PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE DERECHO

EL RÉGIMEN JURÍDICO DEL CONTROL INFORMÁTICO EJERCIDO POR LOS EMPLEADORES EN EL PERÚ

TESIS PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

FRANCISCO JAVIER ALVARADO ICAZA
CÓDIGO 19772075

OCTUBRE 2006

Índice

Introducción

Debido a la extendida aplicación de las tecnologías de la información en todos los ámbitos de la vida social, la información ha ido adquiriendo cada vez mayor valor y, en consecuencia, se ha hecho también cada vez más necesaria su protección. Así, en las organizaciones y empresas, los empleadores se ven en la necesidad de establecer controles y acciones de supervisión, para enfrentar los riesgos e inseguridades que hacen vulnerables sus sistemas de información.

Es en este ámbito en el que los empleadores ejercen las facultades de control y supervisión sobre sus recursos informáticos, basándose en el derecho de libertad de empresa que la Constitución Política del Perú les reconoce.

En ese sentido, los trabajadores, en su condición de usuarios de los recursos informáticos que les proporcionan sus empleadores para desarrollar actividades laborales, son responsables por los errores o infracciones que cometen en materia de seguridad de la información, y como tales, están sujetos a control y supervisión que eventualmente puede vulnerar sus derechos fundamentales como persona.

La investigación pretende reconocer el régimen jurídico que en el Perú sustenta la racional implementación de medios de control y supervisión de los recursos informáticos que el empleador proporciona a sus trabajadores. con el propósito de exponerla ante los profesionales del Derecho, de la información y de los trabajadores usuarios de dichos recursos; además de identificar aquellos límites que deberán respetar con relación a los derechos fundamentales de la persona del trabajador.

Desde las que se consideran como las primeras normas que regularon el uso de las tecnologías de la información y la comunicación en el mundo, la necesidad de proteger los derechos fundamentales, en especial el referido a la intimidad de las personas ha sido uno de los principales temas del derecho informático.

Más aún, cuando la doctrina jurídica reconoce como verdaderos derechos laborales aquellos que, atribuidos con carácter general a los ciudadanos son ejercitados en el seno de una relación laboral, los que han sido denominados por dicha doctrina como: derechos laborales constitucionales inespecíficos o derechos fundamentales de la persona del trabajador.

En el ordenamiento jurídico peruano existe ya una reglamentación para la elaboración y aplicación, por parte de tos empleadores, de normas de seguridad de la información dentro de sus organizaciones. Esta es la norma técnica peruana ISO/IEC 17799:2004 «Código de

buenas prácticas para la gestión de la seguridad de la información» promulgada en julio del 2004 mediante Resolución del Comité de Reglamentos Técnicos y Comerciales del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad intelectual (INDECOPI). De ahí que la implementación de medios de control informático llevado a cabo por los empleadores deba estar precedida de un procedimiento previo de autorregulación.

El presente trabajo recopila, analiza e interpreta los dispositivos legales vigentes, la jurisprudencia constitucional y la doctrina jurídica nacional y extranjera con relación a la regulación y autorregulación de la seguridad de la información, el poder de dirección del empleador y los derechos a la identidad e intimidad personal, a la libertad informática y a la inviolabilidad y secreto de las comunicaciones y documentos privados del trabajador, así como su derecho al «consentimiento informado» con relación a los controles y la supervisión de los sistemas de información en los ámbitos laborales.

Con ello se pretende difundir entre los administradores de sistemas de información de los empleadores peruanos los límites que los derechos fundamentales de los trabajadores imponen a la autorregulación de la gestión de la seguridad de la información, en especial a los mecanismos de control y supervisión sobre el uso de los recursos informáticos.

De otro lado, dar a conocer a los profesionales del derecho las prácticas y aplicación de los principios de gestión de seguridad de la información interpretando los hechos y actos jurídicos que involucran la ejecución de medidas de control y supervisión sobre el uso, por parte de los trabajadores, de los recursos informáticos de los empleadores en el Perú.

CAPÍTULO 1 La era de la información y el Derecho

1.1. La sociedad de la información

La constatación de la presencia masiva de la tecnología de la información en la vida social actual es algo bastante simple en comparación con la comprensión de las tendencias que subyacen a los cambios tecnológicos que repercuten en la estructura de las sociedades y los Estados. De hecho, existe un conjunto de circunstancias de cambio social, económico, político y tecnológico al que, en algunos ámbitos, se le llama sociedad de la información.

En un principio, la denominación sociedad de la información sirvió para caracterizarla reconversión del sector industrial y el traslado del empleo hacia el sector de información; actualmente, más bien hace referencia a las manifestaciones tecnológicas sobre la información y las comunicaciones, especialmente Internet, que han cambiado gran parte de los aspectos De la vida y la producción desde la última década del siglo pasado. Esta nueva versión de la sociedad de la información ha sido acogida de manera explícita por organismos multilaterales y gobiernos, y es el origen de debates que no fueron el motivo de su concepción inicial como categoría analítica de las ciencias sociales.

Esta evolución muestra las dos grandes vertientes del análisis. el discurso académico y las políticas públicas; aunque en la actualidad la mayor parte de la discusión se da en las áreas de políticas públicas, telecomunicaciones, un poco en Derecho y muy poco en las ciencias sociales. Pretender la existencia de una sociedad de la información, parte por reconocer que la información tiene una función central que se hace evidente en la presencia cada vez mayor de redes y sistemas de información globales, que hacen que se viva de una manera distinta. Por ello, no puede entenderse el rol actual de la información sin sus equipos y conexiones, tanto así, que parece ser que en algunos casos son los equipos *y* las conexiones lo importante; lo que necesariamente lleva a indagar sobre las técnicas que ponen a la información en el centro mismo de la discusión. De ahí que la importancia de la sociedad de fa información no esté establecida por los académicos sino por los Estados que tengan la capacidad de aprovechar este concepto para elaborar políticas creativas y útiles para el desarrollo de los pueblos.

El pensador catalán Manuel Castells (2000) en su obra «La era de la información» expone su concepción de lo que denomina la sociedad en red como un *modelo* de desarrollo del sistema económico predominante, el capitalismo. Para ello parte de entender que las socieda-

des se organizan en función a procesos históricos articulados por la producción, la experiencia y el poder.

La producción es la acción del hombre sobre la naturaleza con el fin de convertirla en un producto que pueda ser consumido en parte y cuyo excedente sea acumulado para su inversión en determinados fines dispuestos por la sociedad; por su parte, la experiencia, es la acción de las personas sobre sí mismas en relación con su búsqueda de la satisfacción de sus necesidades y deseos; y por último, el poder, es la imposición de la voluntad de algunos sujetos sobre los demás mediante la violencia física o simbólica.

Las instituciones sociales refuerzan las relaciones de poder, a través de controles, límites y contratos. La producción supone la organización social y el trabajo, y éste último se estratifica según la función de cada trabajador en el mismo proceso de producción; en este proceso, la relación entre el trabajo y la materia requiere del uso de los medios de producción, del conocimiento y de la información; y la tecnología es la forma específica de tal relación. El produclo, resultado del proceso de producción se consume en parte y el excedente es apropiado, distribuido y usado en función a las reglas sociales que constituyen los «modos de producción»; éstos a su vez. determinan la existencia de clases sociales. En el siglo XX los principales modos de producción caracterizados por la apropiación y control de los excedentes, fueron el capitalismo y el estatismo.

La valoración de los excedentes de producción se determina por la productividad de un proceso en concreto, es decir, por la relación entre el valor de la unidad de producto (*output*) y el de la unidad del insumo (*input*). La mayor o menor productividad dependen de la relación entre el producto y los medios de producción aplicados, tales como la mano de obra, la energía o el conocimiento; y el proceso de producción se caracteriza por las relaciones técnicas que definen los «modos de desarrollo». Éstos a su vez, son los dispositivos tecnológicos mediante los cuales el trabajo transforma la materia y crea el producto, determinando en última instancia la cuantía y calidad del excedente.

Un determinado modo de desarrollo se caracteriza por el elemento que promueve la productividad; en el nuevo modo de desarrollo que Castells (2000) denomina «informacional», el fomento de la productividad se funda en la tecnología de la generación de conocimiento, el procesamiento de la información y la comunicación de símbolos: sin embargo, el proceso de producción siempre se basa sobre el conocimiento y el procesamiento de la información, lo que es específico de este modo de desarrollo, es que el conocimiento actúa sobre sí mismo y que el procesamiento de la información se concentra en el perfeccionamiento de la tecnología como fuente de productividad, conformando un círculo virtuoso de interacción del co-

nocimiento de la tecnología y la aplicación de ésta para mejorar la generación de conocimiento y el procesamiento de la información, constituyendo así: «un nuevo paradigma tecnológico basado en la tecnología de la información». (CASTELLS, 2000: 47)

El conocimiento tiene así una función social y un valor económico, la creación de riqueza; el campo del conocimiento es difuso, por lo que se opta por el término información debido a que ésta es perceptible en documentos o bases de datos, cuantificable, fungible y, sobre todo, negociable.

1.1.1. Tecnología y sociedad

Siguiendo el discurso de Castells (2000), este autor descarta el problema del «determinismo tecnológico» argumentando que la aplicación de una tecnología especifica no determina un modelo de sociedad; así como que tampoco la sociedad establece el sentido del cambio tecnológico, debido a que elementos como la iniciativa personal forma parte fundamental de la innovación tecnológica. En definitiva, la tecnología es sociedad y, a su vez, para comprender a ésta es indispensable considerar sus instrumentos técnicos. En este sentido la revolución de la tecnología de la información, cuyo origen se da en la década 1960, se caracterizó por sus movimientos sociales de espíritu libertario que difundió en la cultura material; sin embargo, en cuanto las tecnologías de la información se extendieron por diferentes países. culturas y organizaciones, éstas se adaptaron a toda clase de usos y aplicaciones que retroalimentaron la innovación tecnológica, acelerando la velocidad y ampliando el alcance del cambio tecnológico. A ese respecto un ejemplo significativo es la Internet, que pasó de ser una herramienta con fines académicos y aptitud claramente anticomercial, a convertirse en fundamento del comercio electrónico y la nueva economía, sirve esto para desvirtuar la perspectiva determinista, ya que ha sido el modo de desarrollo informacional lo que forzó el cambio de la Internet, no la tecnología. Se tiende a creer que los cambios son fundamentalmente tecnológicos, cuando lo que sucede es que hay un proceso de cambios en la manera en que la sociedad aprovecha la tecnología.

Hay que tomar en cuenta que, si bien la sociedad no determina la tecnología, si puede impedir su desarrollo, sobre todo mediante la intervención estatal. Por una parte el Estado puede ser. y lo ha sido históricamente en algunos países, una fuerza dirigente de la innovación tecnológica: por otra, y debido a ello. cuando su interés por el desarrollo tecnológico cambia, o no es capaz de llevarlos cabo en distintas condiciones, el modelo estatista torna infecunda la autonomía de la sociedad para crear y aplicar tecnología innovadora. Castells (2000) señala que, desde el punto de vista del cambio histórico, lo importante para los pro-

cesos y formas sociales es la interacción real de los modos de producción y los modos de desarrollo; lo que acelera, canaliza y da forma al paradigma de la tecnología de la información y mueve las formas sociales asociadas a éste, es el proceso de reestructuración capitalista iniciado en 1980, por lo que define al nuevo sistema tecnoeconómico como «capitalismo informacional».

Esta reestructuración se realizó gracias al decaimiento politice de los sindicatos en los países capitalistas *y* a la imposición de una disciplina económica común a todos los países miembros de la Organización para la Cooperación y el Desarrollo Económico (OCDE) con el fin de integrar los mercados financieros globales aplicando las nuevas tecnologías de la información; en esas condiciones, los parámetros básicos de los procesos de reestructuración económica se uniformaron en el ámbito mundial. Así, en el ámbito global. la reestructuración del capitalismo y la expansión del informacionalismo se hicieron inseparables; si bien las sociedades reaccionaron de manera diversa ante estos hechos en razón de sus distintas culturas e instituciones, las sociedades informacionales son capitalistas, en el sentido que sus procesos productivos, la generación de conocimientos. el poder político y militar y los medios de comunicación han sido transformados por el paradigma informacional al estar conectados en redes globales que funcionan según esa lógica. De esa manera, todas las sociedades han sido alteradas por el capitalismo y el informacionalismo.

Resumiendo, para Castells (2000), la organización de la producción está condicionada por las relaciones sociales que lo sustentan, o «modos de producción», y por las relaciones técnicas o «modos de desarrollo»; el capitalismo, como modo de producción, y el informacionalismo, como modo de desarrollo coexisten sin que haya una relación de necesidad entre ellos.

1.1.2. La sociedad red

La red como conjunto de elementos organizados en nodos interconectados para un determinado fin son formas de la actividad humana empleadas desde muy antiguo; sin embargo, actualmente las redes han cobrado un rol principal al convertirse en redes de información. De igual modo como las tecnologías de generación y distribución de energía hicieron posible que la gran empresa se consolidara como la base para la organización de la sociedad industrial, la red global Internet constituye actualmente la base tecnológica para la organización que caracteriza a la sociedad de la información. Internet es un medio de comunicación que permite, por primera vez, la transmisión de datos de muchos a muchos a un nivel global.

Debido a que la actividad humana está basada en la comunicación, esta nueva forma de comunicarse ha transformado profundamente la estructura social.

La sociedad red está compuesta por diversas redes con orientaciones propias, pero unidas en el propósito capitalista, y organizadas en función de flujos de información cuya lógica es independiente de las demás. Las redes existen para los flujos y para ello deben contar con nodos que les permitan interconectarse entre si y en los cuales se realizan las funciones de recopilación, organización y recuperación de información. En los nodos se toman las decisiones que orientan la acción de los participantes de las redes, y la comunicación entre éstos es simultánea gracias a la tecnológica informática y de las telecomunicaciones, por ello no hay dilación entre nodos *de* una misma red, con flujos tan rápidos como la capacidad de interpretarlos. (VILLANUEVA, 2005)

Las nuevas tecnologías de la información están integrando al mundo en redes que se comunican a través de las computadoras, generando así un amplio despliegue de comunidades virtuales. Castells (2000) afirma que los primeros pasos de las sociedades informacionales parece n caracterizarse por la preeminencia de la identidad como principio organizativo, entendiendo por identidad al proceso por el cual una persona se reconoce a sí misma y construye su significado en virtud de un conjunto de atributos culturales determinados, con la exclusión de una referencia a otras estructuras sociales; así, las relaciones sociales se definen frente a los otros en razón de aquellos atributos culturales que especifican la identidad. Asimismo hace suya la afirmación de Alain Touraine al sostener que, "en una sociedad postindustrial, en la que los servicios culturales han reemplazado los bienes materiales en el núcleo de la producción, *la defensa del sujeto, en su personalidad y su cultura, contra la lógica de los aparatos y los mercados, es la que reemplaza la idea de la lucha de clases"* (CASTELLS, 2000: 53).

La experiencia de los grupos sociales interconectados en la red global trae como consecuencia la primacía del interés por lo local y global sobre lo nacional. permitiendo a las masas fuera de los nodos, participar de la sociedad red siquiera de manera ficticia. Si se considera que la cultura es la producción y el consumo de signos, no se puede argumentar que la realidad se agota en lo presencial, como un espacio exclusivamente físico que no incorpora las experiencias que se viven en la red de manera virtual.

Internet se ha convertido en un medio de comunicación y organización primordial en todos los ámbitos de la actividad social, por tanto, resulta comprensible que los movimientos sociales y los representantes políticos la utilicen cada vez más para actuar, informar, movilizar, organizar y dominar. Estos movimientos que actúan colectivamente con la intención de

transformar los valores y las instituciones sociales, en el presente siglo se manifiestan en y a través de Internet. Por ejemplo el movimiento obrero, sobreviviente de la era industrial, así como los movimientos ecologista feminista, de identidad étnica, religiosos, nacionalistas, los diversos grupos pro derechos humanos y los defensores de una inacabable relación de propuestas culturales y causas políticas se conectan, establecen y movilizan con y en Internet.

Dicha red se ha convertido en un foro virtual global de la diversidad de la insatisfacción humana; quizás el ejemplo más significativo de ello sea el de «*Falun Gong*», el movimiento político y espiritualista chino, formado por decenas de millones de seguidores que encontraron en la red el apoyo espiritual y la información necesaria para reunirse en persona en un momento y lugar determinados, mediante una serie de protestas que desafiaron al Partido Comunista chino y hacen frente a una dura represión del gobierno de ese país por el temor que éstos tienen a la posible influencia del movimiento. Internet, por tanto, no es tan sólo un artilugio que se puede utilizar simplemente porque está ahí, sino que además se adecua a las características de la índole de los movimientos sociales que están germinando en la sociedad de la información. Al utilizar Internet para diversos asuntos ésta se va transmutando, de esa interacción se crea un nuevo modelo sociotécnico. (CASTELLS, 2001)

1.1.3. Negocios en la red y la nueva economía

El fenómeno de la internacionalización de la producción que se ha hecho presente desde la reestructuración del capitalismo, se apoya tanto en el beneficio que supone contar con más mercados para la venta de productos como en el flujo de la producción misma. En ese sentido, el nuevo modelo de organización que se desarrolla es el que Castells (2001) denomina la «empresa-red»; ésta no es una red de empresas o una organización intraempresarial en red, es una organización de la actividad económica dúctil constituida en función a proyectos empresariales determinados realizados por redes de diversa composición y origen.

Estas redes tienen la flexibilidad y la adaptabilidad necesarias en una economía global caracterizada por una incesante innovación tecnológica e impulsada por un cambio continuo de la demanda. Es a partir de mediados de los años ochenta, con la aparición de redes de comunicación como las de «Intercambio Electrónico de Datos» EDI (por sus siglas en inglés *Electronic Data Interchange),* y otras redes más primitivas de conexión vía facsímil y telefonía que fue posible la reestructuración organizativa que transformó al mundo de la empresa. Las redes de comunicación informática basadas en la microelectrónica, incluida Internet, retribuyeron la necesidad de transmitir gran cantidad de datos de manera interactiva, en tiempo real y a alta velocidad.

Así como a principios del siglo pasado la producción estandarizada de la *Ford Motor Company* se constituyó como el arquetipo de la organización empresarial de la sociedad industrial, el paradigma del modelo empresarial de la nueva economía que surge con la red global podría ser *Cisco Systems,* empresa que provee los equipos conmutadores y direccionadores que encaminan el flujo de datos en las redes de comunicación, siendo líder del equipamiento esencial de Internet. Sin embargo, al construir una red de proveedores en línea, esta es una empresa que no realiza fabricación alguna; el sistema reticular de *Cisco* se extiende a su vez a sus empleados, éstos están conectados a través de una Intranet que proporciona comunicación instantánea a más de 10,000 trabajadores en todo el mundo, siendo esta empresa la precursora del modelo empresarial reticular global. En definitiva, es el prototipo del círculo virtuoso de la revolución de las tecnologías de la información y la comunicación sobre la base de redes organizativas promovidas por redes de información y se ha convertido en el modelo preponderante para los competidores que más éxito tienen en la mayoría de las industrias y en todo el mundo.

Este modelo organizativo no fue consecuencia inmediata del cambio tecnológico, los métodos de participación de los trabajadores que experimentaran las empresas japonesas, suecas y estadounidenses, -por ejemplo el sistema *kan- ban* que aplicara por primera vez la empresa *Toyota* en 1948 sin enlaces electrónicos en linea— requirieron un cambio de mentalidad más que uno de maquinaria. De hecho, en un inicio la nueva tecnología de la información fue considerada en los Estados Unidos como una herramienta que permitía el ahorro de mano de obra y una me jor forma de ejercer control sobre la misma, más no un componente para el cambio organizativo. El cambio organizativo se dio asi de manera autónoma del cambio tecnológico, como una solución para enfrentar un entorno operativo en constante evolución; sin embargo, una vez que se produjo el cambio sus posibilidades aumentaron considerablemente como resul tado de la aplicación de las nuevas tecnologías de la información.

De otro lado, también la potencialidad de las empresas pequeñas y medianas para vincularse entre si y con las grandes empresas pasó a depender de la disponibilidad de estas nuevas tecnologías, una vez que el ámbito de las redes se hizo global. La complicación para adoptar alianzas estratégicas, acuerdos de subcontratación y la toma de decisiones descentralizada de las grandes empresas no hubiera sido posible de resolver sin el progreso de las redes informáticas: en concreto, sin la potencia de los microprocesadores de las computadoras personales conectadas a través de las redes de telecomunicación de conmutación digital. En estos casos, el cambio organizativo provocó hasta cierto punto el desarrollo de la tecnología; fue debido a los requerimientos de interconexión de las nuevas organizaciones,

grandes y pequeñas, que las computadoras personales y las redes informáticas se multiplicaron de manera explosiva. Así, debido a la multitudinaria necesidad de operar las computadoras de forma interactiva y flexible, el software se convirtió en el segmento más dinámico de la actividad productora de información.

Además de ser programable y adaptable, lo que hace a la computadora representativa del cambio tecnológico es la reducida importancia de la manufactura del aparato; lo significativo es lo que lleva dentro, es decir, el conjunto que forma el microprocesador, las demás partes electrónicas y el software, lo que crea el instrumento que será usado por quienes persiguen expandir su capacidad de hacer y de crear. La computadora es el resultado de una economía basada en el conocimiento.

Los adelantos cualitativos de la tecnología de la información en red de los que se dispuso recién a partir de 1990 hicieron posible que se sucedieran procesos de gestión, producción y distribución plenamente interactivos, basados en la informática y flexibles, que permitieron la colaboración simultánea entre diferentes empresas y sus unidades. En esas condiciones de acelerado cambio tecnológico han sido las redes, y no las empresas, las que se han convertido en las unidades de operación real en la economía; en términos de Castells, "la interacción entre la crisis organizativa y las nuevas tecnologías de la información ha dado lugar a una nueva forma organizativa que es característica de la economía informacional/global: *la empresa-red" .* (CASTELLS, 2000: 226)

Para delimitar esta nueva forma organizativa que expone Castells (2000) hay que recurrir a la definición de organización que éste sostiene: un sistema de medios estructurados dos en torno al propósito de lograr fines específicos; y añadir la distinción analítica de la teoría de Alain Touraine que sostiene una diferencia esencial entre dos tipos de organizaciones: aquellas para las cuales la reproducción de su sistema de recursos es su objeto principal, (burocracias): y aquellas en las que sus fines *y* su cambio dan forma constantemente a la estructura de los recursos (empresas). A partir de esa distinción, el autor propone una definición de la empresa-red como "aquella forma especifica de empresa cuyo sistema de medios está constituido por la intersección de segmentos de sistemas autónomos de fines"; (CASTELLS, 2000: 226) y concluye, los elementos de una empresa-red son a la vez autónomos e independientes de ella por lo que pueden ser partes de otras redes y de otros sistemas de recursos con distintos objetivos. Por tanto, la actuación de una red dependerá de su capacidad de conexión y de su consistencia para compartir intereses con los fines de la propia red y los desus componentes.

1.1.4. Sociedad civil global y postmodernismo

Anthony Giddens, teórico fundamental de la sociología de finales del siglo XX, autor de la «teoría de la estructuración», esfuerzo consciente para unificar las perspectivas de Marx y Weber, considera la idea de la sociedad civil global como una necesidad lejana a la atracción de la tecnología, aunque la aprovecha, y distinta al capitalismo global y su afán de expansión, aunque reconoce la utilidad de entenderlo, y de no dejarse avasallar por su racionalidad ausente de visión colectiva o de largo plazo.

La sociedad civil global vendría a ser el resultado de las declaraciones menos sugestivas de lo que se llama en muchos foros, pero no en el ámbito académico, la sociedad de la información. Uno de dichos espacios es el foro económico de Davos, que se realiza en dicha ciudad Suiza y que sirve para que los llamados capitanes de la industria, los gerentes de transnacionales y los accionistas de grandes fondos de inversión intercambien ideas con intelectuales y políticos sobre cómo promover la globalización integrando a las mayorías. Por su parte, el Foro Social Mundial realizado desde el año 2000, es un espacio para contrarrestar a Davos; ambos son muestras de la importancia de la globalización y de la necesidad de una acción coordinada dado que no existe un sistema político global que de espacio a estas cuestiones; como tales, son manifestaciones de una posible sociedad civil global.

Jean François Lyotard, filósofo francés, uno de los principales exponentes del concepto de una sociedad postmoderna, explaya su interés más allá del tema de la informática destacando la idea de la importancia de la legitimación de cualquier tipo de saber en un discurso capaz de entablar un diálogo con otros puntos de vista esto es, una pragmática; ésta sirve para definir los términos del diálogo pero también para establecer sus límites. En consecuencia, la ciencia alcanza su legitimación ante la sociedad en su capacidad de producir resultados; la técnica asumió, desde la revolución industrial , la tarea de mejorar la productividad, y la unión de la técnica con la obtención de ganancias es anterior a la unión de la técnica con la ciencia; de hecho se puede afirmar que la ciencia se une con la técnica para potenciar la capacidad de esta última de generar ganancias. Así, los planes nacionales para desarrollar la ciencia surgen como una estrategia de legitimación de ésta como generadora de riqueza ante la sociedad.

Lyotard concluye que lo que realmente legitima la actividad de la ciencia y la tecnología es su eficiencia productiva: su capacidad de obtener una relación insumo/producto que propicie la generación de riqueza. En esta lógica, es coherente que los Estados reconozcan la importancia de las tecnologías de información como medios para la creación de riqueza y la obtención de poder, promuevan su aplicación y las consideren indispensables para el desarro-

llo. Entonces la llamada sociedad de la información se muestra como una gran oportunidad pero también como una amenaza, en la medida que las empresas asumen que si no se adaptan y aumentan la productividad no serán capaces de continuar. En resumen, Lyotard propone que la racionalidad de discurso científico surge como motivo para cambiar las premisas mismas de la acción del Estado y la sociedad. (VILLANUEVA, 2005)

1.2. Impacto de la tecnología de la información sobre las relaciones económicas y jurídicas

El proceso de trabajo es un elemento esencial del orden social, y la transformación tecnológica y organizativa de aquél y las relaciones de producción en la emergente empresa-red, constituyen el principal impulso del paradigma informacional y la globalización que mueve fuertemente a la sociedad de la información.

Para la teoría clásica del post industrialismo, el origen de la productividad y el crecimiento económico, es la generación del conocimiento en todas las actividades mediante el procesamiento de la información; asimismo, las actividades económicas migran de la producción de bienes a la prestación de servicios y por consiguiente desaparece el empleo agrícola y el trabajo fabril declina irreversiblemente a favor del sector terciario para constituirse así en la porción más considerable del empleo, cuanto más avance logre una economía más se concentrará su empleo y producción en los servicios ; y por último, la economía post industrial acrecentará los puestos de trabajo que demanden un alto grado de conocimiento e información, los cargos ejecutivos, profesionales y técnicos crecerán en mayor proporción que los demás y formarán el núcleo de la nueva estructura social.

Sin embargo, aunque las economías de finales del siglo pasado se distinguieron nítidamente de tas previas a la Segunda Guerra Mundial, su rasgo distintivo no fue precisamente el au- mento de la productividad sino que la producción agrícola, industrial y de servicios estuvo basada en el conocimiento. Por tanto, la diferencia Que más las distingue históricamente, a unas de las otras, es la revolución de la aplicación de las tecnologías de la información y su expansión a todos los ámbitos de la actividad social y económica , incluyendo el estableci- miento de la infraestructura para la constitución de la economía global. Si algo ha reempla-
zado a la industria como base de una estrategia de crecimiento económico, es la innovación sustentada en el conocimiento, la que produce a su vez nuevas industrias, basadas también en el conocimiento.

De ahí que Castells (2000) proponga cambiar el énfasis analítico del postindustrialismo al informacionalismo. Así, las sociedades serán inforrnacionales cuando organizan su sistema de producción con el fin de expandir la productividad en función al conocimiento, apoyándose en el desarrollo y la difusión de las tecnologías de la información con los recursos humanos e infraestructura de comunicaciones que éstas requieren para su plena utili zación. En cuanto al cambio hacia las actividades de servicios y la desaparición de la manufactura, existe una confusión debida a la separación convencional entre economías avanzadas y economías en vías de desarrollo que, en condiciones de globalización, forman parte de la misma estructura productiva. Además, el concepto de «servicios» usualmente se considera ambiguo y hasta engañoso; por ejemplo, el software, la producción de vídeos, el diseño de microelectrónica, la agricultura sustentada en la biotecnología y muchos otros procesos característicos de las economías avanzadas fusionan de manera intrincada su contenido de información con el soporte material del producto, lo que hace imposible distinguir los límites entre bienes y servicios. Por último, en cuanto a la referencia de la teoría del postindustrialísmo sobre la expansión de los empleos para ejecutivos, profesionales y técnicos convertidos en el núcleo de la nueva estructura ocupacional, ésta tiene la excepción de que el aumento de las ocupaciones en servicios menos calificados, también caracteriza a las sociedades avanzadas por su estructura social cada vez más polarizada, en la que el vértice y la base aumentan su cuota a expensas de la parte media.

1.2.1. El trabajo en la nueva economía

Se sabe que la tecnología no es el elemento principal que distingue a los sistemas de organización del trabajo, sin embargo, cuanto más extensa es la aplicación de la tecnología de la información en las industrias y oficinas mayor es la necesidad de trabajadores autónomos, capaces y hábiles para programar y decidir secuencias enteras del trabajo. Asi, a pesar de los obstáculos que significan el capitalismo explotador y la gestión autócrata, las tecnologías de la información requieren de los empleados mejor informados una mayor libertad para realizar plenamente su potencial de productividad; el trabajador en red es indispensable para el modelo de empresa-red que estas mismas tecnologías han hecho posible, y su amplia difusión tiene efectos similares en cualquiera de las formas de organización laboral. Por ello no resulta extraordinario que reemplacen el trabajo que se puede codificar en una secuencía programable por el empleo que se apoya en el análisis, la toma de decisiones y la capacidad para reprogramar en tiempo real que sólo el cerebro humano puede dominar. El trabajo humano es el fundamento de la productividad, la innovación y la competitividad. y adquiere cada vez mayor trascendencia en una economía que depende del potencial para obtener, procesar y aplicar información.

La nueva economía no puede desarrollarse sin trabajadores con capacidad para navegar en la red, tanto en términos técnicos como de contenidos, pues la vastedad de información debe ser organizada, dirigida y transformada en conocimientos adecuados para las tareas y el propósito del proceso de trabajo. El desarrollo de la empresa-red depende de los trabajadores que operan y utilizan Internet equipados de un capital intelectual.

Según el Instituto Nacional de Estadística e Informática del Perú, para el año 1999 el 80% de las empresas peruanas medianas y grandes -con más de cinco trabajadores- , ya contaba con computadoras como parte del apoyo de las actividades laborales y el 64.2% contaba con acceso a Internet. (INEI, 2001)

En el año 2002, según datos de la encuesta nacional de recursos informáticos elaborada por el mismo instituto, el 31.3% de los trabajadores de la administración pública peruana tenían acceso a computadoras y el 14.3% a la Internet. (INEI, 2002)

El artículo 2 del texto único ordenado del Decreto Legislativo 728, «Ley de productividad y competitividad laboral», establece que: “La introducción de tecnología que eleve los niveles de productividad del trabajo, constituye un derecho y un deber social a cargo de todos los empresarios establecidos en el país”.

1.2.2. La intimidad en la era de la información

El temor al cambio y el impulso innovador, que van paradójicamente unidos, son una constante histórica en la experiencia humana; la resistencia e insatisfacción ante el mundo conectado en red están relacionadas con un conjunto de desafíos; el principal es la libertad. La Internet proporciona comunicación global y ésta se ha hecho esencial en todos los ámbitos de la actividad social, la infraestructura de las redes es mayoritariamente privada y el acceso a las mismas puede ser controlado y sus usos pueden estar sesgados o incluso monopolizados por intereses comerciales, ideológicos y políticos. A medida que Internet se convierte en el medio dominante en nuestras relaciones sociales, la propiedad y el control del acceso a ella se convierten en la principal amenaza a nuestra libertad.

Giddens reconoce que la tendencia al control en las sociedades contemporáneas es capital, y que la existencia de mecanismos de vigilancia es la base del poder. El monopolio de la violencia que caracteriza al Estado moderno, va acompañado por el monopolio de la vigilancia y su cesión a sujetos privados crea condiciones para que los ciudadanos se encuentren en desventaja frente a las empresas que convierten la información que les atañe en un bien comercial. La capacidad de recolectar información, que es esencial para la vigilancia, permi-

te mejorar la calidad de los servicios, vender más bienes y, en general, brindar condiciones de vida más favorables en sociedades cada vez más complejas: pero, al mismo tiempo, es esencial garantizar que no se permita que el afán comercial predomine sobre el interés social.

Los estados se ven en la difícil posición de carecer de agregaciones de información que sí tienen las empresas globales. El temor al control mediante la tecnología se incrementa en la medida que aumentan las capacidades de exploración y recolección de información, lo que llama la atención es que ésta pueda, aunque no deba, ser usada para múltiples formas de control de los individuos. La tendencia hacia la recopilación de informaciónes inexorable, ya que no se puede dejar de controlar o supervisar a la población si se quiere sobrevivir como sociedad. El desafio es evitar caer en un control y supervisión carente de protección a la intimidad de las personas. (VILLANUEVA. 2005)

Américo Pla Rodríguez (1986) hace referencia que en la Memoria del Director de la Organización Internacional del Trabajo (OIT) para la 57º reunión de la Conferencia Internacional del Trabajo realizada en Ginebra en junio de 1972, se recogía ya este temor al plantear como tema: "La técnica al servicio de la libertad" y en especial el capítulo "La erosión de la libertad individual".

Internet en sus primeros años de existencia global presagiaba una nueva era de libertad; la intimidad de los usuarios estaba protegida por el anonimato así como por la dificultad de indagar sobre los orígenes e identificación del contenido de los mensajes transmitidos por medio de los protocolos de comunicación. Este paradigma de libertad tiene fundamentos tecnológicos e insti tucionales: tecnológicamente su arquitectura basada en la conexión informática sin restricciones, actúa sobre protocolos que interpretan la censura como un fallo técnico que se soslaya simplemente, haciendo bastante difícil o casi imposible el control; institucionalmente, el hecho de que Internet se desarrollara inicialmente en los Estados Unidos la situaba bajo el amparo de la protección constitucional de la libertad de expresión, reconocida por sus tribunales.

