Universidad de Costa Rica

Facultad de Derecho

Tesis de Grado para optar por el Título de
Licenciado en Derecho

"LA PROTECCIÓN DE DATOS DEL TRABAJADOR FRENTE A LAS POSIBILIDADES DE CONTROL DEL EMPLEADOR"

Christopher Chaves Zúñiga

Carné 941019

Noviembre, 2009

DEDICATORIA

A mi padre, que me ayudó a llegar hasta aquí y me enseñó que puedo hacerlo hasta donde quiera. Tu fuerza está conmigo cada día. Gracias viejo!!

A mi madre, por su ejemplo de amor, de comprensión, de trabajo y de humildad.

A mis hermanos y mis sobrinos. Son la muestra de todo lo que nos han enseñado pa y ma, y lo importante que es estar juntos.

AGRADECIMIENTOS

A Dios, por la vida.

A todos mis compañeros de BDS. Especialmente a Marco, a Pepe y Alejo, por sus innumerables muestras de amistad, por permitirme ser parte de un sueño y transmitirme su pasión por lo que hacemos.

A Adri y a Sofi. Por su amistad incondicional, por ser mis ángeles y cuidar la casita cuando no estoy. Les toca a ustedes!!

A Boras, Boogie, Milforio, Tito y Negrulis. Es imposible tener mejor amigos!!

A vos, por tu luz.

INDICE GENERAL

INTRODUCCION……...1

TÍTULO PRIMERO:

LA TEORÍA DE PROTECCIÓN DE DATOS PERSONALES……7

CAPÍTULO I. LA PROTECCIÓN DE DATOS DEL TRABAJADOR…….7

A. DELIMITACIÓN DEL CONCEPTO DE PROTECCIÓN DE DATOS DESDE LA PERSPECTIVA LABORAL……..7

1. Definición.....7

    1.1. Los ficheros de datos……..12

2. ¿Cuáles datos se protegen?.....18

B. ALCANCES DE LA PROTECCIÓN DE DATOS……..23

1. Valores que cubre la protección de datos……....23

    1.1. El derecho a la intimidad del trabajador y el concepto de privacidad 23

    1.2. La autodeterminación informativa…….29

    1.3. El derecho al acceso de los datos personales…….30

2. ¿A quiénes protege la protección de datos? Perspectiva laboral……....31

CAPÍTULO II. LA REGULACIÓN DE LA PROTECCIÓN DE DATOS DEL TRABAJADOR. ANÁLISIS DESDE EL DERECHO COMPARADO……..33

A. DESARROLLO DEL CONCEPTO DE PROTECCIÓN DE DATOS DEL TRABAJADOR EN EL DERECHO INTERNACIONAL……...33

1. La experiencia en Europa……34
2. El desarrollo en Latinoamérica……32
   2.1. Argentina……36

B.LA PROTECCIÓN DE DATOS POR MEDIO DEL RECURSO DE HABEAS DATA……..……38

1. Evolución del Recurso de Habeas Data……...38
2. Avances en la tutela de la protección de datos en Costa Rica…….44
   2.1. El proyecto de Ley para la "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales"……...….51

TÍTULO SEGUNDO: LA PROTECCIÓN DE DATOS DEL TRABAJADOR DURANTE LA RELACION LABORAL ……63

CAPÍTULO I. LÍMITES AL MONITOREO DEL TRABAJADOR……...…63

A.GARANTÍAS PARA EL TRABAJADOR……..63

1. Límites que debe respetar el empleador……...63
   1.1. El consentimiento para el uso de datos personales……...64
   1.2. La pertinencia de los datos solicitados al trabajador……..67

2. Los derechos del trabajador frente a las frente a las posibilidades de recolección y uso de datos por parte del empleador……69

2.1. Algunos derechos del trabajador……69

2.2. Acciones legales del trabajador……..……71

2.2.1. El Recurso de Amparo……71

2.2.2. El reclamo en sede laboral……74

B.FORMAS MÁS COMUNES DE CONTROL DE DATOS DEL TRABAJADOR….81

1. Requisitos de validez para el monitoreo de trabajadores……82

1.1. Comunicación oportuna de los procedimientos……..82

1.2. Obligación de confidencialidad aplicada a la protección de datos sensibles……84

2. Algunos ejemplos del control de datos del trabajador……86

2.1. El control del correo electrónico……..89

2.2. El resguardo de la información médica……...102

CAPÍTULO II. LA LEGALIDAD DE LA PRUEBA OBTENIDA A PARTIR DE DATOS DEL TRABAJADOR……..106

A. OBLIGACIONES DEL EMPLEADOR DURANTE LA FASE DE RECLUTAMIENTO Y SELECCIÓN DE TRABAJADORES……..106

1. Los datos que puede exigir el empleador……....107

1.1. La protección de datos del candidato cuando se utilizan empresas de selección y reclutamiento……110

2. ¿Cómo se debe proteger la información?.....116

B. OBLIGACIONES DEL EMPLEADOR EN LA EJECUCIÓN DE LA RELACIÓN LABORAL. LEGALIDAD DE LA PRUEBA OBTENIDA……119

1. La intención de conservar datos del trabajador durante la relación laboral ……119
2. El uso de datos del trabajador como fundamento del poder disciplinario ……124
3. Efectos de la prueba ilícita……129

C. LA PROTECCIÓN DE DATOS DEL EX TRABAJADOR……..130

1. Vigencia de la Protección de Datos……130

CONCLUSIONES……..135

RECOMENDACIONES……140

BIBLIOGRAFIA……..143

FICHA BIBLIOGRAFICA

Chaves Zúñiga, Christopher (2009). **LA PROTECCION DE DATOS DEL TRABAJADOR FRENTE A LAS POSIBILIDADES DE CONTROL DEL EMPLEADOR**. Tesis de Graduación para optar por el grado de Licenciatura en Derecho. Sede Rodrigo Facio: Universidad de Costa Rica.

