento. (Art. 7)

Órgano rector de la Ley: Ministerio de Ciencia y Tecnología. (Art. 8)

Sistema de acreditación voluntario: El Poder Ejecutivo, a través del Ministerio de Ciencia y Tecnología, utilizará un sistema de acreditación voluntario, en el ámbito de los prestadores de servicios de certificación de Firma Digital Avanzada, coordinando para ello con la Autoridad de Acreditación, la cual será un ente con participación activa y equilibrada de los sectores involucrados. (Art. 9)

Certificado digital: Es la certificación digital que vincula unos datos de verificación de firma a un signatario y confirma su identidad. Los certificados de Firma Digital que sean emitidos por entidades no establecidas en Costa Rica, serán equivalentes a los otorgados por prestadores establecidos en el país, cuando hayan sido homologados por estos últimos, bajo su responsabilidad, y

reconocidos por la autoridad de acreditación competente y cumpliendo con los requisitos fijados en esta Ley, su reglamento y normas internacionales correspondientes. (Art. 2 y 12)

Acreditación e inspección de los prestadores de servicios de certificación digital:

Mediante la autoridad competente de acreditación, la cual estará adscrita al Ministerio Rector, las empresas que emitan certificados de Firma digital, deberán someterse al proceso de acreditación que se defina al respecto para estar debidamente acreditados. Las funciones de las empresas certificadoras serán entre otras, las de emitir o cancelar certificados digitales, así como brindar otros servicios inherentes al propio certificado. La Autoridad de Acreditación ejercerá la facultad de inspección sobre los prestadores acreditados. (Art. 13 y 14)

Requisitos de los dispositivos seguros de creación de Firma Digital para considerarse como tales:

- a) Garantizar que datos utilizados en la generación de firma puedan producirse solo una vez y asegurar razonablemente su secreto.
- b) Que exista seguridad razonable de que dichos datos no puedan ser alterados o falsificados.
- c) Que los datos de creación de firma puedan ser protegidos con

fiabilidad por el signatario.

- d) Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que este muestre al signatario antes del proceso de firma. (Art. 17)

Los dispositivos de verificación de Firma Digital avanzada deben garantizar al menos lo siguiente:

- a) Que la firma se verifique de forma fiable y el resultado de la verificación figure correctamente.
- b) Que el verificador pueda establecer de forma fiable la integridad de los datos firmados y detectar si han sido modificados.
- c) Que aparezca correctamente la identidad del signatario.
- d) Que se verifique de forma fiable el certificado.
- e) Que pueda detectarse cualquier cambio relativo a su seguridad e integridad. (Art. 18)

Asimismo, el artículo 19 estipula que las disposiciones de esta Ley no deberán entenderse en el sentido de prohibir la existencia de sistemas de Firma Digital basados en convenios expresos entre las partes, las que podrán a través de un contrato fijar sus derechos y obligaciones, y las condiciones técnicas y de cualquier otra clase, bajo las cuales reconocerán su autoría sobre un documento

digital o mensaje de datos que envíen, o la recepción de un mensaje de datos de su contraparte. (Art. 19).