A lo largo de la historia, el control de la información constituyó siempre la base del poder del Estado y los Estados Unidos no son una excepción a la regla; así, en un intento de ejercer control sobre Internet, el Congreso y el Departamento de Justicia argumentaron sobre la necesidad de proteger a los níiios de los pervertidos sexuales que utilizan la red para promulgar la Ley de Decencia en las Comunicaciones (*Communications Decency Act);* sin embargo en junio de 1996, un tribunal federal de Pennsylvania la declaró inconstitucional bajo el fundamento que: «Igual que podemos afirmar que la fuerza de Internet reside en el caos, el va-

lor de nuestra libertad depende del caos y la diversidad de la expresión sin trabas defendida por la Primera Enmienda». Posteriormente el 26 de junio de 1997 la Corte Suprema sostuvo este «derecho constitucional al caos». En junio de 2000, la Corte de Apelación de Estados Unidos en Filadelfia derogó la Ley para la Protección del Menor En Linea *(Child On fine Protection Act)* de 1998. (CASTELLS, 2001:219)

A pesar de lo expuesto, los puntales de la libertad en Internet están siendo socavados por nuevas tecnologías y nuevas regulaciones. De hecho, aplicaciones de software se pueden configurar sobre Internet para permitir la identificación de rutas de comunicación y contenidos, transgrediendo de esa manera la privacidad debido a que en cuanto se llega a relacionar a determinadas personas con procesos de comunicación en espacios institucionales concretos, es posible utilizar las formas tradicionales de control político y organizativo contra el usuario conectado a ta red. La vulneración de la libertad y la privacidad en Internet es consecuencia directa de su uso comercial, que conlleva, por un lado, la necesidad de asegurar e identificar la comunicación como condición para poder ganar dinero gracias a la red y, por otro, la necesidad de proteger los derechos de propiedad intelectual en la misma. lo que ha derivado en el desarrollo de nuevas arquitecturas de software que posibilitan el control de la comunicación informática. Los gobiernos indistintamente apoyan estas tecnologías de control y se esfuerzan en adoptarlas con el fin de recuperar en parte el poder que corrían el riesgo de perder.

De estos intereses compartidos han surgido una variedad de tecnologias de control, la vigilancia y la investigación, éstas se basan en dos supuestos: el conocimiento asimétrico de los códigos en la red y la capacidad para delimitar un espacio de comunicación que sea susceptible de control. Las tecnologías de vigilancia interceptan mensajes para marcartos de forma que puedan seguirse los flujos de comunicación desde una computadora determinada y controlar su actividad de manera constante; pueden identificar un servídor en el origen de un mensaje y mediante la persuasión o la coacción, los gobiernos, las empresas o los tribunales pueden obtener del proveedor de servicios Internet la identidad del usuario, utilizando tecnologías de identificación o simplemente cotejando en sus listas cuando poseen dicha información. Las tecnologías de investigación corresponden a la creación de bases de datos con los resultados de la vigilancia y la acumulación de información obtenida puntualmente.

Actualmente, cualquier información transmitida electrónicamente puede ser procesada, identificada y combinada dentro do un espacio definido en la red; por ejemplo en la red construida por un determinado proveedor de servicios Internet o la Intranet de una empresa, de una universidad o una agencia gubernamental. En efecto, si bien Internet es una red global, los

puntos de acceso a ésta no lo son, si se colocan filtros en estos accesos, la libertad global termina siendo la sumisión local.

Sin embargo hay una serie de nuevas tecnologías de la libertad, mediante las cuales la sociedad civil se lanza a la defensa, mientras los tribunales de justicia ofrecen un cierto grado de protección contra los abusos en algunos contextos. Si bien Internet ha dejado de ser un espacio absolutamente libre, es una esfera controvertida en la que se disputa una nueva y fundamental campaña en pro de la libertad en la era de la información.

La libertad que caracteriza a Internet concita tanto entusiasmo que comúnmente se pasa por alto la permanencia de prácticas autoritarias de vigilancia en el ámbito más importante de nuestras vidas: el lugar de trabajo. A medida que los empleados dependen cada vez más del trabajo en red, la mayoría de las empresas se atribuyen el derecho irrestricto de controlar el uso que éstos hacen de sus redes. En los Estados Unidos, un estudio hecho público en abril de 2000, indicó que el 73,5% de las empresas ejerce con regularidad alguna clase de vigilancia del uso de Internet por parte de sus empleados y ha habido incontables casos de trabajadores despedidos con el argumento de un uso inapropiado. El control del trabajador en la fábrica constituyó una fuente habitual de conflictos durante la era industrial, todo parece indicar que Internet exacerbará esa tensión debido a su omnipresencia. (CASTELLS, 2001)

La adopción de la tecnología de la información en las organizaciones constituye una gran ventaja para sus miembros; gracias a ésta cuentan con recursos idóneos para la realización de sus actividades, les permite aumentar la productividad y desarrollarse como personas. Pero esta tecnología no sólo conlleva ventajas, sino que también trae conflictos; uno de los más importantes tiene que ver con la intromisión de la vida privada en el espacio organizacional. Es obvio que resulta inapropiado ver televisión, leer el periódico o conversar con amigos en el trabajo, salvo excepciones o cuando las labores lo exigen; pero en la actualidad a través de una computadora se puede hacer todo eso, no solo durante la jornada laboral sino al mismo tiempo en que se realiza el trabajo como consecuencia de la coincidencia de ámbitos que la tecnología permite.

Más aún, en la modalidad del teletrabajo se crean condiciones para introducir el espacio organizacional en el ámbito de la vida privada: mientras que la separación entre lo intimo y lo laboral formó parte de la concepción moderna de la vida diaria, pero el solo hecho de convertir el hogar en el lugar en el que se trabaja trae consigo el desvanecimiento de los ámbitos en los tiempos contemporáneos. La dimensión privada de lo cotidiano se ve invadida por la dimensión organizacional. Ni las organizaciones ni los Estados tienen normatividad com-

pletamente desarrollada a ese respecto y las áreas imprecisas sirven para potenciales abusos de ambos lados.

Este es un tema en debate y, sobre todo, urgente de aclarar para evitar que las expectativas del acceso total y la libertad irrestricta que ofrecen la tecnología terminen siendo constreñidas por interpretaciones excesivas de cualquier extremo. El sentido común indica moderación y cautela, pero es imposible organizar una realidad compleja solo a partir del sentido común; por tanto se hace necesario crear normas que respeten tas libertades, derechos y deberes de ambas partes.

Los derechos humanos y las libertades, incluyendo por supuesto el derecho a la intimidad, son categorías históricas y como tales han experimentado transformaciones en el tiempo, lo que ha determinado sucesivas generaciones de derechos. El carácter reivindicativo de los derechos humanos se muestra actualmente con atributos novedosos, por ello, con gran intensidad se abre paso la evidencia de una tercera generación como réplica al fenómeno denominada «contaminación de las libertades» (del inglés *liberry pollu1ion),* concepto que apunta al deterioro y declinación que sufren tos derechos fundamentales ante determinados usos de tas nuevas tecnologías. En ese sentido se advierte que la generación de nuevos derechos humanos no implica suplantar un repertorio de derechos por otro, sino supone la redefinición de derechos anteriores para adaptarlos al nuevo contexto en que deben ser aplicados: esto es lo que ha sucedido con el derecho a la intimidad que ha adquirido en la actualidad un carácter renovado en la era de ta info rmación, hasta el punto que "debe hablarse de un antes y un después de la informática en cualquier consideración de la intimidad que pretenda ser realista y rigurosa". (PÉREZ. 1983: 18)

1.2.3. El derecho informático

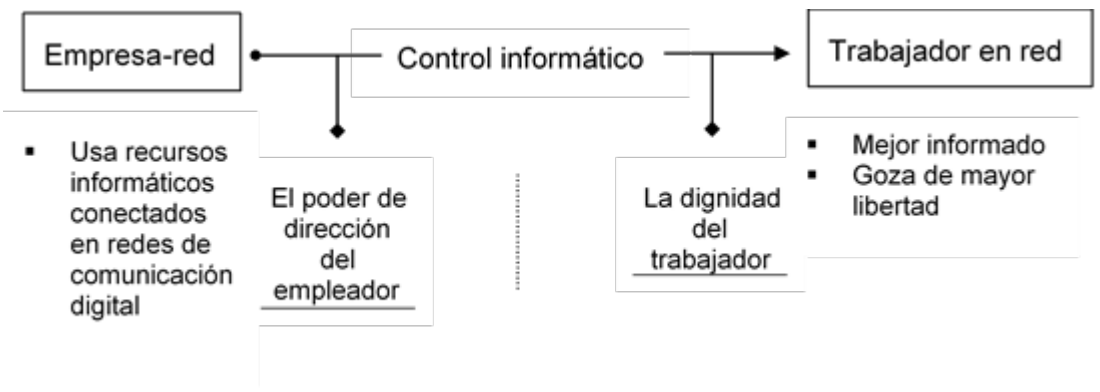
La necesidad de la doctrina jurídica de contar con un marco conceptual a partir del cual abordar tos problemas y cuestiones surgidos de ta interacción entre la tecnología de la información y el ordenamiento jurídico trajo como consecuencia al «derecho informático». Esta es una materia inequívocamente jurídica cuyas notas distintivas la conforman la normatividad de los sistemas legales contemporáneos dirigida a regular el uso y la aplicación de dicha tecnología, así como las sentencias de los tribunales sobre materia informática.

En ese sentido hay que resaltar como antecedente. en et ámbito del derecho público, el concepto de «libertad informática», como defensa de las libertades frente a posibles ataques consumados con la aplicación de la tecnología de la información, como objeto de especial atención por parte del derecho constitucional y administrativo.

El objeto normativo del derecho informático, o sea, la tecnología de la información, condiciona la estructura para su regulación y, su eficacia, depende de la idoneidad para captar el significado y la problemática de este fenómeno de la realidad actual. La expansión de la aplicación de la tecnologia de la información en casi todos los ámbitos de la actividad humana, ineludiblemente tenía que tener correlato jurídico ya que el Derecho supone la principal técnica de organización de la vida social.

Resulta evidente que si la tecnología de la información constituye el objeto inmediato del derecho informático, su objeto mediato es la propia información. La información se descompone en dos fases: la primera es dar forma y significado a un mensaje; la segunda dirigida a su transmisión; éstas son etapas de una función única que consiste en transmitir mensajes, conocimientos e ideas, es decir, la comunicación. La doctrina jurídica distingue en la comunicación: el contenido de la información, el sujeto que la origina y su destinatario; considerando su contenido, la información es generada por quien la forma o expresa y, por ello, puede establecerse entre el autor y la información una relación de posesión en términos de un derecho real; con relación a su destinatario, la información tiene su razón de ser en la comunicación, la realización de ese fin crea una relación necesaria entre el autor y el destinatario. De ello se deduce que los problemas que motivan la protección de los derechos de quienes crean aplicaciones informáticas, así como los contratos para su utilización se consideran en el campo de los derechos sobre la información; en tanto que lo relativo al flujo de datos y la protección de datos personales y libertades frente a la tecnología de la información en el del derecho a la información; ambas problemáticas conforman el objeto general del derecho ínformático.

La relación de los ámbitos informático y jurídico que franquean el vínculo laboral en el que sé suceden los hechos y actos de regulación y autorregulación de la seguridad de la información, que afectan el ejercicio de las facultades de control y supervisión que ejerce el empleador sobre los recursos informáticos que proporciona al trabajador, se representa en la siguiente sinopsis:



CAPÍTULO 2 La protección de los derechos fundamentales del trabajador

2.1. El concepto de derechos fundamentales

Los derechos fundamentales se distinguen de los derechos constitucionales en que estos últimos tienen reconocimiento en la Constitución Politica, en tanto los fundamentales desarrollan los valores establecidos en un ordenamiento jurídico pero no de una manera concluyente sino permeable a la evolución social e histórica, y por tanto gozan de mayor significado y garantías para su ejercicio. Los derechos fundamentales responden a la necesidad de crear y mantener las condiciones para que la libertad y la dignidad de las personas sean eficaces, lo que se obtiene únicamente cuando la libertad en la vida social se garantiza en igual medida que la libertad individual. La exigibilidad de los derechos fundamentales no requiere de desarrollo legislativo, éstos se demandan directamente ante los tribunales y gozan de procedimientos especiales. Justamente el derecho fundamental se define por la falta de disposición del legislador sobre su contenido, a éste le compete la obligación de su desarrollo eficaz, pero no el establecimiento del mismo.

El derecho a la intimidad, como derecho fundamental, no es sólo la potestad de permitir que un extraño conozca o no nuestra vida privada, sino también, la posibilidad de control sobre lo que los demás conozcan de nosotros mismos. En la primera manifestación anotada se muestra como un derecho de defensa, y en la segunda, como un derecho de interpretación expansiva, y, en la medida que la noción de intimidad es una categoría social, cultural e histórica, pretende ser un nivel de calidad en la relación con las demás personas.

En los estados democráticos lo público se rige por la pretensión de igualdad y lo privado como origen de la diversidad de las personas, sus ideas y sus manifestaciones; el respeto a la diferencia implica respeto a la vida privada. La singularidad, por tanto, es intrínseca al concepto de libertad, sin ésta no puede existir aquélla; de ahí que la intimidad sea un ejerci- cio de la libertad. La libertad como elemento de la intimidad alcanza a los dos ámbitos de ésta. La libertad es condición necesaria de fa digniclad humana, y son lo s derechos de la personalidad elementos que configuran el concepto de libertad: así, es hombre libre el que es consciente del valor de su personalidad y de la importancia que tiene el desarrollo de la misma. Si bien no se puede considerar la intimidad ni el derecho a la intimidad como funda- mentos, por si solos, de un orden social, sí se puede deducir que el derecho a la intimidad es parte de lo que la Conslitución Política establece como fines de la organización social;

este es un logro significativo de los ordenamientos jurídicos modernos, producto de las circunstancias culturales, hislóricas y sociales.

El concepto de derechos humanos y el de derechos fundamentales son el resultado de una evolución histórica cuyo transcurrir muestra el dinamismo que, en realidad, es una consecuencia de la dialéctica que existe entre la norma constitucional y la realidad social. Los derechos fundamentales surgen como exigencias o presupuestos de la convivencia en un momento determinado, que los lleva a los textos de las constituciones políticas. Los derechos fundamentales son enunciados jurídicos de un conjunto de valores que, por decisión del constituyente, han de informar a la organización jurídica y política. Pero además, los derechos fundamentales no sólo sirven de base al sistema político, sino también, a la estructura y contenido de las instituciones jurídico-privadas, ya que éstas deben estar condicionadas por la Constitución Política para asegurar en el ámbito del contrato y de la empresa, el desarrollo pleno de una sociedad democrática.

No se puede restringir el ámbito del derecho a la intimidad, al igual que el de los otros derechos fundamentales, a la sola posibilidad que el titular ejercite recursos judiciales cuando exista una violación del mismo, sino que, además, los poderes públicos deben tomar medidas para proteger real y eficazmente a la persona de los ataques contra su intimidad. (LUCAS, 1990; REBOLLO, 2000; VICENTE, 1998)

2.1.1. la eficacia de los derechos fundamentales en las relaciones privadas

La historia de los derechos fundamentales no sólo se ha caracterizado por la oposición entre los individuos y el Estado sino también entre los mismos individuos; sin embargo no parece haber una opinión unánime respecto a la función que desempeñan estos derechos en las relaciones entre privados. Los argumentos que defienden su presencia entre los particulares parecen más convincentes y no sólo desde una reflexión sobre el significado de los derechos, sino desde reflexiones históricas y sociológicas. Es evidente que grupos privados ejercen un poder de hecho tan amenazador a los derechos como el que ejerce el Estado, haciendo de la teórica igualdad entre las partes y de la autonomía de la voluntad, cuestiones relativas. En efecto, la posición del empleador, en el contexto de las relaciones laborales, le permite a éste amenazar el ejercicio del derecho a la intimidad del trabajador con la misma efectividad que el propio poder público.

La manera menos problemática de afrontar tal situación es ampliando la definición de poderes públicos; esta solución se ha adoptado en los Estados Unidos a partir de la doctrina de-

nominada *«state action»,* según la cual, los derechos fundamentales se aplican frente a privados siempre que se considere que la actuación que éstos ejercen es atribuible a los Estados (en inglés *fairy attributable to the states).* Esta solución difiere de la aplicada en Alemania, en donde la eficacia de los derechos fundamentales frente a los privados se ha defendido convirtiendo a éstos en principios objetivos del ordenamiento jurídico con eficacia directa tanto frente a personas públicas como privadas; debido a ello las relaciones laborales se han considerado como ámbito de aplicación de teorías que justifican la eficacia de los derechos fundamentales frente a terceros. Esta tesis es la denominada *«Drittwirkung der Grundrechte»,* según la cual, los derechos fundamentales afectan no sólo a las relaciones de subordinación entre el Estado y los ciudadanos, sino también a las relaciones de coordinación entre los particulares. Históricamente es el autor alemán Hans Carl Nipperdey quien configura doctrinariamente aquella tesis, si embargo su formulación se debe a Hans Peter Ipsen en los años cincuenta del siglo XX; por la *Drittwirkung* se entiende que la vigencia de los derechos fundamentales sería incompleta si no se concibe la capacidad de éstos para producir efectos entre los privados e incluso ante el Estado cuando éste actúa con sujeción al derecho privado; lo que se manifiesta en forma clara en los derechos de la persona y de forma muy significativa en el derecho a la intimidad. Actualmente, la doctrina distingue entre una *Drittwirkung* mediata y otra inmediata; la primera considera que los derechos fundamentales operan entre particulares previa actuación de los poderes públicos para determinar las situaciones jurídicas y su eficacia; la inmediata postula que éstos rigen de forma directa y necesaria entre los particulares, sin necesidad de la intervención de los poderes públicos.

La dignidad de la persona es la síntesis de los derechos personales y debe ser respetada en todo tipo de situaciones y relaciones jurídicas. La mayoría de estos derechos han sido reconocidos como fundamentales, de tal manera que la garantía al respeto de la dignidad de la persona y de los derechos que le son inherentes no sólo se da en las relaciones entre los ciudadanos y los poderes públicos, sino también en el conjunto de las relaciones sociales; en consecuencia, no se excluyen de la protección las violaciones de derechos fundamentales producidas por sujetos privados. En ese sentido, la función de la *Drittwirkung* en el ámbito laboral difícilmente pasa desapercibida, ya que la empresa, en tanto organización jerárquica de poder, le atribuye un conjunto de facultades de actuación al empleador que presentan potencialidad para lesionar los derechos fundamentales de los trabajadores, tal como lo reconoce el artículo 23º de la Constitución Politica del Perú: "(...) Ninguna relación laboral puede limitar el ejercicio de los derechos constitucionales, ni desconocer o rebajar la dignidad del trabajador(...)".

Así, los «derechos fundamentales como límites al poder» en ocasiones se presentan como límites al poder de los ciudadanos, en efecto, dicha fórmula tendría la virtud de producir efectos entre particulares si entendemos el concepto de poder en el sentido que se ejerce no sólo por el Estado, sino también por los grupos económicos, sociales, o de otra índole. En ese concepto se apoya Rafael de Asís (2000) para definir lo que denomina como la «paradoja del limitador limitado», el sujeto titular de los derechos que era el limitador del poder a través de esos derechos, es, desde ese punto de vista, a quien se limita; es posible entonces una limitación de la actuación de los ciudadanos en relación con los derechos fundamentales de los demás. Bajo ese argumento paradójico, las ideas de límite y de actuación delimitada pueden también aplicarse a ciertos poderes de indudable relevancia social como el que ejercen las empresas; el argumento abunda también en favor de determinadas obligaciones cuyo fin sea la promoción de derechos fundamentales, actuando no sólo como no-transgresorassino también como promotoras de estos derechos.

En conclusión, se entiende por poder a todo tipo de fuerza que pueda afectar a ciertas pretensiones o necesidades humanas, tomando esta concepción se puede hablar entonces del Estado como uno de los posibles sujetos que ejercen el poder, no el único, para interferir en el disfrute de los derechos de la persona. La conexión derechos fundamentales y poder permite entender mejor la situación de los derechos frente a elementos de fuerza y los límites de ésta. Los derechos son así limites y, a su vez, delimitadores de la fuerza. (ASÍS, 2000; RODRÍGUEZ, 1998; VICENTE, 1998)

2.1.2. Los derechos fundamentales de la persona del trabajador

Los derechos fundamentales ejercidos por ciudadanos en una relación por la que, al mismo tiempo, son trabajadores, los convierte en verdaderos derechos laborales en razón del sujeto y de la naturaleza de la relación jurídica laboral en que se hacen valer. Es por ello que la doctrina española reconoce dentro del ámbito del derecho laboral a los derechos constitucionales no laborales, y es, en ese sentido, que Manuel Palomeque López acuña la terminología de «derechos constitucionales inespecíficos» por contraposición a los «derechos constitucionales laborales específicos», como son el derecho a la remuneración o a la jornada laboral. Por su parte, es Fernando de Vicente Pachés (1998) quien denomina «derechos fundamentales de la persona del trabajador» a los anteriormente mencionados derechos constitucionales inespecíficos, sosteniendo que la vigencia de tales derechos en el ámbito laboral supone la manifestación más importante de un nuevo modelo de relación que preconiza la calidad de vida y la realización personal del trabajador. El carácter irrenunciable de estos derechos es reconocido por el artículo 26.2 de la Constitución Política del Perú: "En la

relación laboral se respetan los siguientes principios: (...) Carácter irrenunciable de los derechos reconocidos por la Constitución y la ley. (...)"; igualmente por el inciso 8 del artículo IV de la Ley 28175 marco del empleo público, que vincula al Estado como empleador y a las personas que le prestan servicios remunerados bajo subordinación.

2.2. El derecho a la ídentidad personal

En el articulo 2.1 de la Constitución Política peruana de 1993 se reconoce el derecho a la identidad como un derecho fundamental de la persona, considerándolo como un valor propio de la existencia humana y que, como tal, resulta merecedor de protección jurídica. Este derecho consiste, como señala Carlos Fernández Sessarego (1989), en que la persona no sea perturbada en la proyección social de su personalidad.

Es en el fallo de la Corte Suprema italiana de 22 de junio de 1985 que por primera vez se reconoce a este derecho como un "bien esencial" de la persona, como "su manera de ser en el ámbito social"; resaltando así la proyeoción de la personalidad hacia los demás y, con ella, la objetividad que debe siempre acompañar a la determinación de la identidad personal. En la doctrina jurídica, Adriano De Cupis fue el primero que sistematizó y distinguió el bien jurídico de la identidad de las personas el autor italiano sostiene que ser uno mísmo significa serlo en su aspecto exterior, en el conocimiento y en la opinión de los demás; significa serlo también socialmente, ya que es solamente en ese aspecto en el que la identidad puede ser lesionada por terceros y en consecuencia, constituir un bien jurídico que merece tutela. Consiste también, en la determinación que tiene la persona de afirmar su propia individualidad la que se traduce en su deseo de manifestar, en lo social, aquello que realmente son sus cualidades y acciones propias.

Sin embargo, en la obra de De Cupis, Femández Sessarego (1989) advierte una igualación conceptual restrictiva entre la identidad personal y los llamados signos distintivos de la persona, como son el nombre o el seudónimo; ya estos últimos constituyen exclusivamente la faz estática , biológica y registra] de la identidad, lo que equivale únicamente a la idea de identificación, sin tomar en cuenta su aspecto dinamice, es decir, la proyección social de la personalidad. Similar observación hace el mencionado autor peruano de la obra de Francesco Messineo quien equipara también los signos distintivos y la identidad personal; para Messineo, la persona tiene derécho a no ser contundida con los demás, constituyendo así al derecho a la identidad de la persona en función al nombre con lo cual reduce el concepto al estado del sujeto sin considerar ni su patrimonio cultural ni el ideológico. Los signos distintavos como el nombre, los datos del nacimiento, la filiación o la Imagen, constituyen los rasgos

estáticos del individuo que conciernen exclusivamente a su identificación; mas la identidad, como reflejo externo de su esfera espiritual debe ser reconocida de manera dinámica en relación con los cambios que sufre según las diversas conductas asumidas por el sujeto en el transcurso de su vida.

El nombre o el seudónimo de la persona, cumplen una doble función: por un lado individualizar a la persona con el fin de distinguirla de los demás sujetos y en consecuencia aislarlo del contexto social; y por el otro, identificarla con la finalidad de verificar quien es realmente. (FERNÁNDEZ, 1997)

La identidad personal, como un valor vital que merece protección, exige que el ser individual sea representado tal como es, sin alteraciones, distorsiones, ni desnaturalizaciones; esto es, que no se le atribuyan intenciones o conductas que pretendan menguar o realzar su personalidad más allá de lo que corresponde a la verdad. La protección del derecho a la identidad supone el deber de los demás de respetar los sucesos o hechos personales que cada cual proyecta socialmente; a diferencia de los demás derechos de la personalidad, este derecho no se asume de manera negativa como límite a la acción de los demás, sino como expresión positiva de la propia personalidad. De otro lado, frente a este derecho fundamental de la persona existe la facultad de los demás de exigir certeza en las declaraciones de la personalidad del sujeto. En conclusión, la identidad personal comprende tanto el aspecto estático en relación con los signos distintivos, la existencia y el estado registral del sujeto: y la dinámic,a que es el conjunto de rasgos de l ndole cultural, política, sicológica, moral de la persona. (FERNÁNDEZ, 1987)

El derecho a la identidad personal del trabajador, en el contexto del uso de los recursos informáticos proporcionados por el empleador, merece una consideración especial en el debate jurídico debido a los conflictos que se originan por el uso de éstos y a la potencialidad del daño que puede ocasionar al trabajador usuario de los sistemas de información de las empresas que se conectan en red, específicamente a Internet.

En el año 2004 el Tribunal Constitucional peruano sentencia en el expediente 1058-2004-AA sobre la acción de amparo interpuesta contra la empresa de Servicios Postales del Perú S.A. por el trabajador al que le atribuye la comisión de una falta *grave* por el uso indebido de los recursos informáticos, específicamente el correo electrónico. En dicha sentencia el Tribunal pone en cuestión la verificación de la autoli a de los documentos por los que se atribuye al trabajador actos realizados dentro del sistema de red del empleador, llegando a sostener en su decimoquinto fundamento que "si de alguna forma pudieron haberse manipulado

las vías informálicas, con el objeto de hacer aparecer al recurrente como el remitentede los mensajes cuestionados (...) si no existía certeza plena respecto del supuesto remitente"

La consideración del Tribunal pone de manifiesto la obligación que tiene el empleador de respetar el derecho de identidad del trabajador, no sólo con relación a identificarlo ciertamente en ta red de la empresa con la asignación de un seudónimo, sino también a través de mecanismos que aseguren que las acciones llevadas a cabo por el trabajador en ese ámbito no sean tergiversadas con el fin de proyectar una conducta que no corresponda a su identidad corno usuario de la misma.

Como seilala Femández Sessarego, la protección jurídica de la identidad personal debe: "(...) impedir que se imputen a la persona conductas que no le pertenecen, como (...) evitar que otras [personas) asuman la paternidad de aquellas de las que realmente es protagonista. (FERNÁNDEZ, 1997:254)

2.3. El concepto de intimidad

La intimidad está constituida por el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que las personas mantienen en reserva para si, con la plena libertad para decidir a quien darle acceso, lo que impone a los demás la obligación de respetarla y de no ser obligado a develarla salvo por causa debidamente justificada. La intimidad conlleva entonces lo reservado, lo secreto; pero además, es un elemento existencial del sujeto para si y frente a los demás.

> "Cuando se priva a alguien de libertad no se le puede quitar la intimidad. Se puede impedir una serie de actividades relacionadas con la intimidad, con la vida privada: manejar correspondencia, conversar con amigos, manifestar sus ideas, tener relaciones sexuales, estar soto, etcétera. Precisamente, parte del sufrimiento del recluso es no tener el manejo de sí mismo y no tener medios de desarrollo de la intimidad" (MÉJAN, 1996: 72)

Se puede reconocer como raíz etimológica del término intimidad el vocablo latino *intimus*, que significa lo interior o recóndito; ésta será entonces "la interioridad de la persona, como disposición peculiar del ser humano a la introspección, a to recóndito y secreto" (PÉREZ, 1983: 13).

2.3.1. El origen de la noción de intimidad

No se encuentra en el pensamiento de los antiguos griegos antecedente de la noción moderna de intimidad, por el contrario. lo que se manifiesta es una concepción negativa sobre las pretensiones de los individuos a lo reservado; sin embargo, se encuentra en los filósofos clásicos la idea de contemplación, misticismo o retiro espiritual. Posteriormente, es la concepción cristiana la que sitúa a la persona y su fe, como el centro de las pretensiones de la sociedad. En ese sentido, Santo Tomás de Aquino entiende que:

> "La intimidad es propia de las personas *y* consiste en la conciencia que cada uno de nosotros tiene como sujeto irrepetible. No es lo mismo la interioridad que intimidad. La interioridad tiene un cierto sentido espacial, la tienen todos los seres materiales. La intimidad sólo la tienen los seres racionales. Se trata del núcleo más oculto de cada persona, donde se fraguan las decisiones más propias e intransferibles"[1].

Lucrecio Rebollo (2000) sostiene que. en la concepción de intimidad de Santo Tomás, se distingue claramente entre intimidad e interioridad. atribuyéndole a la primera un carácter de voluntariedad que la interioridad no considera y que constituye una característica esencial de la concepción moderna de intimidad.

Será posteriormente con la aparición de la burguesía y la expansión urbana, que la noción de intimidad se generaliza y se identifica a ésta como parte de la propiedad. Recientemente es la ideología liberal, consecuencia del desarrollo del individualismo, la que genera el concepto moderno de intimldad.

La noción de intimidad o privacidad tiene su origen en el proceso de construcción del Estado liberal; en efecto, es la burguesía como clase social triunfante y responsable de aquél proceso la que va a reivindicar y exigir la protección de su privacidad así como otros derechos ligados a la personalidad. La intimidad, como un espacio personal ajeno a la injerencia del prójimo, la sociedad o el Estado, configura li mites al poder social y político: y el respeto que ésta merece constituye una prueba de legitimidad moral y de la libertad como realización plena de la individualidad. Sin embargo, esa idea burguesa de intimidad estaba concebida exclusivam ente para este grupo selecto sin llegar a la población sin recursos económicos, de ahí que esta idea originaria de la intimidad sea, sobre todo, un privilegio de clase.

---

1 Cita recogida por REBOLLO DELGADO de la obra de FARIÑAS MATONI, L. Ma: El derecho a la intimidad. Trivium. Madrid 1983, pág. 290

Así, las primeras manifestaciones sobre la privacidad están relacionadas con la idea patrimonial, constituyendo ésta un bien más, del que podía disponer su titular (*«privacy property right»*). Resulta así, un derecho a hacer público o a ocultar aspectos de la vida privada, que se caracteriza por la exclusividad y pertenencia de las relaciones de dominio. En un momento posterior del contexto histórico en el que se desarrolla el concepto de privacidad, éste experimenta un importante cambio: de fundamentar su origen y naturaleza en la propiedad privada, pasará a concebirse como la «inviolabilidad de la personalidad» (*«privacy personality»*) el principio del que ahora emanan las facultades de exclusión en el ámbito de la intimidad. En consecuencia, la protección de la intimidad pierde su carácter selectivo para considerarse ya no como perteneciente a una determinada clase social con un sentido patrimonial, sino como inherente a la propia condición humana, a que todas las personas se vean libres de injerencias e irrupciones en su esfera privada; en consecuencia, la privacidad se configura como un presupuesto de la libertad individual. (REBOLLO, 2000; VICENTE, 1998)

2.3.2. Intimidad, libertad e individualismo

Es Lucrecio Rebollo (2000) en su obra «El derecho fundamental de la intimidad», quien proporciona un recuento detallado de la tradición del pensamiento inglés en la que autores como Hobbes. Locke y Mili desarrollan una idea caracterizada por el individualismo; y es también quien señala que contrariamente, son Constant y Tocqueville, en la tradición francesa, los que reconocen la naturaleza social del hombre y, como consecuencia de ésta la necesaria existencia de instituciones que protejan las libertades del individuo; para concluir, que es en la unión de ambas doctrinas que se fo ala concepción moderna de la intimidad.

El mismo autor español, en su recuento, nos indica que para Hobbes, las fuerzas presentes en las relaciones humanas son el deseo de poder y la razón, y que para alcanzar un equilibrio entre ambos se establecen pactos que gene-ran libertad para los individuos. La sociedad y el Estado son definidos por Hobbes como convenciones, y de ahí que al individuo lo sitúe como fundamento esencial de ambos, y al Estado como responsable de la seguridad de los ciudadanos. Considera también a la norma como la voluntad del soberano y ubica a la libertad del individuo en el ámbito en donde no se ha prescrito regla alguna, espacio en el que el individuo puede actuar bajo su propio criterio; constituyendo así una concepción negativa de la libertad.

En cambio, nos dice que para Locke la ley se hace superior a la voluntad del monarca y la propiedad es uno de sus elementos centrales. La principal propiedad del individuo es su cuerpo, el cual lleva antes de unirse en sociedad, y por consiguiente, el pacto social persi-

gue proteger esta propiedad primaria como límite a toda acción exterior; ésta es una concepción positiva de la libertad, que entiende que la finalidad de la ley no es restringir ni suprimir la libertad, sino protegerla y ampliarla. La ley entonces sirve para liberar a los individuos de la presión y la violencia que ejercen los demás, y la libertad se fundamenta en la autonomía, en la propiedad oponible frente a los demás individuos y al poder establecido, y en el plan de vida entendido como el organizador de la vida del individuo; es la parte de la actuación libre del individuo que impone límites a las funciones del poder público, es lo que Locke denomina privacidad, es ésta por la que el individuo puede resistirse a la acción pública que se extralimite, en consecuencia, considera al poder como legítimo cuando éste respeta la privacidad del individuo.