RESUMEN

Director: Marco Durante Calvo.

Lista de palabras clave: intimidad, privacidad, autodeterminación informativa, hábeas data, protección de datos, derechos del trabajador.

Resumen del trabajo

Objetivos Generales

A) Analizar el desarrollo de la Teoría de Protección de Datos con especial énfasis en el manejo de datos del trabajador, antes, durante y después de la relación laboral.

B) Analizar el alcance de la Protección de Datos y los derechos del trabajador relacionados con el manejo de su información personal.

C) Estudiar la legalidad de las pruebas obtenidas por el patrono a partir de datos del trabajador.

Objetivos Específicos:

A) Conocer la definición de la Protección de Datos y su aplicación a la tutela de los derechos del Trabajador.

B) Determinar los datos del trabajador que se deben proteger.

C) Estudiar los derechos constitucionales del trabajador relacionados con la protección de datos.

D) Establecer los sujetos amparados con la protección de datos del trabajador.

E) Analizar la experiencia en el derecho comparado.

F) Estudiar los mecanismos legales del trabajador para la protección de datos.

G) Analizar las formas visibles en las que se exige la protección de datos del trabajador durante la relación laboral, incluyendo los procesos de selección y reclutamiento, desarrollo y extinción del contrato de trabajo,

H) Establecer una determinación temporal de la protección de datos del trabajador que le corresponde proteger al patrono.

H) Determinar la validez de las pruebas obtenidas por el patrono, relacionadas con datos personales del trabajador, y su licitud para efectos disciplinarios

Hipótesis

Existen en nuestro país innumerables condiciones en las que se desarrollan los contratos de trabajo y que se debe en gran parte, a los avances de la tecnología que en algunos casos han facilitado al patrono las más diversas formas de ejercer el

poder de fiscalización que les corresponde y, en algunos casos, incluso, desde la intención de contratar a un empleado.

Estas formas de fiscalización, sumadas a una regulación legal que parte de normas constitucionales que establecen la protección de la dignidad y la intimidad del trabajador, pero que podría adolecer de normas particulares claras que regulen la protección de datos del trabajador –por poca aplicación o falta de actualización- hace que, en no pocos casos, los trabajadores resulten afectados con la violación de derechos, como los mencionados, pero, además, causen un perjuicio evidente y un daño a su imagen, propiciando desde su despido hasta la imposibilidad de conseguir un nuevo empleo.

Es aquí donde se considera que muchos patronos en nuestro país desconocen o simplemente manipulan, de forma mal intencionada, los datos del trabajador sin guardar las medidas de protección necesarias y, lo que es peor, tomando medidas disciplinarias basadas en pruebas cuya licitud puede ser gravemente cuestionada.

La intención de esta investigación será demostrar que no existe normativa suficiente que obligue de forma expresa a los empleadores a la protección de datos del trabajador, lo que representado una serie de injusticias y la imposibilidad del trabajador de reclamar el perjuicio sufrido sin ser sancionado o incluso, despedido.

Metodología

Para la presente investigación se utiliza el método Deductivo, el cual se basa en doctrina, jurisprudencia administrativa y judicial, para intentar obtener una visión lo más amplia posible de los temas de estudio.

Conclusiones

La necesidad de contar con una legislación que regule de forma clara la protección de datos del ciudadano ha sido un tema que algunas legislaciones han resuelto desde hace algún tiempo estableciendo incluso instituciones gubernamentales conocidas como Agencias para la Protección de Datos, que se encargan del registro y conservación de la información personal, que además fiscalizan y sancionan a los infractores en caso de incumplimiento.

En nuestro país, la garantía del respeto a la información personal se basa en las normas contenidas en nuestra Constitución Política, específicamente en los artículos 23 y 24, que establecen el derecho del ciudadano a que se respete su intimidad y su autodeterminación informativa. La violación a estos derechos implica la posibilidad del afectado de reclamar su reparación a través de la vía del recurso de amparo, específicamente mediante un recurso de hábeas data.

No obstante, a la fecha el país adolece de legislación expresa y específica que regule este tema, a pesar de los intentos que por alguna u otra razón han quedado en diferentes proyectos de ley que no pasaron de serlo. Desde la perspectiva laboral tampoco contamos con normas específicas que obliguen a los empleadores a conservar y utilizar de forma debida la información personal que obtienen de sus trabajadores precisamente con motivo de la relación laboral.

A partir del desarrollo de la Teoría de Protección de Datos y conceptos doctrinales como la privacidad y la autodeterminación informativa que implican la posibilidad del ciudadano de decidir el tipo de información que desea divulgar de sí y

principalmente el uso que se hará de ella, algunos países como España y Argentina han incluido obligaciones para los patronos que implican conservar la información bajo controles de seguridad mínimos y de acceso únicamente con fines laborales, salvo que el trabajador de forma expresa y voluntaria autorice el uso para otros fines.