Siguiendo su exposición, Rebollo nos dice que Constant desarrolla el concepto moderno de intimidad no ya como una parte de la libertad, sino por el contrario, considerando a la libertad en el ámbito privado y como esencial a éste. Constant considera que son los límites al poder os que aseguran el ejercicio de la libertad, y estos límites son trazados mediante los derechos individuales, por ello identifica el concepto moderno de libertad con el disfrute de la intimidad.

Es importante resaltar en las perspectivas anotadas hasta aqui, la existencia de un componente significativo en los tres autores: la libertad como concepto.

Para Tocquevine, en cambio, si la libertad radica en el individualismo la vida se reduce a un ámbito estrecho en el que se persigue un oontrol del propio entorno, entonces la vida privada se torna el centro de la existencia y el aislamiento social y la importancia del poder configuran el llamado «individualismo colectivo». Es necesario entonces una definición de intimidad tanto desde un concepto negativo de libertad, por el que la extensión de ésta se contrapone a la ausencia de interferencias de los demás, como desde un concepto positivo, que considere la intimidad como el ámbito de soberanía del individuo en el que no existen obstáculos.

En ese mismo sentido, Mill considera la existencia de dos esferas: la pública, que es el espacio del poder que se rige según normas, y a privada, que es el ámbito del individuo en el que rigen sus propias reglas. La libertad, en consecuencia, consiste en la seguridad que da la existencia de un límite entre lo público y lo privado. El pensamiento y la conciencia del individuo son aspectos de su esfera privada y las relaciones con la sociedad y el Estado, son parte de la esfera pública.

La filosofía liberal concluye en una configuración negativa la libertad, que genera la desconfianza hacia el prójimo y que obliga al individuo a defenderse de los potenciales enemigos

en el ámbito de su vida privada o intimidad; éste, a su vez, constituye una necesidad de la condición racional de la persona. Esta concepción negativa de la libertad es criticada por la sociología debido a los peligros que el repliegue en lo privado conlleva; esto es, la pérdida del contacto con la realidad y el empobrecimiento del individuo, los cuales merman la condición humana. Así, para Durkheim, cuando el individuo se libera de la conciencia colectiva que descompone su personalidad alcanza la libertad acorde con las exigencias sociales. A su vez, Weber considera la manifestación de lo intimo, la reserva para con los demás y la acción económica racional, como las tres instituciones de la individualización que dieron lugar al capitalismo. Actualmente, el individualismo es un valor esencial en la sociedad moderna y está estrechamente relacionado con la libertad de conciencia y de acción y con la incuestionable identificación entre libertad e intimidad. (REBOLLO, 2000)

2.3.3. Definiciones y delimitaciones conceptuales

No es tarea simple definir lo que es la intimidad debido a que, en definitiva, se trata de una cualidad que se sustenta en lo psicológico, en lo social y en lo cultural, lo que induce a la mutación del concepto en el tiempo y en el espacio. Esta dificultad se pone de manifiesto desde que no existe un acuerdo en el término a utilizar.

Con el objeto de distinguir el significado de intimidad. resulta útil en este punto del análisis, una revisión de la definición de aquellas palabras que de forma genérica son identificables con ésta. Tomando las definiciones del Diccionario de la Lengua de la Real Academia Española consideramos el término «intimidad» en su segunda acepción: "zona espiritual intima y reservada de una persona o de un grupo, especialmente de una familia"; y si a ésta la contrastamos con «interioridad»: "cosas privativas, por lo común secretas, de las personas, familias o corporaciones"[2], y con «interior»: "el alma como principio de la actividad propiamente humana"[3]; se constata fácilmente que estos tres términos coinciden en la noción de retiro espiritual de la persona. Además en ellas se encuentra una noción de singularidad que también está contenido en el término «privativo»: "propio y peculiar, singularmente de una cosa o de una persona y no de otras"[4]. En consecuencia se afirma que la «intimidad» es un espacio físico y anímico, delimitado y protegido por voluntad del individuo, que pretende la exclusión de los demás y en él que sedispone a plenitud.

---

2 Segunda acepción.

3 Undécima acepción.

4 Segunda acepción.

Una primera distinción se plantea con relación a la palabra «privado»: "particular y personal de cada uno"[5]; si bien «intimidad» y «privado» coinciden en la falta de conocimiento público, no todo lo que se hace en privado tiene que ser necesariamente íntimo.

Una segunda distinción es con respecto a lo «secreto»: "cosa que cuidadosamente se tiene reservada y oculta"; queda claro que el secreto resulta ser un medio útil a la intimidad pero ésta no se consume en él; y por último la distinción con la palabra «reservado»: "cauteloso, reacio a manifestar su interior"[6]. La conclusión es que los términos «privado», «secreto» y «reservado» tienen en común la pretensión de excluir del conocimiento público determinados aspectos de la vida del sujeto, que a diferencia de la «intimidad», no necesariament se relacionan con una zona espiritual o con elementos distintivos del individuo.

También cabe hacer la distinción con lo «personal»: "perteneciente a la persona o propio o particular de ella", con lo «propio»: "característico, peculiar de cada persona o cosa"[7] y con lo «subjetivo»: "perteneciente a lo relativo al sujeto considerado en oposición al mundo externo"; en estos tres términos hay una clara referencia al sujeto, sin embargo no todo lo personal, propio o subjetivo tiene carácter intimo, por lo que no se da necesariamente el contenido similar.

Una no menos importante distinción se debe hacer entre «intimidad» y «vida privada», debido a que en múltiples ocasiones se suelen utilizar estos términos en forma indistinta por tener el mismo objeto; la diferencia estriba en la intensidad con que opera cada uno. La «vida privada» es un concepto genérico que abarca todo aquello que no es, o no se quiere que sea, de conocimiento general; existe en ella un núcleo que se protege con mayor cuidado porque resulta esencial en la formación de la persona, éste es el que denominamos «intimidad». La «intimidad» es lo recóndito; la «vida privada». en cambio, lo más próximo desde la posición de los demás e incluye un elemento de relación con la sociedad ante la que se asume una conducta. La «intimidad» es una parcela de la «vida privada»; no pierde la condición de íntimo ni de vida privada aquello que los demás puntualmente conocen. (REBOLLO, 2000)

5 Segunda acepción.
6 Segunda acepción.
7 Segunda acepción.

2.3.4. Delimitación jurídica entre intimidad, privacidad *(privacy)* y vida privada

La doctrina jurídica alemana en su esfuerzo por la comprensión de lo privado introdujo, mediante el pensamiento de Hubmann, la denominada «teoría de las esferas» (del alemán *Sphärentheorie);* ésta distingue las siguientes ideas: la «esfera íntima» (del alemán *lntimsphäre),* quehace referencia al ámbito de to secreto *y* que se lesiona cuando se conoce por los demás; la «esfera privada» (del alemán *Privarsphiire),* que equivale a la noción de lo íntimo propiamente *y* que protege el ámbito de la vida familiar y personal; y por último, la «esfera individual» (del alemán *Individualsphäre),* que hace mención a la individualidad de la persona. El problema con esta teoría es que las esferas no actúan como compartimientos estancos, sin interrelación; de hecho pueden pasar a formar parte unas de otras mediante el consentimiento de la persona; esta teoría ha sido superada por la jurisprudencia del Tribunal Federal alemán que se pronunciara sobre el Censo de Población *y* que d io origen al denominado derecho de «autodeterminación informativa»; considerando ese nuevo derecho, el concepto de intimidad pasó de ser significado de aislamiento y reserva, a ser también control de lo que pertenecea nuestra vida privada.

La doctrina y la jurisprudencia estadounidenses son las que más han aportado a la evolución conceptual de la intimidad, ésta se puede sintetizar en: la protección de la esfera privada frente a intromisiones indebidas; el respeto a las opciones de asociación o creencia de las personas; la defensa de la libertad de elección y, por último; la posibilidad de acceso y control de los individuos a la información que les pertenece. El concepto de *privacy,* se asocia en puridad con el de vida privada y no con el de intimidad: para los norteamericanos todos los grados de intimidad se incorporan en el concepto de *privacy,* a diferencia de los desarrollos conceptuales en Europa y en especial España, en donde los términos se diferencian tanto etimológica como jurídicamente. La palabra *privacy* está cargada de un sentido que ha sido dado por la cultura de la cual ha surgido y no admite asimilación con la noción grecolatina de intimidad. (GONZÁLEZ, 1990; REBOLLO, 2000)

Otro intento de definición es el propuesto en el Congreso ae Juristas Nórdicos sobre el derecho a la intimidad llevado a cabo en 1967, siendo esta definición amplia e imprecisa: "el derecho a vivir en forma independiente su propia vida, con un mínimo de injerencia ajena", c onsiderando injerencias, entre otras: el uso del nombre o la identidad personal; el acecho, el acoso o et plagio; la violación a la correspondencia o ta re ve lación de hechos penosos de la vida privada o información cubierta por el secreto profesional.

La noción de privacidad muestra un aspecto descriptivo que hace mención al distanciamiento con respecto a los demás, y otro normativo que da origen al *right to privacy*, que ha sido traducido como derecho a ta intimidad, por el que se reconoce el derecho al control del ámbito privado como una relación negativa de no-interfencia entre el individuo y el público. Fue concebido para la defensa ante tos medios de comunicación como un «derecho a ser dejado solo» (del inglés *rigth to be let alone*) siendo identificado con los conceptos de retiro, secreto, propia imagen y autonomía ya que con frecuencia *privacy* hace referencia indistintamente a todos o a cualquiera de ellos. El retiro y el secreto aluden a una zona o extensión de la que se excluye a los demás; en ésta, las actividades, objetos, información e inclusive personas pueden quedar a salvo de irrupciones del público; por et contra rio el concepto de la propia imagen, si bien es un atributo personal, como el nombre, sólo constituye un objeto desde el punto de vista jurídico en tanto las personas hacen uso público de ésta o la explotan económicamente; en consecuencia, el ámbito de la intimidad termina en donde empieza el derecho de la propia imagen. En cuanto a la autonomía, la relación resulta ser complicada: ésta, a diferencia de la intimidad que es una esfera de libertad negativa que hace frente a las intromisiones, es una de libertad positiva o de actuación. Resulta entonces que la autonomía no se asimila al retiro y al secreto, sin embargo, es obvio que ésta es aquello que la zona de retiro y secreto tiene por objeto proporcionar a la persona; si bien la intimidad y la autonomía son conceptos diferentes están vinculados de una manera indispensable para la cabalcompresión del *right to privacy*.

Existe una diferencia entre los conceptos intimidad y *privacy* que constituye una cuestión de grado: la primera hace referencia a la zona de retiro *y* secreto «espiritual», en tanto la segunda lo hace igualmente a una zona de retiro y secreto pero que no necesariamente tiene esta última cualidad.

Toda esta variedad de criterios hace que no exista un concepto único, entonces resulta concluyente que es necesario aceptarlo en su complejidad, variabilidad y alienación social.

A través de la «teoría de la actuación» algunos autores intentan delimitar los ámbitos de la vida pública. la privada y la intimidad, aquéllos consideran la actuación como una acción singular que en sí no es ni pública, ni privada o íntima; sino según sea el contexto, igualmente singular, en el que se desenvuelve. Así, las conductas públicas son necesariamente perceptibles por los demás; las privadas en cambio no pueden serlo, salvo por negligencia del actor o el fisgoneo; y por último, las íntimas son las que están ocultas al observador y sólo se pueden deducir de lo dicho o hecho por el sujeto.

Para ciertos autores, la intimidad se diferencia de la vida privada en razón a que la primera es un fenómeno psicológico y, como tal, está fuera de la aplicación del Derecho; mientras que la segunda se constituye en una manifestación externa que si puede ser conceptuada y regulada jurídicamente. Si bien esta distinción simplifica la actividad de regulación, no toma en cuenta que, como parte de la condición humana, la intimidad es un derecho fundamental que exige un tratamiento profundo. Otros autores pretenden ubicar a las categorías de la vida privada: el dornicilio, la correspondencia, la familia y el secreto profesional, como constitutivas de la intimidad. (MÉJAN, 1996; RODRÍGUEZ, 1998; VICENTE, 1998)

2.3.5. La intimidad y el Derecho

Resulta obvio que el fuero interno de cada individuo está excluido del Derecho en la medida que lo oculto, en su condición de tal, no puede ser regulado por el ordenamiento jurídico, a ello se le concibe como la irrelevancia jurídica de la intención oculta de por sí. Así descrita la intención, se observan similares caracterlsticas que en la noción de intimidad, en consecuencia se afirma que la «intimidad personal» da origen a la intimidad entendida en su sentido más amplio; la personal es lo más central de aquélla, la parte que tiene como referente s ingular al sujeto. Se consideran circunstancias constitutivas de la «intimidad personal» las de la vida familiar; como el nacimiento, el matrimonio, las enfermedades *y* fallecimientos; las de la vida amorosa o profesional; los rasgos del rostro o el comportamiento de la vida cotidiana. (VICENTE, 1998)

Existe intimidad en aquella zona de retiro y secreto que lo es por voluntad propia del individuo, siempre que ésta sea reversible: esto es, que sea posible salir de ella por decisión propia o por la irrupción exterior. (RODRÍGUEZ. 1998)

Las nuevas tecnologías de la información que hacen posible el tratamiento automatizado de datos de carácter personal, aproximan al individuo at riesgo que representa la acumulación de datos por acción del Estado o de los ciudadanos; lo que obliga, bajo el principio de que todo poder o actividad susceptible de lesionar derechos debe estar necesariamente sujeto a Derecho, a normar esa actividad. Se han dado sucesivas fases en la protección jurídica de los datos personales de manera similar a las de l as generaciones de microprocesadores o de los derechos humanos; de éstas distinguimos tres: la autorización previa para la elaboración de los bancos de datos, la garantía sobre los datos sensibles que repercuten en la intimidad, y por último, la prevención de consecuencias sobre la potencialidad y funcionalidad del tratamiento automatizado de aquellos datos. El autor español Pablo Lucas Murillo (1990) introduce el término «autodeterminación informativa» con el objeto de brindar protección a la

información individual frente a un uso incontrolado, tomando esto en consideración, el derecho a la intimidad se disgregarla en una intimidad física o clásica y en una intimidad informativa por la que el individuo dispone cómo y en qué medida se comunica información sobre uno mismo. (REBOLLO, 2000)

2.4. El derecho a la intimidad

La noción de intimidad que la filosofía clásica asimilaba con la soledad y el aislamiento del individuo ha ido siendo descartada en sus sucesivas proyecciones en el campo jurídico. Actualmente, la concepción juridica de intimidad se ha trasladado desde el ámbito de ta soledad al de la convivencia o de las relaciones sociales, pues de otro modo, no tendría relevancia jurídica. El problema de la intimidad se presenta sólo a través de las manifestaciones o incidencias externas de la vida privada cuyo ejercicio se halla garantizado jurídicamente y, como tal, o es un problema jurídico o no existe. La convivencia se ejercita a través de la comunicación como elemento que socializa lo más íntimo del individuo y origina la propia noción de intimidad, como una categoría cultural e histórica. (PÉREZ, 1983)

Siendo la intimidad y la vida en sociedad elementos de la naturaleza humana resulta lógico que la normatividad proteja dicho ámbito personal de las injerencias de los demás. El concepto del derecho a la intimidad es consecuencia de la evolución social del ser humano, su determinación varía según las culturas y ordenamientos jurídicos ya que depende de tas concepciones sociales, y si a ello se incorpora el avance de la tecnología de la información, se pone de manifiesto la complejidad en su delimitación *y* la dificul tad para su ejercicio efectivo.

En los países de habla hispana el consenso para denominar este derecho es el de «intimidad», aunque algunos adoptan el de «vida privada» en consideración a que ésta, como manifestación de la primera, es la que en realidad puede ser regulada por el Derecho; sin embargo, la intimidad es un concepto amplío que comprende tanto la realidad profunda de la naturaleza del ser humano corno sus manifestaciones y, ambas, deben merecer la atención del jurista.

El derecho a la intimidad contiene un elemento de voluntad en la medida en que la condición de intimo o privado depende de que el titular del derecho desee mantenerlo en ese estado, y un elemento de determinación que toma en cuenta la finalidad como críterio para distinguir cuando es ilícito usar una información que conculca el derecho a la intimidad.

El derecho a disfrutar la intimidad consiste en controlar esa zona de retiro y secreto que voluntariamente ha sido dispuesta por el individuo, ese control que define a este derecho fue considerado por el Tribunal Constitucional alemán desde sus primeras decisiones para formar un derecho de autodeterminación (del alemán *Selbstbestimmungsrecht*) sobre nuestras zonas de retiro y secreto.

Con relación al sujeto pasivo del derecho, éste es en principio universal en cuanto la generalidad de las personas están obligadas a respetarlo, sin embargo este sujeto se individualizará al surgir una situacióno hecho que lo obligue a recolectar sólo aquellos datos o información que sean relevantes para los fines solicitados, conservarlos por el tiempo necesario y no utilizarlos ni comunicarlos con propósitos que no sean los debidamente autorizados por el titular. La regulación del derecho a la intimidad, en ese sentido, dispone cuándo se puede o debe develar ésta en caso de necesidad, autorización o bienestar común como consecuencia de un conflicto con otros derechos. Históricamente se ha reconocido el derecho de la colectividad de imponer a los individuos la protección del interés social. (MÉJAN, 1996)

La historia del derecho al respeto de la intimidad del individuo tendrá en el aspecto religioso una significativa importancia; basándose en la concepción moral y la de buenas costumbres, la iglesia y el propio Estado serán los primeros intrusos en el ámbito de la conciencia del individuo y limitadores de las manifestaciones de culto; el carácter benevolente de este respeto evolucionará hacia el reconocimiento normativo de la garantía así como su carácter absoluto, permanente y general. Es en el articulo 126 del Estatuto de Sayona de 1808 que se le da rango constitucional con relación a la inviolabilidad del domicilio: "La casa de todo habitante en el territorio de España y de Indias es un asilo inviolable; no se podra entrar en ella sino de diay para un objeto especial determinado por ley, o por orden que dimane de la autoridad pública", (REBOLLO, 2000: 59)

La Iglesia Católica tuvo, nasta el siglo XIX, el control de la información sobre los individuos que profesaban su fe, la mayoría del pais, en la medida que contaba con el registro de nacimientos, matrimonios y defunciones; el conocimiento del Estado sobre los individuos se restringía hasta esa época a aspectos tributarios o de prestación de servicios: los primeros datos que éste acopia son a través de los censos de población. En la actualidad esta situación ha sufrido un cambio ostensible debido principalmente a la aplicación de la tecnología de información sobre los servicios estatales. El recojo, transformación y comparación de datos con fines estadísticos afecta a los individuos frente a la acumulación de datos, la seguridad de los mismos es el factor para la protección de la intimidad.

2.4.1. Evolución histórica del derecho a la intimidad

En 1873 el juez norteamericano Thomas M. Cooley publica su obra *The elements of torts*, en ella expone la conclusión de que la privacidad constituye el derecho a ser dejado en paz (del inglés *right to be alone);* en 1890 Samuel, Warren y Lou is Brandeis publican su artículo *The right to privacy,* en el que desarrollan ese concepto de forma extensa y con mayores fundamentos jurídicos. A los tres años de esa publicación un tribunal de la ciudad de New York en el caso *Marks v. Joffra* utiliza el concepto de privacidad para argumentar el derecho del estudiante de leyes en contra de la publicación de su fotografía en un periódico promoviendo un concurso de popularidad al que éste se oponía. Sin embargo, el concepto pasará por una desaprobación con mayor repercusión social en el caso *Robinson* v. *Rochester Folding Box Company* presentado ante la Corte de Apelaciones de la propia ciudad de New York en 1902; el argumento de la sentencia frente al reclamo ante el uso de la imagen de la demandante en los empaques de los productos de la demandada sostuvo que, en todo caso, el daño ocasionado sólo era moral y que su reconocimiento originaría una gran cantidad de litigi os que los tribunales serían incapaces de resolver. El rechazo a esa decislón judicial trajo como consecuencia que en la legislatura del año siguiente el Estado de New York incluyera artículos en Ley de Derechos Civiles por los que se dispuso que el uso con fines publicitarios del nombre o la imagen de cualquier persona, sin autorización escrita de ésta, constituyera un ilícito.

No puede pasar desapercibido el hecho que la génesis de este derecho se encuentre en principios generales, en pretensiones personales y en la comprobación de una necesidad social por parte de un particular, sin antecedente normativo, sin la Intervención de un interés económico o sin que ocurra un conflicto social que cause grave perjuicio para el Estado o la sociedad.

El concepto desarrollado por Warren y Brandeis sostiene que el individuo debe contar con la protección plena de su persona y sus propiedades y si bien parten del fundamental derecho a la propiedad, éste no se limita a lo tangible, se extiende a lo inmaterial. Los autores reconocen en el derecho a la propiedad intelectual y artística del *common law*, una aplicación del derecho a la privacidad que no constituye un derecho de propiedad privada, sino la inviolabilidad de la personalidad; sobre este principio que protege cualquier producción del intelecto o las emociones, se funda la protección a la imagen personal, a las expresiones, actos y relaciones personales y familiares.

La concepción estadounidense del derecho a la privacidad basada en la absoluta autonomía del sujeto resulta ser en extremo individualista, a tal punto que la Corte Suprema en el caso

Roe v. *Wade* de 1973 fundamenta en el *right to privacy* su decisión de afirmar el derecho constitucional al aborto. (REBOLLO, 2000)

En el Perú el derecho a la intimidad está reconocido en el artículo 2.7 de la Constitución Po-Política de 1993 y está expresamente referido a la intimidad personal y familiar, considerándose familia a los parientes en línea directa y los colaterales hasta el cuarto grado de consanguinidad y segundo de afinidad. (RUBIO, 1999)

Asimismo el artículo 14 del Código Civil peruano recoge también el derecho a la intimidad personal y familiar declarando que ésta "no puede ser puesta de manifiesto sin el asentimiento de la persona o si ésia ha muerto, sin él de su cónyuge, descendientes, ascendientes o hermanos".

Por último, el artículo 154 del Código Penal peruano tipifica el delito de violación de la intimidad: “El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios (...)”

2.4.2 . El derecho a la intimidad en las normas internacionales

El articulo 5° de la Declaración Americana de Derechos y Deberes del Hombre aprobada en la novena Conferencia Internacional Americana en Bogotá, en 1948 es la primera norma internacional significativa que establece que: "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". Este documento también acoge las dos manifestaciones clásicas de la intimidad, la inviolabilidad del domicilio (artículo 9°) y de la correspondencia (articulo 10°).

La Declaración Universal de los Derechos del Hombre adoptada y proclamada por la Resolución de la Asamblea General 217 A del 10 de diciembre de 1948 establece en el articulo 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 reputación. Toda persona tiene el derecho a la protección de la ley contra tales ataques o injerencias". El objetivo de otorgar protección a la vida privada es el mismo que el de la tutela de la honra y la buena reputación, la dignidad de la persona.

2.4.3. La dignidad de la persona como fundamento del derecho a la intimidad

La característica del constitucionailsmo desarrollado mundialmente a partir de la mitad del siglo pasado es la de considerar a la dignidad del ser humano como el valor jurídico superior. Derecho en el Perú el articulo 1° de la Constitución Política así lo muestra: "La defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado".

La razón por la cual la dignidad es inseparablede la idea de libertad radica en la condición racional de la persona que reclama un ambiente en el que desarrolle su naturaleza humana. La dignidad es sustancial a la persona sea ésta reconocida por el Derecho o no: éste no la crea sino garantiza su respeto y hace posible su desarrollo. La incorporación constitucional de la dignidad de la persona cumple la función de fundamento para la interpretación y legitimación del ordenamiento jurídico y el contenido de los derechos y libertades constitucionales, a la vez que se constituye en una demarcación para los mismos. (REBOLLO, 2000)

2.4.4. Concepto del derecho a la intimidad

Un primer concepto «objetivo» del derecho a la intimidad es el que desarrolla la doctrina jurídica alemana a través de la «teoría de las esferas» expuesta párrafos arriba. Por contraposición, el concepto «subjetivo» del derecho a la intimidad es en esencia el denominado «derecho a la autodeterminación informativa» (del alemán *informationelles Selbstbeslimmungsrecht*), cuyo origen es la sentencia del Tribunal Constitucional alemán en el caso de la Ley del Censo y de Población que interpreta el artículo 2 de la Ley Fundamental de Bonn como: "la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida".

El tratamiento automatizado de los datos personales motiva la concepción de la denominada «teoría del mosaico» que aborda el tema constatando que la separación entre lo público y lo privado resulta relativa y que los datos considerados irrelevantes para la intimidad de la perzona, unidos entre sí, forman. como en un mosaico, un conocimiento que establece un riesgo para la protección de la intimidad; sin embargo, su validez está en la utilidad para resolver casos particulares más que como base para el desarrollo del concepto.

De otro lado. existen planteamientos que han prescindido de la necesidad de elaborar un concepto del derecho a la intimidad y han desarrollado solamente su contenido, sin embar-

go, esto impide distinguirlo con relación al derecho al honor o al de la propia imagen y delimitarlo respecto a otros derechos.

Por último, la posición ecléctica combina los conceptos objetivo y subjetivo para obtener como resultado una concepción que incluye el derecho de defensa y a controlar lo que al individuo le afecta; el derecho a la intimidad protege asi la autorrealización del individuo. En cuanto derecho de defensa está ligado a la dignidad de la persona, en cuanto potestad de control tiene relación con la libertad.

La importancia del control o autodeterminación ha ido acentuándose con directa relación al creciente recojo, registro y uso de datos personales por los poderes públicos, actualmente éste es un aspecto crítico del derecho a la intimidad, un derecho cuyo objeto es brindar al individuo el poder de controlar cuándo y dentro de qué límites ese poder puede obtener y hacer uso de información que le toca personalmente. La autodeterminación es la interpretación juridicade la idea de control que informa al concepto de intimidad, es la noción que permite constatar que es la voluntad del sujeto la que, en última instancia, determina el ámbito de intimidad a que éste tiene derecho; no es pues distinta a la intimidad sino un elemento definitorio de ésta. La «autodeterminacióninformativa» o también llamada «libertad informática» es el control del uso de dichos datos cuando se almacenan en programas informáticos.

Las constituciones políticas han admitido con anterioridad al derecho a la intimidad la protección de áreas específicas de ésta. como son el domicilio y las comunicaciones personales las que atrajeron mayor interés de las personas en razón de estar más expuestas a injerencias; ya desde el reconocimiento de dichos derechos la idea de control o autodeterminación estaba contemplada, pues dentro de ambos la capacidad de control es tal, que simplemente se presume. Se puede así definir el derecho a la intimidad como aquél llamado a controlar o autodeterminar nuestras zonas de retiro y secreto.

Se distingue así en el derecho a la intimidad dos aspectos: uno negativo, que hace alusión a la necesidad de rechazar la posibilidad de conocimiento improcedente de cuanto hace referencia a la persona y otro positivo, que otorga al titular del derecho la facultad de controlar la inforrnación relacionada a su persona.

Es entonces el principio de respeto a la vida privada el que evoluciona en un derecho que sirve de base a la libertad de las personas y, por consiguiente. como fundamento del Estado democrático: el derecho a la intimidad. (REBOLLO. 2000: RODRIGUEZ, 1998; VICENTE. 1998)

2.5. El derecho al secreto y a la inviolabilidad de las comunicaciones y documentos privados

El derecho al secreto de las comunicaciones se reconoce en el año 1790 mediante Decreto de la Asamblea Nacional de Francia, y luego de más de dos siglos de su origen aún sigue siendo un concepto incierto, más aún ahora, debido a la aplicación de las nuevas tecnologías de la información que, al revolucionar la comunicación remota, plantean la necesidad de redefinir la concepción jurídica sobre secreto y comunicación.

La necesidad del secreto de las comunicaciones como un derecho tiene su génesis en la relación con la idea de intimidad; sin embargo, resulta de importancia destacar la necesidad de reconocer su independencia con relación a esta última, caracterizada por su ambigüedad conceptual. La importancia de la protección de la intimidad y del secreto de las comunicaciones como derecho integrado a ella, está en función a la libertad que proporcionan al individuo y su valor para la constitución y desarrollo de los Estados democráticos.

La susceptibilidad al cambio en el concepto de un derecho, comporta siempre la dificultad para establecer qué situaciones quedan dentro de su ámbito de aplicación y cuáles no, y lógicamente , da lugar a interpretaciones diversas a ese respecto. Aquellos derechos de contornos imprecisos, como es el caso del derecho a la intimidad, suelen ser delimitados por los jueces en buena parte de los casos que se les presentan; sin embargo, esto que puede considerarse como una práctica democrática, resulta un contrasentido en la medida en que en realidad constituye una forma de restringir el alcance de los derechos fundamentales, debido a que éstos son derechos de la persona y no de la sociedad. Incluso pueden ser ejercidos en oposición a ésta última, representada por la mayoría de los individuos. De ahí que esa manera de definir los derechos imprecisos venga a ser una visión «reduccionista» de su ámbito de protección. Estas imprecisiones conceptuales de la intimidad, sólo pueden ser superadas mediante la separación de zonas determinadas que se reconocen como derechos autónomos, este es el caso del derecho al secreto de las comunicaciones.

De manera gráfica, Blanca Rodríguez Ruiz (1998) describe la intimidad con relación al derecho al secreto de las comunicaciones, como un «telón de fondo» sobre el que este último se pone de relieve, por lo que la autora lo describe como un subderecho, que si bien cuenta con autonomía en su definición e interpretación, no llega a desprenderse de ese telón de fondo que le brinda, por un lado, modelos de interpretación comunes, y por otro, le sirve de complemento en la cobertura y protección de situaciones que no se ajustan estrictamente dentro de sus límites. De ello se deduce la trascendencia práctica que tiene el derecho a la

intimidad, que si bien es independiente del derecho al secreto de las comunicaciones, actúa con relación a éste como un derecho subsidiario y suplementario.

Según la misma autora, tanto la intimidad corno el derecho que le corresponde, pueden considerarse desde dos puntos de vista: uno individualista y el otro participativo. Desde el primero, la protección de estos derechos responde a un interés subjetivo, en tanto, desde el segundo, se hace posible la libre participación del individuo en lo público o social, ya que en la medida en que la persona no tiene control de hasta qué grado su actividad es conocida, y por quién, ésta no actuará libremente sino condicionada por el temor a que la información que pueda existir sobre ella sea empleada en su perjuicio. Una u otra percepción, o la combinación de ambas, son necesarias para un examen del derecho a la intimidad; las consecuencias prácticas de tomar el enfoque individualista es la reducción del ámbito de protección, en tanto que la perspectiva del derecho como condición para la libre participación define más ampliamente su ámbito de protección. Esta última posición resalta la relación existente entre intimidad y autonomía, ya que la libre participación es un presupuesto para el desarrollo de un Estado democrático.

En conclusión, la intimidad merece protección no sólo porque es deseable contar con una zona de secreto y retiro libre de intromisiones, sino porque ésta permtie a la persona desarrollar actividades al margen de todo tipo de control, es decir, porque le concede un ámbito de libertad de actuación, un espacio dentro del cual puede actuar con plena libertad. El hecho es que la zona de secreto y retiro ofrece cobertura para el libre ejercicio de actividades, que de otro modo no podrían llevarse a cabo, y que la posibilidad de actuar libremente en privado condiciona la libre actuación en público. La protección de la intimidad está al servicio de la libertad tanto en su concepción negativa como positiva, esto es, la liberad de poder controlar nuestra actuación como personas.

Las doctrinas desarrolladas en Alemania y los Estados Unidos son ejemplos extremos de las consecuencias prácticas de estas dos visiones de la intimidad. En el primer caso, el derecho al libre desarrollo de la personalidad reconocido en el artículo 2.1 de la Ley Fundamental de Bonn, comprende al derecho a la intimidad y fue la decisión del Tribunal Constitucional alemán sobre la Ley del Censo de Población, la que acuñó la expresión «autodeterminación informativa», y elaboró además, la doctrina de que la tutela de este derecho es presupuesto para la existencia y mantenimiento del Estado democrático, en términos coincidentes con el carácter participativo del derecho a la intimidad. Esta reflexión expresa que, cuando el derecho a la intimidad entra en conflicto con otros derechos o principios constitucionales, los limites a su protección han de ser estrictamente excepcionales y proporcionales a los objetivos de permanencia del Estado democrático.

En cambio, en los Estados Unidos la visión de la intimidad como bien exclusivamente individual, resulta radicalmente opuesta; en consecuencia, el derecho a un determinado ámbito de intimidad se pierde si no se toman las medidas adecuadas para protegerlo frente a intromisiones de terceros, definición que resulta lo más restrictiva posible e incompatible con la visión participativa descrita. (RODRÍGUEZ, 1998)

2.5.1. La estructura del derecho al secreto de las comunicaciones

El objeto de los derechos fundamentales se da en dos ámbitos: el de «cobertura» y el de «protección»; cuál es la relación entre ambos equivale a analizar su estructura. Esta concepción bivalente de los derechos fundamentales se conoce como «estructura compleja a dos niveles», y define por un lado al «ámbito de cobertura», como un principio que impone el mandato constitucional para el amparo del derecho, no de forma definitiva y en cada oportunidad, sino *prima-facie;* tal mandato se transforma en norma de aplicación inmediata y definitiva en su «ámbito de protección», como resultado de haber ponderado el derecho frente a otros principios constitucionales.

Otra concepción que rechaza aquella estructura bivalente, nace de las denominadas teorías institucionales de los derechos fundamentales, las que entienden a la Constitución Política como un sistema orgánico del que se origina. y en el que se comprende, a todo el orden jurídico; lo que equivale a afirmar que la Constitución Política es la única fuente de definición, no sólo de un ámbito de cobertura, sino también de protección, no existiendo posibilidad de conflictos entre principios constitucionales, pues basta realizar una lectura adecuada de la misma para descubrir las fronteras conceptuales de los principios afectados. Aquello significa que el ámbito de cobertura equivalente al de protección.

Dicho de otra manera, los derechos fundamentales son exclusivamente reglas constitucionales y no una combinación de principios («ámbito de cobertura») y de reglas («ámbito de protección»). Sin embargo, las consecuencias prácticas de esta concepción de estructura simple, lleva a entender que los limites a estos derechos no requieren justificación alguna para ser considerados legítimos, debido a que tales limitaciones no son externas a los derechos, sino inherentes a su propia definición; entonces, no se trataría de límites o restricciones en sentido estricto, sino que ya estarían definidas en la Constitución, y por tanto, no cabría protección frente a interpretaciones restricti vas del ámbito de cobertura-protección de los derechos fundamentales. Otra consecuencia práctica de dicha concepción institucional, es la que se refiere a la ponderació n de los derechos fundamentales entr e si o frente a otros principios constitucionales; la ponderación no sería algo funcional que afectara la aplicación de los de-

rechos en casos concretos, sino algo inherente al concepto de los mismos, y en consecuencia, afectaría la carga de la argumentación en casos de conculcación.

En la concepción de la estructura de los derechos fundamentales a dos niveles, la persona que sostiene haber sufrido una violación a su derecho. debe argumentar con relación al acto que ha afectado al éste en su ámbito de cobertura; y quien es acusado de ese acto de violación, debe argumentar que su actuación respeta los requisitos que le impone la Constitución y el resto del ordenamiento jurídico, por lo que no vulnera el ámbito de protección del derecho. En et caso de una estructura simple en la que los derechos sólo existen dentro de su ámbito de protección, la persona que reclama vulnerado su derecho debe argumentar primero. que ha existido una Interferencia con el ejercicio del mismo, y segundo, que dicha interferencia ha sido inconstitucional al no respetar la ponderación que la Constitución dispone. Este raciocinio plantea dificultades para establecer las circunstancias negativas, debido a que la carga de probar que la actuación violatoria no ha respetado los requisitos constitucionales recae en la persona obligada a argumentar la violación del derecho, a pesar que esas circunstancias se encuentran fuera de su control. Esta dificultad explica porque la tendencia general sea separar el «ámbito de cobertura» del «ámbito de protección». (RODRÍGUEZ, 1998)

2.5.2. El ámbito de cobertura

El artículo 2.10 de la Constitución Política peruana garantiza todo tipo de transmisión de información entre personas con independenciade los medios empleados y de ta distancia entre éstas, así como la inviolabilidad y el secreto de los documentos privados: "Toda persona tiene derecho: (...) Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. (...)"

Este precepto es corroborado por el artículo 16 del Código Civil de 1984: "La correspondencia epistolar, las comunicaciones de cualquier género o las grabaciones de la voz, cuando tengan carácter confidencial o se refieran a la intimidad de la vida personal y familiar, no pueden ser interceptadas o divulgadas sin el asentimiento del autor y, en su caso, del destinatario. (...)"

Además et articulo 4 de la Ley de Telecomunicaciones, cuyo texto único ordenado fue publicado en 1993, reconoce el mismo derecho: "Toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones. (...)"

En cuanto a las características de las comunicaciones, se debe precisar que las que se realizan de manera presencial no ofrecen ninguna garantía de secreto, su naturaleza no asegura que individuos no autorizados puedan percibirlas, oírlas o grabarlas. Por otro lado, las comunicaciones a distancia o telecomunicaciones, se distinguen técnicamente entre las que se realizan por «canal cerrado» de las que lo hacen por «canal abierto»; éstas últimas permiten el acceso a terceros, por ejemplo. las que se transmiten por ondas accesibles desde un receptor de radio ordinario y, por ello, tienen características comunes con las que se realizan de manera presencial.

En cambio en las comunicacionesa distancia por «canal cerrado» el secreto es una característica inherente, pues éste está técnicamente garantizado. Dicha garantía se apoya en una expectativa razonable de intimidad. puesto que la interceptación de esta clase vulnera el secreto en que esa comunicación se lleva a cabo. En la medida en que las comunicaciones presenciales y las telecomunicaciones por «canal abierto» no ofrecen garantías técnicas de secreto, se justifica reconocer un derecho especifico dentro del derecho de la intimidad, un derecho que no se limite a proteger expectativas razonables de secreto, sino el secreto en cuanto elemento característico de un sistema de comunicación.

A partir de esa definición queda por explicar quién de los que toma parte de una comunicación tiene derecho al secreto, o lo que es lo mismo, qué parte tiene una expectativa técnicamente razonable de secreto en el acto de comunicación, más allá de quién tiene un derecho de propiedad sobre lo comunicado. Con relación al contenido de la comunicación, las partes confían en su secreto en la medida en que éste está técnicamente garantizado, en tan to que con relación a las circunstancias que rodean el propio acto de comunicación, las partes tendrán derecho al secreto de aquellas situaciones que conozcan y frente a cualquier persona excluida de dicho acto, incluso frente a la otra parte en la comunicación.

El secreto entonces es inherente al proceso de comunicación y no existe garantia técnica de secreto más allá de éste, sin embargo, el artículo 2.10 de la Constitución no sólo comprende al proceso en sí, sino también al objeto que materializa la comunicación una vez que ésta haya concluido, por ejemplo, las carlas y telegramas una vez recibidos e incluso abiertos, la cinta magnetofónica en la que se haya grabado una conversacióntelefónica, o la copia digital o impresa de un correo electrónico. Pero también existe una expectativa razonable de secreto cuando no existe un soporte técnico alguno, en estos casos debe buscarse un parámetro alternativo que es la idea de control. Sólo aquél que tenga bajo control el objeto de la comunicación y, en la medida en que lo tiene, puede confiar en su secreto y tendrá por tanto derecho a él.

Otro aspecto a explicar es referente a frentea quién existe el derecho al secreto de las comunicaciones. En el caso de las comunicaciones escritas, frente a la persona que actúa como mensajero, el secreto no incumbe al nombre y la dirección del emisor y receptor ni el tiempo en el que se realiza la emisióno recepción de la misma, como tampoco del contenido que aparezca expuesto ante su vista, como en el caso de las tarjetas postales o de los telegramas. Si estarán protegidas, en cambio, las circunstancias y el contenido en la medida en que permanezcan secretos, incluso si conocer dichas circunstancias o el contenido, por parte del interrnediaño, sea indispensable para llevar a cabo la comunicación, por ejemplo el caso de los mensajes enviados por correo electrónico: de ahi que el deber de los proveedores del servicio de mantener en secreto las circunstancias que para ellos no son secretas sea indispensable para el funcionamiento del sistema.

La norma constitucional referida al derecho al secreto de las comunicaciones se aplica entonces a las telecomunicacionespor «canal cerrado», en tanto que el secreto es inherente a éstas. Las que se realizan por «canal abierto», siempre que su contenido sea considerado íntimo, estarán cubiertas por el derecho a la intimidad que cumplirá la función de derecho suplementario; ya que sí bien el hecho de participar en una comunicación de ese tipo supone la renuncia al secreto, no se renunciaa controlar una eventual grabación y distribución posterior, que si violaría el derecho a la intimidad de la parte afectada bajo la aplicación de la noción de autodeterminación. (RODRÍGUEZ, 1998)

2.5.3. El ámbito de protección

El artículo 2.10 de la Constitución Poiítica del Perú exige que las medidas restrictivas del derecho al secreto e inviolabilidad de las comunicaciones y documentos privados se basen en una resolución judicial:

> (..) Las comunciaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado por el juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen. Los documentos privados obtenidos con violación de este precepto no tienenefecto legal. (...)"

Corresponde a los jueces ponderar los intereses involucrados y determinar si ante las circunstancias debe o no prevalecer el derecho, es entonces la motivaciónde la resolución judicial la manera de comprobar que se ha llevado a cabo la correspondiente ponderación que constituye la garantia esencial que justifica la excepción del derecho.

La protección del derecho permite a sus titulares interponer recursos legales contra presuntas intromisiones en su ejercicio con el fin que la instancia correspondiente decida si su ámbito de protección ha sido o no vulnerado. La existencia de estos medios frente a la violación del derecho es la condición de existencia efectiva de los derechos fundamentales. Esta relación de dependencia que los vincula determina que los jueces deban proveer los recursos como parte de su obligación de tutelar los derechos fundamentales. (RODRÍGUEZ 1998)

Así la sentencia del Tribunal Constitucional peruano sobre el expediente 1058-2004-AA referida anteriormente, se pronuncia en el vigésimo primer fundamento en el siguiente sentido:

> "(...) en el presente caso no es (...) que la empresa demandada no haya podido investigar un hecho que, a su juicio, consideraba reprochable. como lo es el uso de un instrumento informático para fines eminentemente personales, sino el procedimiento que ha utilizado a efectos de comprobar la presunta responsabilidad del trabajador investigado. Sobre este particular (...) la única forma de acreditarlo era iniciar una investigación de tipo judicial, habida cuenta que tal configuración procedimental la imponía, para estos casos. la propia Constitución. (...) por tratarse en el caso de autos de la reserva elemental a la que se encuentran sujetas las comunicaciones y documentos privados y la garantía de que tal reserva solo puede verse limitada por mandato judicial y dentro de las garantías predeterminadas por la ley".

Es importante por último, exponer la tipicidad de la infracción al derecho al secreto de las comunicaciones y documentos privados establecidos por el ordenamiento jurídico peruano. Así, el artículo 13° del reglamento de la Ley de Telecomunicaciones, cuyo texto único ordenado fue publicado en julio de 2004 dispone:

> “Se atenta contra la inviolabilidad y el secreto de tas telecomunicaciones, cuando deliberadamente una persona que no es quien origina ni es el destinatario de la comunicación, sustrae, intercepta, interfiere, cambia o altera su texto. desvía su curso, publica, divulga, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación. (...) Los titulares de servicios privados de telecomunicaciones deberán adoptar sus propias medidas de seguridad sobre inviolabilidad y secreto de las comunicaciones.”

Por su parte el Código Penal peruano tipifica el delito de violación de correspondencia en el artículo 161°: "El que abre indebidamente carta, un pliego, telegrama, radiograma, despacho telefónico u otro documento de naturaleza análoga, que no le esté dirigido, o se apodera indebidamente de alguno de estos documentos, aunque no esté cerrado, (...)".

2.6. El derecho al «consentimiento informado»

La legalidad del control y supervisión del uso de ros recursos informáticos requiere dilucidar si para su implementación por parte de los empleadores es necesario el conocimiento o consentimiento previo del trabajador; así lo requiere el numeral 12.1.5 del «Código de buenas prácticas para la gestión de la seguridad de la información» contenido en la norma técnica peruana ISO/IEC 17799:2004. Es en ese sentido que recogemos la tesis del autor espaíiol Fernando Galindo (1998) sobre la necesidad de reconocer el derecho a dar un «consentimiento informado» a la actuación de los informáticos, tal cual como en la doctrina jurídica se sostiene indispensable para la relación médico-paciente. En efecto, el paralelismo al que invoca el autor para justificar la necesidad del consentimiento previo del trabajador para el control y supervisión del empleador sobre el uso de los recursos informáticos que éste proporciona, se funda en la necesaria existencia de medidas que garanticen, dentro del ordenamiento jurídico, que las actividades de los profesionales de la informática respeten la seguridad de las computadoras, redes y programas; la puesta en práctica del principio de autodeterminación informativa o el consentimiento de los usuarios; y su intimidad.

El derecho a la intimidad es considerado como derecho fundamental con anterioridad a su reconocimiento en el ordenamiento jurídico y, junto con los demás derechos personalísimos, es concebido por la doctrina como principio para la elaboración de una nueva institución jurídica, el «consentimiento informado». Este concepto tiene su origen en la jurisprudencia de los Estados Unidos elaborada con base en la relación médico-paciente; y últimamente, ésta siendo también reconocida su aplicación para la actividad de los ingenieros o administradores de sistemas de información con relación al usuario de recursos informáticos.

Es el sustento filosófico-jurídico del derecho al «consentimiento informado» que desarrolla Carlos Fernández Sessarego (2005) el que nos sirve para sentar las bases de un análisis que permita acreditar la aplicación de dicho concepto en el ámbito de la relación laboral. Es como correlato de este derecho que existe el deber del empleador, como proveedor de recursos informáticos al trabajador, de poner a su disposición la información suficiente respecto al control ejercido sobre éstos para obtener su asentimiento con la finalidad de que éste último pueda ejercer libremente la preservación de su intimidad. Bien señala el autor mencionado que, gracias a los aportes de la escuela de la filosofía del existencialismo, se produce desde mediados del siglo pasado el redescubrimientode la libertad como el ser del hombre. En efecto. como resultado de este interés de los filósofos, esta nueva concepción sobre el ser del hombre ha revolucionado los principios tradicionales de las disciplinas humanistas. aunque algún sector de la intelectualidad aún se resista ha admitirlo.

La libertad ontológica le otorga dignidad al ser humano, le da sentido a su vida y, en cuanto constituye su núcleo existencial, lo hace idéntico así mismo, único, y lo distingue de los demás seres; en resumen, la dignidad es el sustento de todos los valores y derechos inherentes al ser humano y, por consiguiente, del «consentimiento informado».

La concepción del pensamiento clásico, por la que el ser humano se consideraba un ser racional, perdió vigencia cuando la importancia ontológica puesta en la racionalidad como cualidad distintiva del mismo se desplazó y se orientó en la libertad: ésta es la que lo hace único, idéntico a si mismo, es a partir de la libertad que el ser humano forja su propia personalidad, en eso radica su dignidad. La libertad ontológica que nos hace ser, se exterioriza, se convierte en actos y conductas; la libertad, en el ámbito subjetivo, es pura decisión.

El Derecho protege estas dos instancias de la libertad: como constitutiva del ser humano y como su realización a través del «proyecto de vida» que es como se exterioriza; su misión es la protección preventiva, unitaria e integral de la persona en su comunidad y de conformidad con el bien común y el respeto de la libertad ajena. El ejercicio de la libertad, en función a la realización personal, no debe dañar los intereses y derechos de la sociedad ni de sus miembros.

Esta nueva concepción del Derecho que protege la libertad de la persona en todas sus expresiones ha influido en todos los sectores de la disciplina jurídica, la persona humana es el nuevo fin supremo del derecho, ahora la protección del patrimonio se halla en función del ser humano. El individualismo paterna!ista se bate en retirada y no obstante su aún notoria presencia, es la concepción humanista del derecho recogida en el derecho positivo la que toma su lugar en la actualidad.

El respeto a la dignidad que conlleva esta estructura existencial del ser humano obliga a los investigadores y a los operadores del derecho a tener en cuenta su calidad de ser libertad, sólo a partir de éste es que el «consentimiento informado» es aceptado como una nueva institución jurídica. que se inicia en los Estados Unidos y posteriormente se extiende a otras regiones del mundo, como la consolidación jurídica del «consentimientoinformado».

El deber de informar del empleador sobre el ejercicio de control y supervisión sobre el uso de los recursos informáticos que proporciona a sus trabajadores está relacionadocon la protección integral *y* unitaria del ser humano, protección que es el sentido y la razón de ser del Derecho. Hablamos de que se produce el «consentimiento informado» cuando quedar, satisfechos dos elementos principales: el conocimiento del control y supervisión que ejerce el empleador sobre el uso de los recursos informáticos y la voluntariedad del trabajador de someterse a los mismos.

CAPÍTULO 3 La racionalidad del poder del empleador

3. 1 El poder de dirección del empleador y sus límites

El poder de dirección del empleador es consustancial a la relación de trabajo, comprende funciones ejecutivas, de instrucción y de control, entre las que se incluyen las medidas de seguridad. En sentido amplio, este poder proviene de la máxima autoridad en la empresa y se manifiesta en el ejercicio de las facultadesde dirigir, dar órdenes e instruccionesy reglamentar la prestación de servicios del trabajador en la empresa. así como las facultades de vigilar, fiscalizar, y sancionar las faltas cometidas por el mismo. En sentido restringido, éste se impone a través de la facultad de impartir órdenes e instrucciones de acuerdo con las necesidades de la empresa, lo que implica, a su vez, la facultad de organizar económica, estructural y técnicamente a ésta. En resumen, el poder directivo del empleador se compone de tres elementos: el mando; el control, que es la actividad que sigue y acompaña al mando; y finalmente, la supervisión que es la actividad que reconoce los mecanismos de inspección.

Son características del poder de dirección: ser unilateral del empleador; estar reconocido por la ley o el contrato sin necesidad del consentimiento del trabajador; ser discrecional, o sea, ni injusto ni arbitrario; ser funcional a los fines de la empresa y a las exigencias de su pro- ducción; ser delegable, generalmente al personal de dirección; y, por último, estar limitado, ya que se ejercita sin desmedro de los derechos del trabajador.

El fundamento del poder de dirección del empleador es tratado por la doctrina jurídica desde distintas perspectivas: conforme a lo que sostiene la tesis «contractuatista» es la consecuencia del estado de subordinación que caracteriza la naturaleza del contrato individual de trabajo; en cambio, para aquellos que suscriben la tesis institucional. es una cualidad inherente al jefe de la empresa y el complemento necesario de su derecho de dirección sobre la producción y los fines de la misma, que son los elementos que, a su vez, justifican el poder de dirección del empleador en su sentido más amplio. (HERNÁNDEZ,1997)

El concepto de subordinación del trabajador, en el que se apoya la tesis «contractualista», es recogido por el ordenamiento jurídico peruano en el artículo 9° del texto único ordenado del Decreto Legislativo 728, Ley de Productividad y Competitividad Laboral:

> "Por la subordinación, el trabajador presta sus servicios bajo dirección de su empleador, el cual tiene facultades para normar reglamentariamente las labores, dictar las

órdenes necesarias para la ejecución de las mismas, y sancionar disciplinariamente, dentro de los límites de la razonabilidad, cualquier infracción o incumplimiento de las obligaciones a cargo del trabajador.(...)"

Por su lado, el derecho de libertad de empresa que sostiene la tesis institucional es recogido por el artículo 59 de la Constitución Política vigente: "El Estado estimula la creación de riqueza y garant iza la libertad de trabajo y la libert ad de empresa, comercio e industria. (...)"

El poder de dirección del empleador involucra tres facultades interdependientes: la de dar reglas generales y particulares a los trabajadores sobre la forma de ejecutar la prestación del servicio; la de ejercer control y supervisión sobre el cumplimiento de las reglas dadas -lo que implica verificar el uso adecuado de medios proporcionados por la empresa-; y, por último, la de imponer sanciones como consecuencia del incumplimiento probado de las directrices dadas.

Bajo los principios de un Estado democrático, la subordinación propia de la relación laboral obliga a imponer ciertos limites al poder de dirección del empleador. El principio de racionalidad, o razonabilidad según la ley de empleo citada, constituye un límite al poder de dirección que, en concreto, busca que las facultades de dar reglas, medidas de control y sanciones no sean arbitrarias. carezcan de sustento objetivo o sean desproporcionadas. Adicionalmente, otro límite al poder de dirección es el principio de la buena fe; que supone una actitud de honestidad y honradez en el ejercicio de los derechos y las obligaciones que se adquieren con el contrato de trabajo; y finalmente, también existe el límite que impone al empleador el respeto a los derechos fundamentales del trabajador.(TOYAMA, 2001)

La perspectiva que considera al Derecho como racionalizador del ejercicio del poder se inspira en los derechos fundamentales. El Derecho, al organizar y racionalizar el poder de dirección del empleador, lo limita; o sea, regula el uso de esa fuerza, y en ese sentido, son los derechos fundamentales de las personas los que se plantean y se enfrentan a decisiones o situaciones de poder con el propósito de salvaguarda. En el origen de la idea de la Constitución Política aparece la consideración de los derechos como límites al poder, por ello ésta surge corno un instrumento para limitar la actuación del poder político, tanto para proteger las libertades como para organizar su ejercicio. Los derechos fundamentlaes son límites no sólo en cuanto a la actuación sino también respecto a la organización del poder. El modelo de conexión entre poder y Derecho se expresa en "la consideración del poder como fundamento de validez del Derecho y la de éste como elemento racionalizador del poder". (ASÍS, 2000: 19)

La paradoja es un método de investigación filosófico útil para refutar una teoría al demostrar que ésta tiene consecuencias inaceptables, o simplemente para reflexionar sobre un problema mostrando a qué consecuencias aparentemente absurdas pueden llevar las consecuencias, aparentemente lógicas, de ideas aceptadas comúnmente. Ciertas paradojas que aparecen en la formulación de los derechos fundamentales como límites del poder pueden servir para destacar algunas características de éstos. William T. Bluhm, en su obra ¿Fuerza o libertad?, plantea la dualidad de ese título como distintiva de todo el pensamiento político moderno. La concepción moderna de libertad se basa en la autonornía del individuo, mientras que la de fuerza deriva del cuerpo como materia estructurada y gobernada por las leyes de la necesidad. La revisión de esta visión dualista y mecanlcis1a es el principio para formular una filosofía de libertad en torno a los valores históricos del hombre público; las libertades acordes a éstos se considerarían legítimas; las hostiles, estarían sometidas a limitaciones, de esa forma se podrá resolver esta paradoja.

Para que los derechos fundamentaleso naturales tengan fuerza y no sean sólo simples proclamaciones sin valor alguno se ha hecho necesario incorporarlos al derecho positivo. Los derechos fundamentales se presentan como límites al poder, pero es el poder el que los reconoce; esto es to que se ha denominado la «paradoja de la positivación». Esta paradoja sirve para recalcar que la idea de los derechos fundamentales como límites al poder obliga a realizar dos consideraciones; en primer lugar, el problema de las obligaciones del Estado, también llamadas autoobligaciones; éstas, desde una perspectiva jurídica, se apoyan en la consideración del Derecho como racionalización del poder. y desde el punto *de* vista sociológico, en que la eficacia de los derechos fundamentales depende *de* su apoyo en el poder.

Por lo tanto, la limitación del poder depende en este caso de él mismo y se proyecta en la segunda consideración de la paradoja de la positivación; esto es, si cualquier tipo de poder es válido para hablar de derechos fundamentales. Si consideramos que los derechos fundamentales, como limites al poder, dependen de la aceptación de éste último, será necesario determinar entonces que tipo de poder es el que en mayor medida los acepta y los reconoce; en ese sentido, la participación en el ejercicio del poder por parte de los ciudadanos garantiza la eficacia de los derecho fundamentales como limitaoores ce la actuación del poder y su existencia como mecanismos eficaces de control al ejercicio del mismo.

La fórmula «derechos fundamentales como limites al poder» hace necesaria una ampliación del signíficado de límite: do la limitación en la actuación a la actuación delimitada. En relación con los poderes públicosla doctrina ha distinguido relativamente entre límite y delimitación. siendo el primero sinónimo de no-actuación mientras el último haria referencia a la actuación positiva del Estado dentro de determinados parámetros. Los derechos fundamenta-

les son límites al poder pero es éste el que los regula mediante los actos del legislativo, del judicial y del ejecutivo; así para que aquellos limiten al poder es necesario que éste a su vez los desarrolle, lo que se conoce como la «paradoja de la regulación». La regulación de los derechos limita el sentido de éstos. pero al mismo tiempo proporciona medios para hacerlos efectivos.

El Derecho como forma de resolución de conflictos para la defensa de ciertas situaciones y bienes ha incorporado la idea de seguridad desde sus orígenes y ha adquirido. a partir de los planteamientos del pensamiento liberal clásico. una relación con el sentido de protección. Respecto a los derechos fundamentales se trata no sólo de una obligación de los Estados de abstenerse de intervenir en determinado ámbito y de actuar para promover o facilitar el disfrute de ciertos derechos. sino también, de proteger ese disfrute. Los derechos fundamentales se presentan así como límites a la actuación del poder, pero es éste, a su vez. el encargado de protegerlos; el mismo poder que puede afectar a los derechos fundamentales los protege contra esa posible actuación, en definitiva. él protege contra su misma actividad; esto es lo que se ha llamado la «paradoja de la protección». (ASÍS, 2000)

Retomando la sentencia del Tribunal Constitucional peruano referida en el capitulo anterior, resulta necesario resaltar el decimosexto y decimoséptimo fundamento expuesto en el sentido de dilucidar si los recursos informáticos que el empleador proporciona al trabajador se consideran: "de dominio absoluto de la entidad o empresa, (...) o si. por el contrario, existe un campo de protección respecto de determinados aspectos en torno de los cuales no le está permitido al empleador incidir de manera irrazonable". El Tribunal sostiene que:

> "(...) cuando tales facilidades [técnicas o informáticas) suponen instrumentos de comunicación y reserva documental no puede asumirse que las mismas carezcan de determinados elementos de autodeterminación personal, pues sabido es que en tales supuestos se trata del reconocimiento de condiciones laborales referidas a derechos fundamentales que, como tales, deben respetar las limitaciones y garantías previstas por la Constitución Política del Estado".

En igual sentido, el decimoctavo fundamento es concluyente:

> "(...) Aunque, ciertamente, puede alegarse que la fuente o el soporte de determinadas comunicaciones y documentos le pertenecen a la empresa o entidad en la que un trabajador labora, ello no significa que la misma pueda arrogarse en forma exclusiva y excluyente la titularidad de tales comunicaciones y documentos, pues con ello evidentemente se estaría distorsionando el esquema de los atributos de la persona,

como si estos pudiesen de alguna forma verse enervados por mantenerse una relación de trabajo."

El poder del empleador tiene un contrapeso en el deber de protección al trabajador, mediante el cual éste está obligado a cuidar que la ejecución de sus órdenes y controles no sean dañosos ni perjudiciales; para lo cual debe contraer una serie de prevencionesy responsabilidades entre las que se considera el respeto a la dignidad e intimidad del trabajador. Por otra parte, en la relación laboral los derechos deben ser ejercidos y las obligaciones ejecutadas según las reglas de la buena fe; la exigencia de buena fe impuesta al empleador requiere de él un especial esmero por los intereses y persona del trabajador que es justamente en lo que el deber de protección consiste.

3. 2 La autorregulación regulada y la racionalidad técnica

3.2.1. La autorregulación y las relaciones entre Estado y sociedad

Actualmente el interés en la autorregulación se debe a que sus efectos están excediendo el ámbito privado en el que se origina, para convertirse en referencia inevitable en las consideraciones de los poderes públicos; esto debido a que las consecuencias de l a autorregulación alcanzan, cada vez más, no sólo a los sujetos que se autorregulan sino que también son referencia para terceros, para el mercado y para los propios poderes públicos. Es aquella autorregulación que tiene efectos públicos la que despierta el interés por su novedad, por las expectativas que suscita su desarrollo, y porque hace evidente las modificaciones en la correlación entre lo privado y lo público. Las tendencias que afectan a esa correlación entre la sociedad y el Estado motivan el auge de la autorregulación, ya que al verse este último desbordado, debe considerar las reglas, referencias y decisiones de la autorregulación social.

Otro factor que explica lo anterior es el impulso tecnológico que en los últimos tiempos ha configurado espacios complejos que resultan impenetrables para los poderes públicos. La extensa aplicación de la tecnología, como es el caso de la informática. se constituye y desenvuelve en gran medida al margen de la regulación e intervención de los poderes estatales, por el hecho de serles incomprensibles y, por ello, incontrolables; lo que supone un desafío que el Derecho debe enfrentar renovando muchos de sus objetivos e instrumentos con el fin de controlar y racionalizar estas nuevas fuerzas que actúan en la sociedad.

La histórica sujeción de los poderes públicos a las normas jurídicas, como objetivo y razón de ser del Estado de Derecho, da paso a la paradoja que a éste se le plantea al requerírsele

someter a Derecho a estos nuevos poderes que se han formado en la sociedad. De ahí que, como señala José Esteve Pardo (2002), se reconozca la necesidad de responsabilidad y prudencia de quienes actúan y toman decisiones de gran trascendencia para autolimitarsea manera de una nueva *«prudéntin civílis»*, pero esta vez no con relación al poder público, sino para controlar y moderar el poder surgido en la sociedad y el sector privado. A estos nuevos poderes de la sociedad corresponde una nueva posición del Derecho a la que se ha denominado «derecho reflexivo», cuyo objetivo es estimular y encaminar la templanza y sujeción de las fuerzas sociales por sus propios agentes.

Es también la renovada confianza en la sociedad que se apoya en la especialización técnica y la profesionalización de ciertos grupos u organizaciones lo que sustenta el interés en la a utorregulación. La estructuración y funcionamiento de la sociedad según la teoría de sistemas nos señala que ésta se organiza en diversos subsistemas sociales diferenciados funcionalmente; esa diferencíación se da como reacción a su extrema complejidad. La especialización de los subsistemas sociales es la que sustenta la mayor efectividad de la autorregulación frente a la regulación estatal, debido a tres razones: la primera se relaciona con el conocimiento, la función que cumplen la ciencia, la técnica o los grupos profesionales hace difícil la regulación, sobre todo si con ésta se busca controlar los riesgos derivados del desarrollo tecnológico; la segunda tiene que ver con la autonomía que da unidad a cada subsistema social y que está relacionada con derechos fundamentales como la libertad de expresión o la libertad de investigación científica, estableciendo límite a la intervención del Estado y, por último, la trascendencia a los límites de las fronteras políticas y territoriales que muestran los individuos, los operadores del mercado, los grupos de profesionales y los expertos.

Otro aspecto del auge de la autorregulación es el que marca el desarrollo del profesionalismo y de la capacidad técnica de la sociedad. La profesión puede definirse como una actividad en la que coinciden unos conocimientos técnicos y una ética común o como señala Mercé Damaculleta (2005) "una organización laboral humana capaz de autorregularse". El conocimiento especializado de un grupo de profesionales resalta la existencia de una racionalidad propia y fundamenta su autoridad técnica. Desde esa perspectiva, la autorregulación y el profesionalismo se tienen como complementarios uno del otro. En los Estados premodernos, era el gremio el encargado de transmitir los conocimientos entre los profesionales fomentando su vinculación a determinados principios de actuación, dando origen a las reglas que se conocen como *«lex artis»*, especificaciones técnicas, normas deontológicas o buenas prácticas de una profesión.

En los Estados modernos ocurrió un cambio radical en el sistema de autorregulación profesional al ser absorbidos los monopolios por parte del Estado, éste conformó un sistema de

control de la autorregulación profesional a partir de la creación de organismos públicos como universidades, colegios profesionales o cámaras de comercio; una burocracia profesional al servicio del Estado que garantiza la seguri dad de los ciudadanos frente a los riesgos generados por el desarrollo industrial a través de normas jurídicas y actos administrativos, amparados en la noción de policía.

Actualmente, la mayor complejidad de las funciones del Estado y sus limitaciones económicas para incrementar y preparar a la burocracia profesional, le ha impuesto la necesidad de contar con la colaboración de los expertos privados, ya que se constata que el conocimiento técnico evoluciona en mayor medida en las áreas de investigación y desarrollo de las grandes empresas; asimismo, el desarrollode las asociaciones profesionales y el aumento de la especialización han llevado a que la transferencia de conocimientos técnicos y la ética aplicada se den a través de éstas y no de los colegios profesionales. Así la regulación de los conocimientos técnicos por la administración pública sobreviene imposible, el propósito regulador sobre la complejidad tecnológica sólo resulta factible con la autorregulación.

Muchas de las reglas propias de un grupo profesional se documentan actualmente en forma de códigos, normas técnicas o protocolos de actuación, haciendo más fácil la relación entre el subsistema profesional y el subsistema jurídico; el consenso sobre la aceptación de las reglas les da el carácter vinculante dentro del subsistema en el que se generan, por tanto, cuanto más organizado esté el grupo profesional más se aproxima este consenso a un acuerdo jurídico. Estos instrumentos que funcionan ya en el campo del derecho privado se han extendido al derecho público mediante remisiones legales y reglamentarias a la norma técnica o a la «mejor tecnología disponible» -denominada la cláusula técnica- estableciendo a través de éstas la conexión entre ambos subsistemas. Así la autorregulación que resulta jurídicamente relevante es la que generada en otros sistemas se vuelve inteligible y aceptable por el sistema del Derecho.

Desde las primeras concepciones sobre la autorregulación se le ha reconocido a ésta como una capacidad innata de la sociedad, sobre todo en su actividad económica, sujeta exclusivamente a la dinámica social o del mercado y por tanto sin control estatal alguno. Dicha concepción no es la que suscita el interés actual, sino aquella que alcanza efectos para el Estado y que por tanto corresponde a una nueva etapa en el desarrollo de las relaciones entre el Estado y la sociedad.

La gestión empresarial requiere también hoy un elevado grado de especialización técnica y profesional por parte de los titulares propietarios y directivos encargados. Las empresas son organizaciones que detentan un poder especifico en la estructura de la sociedad y del Esta-

do. Como correlato a ese poder, la empresa debe justificar éste a través de criterios que lo hagan legítimo, lo que ha dado lugar a asumir su «responsabilidad social». La autorregulación con reladón a la gestión empresarial muestra algunos aspectos destacables; el primero tiene que ver con la cobertura jurídica e institucional, pues ante todo, una empresa es una institución que se identifica con un ordenamiento jurídico privado derivado de sus estatutos y reglamentos internos; en segundo lugar, la gestión empresarial está en relación directa con et ejercicio del derecho de la libertad de empresa. La complejidad técnica y organizativa de las empresas hace necesario que su autorregulación permita controlar los riesgos tecnológicos generados por los propios procesos de producción de bienes y servicios, e impone a los trabajadores el cumplimiento de los objetivos establecidos por la dirección de acuerdo con criterios y técnicas adecuados: aparecen asi reglamentos internos, manuales de buenas prácticas, protocolos de actuación y de seguimiento de la actividad empresarial, o sistemas de control y gestión de riesgos.

3.2.2. Las potencialidades de la autorregulación

Uno de los presupuestos para la autorregulación se da al concentrar en la sociedad los poderes que dan el uso de ta informática y las telecomunicaciones especialmente en lo que se refiere a la amenaza a la intimidad y al procesamiento y transmisión de datos personales; lo que fundamenta su intervención con el fin de prevenir una utilización desordenada de estos medios, ya que ellos pueden incidir de manera dañosa sobre derechos fundamenlales que son protegidos por la Constitución Política.