En mi criterio, en Costa Rica esta falta de regulación incide para que la información del trabajador haya sido utilizada para fines más allá del trabajo, o incluso para la aplicación de sanciones al trabajador a partir de pruebas obtenidas de forma ilegal que podrían representar además una violación a derechos constitucionales del trabajador.

Los contratos de trabajo deben regirse por la buena fe que debe existir entre las partes. Este principio, sumado a la determinación del empleador de utilizar de forma correcta la información que el trabajador le confía, deberían regir en todas las fases de la relación laboral desde el momento de la contratación hasta la salida del trabajador por cualquier motivo.

A lo largo de este trabajo menciono algunos ejemplos a modo de recomendación, para que los patronos del país comprendan de forma clara que el trabajador merece el respeto de su información, lo que implica obligaciones de recopilación, uso y conservación que deban ser claramente conocidas por el personal, de forma que esta comunicación represente también la posibilidad del trabajador de rectificar o corregir los datos que se han desactualizado u obtenidos de forma ilegal.

Además, hago una particular mención al tema del manejo de la prueba utilizada por el empleador para la toma de decisiones relacionadas con la

evaluación del trabajador y la posibilidad de ser sancionado o incluso despedido a partir de información no autorizada u obtenida sin seguir las recomendaciones dadas en este trabajo de investigación.

A la fecha de finalización de este trabajo se discute en la Asamblea Legislativa el Proyecto de “Ley de Tratamiento de la persona frente a sus datos personales” que considero constituye un buen esfuerzo por empezar de una vez por todas a dar importancia al manejo de la información personal del ciudadano. Sin embargo, el proyecto de ley resulta para los efectos de mi propuesta, insuficiente, porque no establece reglas específicas para el tratamiento de los datos durante la relación laboral.

Termino esta labor reafirmando mi posición inicial: no sólo se trata que la ley establezca condiciones claras en esta materia; lo ideal es que la protección de datos del trabajador se convierta en un principio inherente a la cultura de los empleadores en nuestro país. Con este esfuerzo, espero haber contribuido a caminar por esa senda en beneficio del trabajador.

INTRODUCCIÓN

La protección de datos del ciudadano debe ser extensiva a la relación laboral, ya que muchas veces en el ejercicio de los contratos de trabajo, en cualquiera de sus manifestaciones, se producen las más evidentes violaciones a los derechos de los ciudadanos, relacionadas con la divulgación de su información más confidencial.

La comercialización de la información personal, en sus más amplias formas de manifestación, implica el deseo de obtener datos personales para casi cualquier interés, lo cual de alguna manera podría causar un perjuicio para el trabajador, pero en otros es probable, incluso, que la información sea tomada como referencia por agencias de empleo o analizada para efectos de promoción en una misma empresa, lo cual podría beneficiar al trabajador, aún cuando de forma previa no haya autorizado el uso de la información.

Ante esta situación, conviene hacer un análisis de las condiciones en nuestro país y analizar si la regulación legal actual y algunos otros esfuerzos de parte de algunos operadores del derecho han resultado suficientes para controlar el uso de la información personal, y si en la práctica se cumple con la garantía de proteger los derechos del ciudadano que el Sistema Legal Costarricense debe tutelar. Es aquí donde se plantean los cuestionamientos sobre cuáles deben ser los mecanismos legales para solicitar una reparación, en caso que el uso de información personal haya causado algún perjuicio para el trabajador.

Es cierto que todos estos temas han sido analizados ampliamente desde muchas perspectivas legales, principalmente, el derecho constitucional y el derecho

penal. Sin embargo, aquí se plantea la inquietud sobre cómo la necesidad de proteger los datos personales puede afectar la situación legal del trabajador y en qué medida los trabajadores, efectivamente, conocen sobre la tutela de sus derechos y las vías para exigir su cumplimiento.

El interés de esta investigación es concentrarse en las implicaciones laborales que el uso de la información personal pueda representar para el trabajador más allá del análisis que, de forma amplia y reiterada, se ha dado al tema desde la perspectiva del derecho constitucional y los criterios que han venido dando los Tribunales de Justicia Costarricenses, en particular, la Sala Constitucional de la Corte Suprema de Justicia.

Objetivos Generales:

Como objetivos generales de esta labor se investigación, me he planteado los siguientes tres puntos:

A) Analizar el desarrollo de la Teoría de Protección de Datos con especial énfasis en el manejo de datos del trabajador, antes, durante y después de la relación laboral.

B) Analizar el alcance de la Protección de Datos y los derechos del trabajador relacionados con el manejo de su información personal.

C) Estudiar la legalidad de las pruebas obtenidas por el patrono a partir de datos del trabajador.

Objetivos específicos:

Además de los mencionados como objetivos generales, pretendo desarrollar los siguientes objetivos específicos:

A) Conocer la definición de la Protección de Datos y su aplicación a la tutela de los derechos del Trabajador.

B) Determinar los datos del trabajador que se deben proteger.

C) Estudiar los derechos constitucionales del trabajador relacionados con la protección de datos.

D) Establecer los sujetos amparados con la protección de datos del trabajador.

E) Analizar la experiencia en el derecho comparado.

F) Estudiar los mecanismos legales del trabajador para la protección de datos.

G) Analizar las formas visibles en las que se exige la protección de datos del trabajador durante la relación laboral, incluyendo los procesos de selección y reclutamiento, desarrollo y extinción del contrato de trabajo,

H) Establecer una determinación temporal de la protección de datos del trabajador que le corresponde proteger al patrono.

I) Determinar la validez de las pruebas obtenidas por el patrono, relacionadas con datos personales del trabajador, y su licitud para efectos disciplinarios.

Hipótesis:

Existen en nuestro país innumerables condiciones en las que se desarrollan los contratos de trabajo y que se debe en gran parte, a los avances de la tecnología que en algunos casos han facilitado al patrono las más diversas formas de ejercer el poder de fiscalización que les corresponde y, en algunos casos, incluso, desde la intención de contratar a un empleado.

Estas formas de fiscalización, sumadas a una regulación legal que parte de normas constitucionales que establecen la protección de la dignidad y la intimidad del trabajador, pero que podría adolecer de normas particulares claras que regulen la protección de datos del trabajador –por poca aplicación o falta de actualización- hace que, en no pocos casos, los trabajadores resulten afectados con la violación de derechos, como los mencionados, pero, además, causen un perjuicio evidente y un daño a su imagen, propiciando desde su despido hasta la imposibilidad de conseguir un nuevo empleo.

Es aquí donde se considera que muchos patronos en nuestro país desconocen o simplemente manipulan, de forma mal intencionada, los datos del trabajador sin guardar las medidas de protección necesarias y, lo que es peor, tomando medidas disciplinarias basadas en pruebas cuya legalidad puede ser gravemente cuestionada.

La intención de esta investigación será demostrar que no existe normativa suficiente que obligue de forma expresa a los empleadores a la protección de datos del trabajador, lo que desafortunadamente se presta para abusos del uso de información

personal del personal de la empresa, debido a la imposibilidad del trabajador de reclamar el perjuicio sufrido sin ser sancionado o incluso, despedido.

Metodología:

Para la presente investigación se utiliza el método Deductivo, el cual se basa en el análisis de doctrina, jurisprudencia administrativa y judicial, según la experiencia costarricense y los avances de otras legislaciones internacionales en la protección de datos del trabajador. De esta forma se tendrá una visión lo más amplia posible de los temas de estudio.

Estructura:

El presente trabajo de investigación está compuesto de dos títulos principales. En el título primero denominado “la Teoría de Protección de Datos” se ofrece una delimitación del concepto de protección de datos a partir del derecho comparado y se analizan las formas más comunes mediante las que se recopila y se conserva la información del trabajador, así como los principales valores que deben respetarse, tales como la privacidad y la autodeterminación informativa del trabajador.

En el título segundo denominado “La protección de datos del trabajador durante la relación laboral”, se analizan las condiciones que debe cumplir el patrono en relación a la obtención, registro, uso y conservación de la información personal requerida en cualquier fase del contrato de trabajo, es decir, en la fase de selección y reclutamiento,

en el desarrollo de la relación laboral hasta su extinción, así como los medios legales del con que cuenta el trabajador para reclamar la reparación de los perjuicios sufridos en caso de violación de sus datos, según la actual legislación y los proyectos de ley que de esta materia se analizan en Costa Rica. Además, se hace un énfasis especial en la legalidad de la prueba utilizada por el patrono para la aplicación de medidas disciplinarias a partir de información personal del trabajador.

Al finalizar este proceso de investigación se espera llamar la atención sobre la necesidad de regulaciones más claras que obliguen a los empleadores de nuestro país a brindar un manejo adecuado de la información de sus trabajadores e incluso de las personas que alguna vez participaron de un proceso de selección y reclutamiento en la organización. Esto, sin duda, ofrecerá mayor seguridad jurídica al trabajador quien estará plenamente consciente de la información que puede brindar, e incluso, la que por disposición legal debe ofrecer.

TÍTULO PRIMERO: LA PROTECCIÓN DE DATOS DEL TRABAJADOR

CAPÍTULO I. LA TEORÍA DE LA PROTECCIÓN DE DATOS PERSONALES

A. DELIMITACIÓN DEL CONCEPTO DE PROTECCIÓN DE DATOS DESDE LA PERSPECTIVA LABORAL

1. Definición

La protección de datos es una iniciativa legal de algunos Estados, tendiente a la protección de información personal de los ciudadanos que conviven día a día en sus jurisdicciones y que abarca la protección en todos los ámbitos en los que se desarrollan las personas.

La necesidad de regulación del uso de dicha información surge precisamente del uso perjudicial que podría darse de esta información personal y que, en virtud de la tecnificación del archivo de la información, puede recopilarse a través de bases de datos que pueden ser autorizadas o no por los ciudadanos dueños de aquella información.

De esta forma, un régimen de protección de datos personales permite que los ciudadanos puedan ejercer "*un legítimo poder de disposición y control sobre los datos de carácter personal referidos a su persona que se encuentran registrados en bases de datos de titularidad de terceros*"[1].