El conocimiento que poseen quienes desarrollan y aplican las innovaciones tecnológicas es ajeno tanto al legislador como a la administración pública, quienes enfrentan su creciente incapacidad para regular el desarrollo tecnológico y conlrolar sus riesgos.

Otro presupuesto para la autorregutacíón está en la incapacidad de la regulación pública como consecuenciadel conflicto ético entre derechos y libertades que causan los avances de ta ciencia y la técnica ante la dignidad de la persona. Se trata de una complejidad ética a la que no puede dar oportuna solución la regulación pública, por lo que se debe recurrir en gran medida al buen juicio de la comunidad. Garantizar la protección de los derechos constitucionales es un imperativo irrenunciable, de ahi la necesidad de reflexionar sobre una forma de tutela que sea concurrente con las actuales exigencias de desregulación como consecuencia de la restricción del poder y la legitimidad de los Estados.

Es asl como la capacidad de autorregulacíón de tas empresas y los profesionales resulta una fórmula con la que los Estados cuentan para enfrentar sus propias dificultades en el

cumplimiento de la obligación que tienen de proteger la identidad y la dignidad de las personas, en una sociedad en la que la ciencia y la técnica dominan los procesos que generan amenazas en contra de estos bienes jurídicos.

Por ello se fomenta una autorregulación capaz de subvenir a la necesidad de intervención pública: autorregulación que funciona como contrapeso a la desregulacíón y cuya relevancia consiste en complementar o sustituir, en primer lugar, reglamentaciones públicas por reglamentaciones privadas -códigos de conducta, normas técnicas, protocolos y buenas prácticas-; y, ensegundo lugar, controles públicos por controles realizados por sujetos privados.

Esta subvención es resultado de advertir, en primer lugar, la potencialidad de la autorregulación como instrumento que permite superar la deficiencia de la legislación y las directivas de la administración pública; en segundo lugar. como técnica eficiente para que el Estado cumpla con garantizar la protección de la dignidad de la persona; en tercer lugar, su capacidad para establecer una correspondencia entre los responsables directos de las amenazas contra ese bien jurídico y las medidas para garantizar su protección; y por último, en la propiedad de proyectarse en el ámbito internacional, lo que no se aplica a las normas y los controles estatales. Es debido a las razones antes expuestas que la autorregulación s propone como una alternativa ante las ideas de pérdida de soberanía, desregulación, privatización, desburocratización o adelgazamiento del Estado. (DARNACULLETA, 2005)

3.2.3. La regulación pública de la autorregulación

El Estado al utilizar las normas y controles privados de la autorregulación como instrumentos al servicio del interés público considera a ésta como una novedosa fórmula de regulación, y por tanto resulta siendo una «autorregulación regulada», fomentada, dirigida e instrumentalizada por él mismo. De igual forma el Estado considera a las certificaciones privadas que constatan el cumplimiento de las normas técnicas como instrumentos de un sistema público de control regulado. De ello se infiere que el Estado utiliza la autorregulación como una forma de regulación indirecta. Dicha atribución de fines públicos de la autorregulación con el objeto de supeditar a los sujetos a los principios constitucionales se complementa con la regulación del entorno de la propia autorregulación por parte del Estado, como es la adopción de procedimientos o la acreditación pública de requisi tos necesarios para el reconocimiento de organizaciones privadas como organismos de normalización. Por medio de la «autorregulación regulada» la administración pública supervisa los actos de aprobación y cumplimiento de normas y controles privados que garantizan la capacidad técnica y el sometimiento a fi-

nes públicos de los sujetos autorregulados, con el objeto de minimizar los riesgos generados por aquéllos.

Paradójicamente, como anota Darnaculleta (2005), mediante la «autorregulación regulada» una aparente desregulación administrativa constituye un mayor control e intervención pública. La asociación de los Estados en foros internacionales y las organizaciones privadas internacionales con fines comunes a éstos, constituyen parte indispensable de una nueva estructura en las relaciones entre el Estado y la sociedad que de muestra que la «regulación de la autorregulación» no corresponde a un Estado que haya renunciado a las obligaciones que le atribuye la Constitución a los poderes públicos; en la práctica el Estado interviene más y con mayor intensidad.

Uno de los ámbitos en el que mayormente se da la autorregulación es el del control y gestión de riesgos, un espacio en el que se hace evidente un gran desarrollo debido, principalmente, a que en las áreas dominadas por *e* Derecho el objetivo es, justamente la gestión de riesgos. Ello se manifiesta en la abund ante aparición de técnicas, fórmulas e instrumentos con el propósito de conocer, contro lar, gestionar o ornar decisiones sobre riesgos; entre los que destacan las normas técnicas de seguridad y que tienen como rasgo común a todos ellos su origen en la autorregulación. Autorregulación Autorregulación sobre la que los poderes públicos muestran un interés especial ya que constituyen referencias a las que les atribuyen certeza o importancia.

3.2.4. La normalización y la gestión de riesgos

En sentido amplio, la normalización es todo proceso con el objeto de estandarizar una conducta; jurídicamente dicho resultado se formaliza en reglamentos técnicos de carácter obligatorio, o en normas técnicas de carácter voluntario, que pueden ser aprobadas indistintamente, tanto por organismos públicos como por organismos privados de normalización. En tanto que la certificación, es la actividad de verificación y documentación del cumplimiento de una norma técnica.

La existencia de los organismos internacionales de normalización con el objetivo de racionalizar y uniformar la normativa técnica existente responde a una orientación sistémica y global de la autorregulación, siendo los organismos más destacados la *International Organization for Standardization* (ISO) y la Organización Mundial de Comercio (OMC) que se sobreponen a los ordenamientos estatales, es asi como la referencia fundamental de ésta última constituye el «Código de buena conducta para la, elaboración, adopción y aplicación de normas». (ESTEVE, 2002)

La importante función que cumplen los sujetos privados expertos en el desarrollo de las tecnologías. quienes no están legitimados democráticamente para tomar decisiones que afectan a la sociedad, obliga a recurrir al principio de la «responsabilidad social» como criterio para la legitimación del poder que ejercen. Es así como el cumplimiento de las reglas técnicas permite la protección de los bienes más preciados de la sociedad y el Estado en su función de garante de tales bienes, fomenta, regula e impone ese cumplimiento, extendiendo así su intervención hasta límites insospechados. La prevención y la precaución son entonces principios de la responsabilidad compartida por el Estado y la sociedad para enfrentar los riesgos que deben administrar colectivamente, desplegando asi el control estatal hasta confines impensados.

En el Perú, la falta de capacidad de las asociaciones u organizaciones privadas de técnicos o ingenieros fue la que ocasionó que fuesen los burócratas los que formaran parte de las organizaciones internacionales de normalización. La homologación de las reglas técnicas desarrolladas por dichos organismos se produce mediantela aprobación de normas técnicas peruanas de carácter voluntario. En cambio son las organizacionesprivadas las que realizan la certificación del cumplimiento de normas técnicas, que involucran tanto reglamentaciones públicas como normas privadas, ya que para lograruna adecuada gestión de los riesgos, las empresas se deben someter a controles públicos, pero también y principalmente, a sistemas de autocontrol y a controles realizados por sujetos privados.

La elaboración de normas técnicas de aplicación en el mercado global debe contemplar el establecimiento de estándares de seguridad para la producción en las reglamentaciones de los Estados, por ello la normalización se caracteriza tanto por acordar especificaciones técnicas, como por impulsar los niveles de seguridad. La existencia de un organismo de normalización en el ámbito mundial que hiciera posible la universalización requerida por el mercado global tuvo su origen en el sector eléctrico; es a comienzo del siglo XX que la generalizada utilización industrial y comercial de la electricidad requirió una definición previa de las características de construcción de redes, frecuencias, tensiones de corriente y conexiones a las mismas. así como de normas de seguridad; ello impulsó a los organismos de normalización nacionales y a las asociaciones de técnicos e ingenieros a gestar la existencia de una asociación en el ámbito internacional, es asi que en 1925 las delegaciones de diversos países industrializados acordaron crear una asociación no gubernamental que se fundó en 1930 con el nombre de *International Stamdardizing Association* (ISA), la que actualmente es conocida como ISO.

La ISO tiene carácter multisectorial por lo que su trabajo se desarrolla a través de órganos técnicos de normalización especializados en distintos sectores de la producción y servicios.

Sin embargo las normas técnicas de mayor reconocimiento expedidas por este organismo son las relacionadas con los sistemas de calidad, identificada con la denominación ISO 9000, y las del medio ambiente como ISO 14000.

Actualmente se da una estrategia de «regulación de la autorregulación» por la que se atribuye la responsabilidad directa de la gestión de riesgos a los sujetos privados que los originan - principalmente empresas-, y el traslado de esa responsabilidad·a organismos de normalización, entidades de certificación y otros sujetos conocedores de las técnicas que pueden minimizarlos; quedando la función del Estado circunscrita a comprobar el correcto funcionamiento del sistema de autorregulación organizado con relación a la gestión de los riesgos; así queda a disposición de los empresarios un sistema de autorregulación que les permite, a partir de la certificación del cumplimiento de normas voluntarias, endosar su responsabilidad a los sujetos privados que emiten tales certificaciones.

La existencia de normas técnicas de carácter voluntario para un determinado sector, que el Estado pretende regular, hace posible que éste incorpore el contenido de tales normas en sus reglamentaciones técnicas no sólo transcribiendo dichas normas en su articulado, sino también mediante la remisión a las mismas; de manera tal que se establece la obligatoriedad de dichas normas mencionándolas en el reglamento («remisión estática») o, inclusive, haciendo obligatorias las posteriores modificaciones a esas normas («remisión dinámica»). Se viene así imponiendo la obligatoriedad de las normas técnicas; sean éstas propiamente o sean códigos de buenas prácticas, reglamentos técnicos, protocolos y otras de índole similar.

Asi, con independencia de si las normas técnicas son de carácter voluntario u obligatorio, las empresas se ven impelidas a instaurar sistemas de autocontrol, buscando documentación que contenga reglas técnicas útiles para el desarrollo de controles internos. contratando a entidades privadas que les den asesoría en la implementación de tales normas y controles, y a contratar a auditores externos que verifiquen y certifiquen la eficiente gestión de riesgos. Esto debido a que la responsabilidad directa de la reducción de los riesgos corresponde a aquellas empresas u organismos que los generan y los conocen. en tanto corresponde a los poderes públicos garantizar la capacidad técnica de quienes asumen esta responsabilidad, dotándoles cuando sea necesario, de los medios para ejercerla y exigirla jurídicamente. Ello permite afirmar que, vía la «regulación de la autorregulación», el Estado interviene de manera más intensa en la actividad empresarial de la que podria ser con las técnicas comunes de regulación.

La necesidad de técnicas que ayuden a reducir en lo posible los riesgos que se derivan de la actividad empresarial es lo que ha llevado en el último tiempo a los Estados a tomar en cuenta lo que éstas son y los fines que cumplen para determinar las nuevas formas de intervención administrativa. En ese sentido, ha resultado indispensable conocer desde puntos de vista económico, sociológico y jurídico a la empresa para obtener la información que permita transformar la relación entre ésta y la administración pública.

Así, vista desde la concepción económica, una empresa es una asociación de capital y trabajo cuyo objeto es producir bienes o prestar servicios a los consumidores para la obtención de beneficios económicos; lo que significa que la empresa es perceptible a las demandas del mercado, lo que a la postre la lleva al cumplimiento voluntario de determinadas normas de calidad antes que por una imposición de los poderes públicos.

Desde el punto de vista sociológico, la empresa constituye un subsistema social funcionalmente diferenciado por su capacidad de aulorregulación, en este sentido. el establecimiento voluntario de normas técnicas de producción y organización, y la certificación y control del cumplimiento de aquellas, constituye una característica inherente a la gestión empresarial; lo que ha hecho cada vez mas común, por una parte, la documentación de la autorregulación; y por otra, la reflexión sobre la función que las empresas cumplen en la sociedad.

Por último, desde el punto de vista jurldico, la empresa es una organización estructurada en un ordenamiento jurídico privado cuyos estatutos y reglamentos internos regulan relaciones internas y con sus trabajadores, auditores, distribuidores y clientes; estas normas de origen contractual otorgan juridicidad a la autorregulación, transformando sus resultados en obligaciones de carácter vinculante para determinados miembros del subsistema o para todos ellos, y haciendo posible que ésta sea exigible por parte de los poderes públicos.

3.2.5. Concepto y elementos de la autorregulación

Como ya se ha anotado antes, se constata en la vida social el vivo interéspor la autorregulación debido a la confianza que en los últimos años han depositado los poderes públicos en ésta, ello principalmente, por el aumento de su racionalidad, como consecuencia, a su vez, del desarrollo del profesionalismo de las empresas y de su responsabilidad social. De ahí que el concepto de autorregulación haya sido aplicado también al ámbito laboral para explicar la forma en que se desarrollan las relaciones entre empleadores y trabajadores; en efecto, la autorregulación constituye desde el punto de vista jurídico el orden con el que actúan y se relacionan los particulares y las organizaciones privadas. Sin embargo, últimamente se percibe un cambio en la relación entre la autorregulación privada y la regulación pública de-

bido al intercambio cada vez mayor de las funciones del Estado y la sociedad, debido a las dificultades de las administraciones públicas para hacer frente a los desafíos que tienen planteados. La autorregulación y la regulación no son ya dos realidades enfrentadas, sino dos mecanismos cuyos puntos de intersección son cada vez más.

Esta realidad ha dado lugar al concepto de «autorregulación regulada» como una actividad privada de elaboración y control do normas que está condicionada por una actividad pública que establece los derroteros y controles a los que debe sujetarse la autorregulación.

Los instrumentos de ta autorregulación son normativos o declarativos. Son de carácter normativo las normas técnicas. los códigos y manuales de buenas prácticas y los protocolos y procedimientos normalizados de trabajo.

Las normas técnicas son en sentido estricto, reglas aprobadas por organismos de normalización, y en la medida que dichos organismos son mayoritariamente sujetos privados, éstas son producto de la autorregulación. En sentido amplio, son un conjunto de especificaciones técnicas obtenidas como resultado de la cooperación de la ciencia, la tecnología y la experiencia; aprobadas mediante el consenso de todos los sujetos interesados que participan de un organismo de normalización. Además se consideran elementos para su caracterización como tales, su carácter voluntario, su accesibilidad pública, y su vinculación con el cumplimiento de objetivos generales dirigidos a obtener beneficios sociales.

Las normas técnicas al expresarse por escrito tienden a asemejarse a las normas jurídicas y, como consecuencia, pretenden la seguridad y la generalidad; aunque comúnmente están referidas a un producto o una tecnología en particular. Sin embargo, la relación de materias incluidas en las especificaciones técnicas que integran estas normas están ampliándose notablemente en los últimos años a las indicaciones para gestionar una empresa, los controles que deben realizarse para conseguir este fin; o incluso, los requisitos necesarios para ejercer una profesión como el caso de las normas técnicas de acreditación.

El concepto de «buena práctica» se aplica a las acciones de un profesional o de una organización responsable en el ejercicio de su actividad con el fin de obtener aeterminados fines. Las «buenas prácticas» son reglas de cumplimiento voluntario y su aplicación depende del carácter profesional de una actividad o de la conciencia que de ésta tiene el sujeto que la ejerce con relación a la protección de determinados bienes. La aplicación de estas prácticas puede también ser objeto de recomendaciones públicas. Asimismo, éstas suponen la implantación de determinados autocontroles sobre su cumplimiento, los que deben estar documentados.

La documentación de los autocontroles arriba mencionados remite a la existencia de los instrumentos de autorregulación denominados «protocolos y procedimientos normalizados de rta bajo»; éstos se utilizan comúnmente en la ejecución de determinadas actividades profes io na les, incl uso en casos en los que las «buenas prácticas» no están documentadas. Por su contenido se pueden distinguir los procedimientos normalizadosde trabajo como aquellos que detallan como se aplican las «buenas prácticas» por un profesional o en una organización determinados: su función es pues, describir cómo deben ser realizados, controlados, documentados, archivados e informados los actos considerados por aquellos «buenas prácticas». Los protocolos. en cambio, tienen por lo común un contenido más puntual, haciendo referencia a alguno de dichos actos: un ejemplo corresponde en el ámbito de la profesión médica y la investigación clínica cuando se requiere el consentimiento de los pacientes, son los llamados «protocolos de consentimiento informado»

Por su parte, son instrumentos de autorregulación de carácter declarativo aquellos que acreditan el cumplimiento de reglas técnicas o éticas de la autorregulación. Es la certificación el paradigma de éstos y se inscribe en una tendencia, cada vez mas extendida. caracterizada por las actividades de control preventivo por parte de quienes se autorregulan; siendo lo relevante de éstas, que ofrecen una información destinada a los profesionales, a las empresas y al público en general, pero que también resulta de interés para los poderes públicos.

3.2.6. Concepto e instrumentos de regulación

El significado del término regulación es el de regular o someter a una regla, lo que implica heteronomía y autoridad del sujeto regulador sobre el regulado; la regulación por tanto es el instrumento o conjunto de instrumentos por los cuales se sujeta a alguien a una regla determinada: éste es el sentido que se reconoce en el ámbito del Derecho, por lo que la regulación se identifica con la elaboración de normas jurídicas.

Los instrumentos de regulación tienen por finalidad ordenar la actividad del mercado, lo que se caracteriza como regulación económica, o tutelar los bienes y derechos constitucionalmente protegidos, que es la llamada regulación de policía. Esta última determina - mediante reglamentaciones técnicas- las condiciones de seguridad con relación a aquellos bienes y derechos, estableciendo controles preventivos *y* sanciones correspondientes en caso de incumplimiento. Los fines de la regulación de policía son también considerados actualmente como propios de la sociedad, por lo que es a través de la «regulación pública de la autorregulación» que se involucra a los sujetos privados en la consecución de tales fines.

Abunda en esta nueva orientación el hecho señalado de la incapacidad de los poderes públicos debida a la cada vez mayor complejidad organizativa del Estado y de la sociedad, y a la complejidad técnica y ética de los ámbitos en los que debe actuar para cumplir con las obligaciones de tutela constitucional. Por ello, el Estado se enfrenta actualmente al desafío de cumplir con sus fines y con las obligaciones que ha ido asumiendo, paralelamente con un proceso de desregulación y de limitación de su intervención. En este entorno, se combinan así el pensamiento neoliberal que demanda el adelgazamiento del Estado con el mantenimiento de las obligaciones exigidas al mismo. Esta realidad sustenta la necesidad de contar con la colaboración de los agentes sociales y que se recurra a las normas técnicas para poner a la sociedad al servicio de fines públicos.

3.2.7. La autorregulación regulada

Ya se ha expresado aquí que lo que hace de la autorregulación un fenómeno jurídicamente relevante es su consideración por los poderes públicos: este es un punto en el que, como anota Esteve Pardo (2002), la jurisprudencia anglosajona ha sostenido una muy definida posición al considerar que lo determinante no es el interés público (del inglés *public interest*), sinoel interés de los poderes públicos (del inglés *governmental interest),* más allá de lo que es estrictamente el gobierno.

La regulación pública otorga un mayor grado de confianza en la autorregulación cuando le atribuye al cumplimiento de sus normas efectos probatorios en los procedimientos administrativos al otorgar, denegar o controlar autorizaciones: o judiciales, al adoptar aquellas referencias como indicios relevantes para resolver litigios sobre responsabilidad. Estos efectos probatorios, a su vez, adquieren un especial significado cuando las normas jurídicas incorporan conceptos indeterminados como la *lex artis,* las «buenas prácticas», o a «la mejor tecnología disponible». En esos casos el instrumento de autorregulación actúa como un «dictamen pericial anticipado», que puede ser de gran utilidad a los operadores del Derecho que se ven en la necesidad de aplicar las normas que incorporan estos conceptos.

Cuando el Derecho atribuye efectos probatorios a la autorregulación nos sttuamos en el límite entre lo público y lo privado, "a un paso de la transformación de la naturaleza jurídica de la autorregulación" (DARNACULLETA, 2005: 401). Se puede afirmar que todos los instrumentos de autorregulación producen efectos probatorios, ya que éstos brindan información útil tanto en procesos judiciales como en procedimientos administrativos; ya sea como un indicio, una presunción. o como un dictamen pericial relacionados con la certeza de los hechos o con el cumplimiento de las normas que determinan la resolución judicial o adminis-

trativa. Así, en todo proceso en el que exista controversia sobre la diligencia de un profesional o de un empresaño, con relación a sus responsabilidades por la ocasión de daños, los instrumentos de autorregulación constituyen documento de las reglas técnicas que rigen la actividad profesional en cuestión, bien sea éste una certificado o resolución que acredita el cumplimiento o la vulneración.

La titularidad de un certificado técnico que acredite el cumplimiento de los requisitos de seguridad establecidos reglamentariament e puede enervar una acusación, tanto por los daños ocasionados a terceros como en un procedimiento administrativo sancionador. Este ejemplo se puede ampliar en aplicación de la virtualidad de los protocolos, las buenas prácticas o los códigos de conducta como medios de prueba para la determinación de la diligencia de los profesionales o empresas en el ejercicio de su actividad; en estos casos basta con verificar que los instrumentos de autorregulación mencionados sean los adecuados para la comprobación de la diligencia debida y, que el empresario o el profesional ha cumplido con las reglas.

Según el criterio jurídico tradicional se distinguen los efectos probatoños indiciarios de los presunti vos; siendo presunciones aquellos establecidas expresamen te por la ley, en tanto que indicios, aquellos hechos constatados de los que se pueden deducir otros de manera directa; de esa manera, en muchos casos la referencia que ofrece la autorregulación constituye indicio y es tratado así sobre todo en los procesos judiciales. A medida que los poderes legislativos y los tribunales de justicia establezcan disposiciones en materia de responsabilidad en función a presunciones legales con el fin de vencer las dificultades que plantea la complejidad técnica, se presumirá que las empresas y los profesionales que cumplan con instrumentos de autorregulación para el control de riesgos quedarán fuera de cualquier recelo.

Abundando más, el vínculo entre los instrumentos de autorregulación y la especialización técnica de los sujetos que los elaboran pone de manifiesto el concepto de la prueba pericial. Sabido es que el valor de la prueba pericial y la forma en que ésta se practica dependen de su regulación en los correspondiente procesos judiciales o administrativos; por tanto, es posible considerar como prueba pericial a los certificados técnicos que acreditan el cumplimiento de normas técnicas o de normas jurídicas.

El componente experto que tiene la aulorregulación explica la inevitable recurrencia a esta fórmula en aquellos ámbitos a los que el poder del Estado no llega por falta de conocimiento técnico y donde sólo están presentes los técnicos y expertos que operan en ellos: en consecuencia, la única regulación viable y efectiva es la que ellos mismos puedan darse. Cuando

con la autorregulación se quiere dar solución a un problema técnico, aportando el conocimiento experto, los efectos de ésta se declaran como periciales utilizando un término propio del sistema jurídico.

La finalidad de la autorregulación como prueba pericial ya ha sido considerada por la doctrina y la jurisprudencia alemana con relación a las normas técnicas, a las que considera como «dictámenes periciales anticipados» (del alemán *anticipierte Sachvelständige Gutachten).* Dicha concepción reclama el interés debido a que no sólo propone el efecto pericial, sino que también agrega un efecto presuntivo al dar a entender un juicio de validez que puede deshacerse con otra opinión o dictamen con mayor fundamento o certeza; provisionalidad que si no fuese reconocida convertiría a la norma técnica en norma jurídica de facto. Sin embargo, en la práctica, los procesos de racionalización y unificación que desarrollan la autorregulación actualmente, específicamente en la elaboración de las normas técnicas, llevan a la disipación del dictamen contrario. De esa forma la norma técnica, formalmente voluntaria, se convierte de hecho en una referencia prácticamente ineludible.

Las manifestaciones de la autorregulación normativa no son, en principio, Derecho; sin embargo se viene imponiendo por vía contractual la obligatoriedad de autorregulación a las empresas en sus relaciones con terceros y también al interior de sus organizaciones; de ahí que sea cada vez más frecuente que éstas instruyan a sus empleados en la obligación de cumplir con las normas internas de autorregulación en los contratos de trabajo.

De otro lado, la asunción de los resultados de la autorregulación por los poderes públicos sucede a través de fórmulas de remisión. La remisión se produce desde una norma jurídica y tiene como destino una norma suficientemente identificada. Debe tratarse. por tanto, de una remisión objetiva y nominada por la que resueltamente se asuman como propios los resultados de la autorregulación. De esa manera se da una transformación de la autorregulación en norma jurídica o en decisión de los poderes públicos.

La vía de la remisión objetiva implica la plena integración del resultado de la autorregulación -que comúnmente se trata de normas técnicas- en el ordenamiento jurídico; a partir de ésta, resulta de plena aplicación el régimen de vigencia, modificación o derogación propio de las normas jurídicas. La incorporaiócn de la norma técnica al ámbito público supone el abandono del marco del derecho privado propio de la autorregulación, y por tanto, de la voluntariedad.

Con la remisión a la autorregulación, ésta se convierte jurídicamente relevante ya que de esa manera rebasa el marco privado de origen *y* proyecta sus efectos sobre un ámbito más amplio, que en muchos casos es supranacional y alcanza a los poderes públicos. Esta di-

mensión pública que gana la autorregulación sí que es un fenómeno relativamente novedoso.

Éste fenómeno plantea el entrecruzamiento de lo público y lo privado; por un lado las instancias públicas se remiten o se ven obligadas a remitirse a la autorregulación, del otro, en el ámbito privado ciertos instrumentos de autorregulación, como las normas técnicas, alcanzan un rigor y una credibilidad que las hace elevarse hasta et ámbito público y ser considerados como propios de las instancias públicas.

Los efectos vinculantes de la técnica de la remisión han sido reconocidos explícitamente en el caso de las normas técnicas, y se están extendiendo también a los «códigos de buenas prácticas» en materia de seguridad. Asimismo, la utilización de determinados «conceptos jurídicos indeterminados» puede convertir en vinculante de facto a un instrumento normativo de autorregulación debido a que puede ser la única referencia, segura e indiscutible, para integrar el contenido de tales conceptos al ordenamiento jurídico.

La obligatoriedad de los instrumentos de autorregulación se consigue también mediante su inclusión en los estatutos o en las normas privadas que regulan la actividad interna de una organización; transformándose de esa manera en Derecho.

En resumen, se atribuyen efectos vinculantes a la autorregulación normativa mediante su obligatoriedad, su remisión o su integración en una norma jurídica.

En el Perú, de acuerdo a lo dispuesto por el artículo 26 del Decreto Ley 25868 modificado por el Decreto Legislativo 807, la aprobación de normas técnicas es competencia exclusiva del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) en calidad de organismo nacional de normalización, a través de su Comisión de Reglamentos Técnicos y Comerciales (CRT).

En virtud de esas facultades legislativas, la Comisión de Reglamentos Técnicos y Comerciales aprobó el 15 de noviembre de 2000 el «Reglamento de elaboración y aprobación de normas técnicas peruanas» y el «Reglamento de comités técnicos de normalización» mediante Resolución 0072-2000-INDECOPI-CRT. La elaboración de las normas técnicas peruanas es desarrollada por los «Comités Técnicos de Normalización», los cuales son creados por la CRT según campos de actividad claramente definidos de acuerdo a lo establecido en los reglamentos mencionados. Los Comités Técnicos de Normalización están conformados por representantes de los sectores involucrados en ta actividad correspondiente y actúan bajo la supervisión de la CRT, elaboran proyectos de normas técnicas relacionados a la materia de su actividad.

La elaboración de normas técnicas peruanas procede mediante la adopción de normas técnicas internacionales a iniciativa de la CRT, actuando de oficio o a través de un Comité Técnico de Normalización, o a iniciativa de este último. También procede la elaboración de normas técnicas en caso que no existan normas técnicas internacionales que sirvan de antecedente o, existiendo éstas, se hace necesario introducirles correcciones por existir condiciones particulares de aplicación en el país o cuando se presentan propuestas derivadas de investigaciones o innovaciones en determinadas áreas técnicas en las cuales el pais es líder. Las normas técnicas peruanas son revisadas cada cinco ai'los con el propósito de actualizarlas.

Pueden ser miembros de los Comités Técnicos de Normalización las personas naturales y jurídicas con especialización en el área de trabajo correspondiente. La Comisión de Reglamentos Técnicos y Comerciales debe considerar para la designación de miembros de un Comité el que éstos provengan, en la medida de lo posible, de sectores de la producción - gremios y comercializadores- , del consumo - asociaciones de consumidores, consumidores representativos y representantes del Estado-, y de la técnica -e specialistas. entidades académicas, asociaciones técnicas. laboratorios, organismos de certificación y colegios profesionales- .

Con relación al «Reglamento interno de trabajo» como instrumento de autorregulación que determina las condiciones a que deben sujetarse los empleadores *y* tra bajad ores en el cumplimiento de sus prestaciones, el Decreto Supremo 039-91- TR dispone que están obligados a contar con éste los empleadores que ocupen a más de cien trabajadores. La elaboración del mismo es potestad exclusiva del empleador y su aprobación só lo requiere de presentación ante la autoridad adminisrtativa de trabajo. El empleador está obligado a hacer entrega de un ejemplar a los trabajadores. dentro de los cinco días de producido el referido acto.

3.3 La jurisprudencia constitucional

En este punto, resulta indispensable analizar la sentencia del Tribunal Constitucional, antes mencionada, sobre el expediente 1058-2004-AA publicada el 18 de agosto de 2004. Dicha sentencia recae sobre el recurso extraordinario presentado por Rafael Francisco García Mendoza en contra de la sentencia que declara improcedente la acción de amparo frente a la empresa Servicios Postales del Perú S.A. (SERPOST S.A.) solicitando se deje sin efecto el despido, y consecuentemente, la reposición en su puesto de trabajo.

El trabajador sostiene en su demanda que el empleador le atribuye de manera arbitraria, una supuesta falta grave: la de utilizar indebidamente los recursos informáticos en el puesto

y durante el horario de trabajo. Asimismo, alega que no le permitió ejercer adecuadamente su derecho de defensa, que vulneró su derecho de libertad de trabajo, el carácter irrenunciable de sus derechos laborales y su derecho al debido proceso. Por su parte, en la contestación de la demanda el empleador argumenta que si cumplió con el debido proceso, que constató "el envío de material pornográfico a través del sistema de comunicación electrónico, denotando falta de capacidad e idoneidad para el desempeño del cargo e inobservancia del Reglamento Interno de Trabajo" y que en consecuencia aplicó la sanción prevista en la legislación vigente y en el reglamento interno de trabajo, y por tanto, el despido fue justificado y legal.

Inicialmente, el juzgado declaró fundada la acción de amparo en contra del empleador por haber vulnerado los derechos constitucionales de tipicidad, inmediatez y de defensa. La recurrida, en contrario, revoca la sentencia apelada y declara improcedente el amparo, por considerar que la falta cometida si estaba debidamente tipificada y que se dieron al trabajador las condiciones de respeto a su derecho de defensa.

Los fundamentos expueslos por el Tribunal parten de reconocer que las causas de extinción del contrato de trabajo, entre las cuales está considerado el despido, se hayan reguladas en la ya citada Ley de Productividad y Competitividad Laboral contenida en el Decreto Legislativo 728, cuyo texto único ordenado fue promulgado mediante Decreto Supremo 003-97-TR. En dicha disposición se establece que el despido procede sólo en los casos y forma permitidos por la ley; por lo que, tratándose de un trabajador sujeto al régimen de la actividad privada. es indispensable la existencia de una causa justa debidamente comprobada. La causa justa, cuando está relacionada con la conducta del trabajador, se sustenta en la comisión de una falta grave. Según la ley bajo análisis. se considera como falta grave aquella infracción de los deberes esenciales del contrato de trabajo que hace irrazonable la subsistencia del mismo. Asimismo, la propia ley describe un conjunto de conductas que constituyen faltas graves. De otro lado, establece que el despido por causa justa no procede sin que el empleador otorgue al trabajador, previamente y por escrito, un plazo razonable no menor de seis días naturales para que éste pueda defenderse por escrito de los cargos que se le formulen, salvo en casos de falta grave flagrante Si el trabajador impugna el despido en un proceso judicial, la demostración de la causa justa corresponde al empleador. Ese es el régimen que legisla la adecuada protección contra el despido arbitrario del trabajador establecido por el artículo 27 de la Constitución Politica. En este sentido, la Jurisprudencia del Tribunal Constitucional ha sentado como precedente que ante el despido arbitrario existen dos opciones: una general y compensatoria, por la que el juez laboral ordena el pago de indemnización para el trabajador de la actividad privada; y otra especial y reparador a, en la que el

juez constitucional repone las cosas al estado anterior a la amenaza o violación de un derecho constitucional., lo que supone restituir al trabajador en caso de despido nulo, sin causa justa o fraudulento.

El Tribunal Constitucional consideró que en el procedimiento disciplinario materia de controversia, el empleador incurrió en una serie de infracciones. En primer lugar, porque la jurisprudencia constitucional ya ha señalado que los procedimientos disciplinarios, de cualquier índole, se rigen por el principio de tipicidad sancionatoria; lo que en el presente caso determina que la conducta atribuida al trabajador esté comprendida en los alcances del inciso a) del articulo 25 de la Ley de Productividad y Competitividad Laboral; esto es, que constituya un incumplimiento de las obligaciones de traba jo que suponga el quebrantamiento de la buena fe laboral, la reiterada resistencia a las órdenes relacionadas con las labores, la paralización intempestiva de labores, así como la inobservancia del reglamento Interno de trabajo, todo ello, siempre que revista gravedad. En ese sentido, el Tribunal no observó coherencia entre el mandato legal y la conducta atribuida al trabajador y con relación a las disposiciones del reglamento interno de trabajo, aún asumiendo que los hechos imputados constituyen una disminución deliberada y reiterada del rendimiento en las labores y una utilización indebida de los bienes o servicios del empleador, estos hechos no son calificados como faltas graves, y en consecuencia, no constttuyen causa justificada de despido.

En segundo lugar, con relación a la intensidad de la sanción, el Tribunal consideró que, según el mencionado reglamento interno de trabajo, la sanción debió ser establecida tomando en cuenta los hechos, la gravedad de las faltas y los antecedentes del trabajador; lo que resultó desproporcionado e irrazonable en tanto que el empleador procedió de manera inmediata y sin ponderar la aplicación de la sanción más grave prevista, el despido. Por tanto, el Tribunal Consti1ucional opinó que esa circunstancia tergiversa los alcances del debido proceso, tanto en términos formales como sustantivos.

En efecto, el debido proceso es un medio que hace posible el ejercicio de otros derechos y un factor que delimita el accionar de quien tiene autoridad, evitando el abuso del poder. El concepto de debido proceso es un aporte hecho por la doctrina estadounidense que derivó en el sustento constitucional del *right to privacy*. Tomando en cuenta que el sistema de derecho peruano se sitúa, como consecuencia de la influencia europea. en la dignidad de la persona, el aporte derivado del debido proceso sustantivo resulta en el concepto de razonabilidad que incluye, a su vez, los principios de causalidad y proporcionalidad. El debido proceso sustantivo incluye la necesidad de que quien ejerce poder lo haga de acuerdo a fines lícitos, sobre todo si dicho ejercicio amenaza los derechos fundamentales, por tanto, el objeto del concepto de razonabilidad es que la actuación del poder consider e los fines respetando el

principio de causalidad y también los medios empleados para su ejercicio, bajo el principio de proporcionalidad, el cual incluye una evaluación de la utilidad e idoneidad de dichos medios. (ESPINOSA. 2004)

El tercer aspecto cuestionado por el Tribunal es el relacionado a la verificación de las pruebas que debió permitir al empleador llegar a la conclusión de incriminar al trabajador, y a la notificación de los hechos objetivos a este último con el fin de que ejerciera adecuadamente su derecho de defensa. El Tribunal concluye que la acreditación de la veracidad de la autoría de los mensajes de correo electrónico, llevada a cabo por el empleador, tuvo carácter preliminar y no fue seguida por una investigación sólida y concluyente que determinara si efectivamente los mensajes fueron remitidos por el trabajador y, asimismo. impidió que éste pudiese acceder a los recursos informáticos con el fin de permitirle recoger datos e información que hicieran posible sustentar adecuadamente sus descargos.

Con relación a este punto, cabe resaltar que si bíen al momento de la expedición de la sentencia analizada ya se encontraba vigente la Resolución Ministerial 224-2004-PCM que estableció el uso obligatorio de la norma técnica peruana ISO/IEC 17799:2004 para las entidades del Sistema Nacional de Informática, entre las que se encuentra considerada SERPOST; al momento de los hechos esta aún no se encontraba vigente. Además hay que tomar en consideración que dicho dispositivo dispuso la implantación de las buenas prácticas para la gestión de la seguridad de la información en un plazo de 18 meses a partir de su publicación. En todo caso, resulta evidente que la correcla verificación de los hechos ocurridos en el sistema de información del empleador, deberá en el fuluro, ceñirse a los parámetros establecidos por la mencionada norma, subsanando así el método deficiente que, a todas luces, constituyó la constatación notarial.

El cuarto aspecto considerado por el Tribunal Constitucional, es la relación existente entre el procedimiento por el cual se llevó a cabo el despido del trabajador y la protección de sus derechos constitucionales a la privacidad y a la reserva de comunicaciones, en tanto que se constata en el mismo, tanto la existencia de los mensajes como su contenido. En efecto, de la lectura de la constatación notarial Que acredita la existencia y el contenido de los mensajes de correo electrónico, el Tribunal llega a tres conclusiones: que el usuario del recurso informático en donde fueron vistos los mensajes fue un tercero distinto al emisor y receptor de los mismos; que dicho usuario, ajeno a la comunicación, actuó por propia voluntad sin la debida autorización del destinatario, y que por último, no siendo éste el destinatario del mensaje no se le podía considerar agraviado. Asimismo. el Tribunal consideró que el empleador debió realizar un proceso de investigación profundo y detallado con el fin de verificar técnicamente el origen de la remisión de los mensajes, que partiera de asegurar que los re-

cursos informáticos utilizados para la comunicación no hubiesen sido manipulados de tal manera de adulterar la identidad del remitente o la autoría del contenido. En este último punto, el Tribunal deja en cfaro que la naturalez;a técnica del medio informático exige una verificación de igual naturaleza, lo que supone recurrir necesarí amente en estos casos, al cumplimiento de las buenas prácticas de la norma técnica *en* mención y que es analizada en detalle en el siguíente capítulo.

Además de los aspectos tratados con relación al procedimiento, el Tribunal Constitucional considera pertinente pronunciarse sobre el hecho de saber si los recursos informáticos proporcionados a los trabajadores para el desempeño de sus abores, pueden atribuirse como de dominio absoluto de sus empleadores, o si por el contrario, existe un ámbito de protección en el que éstos no podrán intervenir de manera irrazonable. En ese sentido, el Tribunal Constitucional resalta la característica de los recursos informáticos como instrumentos de comunicación y reserva documental, y como tales. les reconoce elementos de autodeterminación personal que se presentan en aquellas condiciones laborales referidas a los derechos fundamentales como límites previstos por la Constitución Política.

Así, como lo establece el artículo 2.10 de Constitución Política, toda persona tiene derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados; y si bien en este caso el soporte de las comunicaciones y documentos electrónicos pertenece al empleador, para el Tribunal Constitucional esto, no significa que aquél pueda arrogarse de manera exclusiva, ni excluyente, la titularidad los mismos, ya que de otro modo se estaría aceptando que la relación laboral puede enervar el esquema de atributos de la persona. En consecuencia el empleador debe abstenerse de descubrir el contenido reservado de las comunicaciones o sus instrumentos, de apoderarse arbitrariamente de éstos antes de que lleguen a su destino, o de espiarl.as; salvo que lo haga por mandamiento motivado de Juez, y guardando el secreto sobre los asuntos ajenos al hecho que motiva su examen.

El Tribunal Constitucional reconoce que el trabajador, por el hecho de estar obligado al cumplimiento de las obligaciones establecidas en la relación laboral, no deja de ser titular de los derechos fundamentales que la Constituc.ión Política le reconoce como persona, esto, en concordancia con lo establecido por el artículo 23 de la misma y con la teoría de la *Drittwirkung;* por lo que, como reafirma el Tribunal, resulta inobjetable el respeto que deben los empleadores al contenido esencial de los derechos del trabajador.

El Tribunal Constitucional aborda en ese punto uno de los problemas más serios en la dogmática de los derechos fundamentales, el referido a sus posibles límites y al necesario respeto a una valla infranqueable que en algunos ordenamientos europeos han denominado

«contenido esencial». Los derechos fundamentales se encuentran sujetos a determinados limites razonables que deben ser adecuadamente justificados. La existencia de tales límites se justifica, entre otras razones, por el reconocimiento de su coexistencia con otros derechos fundamentales y otros bienes jurídicos que también gozan de protección constitucional. Sin embargo, no resulta posible que todas las posibles restricciones a estos derechos puedan regularse en los textos constitucionales, de ahi el interés por conocer la jurisprudencia constitucional, pues será esta la que en definitiva determine la validez de los limites establecidos.

Los límites necesarios para la protección de otros bienes constitucionalmente tutelados, derivados directa o indirectamente del texto fundamental, encuentran justificación en la llamada «teoría de los límites inmanentes a los derechos fundamentales»; la cual postula que tales derechos, al ser parte de un ordenamiento jurídico, no pueden hacerse valer de manera absoluta frente a los demás bienes que dicho ordenamiento protege. Los bienes constitucionalmente protegidos no forman parte de un orden jerarquizado, por tanto, no es posible resolver un conflicto entre aquéllos aceptando la superioridad de unos sobre otros; el conflicto debe ser resuelto entonces como resultado de una ponderación que busque la «concordancia práctica», principio de interpretación constitucional que exige la coordinación de los bienes jurídicos protegidos para que al momento de resolver el conflicto todos ellos conserven su identidad, siendo el elemento «proporcionalidad» un criterio de interpretación indispensable.

El contenido esencial de un derecho fundamental es un concepto jurídico indeterminado, cuyo ámbito y significado no se establece de manera general sino que se precisa para un derecho fundamental determinado; constituyendo su contenido esencial aquellas facultades indispensables para que el derecho sea reconocible como tal. En ese sentido, se desconoce el contenido esencial cuando el derecho es limitado, de tal manera, que su ejercicio se torna impracticable, se estorba más allá de lo razonable o se le quita la protección necesaria. El respeto al contenido esencial ha sido entendido como el «límite de los límites» más allá del cual no es posible la actividad delimitadora; y si bien éste ha sido formulado con relación a la intervención del legislador, exige un alcance que comprende la aplicación del derecho mismo. (ABAD, 1992)

En ese sentido, nuestra opinión es que el respeto al contenido esencial al derecho a la intimidad del trabajador desvirtúa la práctica llevada a cabo por algunos empleadores al requerirles su consentimiento para acceder de manera irrestricta al contenido de los mensajes oloclróni cos enviados o recibidos por éstos a través do los sistemas de información de su propiedad.

Sin embargo, el Tribunal también opina que su alegato al reconocimiento y respeto que deben los empleadores a los derechos fundamentales de los trabajadores no es obstáculo para que aquellos ejerciten su poder fiscalizador y disciplinario, siempre que éste, esté delimitado por el respeto a los mencionados derechos y que se ejercite mediante mecanismos razonables que cumplan con los objetivos laborales de la organización. Lo que el Tribunal pone en cuestión es el procedimiento de investigación llevado a cabo por el empleador con el fin de probar la responsabilidad del trabajador y, en este sentido, sostiene que la sola facultad fiscalizadora de aquél no le permite acceder al contenido reservado de los mensajes de correo electrónico enviados o recibidos por los trabajadores, en tanto éstos se encuentran sujetos al derecho al secreto elemental de las comunicaciones y documentos privados que, según la garantía constitucional, sólo puede limitarse por mandato judicial.

En esa misma linea, al cuestionar el proceder del empleador para la obtención de los mensajes de correo electrónico que vulneró el secreto de la comunicación y la garantía de judicialidad, el Tribunal sostiene la invalidez de dichos mensajes como elementos probatorios. Ello debido a lo dispuesto en el tercer párrafo del articulo 2.10 de la Constitución: “Los documentos privados obtenidos con violación de este precepto no tienen e fecto legal”. En conclusión, los mensajes de correo electrónico obtenidos de la manera descrita en el expediente carecen de valor probatorio y, al no producir estos efecto jurídico, el acto de despido con el que el culminó el procedimiento disciplinario deviene en nulo. Con ello. sostiene el Tribunal. se garantiza que los medios de prueba obtenidos ilícitamente no desnaturalicen los derechos del trabajador como persona ni generen efectos en su perjuicio.

Por lo anterior, el Tribunal Constitucional declara inconsti tucional el procedimiento de fiscalización seguido por el empleador, y concluye que, en general, los empleadores están sujetos a la obligación de implementar medios adecuados de control y fiscalización de la labor y la eficiencia del trabajador, de llevarlos a cabo de manera razonable con relación a los fines de la relación laboral y sin perjudicar los ámbitos propios de la autodeterminación de los trabajadores.

CAPÍTULO 4 La seguridad de la información y el control informático

4.1. La información: su clasificación y seguridad

La información se define como la capacidad de elaborar, acumular y distribuir experiencias humanas por medio del lenguaje oral, gestual o simbólico. Se adquier e información cuando se conoce algo que con anterioridad no se conocía. Disponer de determinada información, cuyo conocimiento no es generalizado, permite usarla y ma nip u larla en beneficio propio. La información se estima como un bien de utilidad social y se valora también en términos económicos, pero no ha sido hasta la sociedad contemporánea que se le ha considerado como un bien jurídico, merecedor como tal de protección adecuada.

Con el avance de la tecnología, el tratamiento automatizado de la información ha planteado nuevos problemas sociales, económicos y jurídicos. La informática puede conservar, ceder, hacer inaccesible o propagar la información en forma instantánea e ilimitada en el espacio; y puede modificarla como una cosa. La información ha devenido en una mercancía no sólo por su contenido, sino también por su forma mensurable en términos de valor de mercado (FROSINI, 1998).

Los logros de las avanzadas tecnologías en la utilización y transmisión de la información tienen corno contraparte el grave aumento de los riesgos a su seguridad. por ello, los administradores de los sistemas de información se ven en la necesidad de establecer políticas de seguridad basándose en un análisis de los riesgos y en un conjunto de prevenciones que permitan conseguir la seguridad de la información. La gestión de la seguridad de la información se caracteriza así por un conjunto de políticas, prácticas, procedimientos, estructuras organizativas y fun ciones de software dirigidas a preservar la confidencialidad, integridad y disponibilidad de la información (MORANT et al., 1994).

Un sistema de información es el conjunto de elementos –personal, datos, programas y equipos- que permiten el almacenamiento, proceso y transmisión de información con el objetivo de realizar tareas; la aplicación de la automatización o informática los han ido haciendo cada vez más complejos y en igual sentido, exponiendo una mayor cantidad de puntos vulnerables.

Se identifican cuatro tipos de amenazas a los sistemas de información:

- la interceptación, cuyo origen es el acceso a una parte del sistema al que no se está autorizado;

- la modificación, que involucra el cambio en parte o en todo del funcionamiento del sistema;

- la interrupción, que puede ser temporal o permanente e incluye la posibilidad de destrucción de equipos, borrado de archivos, bases de datos, registros, programas, etc., y;

- la generación, referida a la posibilidad de incluir campos y registros en una base de datos, añadir líneas de código a un programa o un programa completo, como los denominados virus informáticos, introducir mensajes no autorizados, etc. (MORANT et al., 1994).

Las políticas de seguridad que los administradores de sistemas establezcan, son el resultado de un exhaustivo análisis de riesgos y se ejecutan a través de un conjunto de medidas y mecanismos que permiten alcanzar niveles de seguridad proporcionales al coste del valor de la información que se protege.

Las medidas de seguridad para la protección de los sistemas de información son de cuatro tipos: lógicas, de carácter físico, de carácter administrativo y legal. De ahi que los empleadores deben conocer el ordenamiento jurídico vigente para decidir contra cuales amenazas se debe proteger al sistema y, además, establecer las normas de carácter administrativo para determinar responsabilidades ante los ataques.

La seguridad lógica busca la protección de la información con valor patrimonial, tanto la contenida en las bases de datos y doc u mentos electrónicos como las propias aplicaciones informáticas; se realiza principalmente con la utilización de métodos criptográficos; contraseñas, conocimientos y hábitos del usuario y firmas digitales. La seguridad administrativa se funda en la definición y vigencia de las politicas de seguridad, de personal y de contratación así como de los análisis de riesgos y los planes de contingencia a e jecu tar por los responsables de los sistemas de información. (PESO, 2000)

En general, los sistemas informáticos incorporan mecanismos que ofrecen servicios de seguridad de la información a los usuarios; éstos proporcionan tres propiedades o características fundamentales:

- La confidencialidad, por la que la información sólo está disponible para los usuarios autorizados, es decir, para aquellas personas, entidades o programas que tengan derecho legal a usarla, incluyendo la protección contra el análisis de tráfico.

- La integridad, por la que se asegura la exactitud de la información y sus métodos de proceso.

- La disponibilidad, que asegura que los usuarios autorizados tienen acceso a la información en el momento en que lo requieran.

En especial con relación a las redes de datos, las siguientes son características de su seguridad:

- La autenticidad, que permite asegurar el origen y destino de la información y;

- La no refutabilidad, reconocida en el lenguaje técnico como «no-repudio», permite que cualquier usuario que envía o recibe información no pueda alegar válidamente que no la envió o recibió.

La norma técnica peruana ISO/IEC 17799:2004 recomienda. con relación a la clasificación y control de activos de información, asignar un propietario para todos y cada uno de los activos importantes; la responsabilidad del propietario sobre éstos ayuda a asegurar que se mantenga la protección adecuada.

Las organizaciones tienen que identificar sus activos y el valor e importancia relativos. El inventario ayuda a asegurar una protección eficaz de la información y sobre éste se pueden establecer diversos niveles de protección, proporcionales al valor e importancia determinados. En el item 5.5.1 de la norma técnica se recomienda establecer y mantener un libro de inventarios de tos activos de información importantes; cada activo debe identificarse claramente, acordar y documentar su seguridad y pertenencia, y su situación.

Son ejemplo de «activos de información»: los archivos y bases de datos, la documentación del sistema, los manuales de los usuarios, el material de form ación, los procedimientos operativoso de soporte, losplanesde continuidad, la configuraicón del soporte de recuperación, la información archivada: el software de aplicación, el software del sistema, y las herramientas y programas de desarrollo.

La clasificación de la información facilita la seguridad de los recursos y los dalos, por ello la necesidad de tener clasificada la información es obvia: sin embargo, no son muchas las organizaciones que la tienen establecida y que en realidad conocen el valor patrimonial de su

información. la clasificación de la información, utilizada de manera adecuada, es un medio para dar a conocer a los usuarios la protección que requiere cada uno de los elementos del sistema de información.

Los criterios de clasificación son un aspecto importantepara la seguridad de la información; la «clasificación por niveles» se cimenta en un orden jerárquico en el que el nivel más bajo es, comúnmente, «no clasificado»y el nivel más alto, «secreto»; el orden de los niveles corresponde a la importancia de los datos y los requisitos de los procedimientos de seguridad. La «clasificación por categorías», por otro lado, se utiliza para identificar grupos independientes de datos y recursos que necesiten procedimientos similares de protección; las categorías no tienen relación alguna y se asignan tanto a usuarios como a datos.

Los criterios deben elegirse con relación a riesgos tales como la destrucción, que afecta la disponibilidad de la información y se refiere al borrado o a no contar con los recursos, datos o programas cuando se requieren; toda aquella información que es necesaria para la continuación de las actividades del negocio es sensible a su destrucción. También se puede considerar el riesgo de modificación, que atenta contra la integridad de la información y se refiere al cambio no autorizado o no detectado de los datos o de los programas. Por último el riesgo de difusión, que se refiere al conocimiento que se adquiere a través de los datos obtenidos y que afecta la confidencialidad de la información.

Por ejemplo, una clasificación por nivelesque utiliza como criterio la sensibilidad al riesgo de difusión de la información considerará como tales a: «datos confidenciales», aquellos de difusión no autorizada debido a que su uso indiscriminado puede ser la causa de un daño importante; «datos restringidos», también de difusión no autorizada debido a que su utilización puede estar en contra de los intereses de sus propietarios o clientes; «datos de uso interno», que no necesitan ningún grado de protección para su difusión dentro de la organización y, por último; «datos no clasificados», que no tienen restricción alguna para su difusión pública.

La clasificación tiene por objetivo asegurar un nivel de protección adecuado a los activos de información. La norma técnica recoge. en el ítem 5.1.2, la práctica de clasificarlos para indicar la necesidad, prioridades y grado de protección, asimismo, la de elaborar catálogos que describan los activos de información y los resultados de los sistemas que manejan datos clasificados con relación al valor e importancia para la organización.

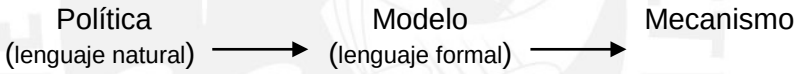
La clasificación de la información debería tomar en cuenta la necesidad de la organización de compartir o restringir ésta, en función al negocio y los efectos negativos asociados: la clasificación es una forma abreviada de manejar y proteger la información. El responsable

de la clasificación de un elemento de información, por ejemplo, un documento, un registro, un archivo o un disco, debería ser el propietario de los mismos. Es importante que la organización defina procedimientos para marcar y tratar los elementos de información de acuerdo con la clasificación, antes de llevar a cabo acciones como copia, almacenamiento, transmisión o destrucción.

4.2. Las *políticas, modelos y mecanismos de seguridad*

La politica de seguridad de la información define la manera como ésta. en cada nivel de la organización o empresa, se sistematiza, gestiona, protege y distribuye; dicha política constituye el conjunto de directrices generales que deben guiar la seguridad de la información. Las directrices son dadas por los niveles directivos de la organización o impuestas legalmente.

Previa transformación al lenguaje matemático que da como resul tado un modelo de seguridad, las directrices de la política de seguridad se implantan en las computadoras electrónicas en forma de mecanismos de seguridad aplicados tanto al hardware como al software, estableciéndose la siguiente secuencia:



Un modelo de seguridad capacita a tos usuarios para trabajar con el sistema de manera eficiente, da a entender a los administradores de sistemas qué controles construir y marca el patrón a los auditores para determinar si el sistema de seguridad es consistente con las políticas y si está implementadocorrectamente.

El control de acceso a los recursos informáticos es uno de los asuntos más importantes que rigen las directrices de política de seguridad de la información aprobadas por una organización o empresa; mediante éstas se establecen las condiciones bajo las que un usuario o programa puede acceder a un objeto que contiene o recibe información. Un objeto suele ser un docume nto electrónico, un directorio de documentos, una estructura de datos, una tabla del sistema operativo, un segmento o página de memoria. un dispositivo auxiliar, etc. (MORANT et al.,1994)

4.3. La norma técnica peruana ISOIIEC 17799:2004 y el cumplimiento de la legalidad

Como ya se anotó anteriormente, las normas técnicas peruanas son aprobadas por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) en su calidad de organismo peruano de normalización. La norma a que se hace referencia, es resultado de la adaptación de la norma de la Organización Internacional de Normalización ISO/IEC 17799:2000 *lnformation technology - Code of practice for information security management;* realiz ada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos y presentada para su aprobación a la Comisión de Reglamentos Técnicos *y* Comerciales. No habiéndose presentado ninguna observación fue promulgada como «NTP-ISO/IEC 17799:2004 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 1ª Edición», el 27 de marzo de 2004.

Las normas técnicas en general son de cumplimiento voluntario, sin embargo, si su inaplicación afecta la seguridad, la salud, la protección al consumidor o el ambiente; los organismos competentes las pueden hacer obligatorias. Asimismo, como se mencionara con anterioridad, la obligatoriedad de las normas técnicas puede ser también consecuencia de la remisión que haga el ordenamiento jurídico; ese es el caso de la norma técnica peruana en cuestión que, por Resolución Ministerial 224 de la Presidencia del Consejo de Ministros promulgada el 26 de julio de 2004, es obligatoria en todas las entidades integrantes del Sistema Nacional de Informática.

Son parte del Sistema Nacional de Informática, según el artículo 7 del Decreto Legislativo 604 «Ley de organización y funciones del Instituto Nacional de Estadistica e Informática»: los ministerios, los organismos centrales, las instituciones públicas descentralizadas, las empresas del Estado, los gobiernos regionales, las municipalidades, los poderes públicos y los organismos autónomos.

El objetivo de la norma técnica ISO/IEC 17799 es evitar el incumplimiento de las leyes y reglamentos, estatutos, obligaciones contractuales y de todo requisito de seguridad por parte de las organizaciones y empresas; en ese sentido, la norma recomienda la asesoría de profesionales del derecho sobre la normatividad aplicable para determinar las obligaciones legales especificas y documentar aquellos requisitos para cada sistema de información en particular.

La determinación de los requisi tos de seguridad es esencial, éstos se establecen a partir de tres fuentes principales: la valoración de los riesgos; las obligaciones legales, estatutarias y contractuales; y los principios, objetivos y requisitos del tratamiento de la información del sistema de la organización o empresa. La evaluación de riesgos considera el impacto económico y moral de ocurrir un fallo de seguridad y la probabilidad de la propia ocurrencia.

El uso de una computadora electrónica puede ser el medio para la comisión de un delito, ello es uno de los principales riesgos que inducen a la protección contra el mal uso de la informática en las organizaciones y empresas; de ahí que sea esencial que los usuarios de los recursos informáticos conozcan el alcance del acceso que se les permite, por ejemplo, con una autorización documentada en la que se informe a los trabajadores que se considera impropio todo uso de dichos recursos para fines no autorizados o ajenos al negocio y que la infracción dará lugar a la acción disciplinaria apropiada.

Determinados los requisitos de seguridad se seleccionan e implantan controles que aseguren la reducción del riesgo a un nivel aceptable. Los controles expuestos en la norma técnica peruana ISO/IEC 17799:2004 se consideran principios que guían la gestión de la seguridad de la información, algunos de ellos son esenciales, como la protección de los datos de carácter personal y la intimidad de las personas; la salvaguarda de la documentación oficial de la organización o empresa; y los derechos de la propiedad intelectual. La norma también considera como controles que constituyen buenas prácticas para la gestión de la seguridad de la información: documentar la politica de seguri dad de la información, asignar responsabilidades de seguridad, formar y capacitar al personal para la seguridad de la información, registrar las incidencias de seguridad, y gestionar la continuidad del negocio.

Además de la remisión a la norma técnica peruana a que se ha hecho mención, las «buenas prácticas» también han sido integradas al ordenamiento jurídico peruano a través de la Circular G-105-2002 emitida por la Superintendencia de Banca y Seguros con referencia a los riesgos de tecnología de la información con fecha 22 de febrero de 2002, en el marco del «Reglamento para la administración de los riesgos de operación» aprobado por la Resolución S. B. S. 006 - 2002 del 4 de enero del mismo año. El ámbito de aplicación de estas normas comprende a las empresas bancarias y financieras; las cajas municipales de ahorro y crédito; las entidades de desarrollo a la pequeña y micro empresa (EDPYME); las cooperativas de ahorro y crédito autorizadas a captar recursos del público; las cajas rurales de ahorro y crédito: las empresas de capitalización inmobiliaria, de arrendamiento financiero y de *factoring:* las empresas afianzadoras y de garantías; las empresas de servicios fiduciarios; los bancos de inversión; las empresas de seguros *y* de reaseguros; los almacenes generales de depósito; las empresas de transporte, custodia y administración de numerario; las

empresas emisoras de tarjetas de crédito y/o de débito; las empresas de servicios de canje y de transferencia de fondos; así como el Banco Agropecuario; la Corporación Financiera de Desarrollo S.A. (COFIDE); el Banco de la Nación: la Fundación Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI) y las derramas y cajas de beneficios que se encuentran bajo la supervisión de la mencionada Superintenden cia.

Según la mencionada Circular. las organizaciones descritas deben establecer, mantener y documentar un sistema de administración de la seguridad de la información denominado "Plan de Seguri dad de la información" el cual debe implementarse con la definición de una política de seguridad. la evaluación de riesgos de seguridad a los que está expuesta la información y la selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión. Para la administración de la seguridad de la información deben considerarse aspectos de seguridad lógica definiendo una política para el control de accesos a los sistemas de información, redes y sistemas operativos, que otorgue a los usuarios una identificación para su uso personal de tal manera que las posibles responsabilidades puedan ser seguidas e identi ficadas. En cuanto a la seguridad de personal, deben definir procedimientos para reducir los riesgos asociados al error humano, robo, fraude o mal uso de activos vinculados al riesgo del uso de la tecnología de información. Con relación a la clasificaciónde información, deben realizar un inventario periódico de activos asociados a la tecnología para una posterior clasificación de seguridad de dichos activos: y, en cuanto al cumplimiento normativo, deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos y, cuando corresponda. incorporarlos en la lógica interna de las aplicaciones informáticas.

4.4. El control de accesos a *la información*

Controlar los accesos a la información es un requisito indispensable de seguridad que debería establecerse clararnenle en reglas y derechos de acceso para cada usuario o grupo de usuarios estandarizados, según las categorías comunes de trabajo.

La gestión del acceso de usuarios tiene como objetivo evitar accesos no autorizados a los sistemas de información, estableciendo procedimientos formales para controlar la asignación de los derechos de acceso, tomando en consideración: la clasificación y distribución de la información y las autorizaciones, las obligaciones respecto a la protección de datos y la administraciónde los derechos de acceso a la red.

El control de accesos debe detectar todos los accesos a los objetos de información, asi como los comandos que otorgan, transfieren o revocan los derechos de acceso a los mismos.

El mecanismo de control más simple se asemeja a un directorio de archivos en el que cada archivo (objeto) tiene un único usuario propietario (sujeto) que posee todos los derechos sobre él, incluyendo los de otorgar o revocar esos mismos derechos a otros usuarios; a cada usuario corresponde un directorio que lista todos los archivos a los que tiene acceso con sus derechos correspondientes.

Otro mecanismo es el de una matriz de accesos cuyas filas representan sujetos y cuyas columnas simbolizan objetos, cualquier intersección de fila y columna define los derechos del sujeto respecto del objeto. Además del derecho del propietario por el que puede otorgar y revocar los derechos originales sobre el objeto poseído, los derechos de acceso varían según el objeto; así por ejemplo, en el caso de archivos, los más comunes son los derechos de lectura, de escritura y de ejecució n. (MORANT et al. 1994)

4.4.1. La identificación y autenticación de los usuarios

El mantenimiento de un registro formal de las personas autorizadas a usar el sistema de información de la organización o empresa, y un procedimiento formal de registro de altas y baja s de éstos usuarios, son la garantía de un acceso autorizado. Dichos procedimientos deberían incluir, según el ítem 9.2.1 de la norma técnica, las prácticas siguientes:

- utilizar un identificador único para cada usuario con el fin de vincularlo y hacerle responsable de sus acciones;
- comprobar la autorización de uso por el propietario del activo de información o por la gerencia
- entregar al usuario una relación de sus derechos de acceso y solicttarle su reconocimiento;
- garantizar que no se provea acceso hasta completar el procedimiento de autenticación;
- eliminar inmediatamente las autorizaciones de acceso a los usuarios que dejan la organización o cambien de puesto de trabajo y no reasignar sus identificadores; y
- revisar y eliminar periódicamente identificadores y cuentas de usuario redundantes.

Como ya se mencionó y trató en el capítulo anterior, el derecho a la identidad personal es un derecho fundamental recogido por el inciso 1 del artículo 2° la Constitución Política. Además, el derecho de toda persona a ser identificada e individualizada es reconocido por el Código

Civil peruano en el título tercero de la primera sección del libro del derecho de las personas, en donde se regula los derechos al nombre y al seudónimo. El nombre es la expresión mediante la cual se identifica a la persona.

El derecho a la identidad comprende el derecho a llevar un nombre, lo que supone reconocer a cada persona como un ser único con identidad psicosomática propia; a partir de ese reconocimiento la persona tiene la facultad y el deber de asumir sus actos e impedir se le atribuyan comportamientos ajenos. La jurisprudencia nacional ha protegido el derecho a la identidad tanto en el sentido de impedir que se imputen conductas que no pertenecen a la persona, como en evitar que otras personas asuman aquéllas de las que ésta es realmente protagonista. (FERNÁNDEZ, 2004)

El derecho que le reconoce a toda persona el articulo 26° del Código Civil, a exigir que se le designe por su nombre, o lo que es lo mismo, de llevar un nombre: es la más importante manifestación de la identidad de la persona y, en consecuencia, su protección permite oponerse a todo acto destinado a usurparlo. "Mediante el nombre se designa e individualiza socialmente al sujeto de derecho. De ahí que el llevar un nombre no sólo constituya un derecho de la persona sino que es un deber el detentarlo. Este deber, cuyo pretensor o facultado es la sociedad juridicamente organizada, fundamenta la regla". (FERNÁNDEZ, 2004: 117)

Pero como ya se expuso en el capítulo anterior, la protección no se agota en los signos distintivos de la persona sino que trasciende a la proyección social de los actos de ésta. El derecho a la identidad personal de los trabajadores, usuarios de los recursos informaticos proporcionados por el empleador, obliga a éste último ha implementar una política de control de accesos al sistema de información acorde con la «buenas prácticas» de la norma técnica peruana ISO/IEC 17799:2004, con el fin de asegurar que las actividades que realizan los trabajadores no alteren, distorsionen o desnaturalicen su identidad, imputándoles acciones o comportamientos que no le corresponden.

4.4.2. El control y seguimiento de accesos y usos del sistema operativo y las aplicaciones

El «sistema operativo» es un tipo de software destinado a la comunicación del usuario con la computadora electrónica y a la gestión eficiente de los recursos de la misma. El estado de desarrollo actual de los sistemas operativos ha llevado a contar con características de administración de múltiples usuarios (sistemas operativos multiusuario), que permite que varios usuarios ejecuten programas de manera concurrente o separada, utilizando métodos de protección de manera que un programa no pueda usar o cambiar los datos de otro usuario.

> "Para que un sistema operativo sea seguro debe ser diseñado de modo que: identifique y autentifique a todos los usuarios: controle el acceso a todos los recursos *e* informaciones; contabilice todas las acciones realizadas por usuarios (o procesos invocados por ellos); audite los acontecimientos que puedan representar amenazas a la seguridad; garantice la integridad de los datos: mantenga la disponibilidad de recursos e informaciones: (...)(MORANT et al., 1994: 227)

Antes de utilizar un recurso informático que cuenta con un sistema operativo seguro, éste procede a identificar y autenticar al usuario que va a ser su interlocutor, quien, comúnmente mediante la introducción de un par de parámetros: el «nombre de enlace» (del inglés *Log in name*) que consiste en un código o conjunto de caracteres alfanuméricos que identifican al usuario, y la «contraseña» (del inglés *password)*. El primero de estos parámetros es asignado por el administrador del sistema a cada usuario y por tanto es de conocimiento compartido: comúnmente cuando el usuario se conecta a la computadora su sistema operativo le solicita, en primer lugar, su «nombre de enlace» y luego procede a su identificación. Luego de una identificación positiva, el sistema operativo solicita la «contraseña» que sólo conoce el usuario y por tanto es secreta, ingresada esta realiza la autenticación y otorga acceso al sistema sólo si ambos parámetros son válidos, o responde con un mensaje de error sin detallar si éste se dio en el nombre de enlace o en la contraseña. La máxima seguridad exige que las contraseñas se encuentren cifradas en un registro al que sólo tiene acceso el administrador del sistema, de esa manera al introducir el usuario su contraseña, el sistema la cifra y la compara con el registro correspondiente. (MORANT et al., 1994)

El «nombre de enlace», o nombre de usuario, es un medio de individualización utilizado para una determinada actividad de la persona, en este caso, el uso autorizado de un recurso informático; y como tal, constituye un seudónimo. “El seudónimo no es un atributo de la persona (...) deviene importante en lo que concierne a la individualización de la persona.” (FERNANDEZ. 2004: 126). El seudónimo, cuando como en este caso adquiere la importancia del nombre, goza de la misma protección jurídica dispensada al nombre según dispone el artículo 32° del Código Civil sobre la protección jurídica del seudónimo.