[1] Tomado de www.protecciondedatos.com.ar; julio 2008

Sobre este tema, el Tribunal Constitucional Español señaló en una ocasión que la protección de datos persigue garantizar el poder de control sobre sus datos personales, su uso y destino; con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado [2].

A partir de lo dicho hasta ahora se piensa que esta regulación legal puede tener dos aristas principales:

- a) La responsabilidad de los sujetos obligados a resguardar el derecho relativo a la tutela de la confidencialidad de los datos personales que se encuentren en su poder y que puede corresponder a diferentes sujetos de derecho, pero que, para efectos de esta investigación, corresponde exclusivamente al empleador, es decir, a la persona física o jurídica que contrata los servicios personales de una persona física bajo la figura de una relación laboral en cualquiera de sus manifestaciones, e incluso, cuando la intención inicial del contrato es desnaturalizar una posible relación laboral, pero, en la práctica, subsisten los elementos necesarios para la determinación de una verdadera relación laboral.

- b) El ejercicio del titular de los datos personales, es decir, del trabajador para: acceder, actualizar, corregir, rectificar, suprimir o mantener la confidencialidad de dicha información. Este ejercicio debe incluir también la posibilidad de reclamar y ser resarcido por el abuso en el uso no autorizado de dicha información, la cual debe ser respaldada por mecanismos legales claramente

[2] Al respecto veáse lo dicho por el Tribunal Constitucional Español, Sentencia del 30/11/2000, Fundamento 6.

establecidos en la legislación ordinaria y de aplicación obligatoria por parte de los tribunales de justicia que correspondan.

Sobre la posibilidad que debe tener el ciudadano de actualizar su información, la Sala Constitucional de la Corte Suprema de Justicia se ha referido a ello cuando, en un reciente fallo, ordenó al Estado permitir a un docente la oportunidad de actualizar su información profesional. Señala, por tanto, la mencionada resolución:

> *Indica el recurrente que es profesional en Educación, tiene bachillerato en I y II Ciclos, Licenciatura en I y II Ciclos, Maestría en I y II Ciclos y una Maestría en Administración Educativa. En el último concurso del año 2007 fue reclutada como PT5 y desde ese año no ha vuelto a haber otro concurso, por lo que su currículum no ha podido ser actualizado, pese a su esfuerzo en el estudio para prepararse, y los títulos que posee no han sido válidos para efecto de nombramiento, dado que no ha vuelto a haber un reclutamiento a nivel de Servicio Civil y no tiene la misma oportunidad de ser nombrada en un puesto docente si la información sobre su persona estuviera actualizada. Manifiesta que en los años anteriores estuvo trabajando en la Escuela Los Parques, en el Circuito 03 de la Dirección Regional de Guápiles, en Limón, pero actualmente no tiene nombramiento porque el puesto que ocupaba como docente fue adquirido en propiedad por otro compañero. Se declara con lugar el recurso. Se ordena al Director General de Personal del Ministerio de Educación Pública, que gire las órdenes respectivas para que de forma inmediata se actualicen los datos de la recurrente, para efectos de ser considerada para futuros nombramientos como docente*[3]*.*

El desarrollo a nivel internacional de la Teoría de Protección de Datos produjo también la evolución del concepto del derecho a la vida privada, ya que se pasó de concebir la libertad negativa de rechazar u oponerse al uso de la información personal para convertirse en la libertad positiva de supervisar su uso, concepto muy próximo al denominado de autodeterminación informativa, y que más adelante se analiza.

[3] Voto número 4336 del año 2009. Sala Constitucional de la Corte Suprema de Justicia.

Ahora bien, todas las legislaciones que han adoptado en su normativa la protección de datos personal han previsto un organismo para el control y sanción. Por ejemplo, en Argentina existe la denominada "Dirección Nacional de Protección de Datos Personales" y en España la "Agencia Española de Protección de Datos Personales". Estas instituciones legales se encargan, entre otras cosas, de revisar los casos que puedan presentarse en cualquier ámbito del ser humano, incluidas las relaciones de trabajo cuyas resoluciones que atañen a este estudio serán analizadas conforme el esquema de trabajo propuesto.

En cuanto a la aplicación de las corrientes de protección de datos personales al campo estrictamente laboral se menciona que el mes de octubre de 1996, la Organización Internacional de Trabajo celebró en Ginebra una reunión de expertos con el fin de analizar la protección de la vida privada de los trabajadores. En dicha conferencia "*se debatió fundamentalmente la necesidad de equilibrar el derecho de los trabajadores a proteger la vida privada con la exigencia de los empleadores de obtener información sobre ellos. El resultado fue un Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores, que no tienen carácter obligatorio y que no suple a la legislación nacional ni a las normas* internacionales"[4]*.*

En general, las recomendaciones de la Organización del Trabajo expresadas en la recomendación número OIT/96/29 del 07 de octubre de 1996, relacionadas con la

[4] Cuervo, Jose. La intimidad informática del trabajador. Artículo tomado de http://www.informatica-juridica.com., junio 2008.

recopilación y protección de datos del trabajador, señalan que son tres los casos en los que se puede compilar información de un trabajador:

a) Para determinar si el trabajador puede ocupar un puesto de trabajo específico.

b) Para cumplir con los requisitos en materia de salud y seguridad en el trabajo y.

c) Para determinar el derecho a prestaciones sociales y su disfrute.

De forma específica se podría entonces mencionar que las principales recomendaciones de la Organización Internacional del Trabajo son las siguientes:

- Que, salvo circunstancias excepcionales, no se deberían recopilar datos que se refieran a la vida sexual del trabajador, a sus ideas políticas o religiosas y a sus antecedentes penales.
- Que sea el trabajador quien proporcione todos los datos personales y, de no ser posible, dé su consentimiento explícito cuando los datos se faciliten por terceros.
- Que no se proceda a la recopilación de datos personales sobre la afiliación del trabajador a un sindicato o sobre sus actividades sindicales, salvo si la legislación o los convenios colectivos así lo estipulan o autorizan.
- Que solamente se recopilen datos médicos de conformidad con la legislación nacional, el respeto del secreto médico y los principios generales de la salud y seguridad en el trabajo, y únicamente cuando se precisen.

La protección de datos del trabajador abarca todas las facetas en las que una persona se desenvuelve durante su vida. Sin embargo, este estudio se concentra únicamente en la protección de datos personales durante las diferentes etapas en las que normalmente se desarrolla una relación laboral. Principalmente: ¿cómo se obtiene la información de un trabajador?, ¿cómo se debe proteger la información del trabajador?, ¿hasta cuándo se debe proteger?, ¿cuáles acciones legales tiene el trabajador para reclamar el uso y el abuso de sus datos personales? Estas son las preguntas que procuro responder con la realización de este trabajo, de forma que pueda proponer algunas recomendaciones para que, tanto empleadores como trabajadores, vivan una relación de trabajo más armonioso, pero sobre todo digna para todas las partes involucradas.

1.1. Los Ficheros de Datos

En general, un fichero de datos es cualquier conjunto organizado de datos de carácter personal, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Por lo tanto, un fichero puede ser una unidad de almacenamiento digital, desde sus formas más avanzadas como un disco duro o un servidor de respaldo de información, hasta las formas más clásicas de almacenamiento de la información; por ejemplo, un cuaderno. Ahora bien, para efectos de esta investigación se toman únicamente a los ficheros que contienen información personal de un trabajador y que son creados y estructurados por los empleadores.

En el caso de España, donde la Ley Orgánica de Protección de Datos señala que todo patrono que trate datos de carácter personal, debe proceder a la inscripción del fichero ante la “Agencia Española de Protección de Datos de Carácter Personal”, declarando cualquiera de los ficheros que se hayan utilizado, por ejemplo, durante un proceso de contratación. La nota común de todos los sistemas de protección de datos personales que se han desarrollado en el mundo radica en el establecimiento de una serie de obligaciones legales para aquellas personas físicas o jurídicas que posean ficheros con datos de carácter personal, entre los cuales se debe considerar siempre a los empleadores.

Dentro de estas obligaciones se encuentra la de suministrar a la entidad correspondiente de control los ficheros donde se almacena la información, claro está, dependiente del contenido de la información y el fin para el que fueron creados. Esto conlleva la obligación de las empresas de poner en marcha diversas medidas destinadas a garantizar la protección de datos, incluso estableciendo la posibilidad de controlar y monitorear sistemas informáticos, archivos de soportes de almacenamiento, personal, procedimientos operativos, entre otros.

Además, los ficheros de datos pueden obtenerse, en el caso de las relaciones laborales, como resultado de los procedimientos de monitoreo y control que implemente el patrono, como por ejemplo: grabaciones de llamadas, videos, registros de accesos a Internet en utilización del equipo informático de la empresa.

Los niveles de seguridad de estos ficheros de almacenamiento de datos y, por lo tanto, de toda la información del trabajador, deberían ser adoptados en función de los

distintos tipos de datos personales: datos de salud, ideología, religión, creencias, infracciones administrativas, de morosidad, entre otros. Es decir, cualquier patrono que recopile información personal de sus trabajadores debería estar en la capacidad de organizar la información por el tipo de datos que maneja y establecer mecanismos de protección a partir de las implicaciones que para el trabajador pudiera representar la divulgación no autoriza de los datos.

A modo de ejemplo se cita la clasificación que establece la Ley Orgánica de Protección de Datos de España, tomada de la web www.portaley.com/protecciónde datos en el mes de junio de 2009:

	NIVEL BÁSICO
TIPO DE DATOS	• Nombre. • Apellidos. • Direcciones de contacto (tanto físicas como electrónicas). • Teléfono (tanto fijo como móvil). • Otros.
MEDIDAS DE SEGURIDAD OBLIGATORIAS	• Documento de seguridad. • Régimen de funciones y obligaciones del personal. • Registro de incidencias. • Identificación y autenticación de usuarios.

	• Control de acceso. • Gestión de soportes. • Copias de respaldo y recuperación.

	NIVEL MEDIO
TIPO DE DATOS	• Comisión infracciones penales. • Comisión infracciones administrativas. • Información de Hacienda Pública. • Información de servicios financieros.
MEDIDAS DE SEGURIDAD OBLIGATORIAS	• Medidas de seguridad de nivel básico. • Responsable de Seguridad. • Auditoría bianual. • Medidas adicionales de Identificación y autenticación de usuarios. • Control de acceso físico.