Las contraseñas son los medios utilizados para verificar la identidad de un usuario con el fin de darle acceso a un sistema de información, están basadas en un secreto que sólo él conoce. La norma técnica recomienda en el ítem 9.2.3 controlar la asignación de contraseñas por medio de un proceso de gestión formal que requiera al usuario asumir el compromiso de mantener en secreto su contraseña (compromiso que podría incluirse en los términos y condiciones del contrato de trabajo); y que proporcione al usuario una contraseña inicial me-

diante un conducto seguro y el acuse de recibo correspondiente, contraseña que forzosamente el usuario deberá cambiar inmediatamente después de acceder al sistema.

El objetivo del control de acceso al sistema opera tivo es evitar entradas no autorizadas a las computadoras de la organización o empresa. La norma técnica considera un buen sistema de gestión de contraseñas aquél que impone el uso de contraseñas individuales de calidad con el fin de establecer responsabilidades y, que a su vez, permite a los usuarios resolver sus propias contraseñas mediante un procedimiento de confirmación para evitar errores al introducirlas, les impone su cambio periódico e impide su reutilización, que no muestra las contraseñas en pantalla y que almacena las contraseñas en forma cifrada mediante un algoritmo, separadas de los datos del sistema de aplicaciones.

En informática se denominan «aplicaciones» a los programas o conjunto de software que tienen la función específica de permitirle al usuario realizar cosas útiles con las computadoras y demás recursos informáticos. Entre los tipos más populares de programas de aplicación se pueden identificar los siguientes: procesadores de texto, de diseño, de edición, de cálculo, de manejo de base de datos, de comunicación de datos, de multimedia y de presentación. El control de acceso a las aplicaciones además de evitar la entrada no autorizada a la información contenida en los sistemas, comprueba los derechos de acceso como por ejemplo lectura, escritura, borrado y ejecución.

El seguimiento de usos del sistema operativo tiene como objetivo: detectar actividades no autorizadas mediante el registro de eventos observables que proporcionen evidencias para detectar desviaciones de la política de control de accesos y comprobar la efectividad de los controles instalados. La norma técnica recomienda que el registro en que se funda ese seguimiento se mantenga durante un período adecuado que permita futuras investigaciones, y el seguimiento del control de los accesos. Estos registros de seguimiento o auditoría, denominados por la norma técnica «registro de incidencias» (ítem 9.7.1), deben anotar: el nombre de usuario, la fecha y hora de conexión y desconexión, la identificación del terminal, y el registro de los intentos de acceso aceptados y rechazados al sistema, a los datos y a otros recursos.

Son necesarios procedimientos de seguimiento o supervisión del uso de losrecursos informáticos para asegurar que los usuarios únicamente realizan procesos para los que han sido autorizados de forma expresa. Según la norma técnica, la frecuencia de supervisión sobre el resultado de las actividades de seguimiento debería depender de los siguientes riesgos: la criticidad de los procesos de aplicación (por ejemplo, la copia de seguridad); el valor, sensi-

bilidad o criticidad de la información implicada; la experiencia sobre infiltración y mal uso del sistema: y la extensión de las interconexiones del sistemacon redes públicas.

Los registros de incidencias del sistema contienen gran cantidad de información en su mayor parte ajena al seguimiento de la seguridad; la norma técnica recomienda la copia automática, a un segundo registro, sólo de los tipos de mensajes apropiados o emplear las herramientas de auditoría que faciliten la identificación de aquellos eventos significativos para la seguridad.

La gestión de incidencias en materia de seguridad de la información requiere establecer responsabilidades y procedimientos con el objeto de conseguir respuestas rápidas, eficientes y ordenadas. La norma técnica recomienda recoger y asegurar debidamente las pistas de auditoria y evidencias como prueba de posible incumplimiento de obligaciones contractuales, requisitos reglamentarios o disposiciones legales en que se estuviera incurriendo, por ejemplo, el mal uso de los recursos informáticos.

La revisión de los registros implica la comprensión de las amenazas al sistema de información y la forma en que éstas se presentan: la norma técnica recomienda que cuando se designen a los responsables de ésta, se debería realizar una segregación de funciones entre quienes se ocupen de las actividades de control y seguimiento y quienes asuman las de supervisión.

La correcta sincronización de los relojes de los procesadores de las computadoras y demás recursos informáticos es una práctica esencial que recoge la norma técnica, con el fin de establecer la exactitud de los registros de auditoria que podrían necesitarse para la investigación de incidencias o como prueba en casos legales o disciplinarios.

Los requisitos fundamentales de seguridad permiten evaluar los sistemas operativos comprobando si las funciones de seguridad están presentes y si trabajan correctamente. Los requisitos son: la existencia de una política de seguridad explícita y bien definida implantada en el sistema, el etiquetado de objetos para el control de accesos. la identificación de los usuarios y la contabilidad de datos relevantes a efecto de realizar auditoria y rastrear las acciones que afecten a la seguridad.

El objeto de la existencia de una política de seguridad de la información es reconocer a todos los sujetos y objetos en el sistema, para determinar que usuarios pueden acceder a que objetos. El propósito del etiquetado es aplicar a los objetos de información un conjunto de reglas para el control de accesos no discrecional u obligatorio. La identificación de los usualios hace posible que cada intento de acceso a la información sea controlado, comprobando

quién pretende el acceso solicitado. La contabilidad mantiene un sistema fiable de registro de todos los acontecimientos relevantes, a efectos de seguridad, en un registro de auditoría.

Para demostrar que el sistema operativo cumple los requisitos fundamentales de manera adecuada, éste debe contener mecanismos de hardware y software que puedan ser evaluados independientemente *y* que estén continuamente protegidos contra ataques y alteraciones no autorizadas. "Ningún sistem se puede considerar seguro si sus mecanismos de seguridad son susceptibles de ser destruidos o modificados". (MORANT et al., 1994: 278)

4.4.3. El control de acceso a la red y sus comunicaciones

Desde la perspectiva informática la definición de una red es: un entorno computacional con más de un procesador autónomo, independientemente del tamaño y distancia entre los distintos sistemas de cómputo, en ella sólo importa la independencia y su interconexión; cada sistema se denomina nodo y su procesador anfitrión (del inglés *host).* La interconexión vía redes de informaciónpresenta una serie de ventajas como el hecho de compartir recursos. pero, al mismo tiempo, plantean más problemas de seguridad, como que:

> "(...) hay que suponer un mayor número de usuarios, que cada usuario accede a la red a través de nodos diferentes y, presumiblemente, con controles de acceso diferentes y con la posibilidad de que el control de acceso realizado por un sistema no sea suficientemente bueno para otro. Es más, (...) no sólo hay que autenticar a los usuarios, sino también a los nodos. (...) debido a su facilidad de expansión, es necesario tener en cuenta la inseguridad que proporciona la incorporación de nuevos usuarios. pues en una red existen muchos más puntos de ataque y más posibilidades de llevarlos a cabo". (MORANT et al.. 1994: 340)

Con el propósito de proteger los servicios de red, la norma técnica recomienda el control de los accesos de los usuarios a los servicios de información de las redes internas y externas con mecanismos adecuados de autenticación para los usuarios y los equipos; ello supone formular una política de uso coherente con la política de control de accesos de la organización o empresa, que cubra las redes y los servicios de la red a los que se puede acceder, los procedimienlos de autorización, y los controles y procedimientos de gestión para proteger el acceso a las conexiones.

Las conexiones externas de una red son una fuente potencial de accesos no autorizados, por tanto es necesario que las organizaciones o empresas incorporen a sus sistemas controles que filtren el tráfico entre redes por medio de reglas que restrinjan las capacidades de

conexión de los usuarios, sobre todo aquellas conexiones por las que fluye información fuera de sus fronteras. Estos controles de conexión pueden establecerse mediante una ruta forzosa (del inglés *gateway)* y el control activo de las comunicaciones de origen a destino por medio de cortafuegos (del inglés *firewall).* Las restricciones que se impongan podrían ser, por ejemplo, sobre el uso del correo electrónico, sobre la transferencia de archivos en una o en ambas direcciones, o sobre el acceso interactivo. (MORANT et al., 1994 .)

Los métodos más comunes de comunicación en una red de información pueden ser agrupados en:

- mensajes uno a uno, por ejemplo el correo electrónico (del inglés *e-mail*). En Internet éstos no están dirigidos a través de un punto de control central tomando variadas rutas hacia sus destinatarios en las que pueden ser interceptados y leídos si no son cifrados;

- mensajes de uno a varios, utilizados para la suscripción a discusiones abiertas e intercambios en lemas particulares corno las listas de servicios (del inglés *listserv)* o distribuidos por bases de datos como es el caso de los grupos de noticias de usuarios de Internet (del inglés *usenet newsgroups*);

- comunicación en tiempo real, que permite a los individuos vincularse en un diálogo inmediato con otras personas. En Internet lo que es análogo a la llamada en teleconferencia como la denominada charla en línea (del inglés *lnternet relay chat*);

- uso remoto de computadoras en línea (del inglés *telnet*);

- recuperación de infonnación a distancia para listar y transferir archivos disponibles en una computadora remota hacia la computadora local, como con el uso del protocolo de transferencia de archivos conocido por las siglas «FTP» (del inglés *file transfer protocol*) , el acceso a la información a través de menús (del inglés *gopher*) y la navegación Web que utiliza un lenguaje de formato denominado hipertexto (del inglés *hypertext markup language*), que permite organizar, localizar y recuperar eficazmente información relacionada aun cuando se encuentre en distintas computadoras alrededor del mundo (del inglés *World Wide Web).* (PARDINI, 2002)

La gestión de la seguridad de las comunicaciones tiene entre sus objetivos evitar la pérdida, modificación o mal uso de la información y software intercambiados entre organizaciones.

El uso del correo electrónico ha reemplazado a las formas tradicionales de comunicación empresarial y la gestión de su seguridad debe tomar en cuenta sus características particulares como la velocidad, la estructura del mensaje, el grado de formalización y la vulnerabilidada las acciones no autorizadas. La norma técnica en el ítem 8.7.4.1 recomienda considerar la necesidad de controles y medidas para reducir la vulnerabilidad de los mensajes a la interceptación , modificación o denegación del servicio; por consideraciones legales, como la posi ble necesidad de constituir prueba de origen, despacho, entrega y aceptación; por las implicaciones de la publicación del directorio de usuarios; y para el control del acceso de usuarios remotos (fuera de la red) a las cuentas del correo electrónico.

Además, considera que deben establecerse reglas claras sobre: cuando usar o no el correo electrónico; la responsabilidad del trabajador cuyo mal uso compromete a la empresas si, por ejemplo, realiza difamaciones, hostigamiento o compras no autorizadas con ayuda del correo electrónico; la retención de los mensajes que podrían requerirse en caso de litigio, si se almacenaran; y controles y medidas adicionales para examinar los mensajes no autenticados. (ítem 8.7.4.2)

4.5. La responsabilidad de los usuarios y las condiciones de la relación laboral

La seguridad de la información es una responsabiildad organizativa, la asignación de funciones y responsabilidades sobre activos físicos y de información se guía por la política correspondiente; sin embargo, la responsabilidad de proporcionar recursos e implantar las medidas de control recae en los directivos de la organización. La norma técnica recomienda la práctica de designar un miembro de la gerencia como responsable de todas las actividades relacionadas con la seguridad de la información y un propietario para cada activo de información como responsable de su seguridad.

La norma técnica considera «buena práctica» (ítem 4.1.4) la autorización previa al uso de computadoras personales en el puesto de trabajo para el tratamiento de la información de la organización, así como a los controles necesarios; siendo ésta última especialmente importante en un entorno de red. Además, la organización o empresa debería requerir un acuerdo de confidencialidad o no-divulgación a los trabajadores usuarios de aplicaciones de tratamiento de información. como parte de los términos y condiciones contractuales, para notificar qué inforrnación es secreta o confidencial.

Los términos y condiciones del contrato de trabajo deben incluir expresamente la responsabilidad por la clasificación y gestión de los datos del empleador; las responsabilidades y obligaciones el gales respecto a las leyes de propiedad intelectual o de protección de datos; y, cuando proceda, por ejemplo en el caso del trabajo en casa o teletrabajo, que dichas responsabilidades se extiendan fuera del ámbito de la organización y de las horas normales de trabajo.

Los trabajadores usuarios de los recursos informáticos deben recibir capacitación en las políticasy pro cedimie n tos de la organización, los requisi tos de seguridad, las responsabilidades legales, así como práctica en el uso correcto de los mismos antes de obtener acceso a la información o los servicios. Un procedimiento disciplinario formal debería asegurar un trato adecuado y justo a trabajadores sospechosos de cometer violaciones serias o continuadas de las políticas y procedimientos de seguridad.

4.6. Los riesgos por el uso indebido de los recursos informáticos.

La doctrina ha reconocidocomo contingencias de daño ocasionadas por el uso indebido de recursos informáticos en el puesto de trabajo, principalmente a:

- El absentismo o pérdida de tiempo en el desempeño de funciones y deberes en especial por el acceso a la Internet o el uso del correo electrónico para fines personales del trabajador.

- La utilización de los recursos informáticos por parte de los trabajadores para la comisión de delitos o faltas. así como para la conculcación de los derechos de la propiedad intelectual o de la protección de datos personales que puedan derivar en responsabilidad para el empleador en razón de la culpa «in vigilando».

- La fuga de información, el espionaje industrial, la inutilización de los sistemas de información, la invasión de virus informáticos y en general, los diversos riesgos sobre la seguridad de la información de las organizaciones.

Tomando en consideración los riesgos que afectan de esa manera los negocios de los empleadores, estos últimos tienen razones suficientes como para justificar el control informático que ejercen sobre los trabajadores que utilizan los recursos que les son proporcionados para el desempeño de sus funciones. En consecuencia. dicho control se ejerce con los objetivos siguientes:

- Controlar la productividad de lostrabajadores.

- Maximizar el uso productivo de los sistemas de cómputo por parte de los trabajado-
- Controlar el cumplimiento, por parte de los trabajadores, de las políticas establecidas por el empleador para el uso de las computadoras, el sistema de correo electrónico y el acceso a Internet.
- Llevar a cabo la investigación de quejas en contra de los trabajadores por la comisión de faltas.
- Prevenir y detectar el espionaje industrial que se realice a través del robo de secretos comerciales e información de propiedad de la organización, las infracciones contra los derechos de autor y las patentes o marcas comerciales ya sea por parte de los trabajadores o de terceros.
- Evitar accesos no autorizados a los sistemas de información.
- Proteger las redes de información contra la sobresaturación provocada por la descarga de archivos de gran extensión.
- Prevenir y detectar el uso no autorizado de los sistemas de cómputo para actividades ilegales.
- Sustentar la defensa contra demandas judiciales o quejas administrativas planteadas por trabajadores con relación a actos de discriminación. acoso, sanciones o despido.
- Obtener pruebas para enfrentar litigios con relación a evidencia de carácter electrónico.

Para minimizar los riesgos asociados con el uso de los servicios de correo electrónico y el acceso a Internet proveído por el empleador, éstos deben implementar una política escrita que disua da las expectativas de intimidad por parte de los trabajadores y que les establezca las reglas a seguir, especificamente aquellas conductas prohibidas, como por ejemplo la amenaza, intimidación o acoso a los demás trabajadores; el uso de lenguaje obsceno, peyorativo o soez: la creación, exhibición o transmisión de imágenes ofensivas o despectivas y el envío de material confidencial fuera de la red de la organización o a personal no autorizado para su conocimiento.

Por último, una vez implementada la política, es recomendable llevar a cabo sesiones de capacitación a los trabajadores para la toma de conciencia de las reglas y de los riesgos que

comportan el uso inapropiado de los recursos informáticos; y que el incumplimiento de las primeras conduce a la aplicación de sanciones incluyendo el despido.

4.7. El control informático

Los trabajadores que utilizan Internet en sus puestos de trabajo para propósitos personales, mantienen expectativa de intimidad en su uso; sin embargo, la recolección de información de carácter íntimo que a través del control informático practican los empleadores hace posiblea estos últimos elaborar perfiles virtuales de los trabajadores, lo que comúnmente va más allá de las necesidades legitimas de control.

El control informático comprende tres conceptos: primero, la revisión y evaluación del desempeño de los trabajadores: segundo, la observación de las acciones de los trabajadores mientras no están ejecutando tareas propiamente laborales, por ejemplo, cuando se lleva a cabo una investigación sobre dichos actos, y tercero; en la aplicación de las técnicas conocidas como «computación forense» hechas para la recuperación y reconstrucción de datos luego de su supresión, ocultamiento o intento de destrucción; por ejemplo, en los casos en los que el empleador utilice software especializado para recobrar mensajes de correo con relación a una investigación de una presunta apropiación ilegal de secretos industriales, mediante el rescate y reconstrucción de los mensajes enviados por trabajadores sospechosos a personas fuera de la organización.

Existen diversas maneras como los empleadores utilizan la tecnología de la información para controlar las labores concernientes al trabajo; por ejemplo, sobre el uso de los teclados de las computadoras podrán emplear aplicaciones para registrar el número de golpes de tecla Por minuto, el tiempo exacto y lugar de los errores, la cantidad de tiempo que toma culminar cada tarea y la duración de las pausas. Igualmente sobre el uso del servicio telefónico, programando a las computadoras para que contabilicen el número de llamadas, el retomo de llamadas, mensajes, mensajes no respondidos, tiempo transcurrido antes de la respuesta a una llamada, el número de oportunidades en que una llamada es puesta en espera, la extensión exacta de cada llamada y el período de tiempo entre cada llamada. También los empleadores pueden controlar el número de proyectos y rev isiones para cada documento electrónico elaborado por el trabajador.

Asimismo, dicha tecnología amplía la capacidad de control del empleador sobre el uso de las redes de computadoras e Internet en el mismo contexto. Determinadas aplicaciones informáticas permiten capturar imágenes de la pantalla del computador o las activdidades en línea de los trabajadores, incluyendo las páginas Web visitadas y el tiempo de cada visita. El

uso de los «salones de charla» en línea, los programas ejecutados, el tiempo empleado en juegos en linea, los archivos usados, los *bytes* transferidos o descargados y los mensajes de correo enviados y recibidos. Adicionalmente, pueden llevar a cabo el control sobre los discos duros para detectar archivos que contengan pornografía, música o videos que contravengan las normas sobre derechos de autor o las políticas de la organización.

4.7.1. La legitimidad del control informático

La finalidad del control informático que ejerce el empleador es evitar, por parte de los trabajadores, el uso negligente de los recursos, la pérdida de tiempo y el mantenimiento de la seguridad de la información.

Se justifica el control informático, principalmente a una necesaria política de seguridad de la información; tal es su importancia que ésta en ocasiones se impone como una obligación legal o reglamentaria. De ahí que el empleador debe comprobar si el trabajador cumple o no sus deberes laborales, mantiene su productividad con relación al trabajo convenido y utiliza eficazmente los recursos destinados a ello. Asimismo, debe velar por la custodia de los secretos profesionales y generar las pruebas que lo protejan frente a posibles responsabilidades derivadasde los actos de sus trabajadores.

La racionalidad para establecer medidas de control informático se sustenta en: establecer límites para una conducta apropiada de los trabajadores; disuadir expectativas de intimidad del trabajador en el uso de los recursos, y obtener el consentimiento informado del mismo.

Una clara política de seguridad de la información ayuda a reducir la vulnerabilidad de los em pleadores a acciones judiciales o administrativas incoadas por los trabajadores incluyendo la violación a su derecho a la intimidad. Los empleadores deberán establecer una política de seguridad de la información que describa los usos permitidos y prohibidos de Internet y correo electrónico, la cual deberá incluir declaraciones en las que claramente se establezca que los mensajes de correo electrónico y el tráfico hacia Internet proveídos por los sistemas de información de la organización, no son propiedad privada de los trabajadores y que el empleador tiene el de recho de controlarlos.

Son asuntos que deberán incluirse como declaraciones de la política de seguridad de la información:

- Que los sistemas de acceso a Internet y correo electrónico deben ser usados de manera consistente con las demás políticas de la organización, como por ejemplo, aquellas que prohíben el acoso u hostigamiento a otros trabajadores.

- Que el sistema de información es para uso exclusivo de los negocios de la organización y el uso personal está prohibido, o que aquél es principalmente usado para el negocio y que un uso personal limitado es permitido. siempre que no sea excesivo y que no interfiera con las necesidades del negocio y sus operaciones.

- Que los recursos informáticos para el acceso a Internet y el correo electrónico son de propiedad de la organización, y que los códigos de paso a Internet y los mensajes de correo electrónico elaborados, enviados y recibidos, asi como sus adjuntos, son también propiedad de la organización. Por lo tanto, los trabajadores no podrán considerar la información del sistema como privada, incluyendo los mensajes de correo electrónico, el contenido adjunto y los sitios Web visitados.

- Que los mensajes recibidos y enviados, así como sus adjuntos, podrán ser controlados y supervisados por el empleador en el curso ordinario de su negocio, a discreción de éste y en cualquier momento, con o sin aviso; asimismo, que el empleador tiene la capacidad, y se reserva el derecho, de seguir y controlar el acceso a Internet por parte del trabajador, incluyendo los sitios visitados en la Web y los archivos descargados.

- Que los sistemas de acceso a Internet y de correo electrónico no podrán ser usados para crear mensajes ofensivos o intimidatorios, considerándose como ofensivos aquellos que contengan implicancias sexuales, calumnias raciales o étnicas u otros comentarios dirigidos a ofender en razón de la edad, sexo, orie ntación sexual, religión, origen nacional, ancestral o incapacidad. Además, el sistema no deberá ser usado para comunicar otros mensajes impropios, como por ejemplo, mensajes o material difamatorio, obsceno o inapropiado. Tampoco deberán ser usados para la comisión de delitos incluyendo,pero no limitado a, el envío de mensajes obscenos con la intención de enfadar, abusar, amenazar o acosar a otra persona, ni deberán enviar o reenviar mensajes en cadena o vinculados a «correo no deseado» (del inglés *spam*). Asimismo, que los trabajadores no deberán visitar sitios en la Web con contenido explícitamente sexual, ofensivo o cualquier otro inapropiado, o vincular a la computadora a juegos o actividades de ocio.

- Que el sistema de información no será usado para incumplir leyes, reglamentos o políticas de la organización; así como para enviar o recibir materiales protegidos por derechos de autor, secretos comerciales, información financiera reservada o similares, sin la autorización previa de los directivos de la organización.

- Que los trabajadores no deben utilizar et sistema para solicitar negocios personales o compromisos no relacionados con el trabajo, o asislir a otros en ello.

- Que los trabajadores no accederán al sistema de información, en particular al servicio de correo electrónico, utilizando la identidad de otros trabajadores, sin la previa autorización de los directivos de la organización.

- Que el simple borrado de un mensaje o archivo no lo elimina del sistema.

- Que ningún ex trabajador podrá tener acceso o uso del sistema, sin la autorización correspondiente.

- Que los trabajadores que requieran asistencia para la comprensión de la política de seguridad de la información o que descubran una violación de la misma, deberán notificarlo a quien designe el empleador; y que el incumplimiento de dicha política traerá como consecuencia una acción disciplinaría que irá gradualmente desde una amonestación o suspensión de los privilegios en el sistema, hasta el despido.

Los límites al control informático son una necesidad impuesta por la seguridad jurídica que busca sustentarlo en un ejercicio legítimo. La existencia de un conflicto de derechos fundamentales no es tal, si no son las conductas que íntentan ampararse en una conjetura de derecho las que el juez debe despejar en cada caso concreto, luego de examinar los hechos y comprobar si éstos se ajustan al derecho que se invoca. Los derechos fundamentales se relacionan entre si de manera coordinada, no subordinada; por tanto ni la capacidad de control es incondicional ni los derechos del trabajador son ilimttados; ambos se encuentran sujetos al principio de la buena fe contractual. El respeto a los derechos fundamentales sólo puede ser racionalmente exigido en la medida en que se ejerzan conforme a una convivencia que garantice los derechos de los demás y la paz social.

La facultad de control sobre el correo electrónico proporcionado al trabajador deberá limitarse a comprobar si se utiliza para el fin al que se destinó, en todo caso debe mantenerse la privacidad de los mensajes, sin que un acceso indiscriminado por parte del empleador sea aceptable. El hecho de ser una herramienta de trabajo no obsta a que su interceptación, sin la debida justificación, pueda considerarse lesiva para los derechos fundamentales del tra-

bajador. En el caso del correo electrónico particular del trabajador al cual pueda acceder a través de la red del empleador, es evidente que cualquier intromisión en el mismo supone una vulneración de sus derechos fundamentales; lo que no obsta para que se establezca la prohibición o restricción de su uso durante la jornada laboral.

Para llevar a cabo el control sobre el uso del correo electrónico, el empleador debe demostrar que éste interfiere en el trabajo, ya que el secreto de las comunicaciones protege contra la interceptación o el conocimiento antijurídico, sólo mediante resolución judicial puede levantarse este; por tanto puede constituir un delito contra la intimidad si no cuenta con el consentimiento inequívoco del trabajador; o se fundamente en las necesidades de seguridad siempre que se limite al principio de la proporcionalidad.

El principio de proporcionalidad es respetado cuando la medida restrictiva es susceptible de conseguir el objetivo propuesto (idónea): si además no existe ninguna otra medida más moderada para la obtención eficaz del propósito (necesaria); y si resulta ser más beneficiosa que perjudicial para el interés general (ponderada o equilibrada).

La justificación de las medidas de control debe ser exteriorizada con el fin que los trabajadores conozcan las razones por las cuales renuncian a sus derechos. También se justifican aquellas medidas, con el consentimiento del limite que se impone el mismo trabajador, como titular del derecho. La tutela efectiva de la intimidad puede, en determinados casos, ser limitada por condicionamientos que imponen los valores culturales del momento y por el propio concepto de cada persona, por lo que si ésta descuida su derecho o conciente la injerencia, no se hará merecedor de la correspondiente tutela jurídica.

La libertad de empresa de la que goza el empleador, es sólo libertad de actuar en un ámbito definido legalmente. Por otro lado, la libertad de información también tiene un contenido preciso vinculado con asuntos de interés general y que, por tanto, contribuyen a la formación de la opinión pública.

En conclusión, no corresponde que el empleador tenga un acceso indefinido y flagrante sobre el uso de los recursos informáticos por parte del trabajador, ya que no puede desconocer que las relaciones laborales deben regirse por los principios de buena fe; es por lo tanto indispensable, que éste cuente con una política adecuada de control que favorezca un ambiente laboral distendido y confiado. que proporcione autonomía e intimidad a sus trabajadores.

4.7.2. Los principios del control informático

En el Perú no existen leyes ni regulaciones sobre el control informático que ejercen los empleadores, sin embargo, debido a la similitud con la ordenamiento jurídico europeo que reconoce la preeminencia de los derechos fundamentales del trabajador, así como por constituir la Directiva 95/46/CE de la Unión Europea *«Data Privacy Directive»* antecedente del proyecto de ley de datos personales, se deben tornar en consideración las directrices elaboradas por el grupo de trabajo creado por el artículo 29 de la Directiva en mención. Dicho grupo de trabajo, a finales del 2001, con relación al procesamiento de información personal en el contexto de la relación laboral. ("2001 *Working Opinion"*), reconoce que el empleador posee legítimo interés para controlar el funcionamiento de sus negocios y defenderse contra acciones ilegítimas de los trabajadores que puedan exponer lo a responsabilidad en caso de daños, y la disponibilidad que éste tiene de diversas formas de supervisión; sin embargo, se concentra en las dos más comunes: el control sobre el correo electrónico de los trabajadores y uso de Internet. Con respecto al control informático de los trabajadores el grupo concluye que la recolección, uso o almacenamiento de información sobre los trabajadores mediante medios informáticos forma parte del ámbito de la legislación sobre protección de datos personales. Este es también el caso del control del empleador sobre el uso de los trabajadores del correo electrónico y el acceso a Internet. El control sobre el correo electrónico se incluye necesariamente en el procesamiento de datos personales.

Antes que el empleador proceda a realizar una actividad de control debe considerar que ésta sea legal y justificada, para lo cual debe cumplirse con siete principios fundamentales de protección de datos personales: necesidad, finalidad, transparencia, legitimidad, proporcionalidad, concisión de datos y seguridad.

El principio de necesidad requiere que el control sea absolutamente indispensable para los propósitos del empleador, por ejemplo, en circunstancias en las que el trabajador resulta sospechoso de haber cometido un acto criminal o ilícito por el cual el empleador pueda estar vinculado y ser responsabilizado, entonces resulta necesario llevar a cabo un control sobre el uso del correo electrónico, o en el caso del control de virus informáticos con el tln de garantizar la seguridad del sistema.

El principio de finalidad demanda la recolección de información para un propósito específico, explicito y legitimo. por ejemplo, si el control se justifica en la seguridad del sistema. no pudiendo el empleador usarlo para realizar un seguimiento a la conducta de un trabajador en particular.

El principio de transparencia significa que el empleador deba ser sincero y leal sobre sus actividades de control, las que deben ser claramente expuestas al conocimiento de todos los trabajadores sujetos al mismo, así como las razones por las cuales se lleva a cabo.

La legitimidad se sustenta en el cumplimiento de las obligaciones legales del empleador, en las obligaciones necesarias para la ejecución del contrato de trabajo o en el consentimiento inequívoco del trabajador, en el entendido que dicho consentimiento esté confinado a los casos en los que el trabajador pueda tomar un decisión genuinamente libre; esto significa, que sea capaz de negar su consentimiento sin sufrir perjuicio alguno. El interés legitimo del empleador legitima el control, excepto cuando dicho interés es aventajado por los derechos fundamentales del trabajador; es bajo esta previsión que el empleador encuentra sustento para controlar que sus trabajadores cumplan con las políticas de la organización, por ejemplo, para prevenir el acoso a otros trabajadores, o la protección contra el robo de secretos comerciales.

El principio de proporcionalidad prescribe que los datos personales sean adecuados, relevantes y no excesivos con relación a los propósitos de la recolección y posterior procesamiento. La política de control del empleador debe ceñirse a las clases y grado de riesgo que éste enfrenta, lo que significa que un control automático y continuo sobre el uso del correo electrónico y el acceso a Internet no debe ser permitido. El control sobre el uso del correo electrónico debe constreñirse al tráfico de datos y al tamaño y tipo de los archivos adjuntos, sin inmiscuirse en el contenido de los mensajes enviados o recibidos.

La concisión de datos hace referencia a que el registro de éstos deba ser preciso, actual y conservado el tiempo necesario para el legítimo control del empleador. Respecto a esto último, el grupo de trabajo europeo recomienda como plazo de referencia para la retención de datos no más allá de tres meses.

Por último, el principio de seguridad requiere al empleador implementar en su sistema de información las medidas técnicas que salvaguarden los datos personales de los trabajadores. En ese sentido, por ejemplo. el empleador debe proteger éstos contra el ataque de virus informáticos mediante el uso de exploradores automáticos del correo electrónico y del tráfico en las redes de información.

4.7.3. Elementos para la implementación de políticas de control informático

Nunca como ahora resulta imperativoque los empleadores implementenuna política de control informático, especialmente con relación al uso del correo electrónico y el acceso a Internet, con el propósito de reducir la posibilidad de hacerse responsables por las demandas de abuso sobre los derechos a la intimidad de sus trabajadores.

Esas políticas serán particularizadas en función a las necesidades del negocio de cada empleador, pero en todo caso, deberán ser aplicadas a todos los trabajadores y deberán incluirse en los manualesoperativos.

En todo caso, los siguientes elementos deberán ser considerados en éstas:

1. Poner en conocimiento de los trabajadores que los sistemas de correo electrónico y acceso a Internet son principalmente para la ejecución de tareas propias del negocio y que la organización se reserva el derechode controlar o supervisar la información enviada desde el sistema o almacenada en los dispositivosde éste. Adicionalmente a la comunicación de la política mediante su incorporación en el reglamento interno, manual operativo u otros medios escritos, una notificación debe ser programada en el sistema mediante un mensaje que aparezca en la panlalla de la computadora de los trabajadores cada vez que éstos accedan al sistemade información.

2. Especificar que los sistemas no deben ser usados con propósitos inapropiados como. por ejemplo, para el envío o recopilación de información insultante, difarnante u obscena.

3. Expresar con claridad que el uso de contraseñas privadas por parte de los trabajadores no limita al empleador en su capacidad de controlar el sistema de información.

4. Advertir expresamente que el simple borrado de un mensaje o un archivo no elimina por completo a éstos del sistema.

5. Debe incluir una forma escrita en la cual los trabajadores dejen constancia de aceptación mediante su firma, que han leído la politica de la organización y reconocen el derecho del empleador a controlar la información del sistema: lo cual también deberá ser ratificado al momento en el que el trabajador acceda al sis-

tema, con el fin de prevenir reclamos que argumenten su desconocimiento de la política.

6. Dejar en claro que el incumplimiento de la política por parte del trabajador acarrea acciones disciplinarias, inclusive el despido, si la gravedad lo amerita.

7. El control informático estará limitado a situaciones que hacen necesaria la protección de los intereses propios del negocio del empleador; cuidandoque los métodos de control sean lo menos entrometidos y evitando en lo posible la inmiscuirse en la intimidad de los trabajadores.

8. Limitar la revelación de la informacióncontenida en el sistema a aquella que sea legítimamente necesario conocer.

Además, los empleadores, dependiendo del tipo de negocio, sus objetivos y la cultura de la organización, deberán tomar en consideración incluir algunas de las siguientes previsiones:

- Tratar al correo electrónico de los trabajadores de manera consistente con la política de retención de documentos de la organización.

- Establecer la confidencialidad de las contraseñas de los trabajadores, haciendo a éstos responsables por toda actividad realizada en el sistema de la organizaciónbajo su contraseña.

- Cuidar que los trabajadores con acceso a Internet entiendan y cumplan las leyes sobre derechos de autor, marcas comerciales, libelos, difamaciones y discursos públicos de los países en los cuales la organización mantiene presencia.