	NIVEL ALTO
TIPO DE DATOS	• Ideología. • Religión. • Creencias. • Origen racial. • Salud. • Vida.
MEDIDAS DE SEGURIDAD OBLIGATORIAS	• Medidas de seguridad de nivel básico y medio. • Seguridad en la distribución de soportes. • Registro de accesos. • Medidas adicionales de copias de respaldo. • Cifrado de telecomunicaciones.

Si se continúa usando, sólo a modo de referencia, el modelo español, dependiendo de la clasificación de información que hagan las propias empresas, se obligan a implementar los denominados *"documentos de seguridad",* mediante los que se elaboran y adoptan las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal. Estos documentos de seguridad se refieren al uso y conservación de los ficheros donde se almacena la información del ciudadano. En el caso particular de la presente investigación, interesa conocer el

tratamiento de información del trabajador realizado por la empresa dueña de la información y de las personas que, en uno u otro caso, podrían manipularla. En el caso de España, la utilización de estos documentos de seguridad es obligatoria desde la promulgación de "El Real Decreto 994/1999 del 11 de junio", mediante el que se aprobó el "Reglamento de Medidas de Seguridad", además de estar establecido en el párrafo 1 del artículo 9 de la Ley Orgánica de Protección de Datos Personales que señala:

> *El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

Hechas estas reflexiones se puede hacer una primera aproximación en relación al tema de esta investigación: todos los empleadores, como parte de su normal proceso de contratación de trabajadores necesitan recopilar alguna información de los trabajadores. Las formas de almacenamiento son diversas y dependen de las capacidades técnicas de sus sistemas de operación; pero todos, lo quieran o no, los poseen. Por ello deberían implementar mecanismos que clasifiquen la información según su contenido y, a partir de allí, se establezcan los controles de seguridad necesarios para evitar que la fuga de la información o el uso no autorizado para otros fines, distintos a los laborales, afecten la situación individual de cada trabajador.

2. ¿Cuáles datos se protegen?

En términos generales, la iniciativa de regulación de datos personales pretende la protección de toda la información del ciudadano. Sin embargo, para efectos de esta investigación se protegen, principalmente, aquellos datos conocidos como "datos sensibles" y que suelen referirse a "*la información sobre una persona física identificada o identificable mediante números, signos, uno o varios elementos específicos característicos de su identidad física, moral, emocional, fisiológica, psíquica, económica, cultural, étnica, racial, social o relacionada con su vida afectiva y familiar, estado civil, domicilio, número telefónico, patrimonio, ideología y opiniones o convicciones políticas, creencias religiosas o filosóficas, preferencias u orientación sexual, así como cualquier otra análoga que afecte su privacidad e intimidad*"[5].

Algunas legislaciones como la Argentina plantean que no todos los datos personales deben protegerse de la misma forma, distinguiendo entre datos personales y datos sensibles. Los datos personales se refieren a cualquier tipo de información referida a personas físicas, por ejemplo, el número de cédula de identidad de un trabajador; mientras que los datos sensibles son *"aquellos datos personales que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual*"[6] En la opinión de quien realiza esta investigación la distinción resulta bastante lógica, puesto que los datos sensibles mencionados suelen constituir información que da lugar a discriminaciones en el empleo, mientras que existe algún otra información de carácter

[5] Definición tomada del Portal Único de transparencia del Gobierno de Chiapas, México. Tomado de www.contraloriachiapas.gob.mx/transparencia/inicio/glosario3.php; julio 2008
[6] Información tomada de www.protecciondedatos.com.ar, julio 2008

público, como el número de cédula de identidad de un trabajador que, por sí misma, no debería representar un riesgo para el trabajador y que se justifica por motivos de registro de los nacionales de un país.

La experiencia de muchas empresas costarricenses, desafortunadamente, indica que nadie quiere tener en su organización a una persona que formó parte de un sindicato de trabajadores o que perteneció a determinado partido político, por ejemplo. En situaciones como esta es donde parece conveniente que los trabajadores deberían tener la posibilidad de controlar su información de forma que, por ejemplo, la afiliación sindical no represente una información que pueda ser utilizada en su perjuicio, por un empleador que no desee contar con trabajadores que hayan participado de este tipo de organizaciones. Esto es entonces lo que se podría señalar como un caso de datos sensibles, toda vez que de forma ilegítima podría implicar la no contratación de un candidato que quizás era idóneo para el puesto, pero que termina siendo discriminado por este motivo.

Los medios por los cuales se pueden obtener o archivar estos datos son innumerables y pueden estar contenidos en archivos, registros, bases de datos, u otros medios técnicos de tratamiento de datos, públicos o privados destinados a dar informes, o bien ser obtenidos a través de procesos tan rudimentarios como la solicitud al propio trabajador o la verificación de referencias personales y laborales por cualquier medio que se pueda imaginar. Se trata de cualquier forma mediante la que circula la información del trabajador, pudiendo ser entonces formas colectivas o individuales. Es decir, los datos sensibles del trabajador terminan por recopilarse en registros del empleador.