- Incluir las advertencias y salvaguardas apropiadas o utilizar cifrado para el envío, vía Internet, de información confidencial o privilegiada.

- Utilizar exclusivamente los métodos de cifrado aprobados por la organización y tan sólo por los trabajadores autorizados a ello.

- Cuidar que los trabajadores dejen bien en claro cuando no estén representando a la organización en sus comunicaciones via Internet o correo electrónico;

- Dejar sentado claramente si los trabajadores pueden o no comunicarse mediante aplicaciones de charla o salones de charla en línea (del inglés *chat* y *chatrooms*), o mediante pizarras de boletines (del inglés *bulletin boards)* teniendo acceso a Internet a través de la red de la organización.

- Permitir sólo previa autorización, la descarga de archivos de programas desde las redes.

- Cuidar que los trabajadores no abran mensajes de correo electrónico o archivos adjuntos a menos que confíen en la identidad del remitente.

Adicionalmente, la política de la organización sobre el acceso a Internet y el uso del correo electrónico deberá ser distribuida a todos los trabajadores in volucrados y se deberá recavar su firma en un documento de consentimiento que ellos deberán recibir y leer, expresando que no tienen expectativas de intimidad al acceder a Internet y usar el correo electrónico, y que comprenden que el empleador podrá ejercer control sobre ellos. Como ya se anotó anteriormente, es recomendable programar en los sistemas la aparición de mensajes emergentes al ingresar a los servicios de Internet y correo electrónico en los que se declare que la conexión o uso del sistema constituye un consentimiento expreso de la política de seguridad del empleador, incluyendo el control.

Desafortunadamente por lo común. los empleadores se encuentran a si mismos en medio de un problema serio o una investigación interna sin haber adoptado previamente una política de acceso a Internet o uso del correo electrónico; por ello deben evitar estar en la posición de no contar con una política o contar con una política ambigua que no les permita definir si pueden o podrán examinar el tráfico vía Internet o mensajes de correo electrónico durante una investigación sobre acoso o fraude, por ejemplo. Para evitar esas situaciones, las organizaciones deben ser proactivas en el desarrollo de sus políticas sobre el uso y control de la Internet y el correo electrónico, anticipándosea estos posibles dilemas. La ausencia de poiíticas, en ningún caso, elimina el deber del empleador de investigar el mal uso del correo electrónico e Internet por parte de los trabajadores.

Resulta evidente que el cumplimiento de determinadas prácticas incluidas en las políticas de la organización pueden presentar dilemas a enfrentar. Uno de los mayores asuntos se encuentra en el balance entre los controles apropiados y cuales de éstos pueden ser considerados medidas draconianas. Entre estas cuestiones requieren consideración:

- Si algunas medidas de control originarán en los trabajadores resentimientos o disminución en la confianza hacia el empleador.

- Si debe ser permitido el uso privado de los recursos informáticos en el trabajo, y si ello es posible, cuánto *y* cómo debe ser controlado

- Si la autorización para el uso privado crea un expectativa de intimidad en el trabajador y como debe ser est limitada.

- Qué prácticas deben ser autorizadas para el uso del sistema de la organización desde fuera del centro de trabajo, via acceso remoto, o fuera del horario de trabajo o de sitios o servicios de correo electrónico personales en la Web.

- Cómo debe ser evaluadala gravedad del incumplimiento de la política, que disciplina debe ser ejercida y en que instancias.

Las respuestas a estas preguntas deben ceñirse a las regulaciones internas y a la cultura particular de la organización. Por ejemplo, en ciertos centros de trabajo el uso privado del correo electrónico y la Internet es algo comúnmente aceptado, en aquellos los empleadores están convencidos que políticas que prohiban el uso privado disuaden la contratación de personal o causan desafecto entre los trabajadores.

CONCLUSIONES

El fenómeno denominado «sociedad informacional», cuyo origen es la reestructuración capitalista llevada a cabo a partir de la década de los años 80 del siglo pasado, tiene su correlato en el ámbito jurídico en el denominado «derecho informático». La expansión del fenómeno descrito supone considerar que el conocimiento tiene una función central en todos los ámbi tos actuales del desarrollo humano y en especial en la economía. La aplicación del conocimiento que se materializa a través de la presencia de sistemas y redes de información globales, es la causa del cambio de gran parte de los aspectos de la vida y la producción. En especial, la red Internet, es la base tecnológica para la comunicación en la era actual.

La internacionalización de la producción, resultado de dicha reestructuración del capitalismo, ha hecho no solo posible más mercados para la venta de bienes y servicios, sino también el flujo de bienes para la producción en función a proyectos empresariales realizados por redes de información. La reforma en la organización corporativa que aquellos proyectos impulsan, ha sido caracterizada por el modelo descrito como la «empresa-red» cuya mayor competitividad es resultado de la participación de sus trabajadores, las alianzas estratégicas, los acuerdos de subcontratación y las decisiones descentralizadas; todo lo cual solo ha sido posible gracias al uso de computadoras personales conectadas en redes de comunicación digital.

Las empresas-red propias de esta nueva economía requieren de trabajadores en red que operen y utilicen Internet. con capacidad intelectual para transformar la mayor información disponible en conocimientos. La aplicación de las tecnologias de la información en la empresa demanda trabajadores mejor informados y con mayor libertad. Sin embargo, la propiedad de las redes de información, como hase del poder cedido a los sujetos privados y el control del acceso a la Internet a través de mecanismos de vigilancia, constituyen una amenaza a la libertad de los trabajadores; el desafio que esa realidad impone es evitar un control carente de protección a la intimidad. La concurrencia del ámbito privado del trabajador y el espacio organízacional de la empresa, que el uso de las nuevas tecnologías de la información hace posible, suscita abusos de ambos lados.

La eficacia de la protección de los derechos fundamentales en las relaciones privadas se sustenta en aceptar que el ejercicio del poder por los sujetos privados resulta tan amenazador a éstos como el que ejerce el Estado, lo que hace que la igualdad entre las partes y la autonomía de la voluntad sean relativas. Tal como sostiene la teoría alemana denominada *«Drittwirkung der Grundrechte»,* considero que los derechos fundamentales son principios objetivos del ordenamiento jurídico, por tanto su vigencia estaría restringida sino se aceptara

su capacidad de producir efectos de forma directa y necesaria, sin necesidad de intervención de los poderes públicos, entre los sujetos privados; sobre todo frente a los derechos de la persona y en especial al derecho a la intimidad. La dignidad de la persona es la síntesis de los derechos personales y debe ser respetada y protegida, así como los derechos que le son inherentes, en todas las relaciones sociales y, en concreto, en el ámbito de las relaciones laborales.

De ahí que los derechos fundamentales también sean límites al poder que ejercen los grupos económicos. En efecto, las ideas de límite y de actuación delimitada se aplican a los poderes que ejercen las empresas, y en consecuencia, los derechos fundamentales de los ciudadanos trabajadores tienen el carácter irrenunciable de los derechos laborales en razón del sujeto y de la relación jurídica en que se hacen valer, y constituyen la manifestación más importante de un nuevo modelo de relación que preconiza la calidad de vida y la realización personal del trabajador.

La intimidad es el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que las personas mantienen en reserva. La autodeterminación es la interpretación jurídica del control sobre la intimidad y es un elemento constitutivo y definitorio de ésta. La «autodeterminación informativa» o «libertad informática» es el control sobre el uso de datos informáticos relacionados con la intimidad de las personas, constituye la libertad para decidir a quien darle acceso, impone el respeto de los demás y el no ser obligado a develarlos salvo por causa debidamente justificada. Esta posición ecléctica combina los conceptos objetivo y subjetivo del derecho a la intimidad que incluyen la defensa y el control sobre lo que al individuo le afecta. La regulación del derecho a la intimidad dispone cuando develar ésta en casos de necesidad, autorización o bienestar común.

Considero a la intimidad y el derecho a ésta desde un punto de vista participativo, por el cual ambos hacen posible la libre participación del individuo en lo público o social, ya que actuar libremente en privado condiciona la libre actuación en público. La «autodeterminación informativa» es presupuesto para la existencia y mantenimiento del Estado democrático en términos coincidentes con el carácter participativo del derecho a la intimidad. Cuando el derecho a la intimidad entra en conflicto con otros derechos constitucionales, los límites de protección han de ser estrictamente excepcionales y proporcionales.

La comunicación, como ejercicio de la convivencia, socializa lo más intimo del individuo, por tanto, el derecho a la intimidad actúa como un derecho subsidiario y suplementario del derecho al secreto de las comunicaciones. El derecho al secreto de las comunicaciones se aplica a las telecomunicaciones por «canal cerrado» en tanto que el secreto es inherente a éstas;

sobre las comunicaciones por «canal abierto» se renuncia al secreto, pero si su contenido corresponde a la intimidad de las personas, éstas estarán cubiertas de manera supletoria por el derecho a la intimidad, por lo que no se renuncia al control de su distribución posterior bajo la noción de autodeterminación. Corresponde a los jueces ponderar los intereses y determinar si prevalece el derecho al secreto de las comunicaciones. En concreto, con relación a este derecho, la jurisprudencia del Tribunal Constitucional ha fijado como precedente que el empleador no podrá abrir, incautar, interceptar o intervenir las comunicaciones ni los documentos privados del trabaíador sino por mandamiento motivado por el juez y con las garantías previstas en la ley.

El poder del empleador se compone del mando, el control y la supervisión, y se caracteriza por ser unilateral, discrecional, funcional, delegable y limitado. Este poder se fundamenta en el estado de subordinación propio de la naturaleza del contrato de trabajo y en el derecho de direcció n del empleador sobre la producción y los fines de la empresa. En los Estados democráticos los limites del poder del empleador se rigen por los principios de racionalidad, buena fe contractual y los derechos fundamentales del trabajador. El ejercicio de ese poder debe proteger contra su propia actividad, respetando los derechos fundamentales como límites de su actuación, en eso consiste la paradoja de la protección.

El cumplimiento de las «buenas prácticas» de seguridad de la información contenidas en la norma técnica peruana ISO/IEC 17799:2004 «Código de buenas prácticas para la gestión de la seguridad de la información» constituye el límite de razonabilidad que exige el ordenamiento jurídico, específicamente la ley de fomento al empleo, para el ejercicio legitimo del poder del empleador en el ejercicio de mecanismos de control y supervisión sobre el uso de los recursos informáticos proporcionados a sus trabajadores.

La gestión empresarial requiere un alto grado de especialización técnica y profesional y las empresas, como detentadoras de poder, deben legitimar su ejercicio a través de criterios de responsabilidad social. La autorregulación está en relación directa con el ejercicio del derecho a la libertad de empresa *y* se identifica con un ordenamiento jurídico privado derivado de sus estatutos; mediante ésta se controlan los riesgos tecnológicos a partir de reglamentos internos, manuales de buenas prácticas, protocolos de actuación o sistemas de control y gestión de riesgos. Uno de los fundamentos para el ejercicio de la autorregulación se da por la concentración del poder que da el uso de la informática a la sociedad, especialmente por la amenaza a la intimidad de las personas. La necesidad de proteger los derechos fundamentales concurre con las actuales exigencias de desregulación por parte de los Estados; la autorregulación es la fórmula para proteger la identidad y la dignidad de las personas. La autorregulación, como contrapeso de la desregulación, complementa o sustituye las regla-

mentaciones y controles públicos por los privados; supera la deficiencia de la legislación en la materia y establece una correspondencia entre los responsables de la amenaza y las medidas para la protección de la intimidadcomo bien juridico.

La estrategia de regulación de la autorregulación por la que el poder público atribuye responsabilidad directa de la gestión de riesgos a los sujetos privados que los originan, traslada dicha responsabilidad a los organismos de normalización y a las entidades de certificación. circunscribiendo la función del Estado a comprobar el correcto funcionamiento del «sistema de autorregulación». El objeto de la normalización es la estandarización jurídica de una conducta que se formaliza en reglamentos técnicos obligatorios o normas técnicas voluntarias, a través de organismos públicos o privados de normalización. El objeto de la certificación es la verificación y documentación del cumplimiento de la normalización. La función de los sujetos privados expertos en tecnologías, quienes no están legitimados para tomar decisiones que afecten a la sociedad, obliga a recurrir a la prevención y a la precaución como principios de responsabilidad social que comparten el Estado y la sociedad.

Las normas técnicas facilitan la relación entre el subsistema profesional y el subsistema jurídico: el consenso en que éstas se basan da el carácter vinculante y las aproxima a un acuerdo jurídico. A través de las remisiones legales a las normas técnicas. estos instrumentos se han incorporado al derecho público. El Estado atribuye fines públicos a la autorregulación utilizando a ésta como una regulación indirecta con el objeto de supeditar a los sujetos privados a los principios constitucionales, y la complementa con la acreditación de los organismosde normalización; esta «autorregulación regulada» garantiza la capacidad técnica y el sometimiento de los sujetos autorregulados con el objeto de minimizar los riesgos que éstos generan. El control y gestión de riesgos es uno de los principales ámbitos de la autorregulación y se manifiesta en la abundante aparición de normas técnicas de seguridad.

La regulación otorga confianza a la autorregulación cuando le atribuye a ésta efectos probatorios en los procedimientos administrativos y judiciales, considerándola indicio relevante para resolver litigios sobre responsabilidad. Los efectos probatorios adquieren un especial significado cuando las normas jurídicas incorporan las «buenas prácticas», en cuyo caso los instrumentos de autorregulación actúan como un «dictamen pericial anticipado». Es posible considerar como prueba pericial a los certificados técnicos que acreditan el cumplimiento de normas técnicas. La finalidad de la autorregulación como prueba pericial agrega un efecto presuntivo al dar a entender un juicio de validez, de ese modo la norma técnica, formalmente voluntaria, se convierte de hecho en una referencia ineludible.

Los efectos probatorios del cumplimiento de las «buenas prácticas» en materia de seguridad de la información acreditado en un certificado, en especial las establecidas por la norma técnica peruana ISO/IEC 17799:2004, constituye un indicio, una presunción, o un dictamen pericial anticipado en todo proceso en el que exista controversia sobre la diligencia del empleador con relación a su respon sabilidad en el ejercicio de control y supervisión de los recursos informáticos puestos a disposición de sus trabajadores, con el efecto de invalidar una acusación de negligencia.

La remisión a los resultados de la autorregulación desde una norma jurídica implica la plena integración de las normas técnicas en el ordenamiento jurídico, constituyendo un fenómeno novedoso. Los efectos vinculantes de la técnica de la remisión se están extendiendo a los «códigos de buenas prácticas» en materia de seguridad. La obligatoriedad de los instrumentos de autorregulación se consigue también mediante la inclusión en los estatutos o normas privadas que regulan la actividad de las organizaciones.

El cumplimiento de las «buenas prácticasl» de seguridad de la información comprendidas en la norma técnica peruana ISO/IEC 17799:2004 es obligatorio para los organismos y empresas que forman parte del «sistema nacional de informática» del sector público nacional, en virtud de la remisión objetiva hecha por la Resolución Ministerial 224-2004-PCM.

El cumplimiento de las «buenas prácticas» de seguridad de la información integradas a la Circular G-105-2002 de la Superintendenc ia de Banca, Seguros y AFP, referida a los riesgos de tecnología de información, emitida dentro del marco del «Reglamento para la administración de los riesgos de operación»; es obligatorio para las empresas financieras, bancarias, complementarias y otras del sector financiero, así como las empresas de seguros, derramas, cajas de beneficios y similares que se encuentren bajo la supervisión de dicha Superintendencia.

La información como bien de utilidad social y valor económico se considera como un bien jurídico merecedor de protección. Por su contenido y por su forma mensurable en términos de valor de mercado, la información deviene en una mercancía. El aumento de los riesgos a su seguridad por la aplicación de las nuevas tecnologías hace necesario establecer políticas de seguridad para preservar su confidencialidad, integridad y disponibilidad. Con relación a las redes de información, los sistemas informáticos proporcionan características de autenticidad, que permiten asegurar el origen y el destino de la información y, el no-repudio, que permite que el usuario que envía o recibe información no pueda alegar válidamente que no la envió o recibió. La clasificación y control de la información permite establecer la responsabilidad de los usuarios sobre ésta y su protección adecuada.

La comisión de delitos a través de computadoras es uno de los principales riesgos que induce a las empresas a la protección contra el mal uso de recursos informáticos, de ahí que sea esencial que los usuarios de dichos equipos conozcan et alcance del acceso permitido a través de autorizaciones documentadas en las que se informe a los trabajadores sobre lo que se considera uso inapropiado o fines no autorizados o ajenos al negocio, así como la acción disciplinaria correspondiente. Los requisitos de seguridad determinan la selección e implantación de controles entre los que la norma técnica peruana ISO/IEC 17799:2004 destaca, la documentación de la política de seguridad.

La norma técnica peruana ISO/IEC 17799:2004 considera necesaria la autorización previa al uso de computadoras en el puesto de trabajo, así como la capacitación de los trabajadores en las políticas y procedimientos de la organización, los requisitos de seguridad, las responsabilidades legales y el uso correcto de los recursos informáticos. Igualmente, un procedimiento disciplinario formal que asegure un trato adecuado y justo a trabajadores sospechosos de violaciones serias y continuas de las políticas y procedimientos de seguridad. Según la misma norma, el control de accesos a la información es requisito indispensable de seguridad y para ello es necesario la utilización de un identificador único para cada usuario con el fin de vincularlo y hacerlo responsable de sus acciones. El «nombre de usuario» es un medio de individualización de la persona para el uso autorizado de un recurso informático que jurídicamente constituye un seudónimo y goza de la misma protección dispensada al nombre. El uso de contraseñas para el acceso a un sistema de información verifica la identidad del usuario con base a un secreto que sólo éste conoce. Un buen sistema de gestión de contraseñas impone su uso con el fin de establecer responsabilidades.

El derecho a la identidad personal es un derecho fundamental y constituye un valor propio de la existencia humana; se le reconoce como la manera de ser de la persona en el ámbito social. Consiste también en la determinación de la persona de afirmar su propia individualidad. Los signos distintivos de la persona son la faz estática de la identidad personal y equivalen a la idea de la identificación, en cambio el aspecto dinámico de ésta es su proyección social que se nutre de las conductas asumidas en el transcurso de la vida. La protección de la identidad personal cautela que no se atribuyan intenciones o conductas que pretendan menguar o realzar la personalidad del sujeto, más allá de lo que corresponde a la verdad. El derecho a la identidad personal del trabajador con relación al uso de los recursos informáticos merece una consideración especial por la potencialidad de daño que puede ocasionar, específicamente por el uso de la Internet.

El establecimiento de una documentada política de control de accesos a los sistemas operativos de las computadoras y las redes de información de los empleadores, considerada co-

mo «buena práctica» por la norma técnica peruana ISO/IEC 17799:2004, constituye la forma de certificar la protección al derecho a la identidad personal de los trabajadores que utilizan dichos recursos informáticos.

Los requisitos fundamen tales de la seguridad de la información contenidos en la norma técnica peruana son: una política de seguridad documentada, la clasificación de activos de información para el control de accesos, la identificación de los usuarios y la auditoría de las acciones que afecten la seguridad.

El control que ejercen los empleadores en el Perú sobre el uso de los recursos informáticos que proporcionan para el desempeño de actividades laborales, debe respetar los derechos fundamentales, en especial el derecho a la identidad personal, el derecho a la intimidad personal y familiar y el derecho al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. El derecho informático, cuyo objeto normativo es la correcta aplicación de las tecnologías de la información, constituye el correspondiente jurídico llamado a cautelar que dicho uso se ejerza con racionalidad y con respeto por los derechos fundamentales del trabajador.

El sustento filosófico-jurídico del derecho al «consentimiento informado» es el aporte del existencialismo que redescubre la libertad como el ser del hombre; la libertad le otorga la dignidad que sustenta a este derecho. A partir del respeto a la dignidad del ser humano el «consentimiento informado» es aceptado como una nueva institución jurídica.

El derecho a la intimidad es el principio del «consentimiento in formado». Es deber del empleador, como proveedor de recursos informáticos, poner a disposición del trabajador la información suficiente para obtener su asentimiento para que este último ejerza libremente la preservación de su intimidad. El «consentimiento informado» contiene dos elementos principales: el conocimiento del control y la voluntariedad del trabajador de someterse al mismo

El derecho al «consentimiento informado» del trabajador satisface el principio de la buena fe contractual como límite al poder del empleador y, por tanto, constituye requisito indispensable para la ejecución de mecanismos de control y supervisión que éste ejerce sobre el archivo de documentos privados o el envio y recepción de comunicaciones de la misma índole en el ámbito de los sistemas operativos, aplicaciones y redes que conforman el sistema de información de la organización. El «consentimiento informado» no sirve solamente como un medio de protección de los derechos fundamentales del trabajador, sino que permite que éste tenga conciencia sobre el alcance de sus responsabilidades y riesgos.

Son razones suficientes para justificar el control informático que ejercen los empleadores sobre el uso de recursos informáticos en el puesto de trabajo, el absentismo o pérdida de tiempo, la comisión de delitos o faltas, la conculcación de los derechos de la propiedad intelectual o de protección de datos personales que puedan derivar en responsabilidad para el empleador y la fuga de información, el espionaje industrial, la inutilización de los sistemas de información y, en general, los riesgos sobre la seguridad de la información. El control informático comprende, por tanto, la revisión y evaluación del desempeño de los trabajadores, la investigación de sus acciones y la «computación forense». La racionalidad para establecer medidas de control informático busca establecer límites para una conducta apropiada de los trabajadores, disuadir sus expectativas de intimidad en el uso de los recursos informáticos y obtener su «consentimiento informado». En ese sentido, los empleadores deben establecer una política de seguridad de la información que describa los usos permitidos y prohibidos de Internet y el correo electrónico.

Los límites al control informático tienen el propósito de sustentar un ejercicio legítimo del mismo. Para llevar a cabo el control sobre el uso del correo electrónico, el empleador debe demostrar que éste interfiere en el trabajo; el derecho al secreto de las comunicaciones y documentos privados protege contra el conocimiento antíjuridico de su contenido, sólo mediante resolución judicial o el consentimiento inequívoco del trabajador, puede levantarse dicho secreto.

BIBLIOGRAFÍA

ABAD Yupanqui, Samuel, "Límites y respeto al contenido esencial de los derechos fundamentales: estudio preliminar", en: Themis -- No. 21 (1992) pp. 7-15

ASIS ROIG, Rafael de, Las paradojas de los derechos fundamentales como límites al poder, Madrid: Dykinson, 2000, 118 p.

BATLLORI BAS, Martí. Acerca del control del correo electrónico en la empresa. Febrero 2001. [En línea] <www.juridicas.com/areas_virtual/Artículos/40-Derecho%20Laboral/200102-05512911015390.html> [16JUL2005]

CASTELLS, Manuel, La era de la información: economía sociedad y cultura. 2ª ed. Madrid: Alianza Editorial, 2000 v 1. La sociedad red 645 p.

– La galaxia Internet, Barcelona: Random House Mondadori, 2001, 363 p.

CAMPUZANO TOMÉ, Herminia, Vida privada y datos personales: su protección juridica frente a la sociedad de la información, Madrid: Tecnos, 2000. 179 p.

DARNACULLETA I GARDELLA, María Merce, Autorregulación y derecho público: la autorregulación regulada, Madrid: Marcial Pons, 2005, 490 p.

DICHTER Mark S.,Michael S. BURKHARDT. *Electronic interaction in the workplace: Monitoring, retrieving and storing employee communications in the Internet age. June,* 1999. [En línea] < www.morganlewis.com/PDFs/ASC845ED-S75B -4ADC-8A47F2801DG3594C_PUBLICATION.PDF> [17FEB2005]

ESPINOSA-SALDAÑA Barrera, Eloy, "El debido proceso sustantivo: su desarrollo en el derecho comparado y su evolución en el Perú", en: Revista jurídica del Perú -- No. 55 (Mar.-abr. 2004) p.p 57-77

ESTEVE PARDO. José, Autorregulación: génesis *y* efec tos, Navarra: Aranzadi, 2002, 183p.

FALGUERA I BARÓ, Miquel Ángel, Uso por el trabajador del correo electrónico de la empresa para fines extraproductivos y competencias de control del empleador, [En línea], < http://www.comfia.net/historico/documento/estudio/falguera_ce.pdf>. Barcelona, 2000, 36 p.

FERNÁNDEZ SESSAREGO, Carlos, "Fundamento filosófico-jurídico del «consentimiento in formado»", en: Revista Jurídica del Perú. Lima, enero-febrero 2005. Nº 60, pp. 217-236.

– Derecho de las personas: exposición *de* motivos y comen tarios al libro primero del Código civil peruano, 9° ed., Lima: Grijley, 2004, 478 p.

– "El derecho a la identidad personal", en: Revista de Derecho y Ciencia Política. Lima, 1987-89. Vol. 47, pp. 13 - 57.

– "Daño a la identidad personal", en: Themis. Lima, noviembre 1997, Nº 36, pp. 245-272

FROSINI, Vittorio, Informática y Derecho. Bogotá: Temis S.A., 1988, 179 p.

GALINDO, Fernando. Derecho e informática, Madrid: La Ley-Actualidad, 1998, 635 p.

GARCIA TORRES, Jesús, Derechos fundamentales y relaciones entre particulares: la *Drittwirkung* en la jurisprudencia del Tribunal Constitucional, Madrid: Civitas, 1986, 149 p.

GONZÁLEZ GAITANO, Norberto, El deber de respeto a la intimidad: Información pública y relación social, Pamplona: Universidad de Na varra S. A., 1990, 199 p.

HERNÁNDEZ RUEDA. Lupo, "Poder de dirección del empleador", en: Instituciones de Derecho del Trabajo y de la Seguridad social, [En línea], Instituto de Investigaciones Jurídicas UNAM, México, Serie G, Estudios Doctrinales, Núm. 188, 1997 pp. 405-419 <http://www.bibliojuridica.org/libros/1/139/26.pdf> [13ABR2005]

HERRERA BRAVO. Rodolfo, "La legitimidad del control tecnológico del empleador sobre el trabajador". en: Revista Electrónica de Derecho Informático - Número 35 (Junio de 2001)

HERRERA V., E. Liliana, "El nuevo sistema peruano de normalización", en: Calidad y excelencia -- Año 2, no. 8, pp. 50-51.

INEI (Perú), IV Encuesta nacional de recursos informáticos y tecnológicos en las entidades de la administración pública, Lima, octubre de 2002.

— Indicadores de tecnotogías de información y comunicación en las empresas. Lima, noviembre de 2001, 74 p.

KENNEDY, Charles, Waller STELLA. *"Big Brother Employer May Be Watching: Monitoring Employees' On Line Communications in The Workplace",* en: *Employment law Commentary,* vol. 15 n. 5 *May* 2003 [En línea] < http://www.mofo.com/news/updates/bulletins/bulletin1009.html#01> [17FEB2005]

KROTOSCHIN, Ernesto, "Aspectos de fa protección de los derechos de la persona del trabajador en la empresa moderna", en: La Ley: Revista Jurídica Argentina. Buenos Aires, 1972. Nº 147 pp. 1018- 1025.

LASPROGATA Gail, et. al..« *Regulation of Electronic Employee Monitoring: Identifying Fundamental, Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada"*, en: 2004 *Stanford Technology Law Review* 4 [En línea] <http://stlr.stanford.edu/STLR/Articles/04_STLR_4> [29ENE2005]

LIZAMA, Luis, "Nuevas tecnologías, pero antiguos problemas. El respeto a la intimidad de los trabajadores", en: Revisla Jurídica del Perú, Lima, enero 2002. Nº 30, pp. 137-143.

LLOYD, lan J., *Infomation technology law, Third ed. London: Buttterworth,* 2000, 634 p.

LUCAS MURILLO DE LA CUEVA, Pablo, El derecho a la aulodeterminación informativa: la protección de los datos personales frente al uso de la informática, Madrid: Tecnos, 1990, 207 p.

MÉJAN, Luis Manuel C., El derecho a la intimidad y la informática, 2ª ed. México D. F.: Porrúa, 1996, 146 p.

MORALES GODO, Juan, Derecho a la intimidad (estudio comparado con el *right of privacy* del derecho norteamericano) Lima: Palestra, 2002, 177 p.

MORANT RAMÓN, José Luis, Seguridad y protección de la información / Arturo Ribagorda Garnacho, Justo Sancho Rodríguez. Madrid: Centro de Estudios Ramón Areces, 1994, 388 p.

NUÑEZ PAZ, Sandro Alberto, "¡Alerta: tienes un e-mail! La facultad fiscalizadora y la inviolabilidad de las comunicaciones", en: Revista Actualidad Laboral, octubre 2004, pp. 20-30.

NÚÑEZ PONCE, Julio, Derecho Informático: nueva disciplina jurídica para una sociedad moderna, Manuel R. Sotórzano Martinez, Trujillo - Perú, 1996, 366 p.

P ALACIOS, Rosa María. "La normalización en el Perú", en: Calidad y excelencia -- Año 1, no. 1 (Abr.-may. 1994), pp. 35-37.

PARDINI, Aníbal A., Derecho de Internet. Buenos Aires: La Rocca. 2002, 381 p.

PEÑA, Tatiana, "Seguridad de la información", en: Calidad & Excelencia. Lima, 2004. N° 40, pp. 34-39.

PETROVICH, Aleksandar, "Derecho al consentimientoinformado",en: Revista del Foro. Lima, agosto 1997. Nº 4, pp, 29-35.

PÉREZ LUÑO, Antonio-Enrique,"Dilemas de la protección a la intimidad", en: lus et praxis -- No. 21-22 (Ene.-dic. 1993), pp. 11 -38.

— Manual de informática y derecho, Barcelona: Ariel, 1996, 222 p.

PESO NAVARRO. Emilio del, "La seguridad de la información en la Ley de protección de datos de carácter personal", en: Universidad Pontificia Comillas, Madrid Conferencia: Encuentros sobre Informática y Derecho (13: 1999-2000: Madrid) Navarra: Aranzadi, 2000 p,p 41-58.

PINTOS CLAPÉS, Ignacio. El control de los medios informáticos en el ámbito de la empresa. {En Linea}
<http://www.microsoft.com/spain/empresasiasesoira/20040218_control_medios_empresa.mspx> [16JUL2005].

PLA RODRÍGUEZ, Américo, "El derecho laboral y la protección de la intimidad def trabajado", en Derecho laboral (Montevideo) T. XXIX Nº 144, 1986 pp. 525-611.

REAL ACADEMIA ESPAÑOLA, Diccionario de la lengua española, 22ª ed. [En línea] <http://www.rae.es/>

REBOLLO DELGADO, Lucrecio, El derecho fundamental a la intimidad, Madrid: Dykinson. 2000, 299 p.

RODRIGUEZ RUÍZ, Blanca, El secreto de las comunicaciones: tecnología e intimidad, Madrid: McGraw Hill, 1998, 185 p.

RUBIO CORREA, Marcial, La interpretación de la Constitución según el Tribunal Constitucional, Lima: PUCP. Fondo Editorial, 2005, 455 p.

— Estudio de la Constitución Política de 1993, Lima: PUCP. Fondo Editoñal, 1999 v.1, 554p.

SCHREIBER, Mark E. *Employee E-mail and Internet Risks: Policy Guidelines and Investigations,* 2000[En línea] < http://whitepapers.zdnet.co.uk/0,3902 5945,G0021650p-39000620q,00.htm> [12F EB2005]

TORRES ALVAREZ, Hemán, "El derecho a la intimidad del trabajador y la facultad de fiscalización del empleador en el uso del correo electrónico", en: Revista Actualidad Laboral, febrero 2003. pp, 47-53.

TOYAMA MIYAGUSUKU, Jorge, "Correo electrónico y falta grave laboral", en: Diálogo con la Jurisprudencia, Tomo 38, noviembre 2001 [CD-ROM].

VEGA MERE, Yuri, "Intimidad, identidad e informática. A propósito de la Constitución peruana de 1993", en : lus et Praxis , Lima, Universidad de Lima. Enero-diciembre 1996. N° 26, pp. 45-57.

VICENTE PACHÉS, Femando de, El derecho del trabajador al respeto de su intimidad, Madrid: Consejo Económico y Social, 1998, 383 pp.

VILLANUEVA MANSILLA, Eduardo, Senderos que se bifurcan: dilemas y retos de la sociedad de la información, Lima: PUCP. Fondo Editorial, 2005, 393 p.

Legislación y jurisprudencia

Decreto Legislativo 295, Código Civil [14NOV1984]

Decreto Legislativo 635, Código Penal [8ABR1991]

Decreto Supremo 039-91-TR, Reglamento interno de trabajo [30DIC1991]

Decreto Supremo 013-93 TCC, texto único ordenado de la Ley de Telecomunicaciones [28ABR93]

Constitución Política del Perú [30DIC1993]

Decreto Supremo 001-96-TR. Reglamento de Ley de Fomento al Empleo [24ENE1996]

Decreto Supremo 003-97-TR, texto único ordenado de la Decreto Legislativo 728, Ley de Productividad y Competitividad Laboral [21MAR1997]

Resolución 0072-2000/INDECOPI-CRT, Reglamento para la elaboración y aprobación de normas técnicas peruanas y reglamento de comités técnicos de normalización [29NOV2000]

Resolución Superintendencia de Banca y Seguros 006-2002, Reglamento para la administración de los riesgos de operación [4ENE2002]

Circular Superintendencia de Banca y Seguros G-105-2002, Riesgos de tecnología de información [22FEB2002]

Ley 28175, Ley marco del empleo público [20FE82004]

Resolución 0026-2004/CRT-INDECOPI, Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 1ª Edición" [27MAR2004]

Decreto Supremo 027-2004-MTC, texto único ordenado del Reglamento de Ley de Telecomunicaciones [9JUL2004]

Resolución Ministerial 224-2004-PCM, Uso obligatorio de la "NTP-ISO/IEC 17799:2004 en entidades del Sistema Nacional de Informática [23JUL2004]

Sentencia del Tribunal Constitucional, Expedien te 1058-2004-AA/TC, Rafael Francisco García Mendoza c/. SERPOST S.A. [18AGO2004.]