En la doctrina internacional sobre el tema se ha dicho que los archivos, registros o bases de datos, de donde se obtienen los datos del trabajador, son aquellos "*bancos de datos privados que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito*"[7] . Es decir, aplicando el concepto a la realidad costarricense podemos entonces decir que se trata, por ejemplo, de las bases de datos de trabajadores y, en general, de personas que han participado en algún momento de los procesos de selección y reclutamiento de una empresa. Toda esta información pasa a formar parte de su patrimonio y, aunque las compañías no tengan necesariamente un valor económico definido, sí forman parte de sus más preciados recursos. Es la forma en la que reclutan personal de forma rápida y sistematizada, y sus bases de datos se convierten, además, en un claro elemento de competitividad en relación a otras empresas competidoras. Una vez que el trabajador se incorpora a la nómina de la compañía, los registros de su personal se constituyen en claros mecanismos de control y evaluación, constituyéndose entonces en poderosos instrumentos para la toma de decisiones dentro de la empresa, como: ascensos, aumentos de salarios, e incluso evaluación del rendimiento del trabajador con miras a la aplicación de alguna sanción disciplinaria.

Estas bases de datos de carácter privado creadas y manipuladas por cada empleador no son las únicas que encontramos en nuestro medio. Existen compañías dedicadas a la comercialización de bases de datos de trabajadores con una intención evidentemente comercial. Los defensores de este tipo de bases de datos suelen

[7] Definición tomada de www.protecciondedatos.com.ar; julio 2009

argumentar que se nutren de información pública, es decir, datos referidos a: contratos inscritos en los Registros Públicos, tarjetas de créditos, leasing, reportes de salarios a instituciones públicas; y, en general, cualquier obligación del trabajador de contenido patrimonial y alegan que toda esta información puede ser verificada por cualquier persona, a fin de calificar y precisar su contenido y veracidad.

Este tema ha sido ampliamente analizado en otras tesis de grado, por lo que no corresponde hacerlo ahora, pero, a modo de síntesis, podemos decir que la obtención de información a través de empresas que se dedican a la comercialización de datos ha sido ampliamente cuestionada, por lo que debe ser manejada con suma delicadeza por sus usuarios. Sobre este tema, la Sala Constitucional ha mantenido el criterio reiterado de que:

> *Alega la recurrente que hace unos días, se dio a la tarea de indagar qué clase de información suya almacenan, y en su caso, suministran las empresas recurridas. Que logró informarse que las protectoras de crédito recurridas Teletec SA, Datum y Cero Riesgo Información Crediticia Digitalizada SA, mantienen y distribuyen a sus clientes, datos privados sobre él, familiares, salarios, teléfonos, dirección de su residencia, entre otros. Se declara parcialmente con lugar el recurso, por la lesión del derecho de autodeterminación informativa, tutelado por el artículo 24 de la Constitución Política. Se ordena al Presidente con facultades de Apoderado Generalísimo de Cero Riesgo Información Crediticia Digitalizada S.A. y al Representante Judicial de Aludel Limita, que, de manera inmediata, supriman de sus correspondientes bases de datos cualquier referencia a la dirección exacta de la casa de habitación de la amparada*[8].

Conviene aclarar que no es necesario que los datos personales hayan sido sometidos a tratamiento o procesamiento electrónico o automatizado, es decir, que consten en una base de datos particular o privada. Los sistemas de protección de

[8] Voto número 1283 del año 2009. Sala Segunda de la Corte Suprema de Justicia.

datos procuran el respeto de cualquier información personal del trabajador, independientemente del método o la forma en la que hayan sido obtenidos. Es decir, basta la simple información que corre de “boca en boca” para que el empleador se encuentre obligado a protegerla. Por ejemplo, la información que un trabajador le confía a una empresa durante una entrevista de trabajo, haya sido o no documentada en un registro específico, debe ser conservada y protegida de forma eficiente por el empleador, toda vez que dicha información fue facilitada con un claro fin: participar del proceso de reclutamiento y selección en el que el candidato participa de forma voluntaria.

B. ALCANCES DE LA PROTECCIÓN DE DATOS PERSONALES

1. Valores que cubre la protección de datos

La iniciativa de garantizar a los ciudadanos un régimen de protección de datos que pueda ser utilizado también en el desarrollo de una relación laboral, no es otra cosa más que dotar al empleador del poder de disposición y control sobre los datos personales que han sido y serán utilizados exclusivamente en la relación laboral. Es decir, se trata de que el trabajador pueda consentir la recopilación y el acceso a sus datos personales, su posterior almacenamiento y, eventualmente, el uso por parte de terceros ajenos a la relación laboral, como ya verá más adelante.

Como todo sistema de regulación legal, los procedimientos de protección de datos, enfocados desde la perspectiva laboral, buscan el respeto de algunos valores considerados esenciales para el trabajador y que se resumen en tres principales:

- La intimidad del trabajador.
- La autodeterminación informativa.
- El derecho al acceso a la información que posea el patrono del trabajador.

1.1 El derecho a la intimidad del trabajador y el concepto de privacidad

Mucho se ha escrito sobre el concepto y naturaleza jurídica de la intimidad de la persona y, en particular, del trabajador, ya que es probablemente uno de los derechos más alegados en virtud de abusos por parte de los empleadores. Y con toda la razón,

debido a sus diferentes aristas y la importancia que su garantía reviste para el ser humano.

El concepto más tradicional de intimidad es el que la define como aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservadas a su titular, y sobre las que se ejercen alguna forma de control cuando se ven implicados terceros. Sin embargo, el camino hacia una definición clara e inequívoca no ha sido fácil y, de hecho, es un término legal que se modifica constantemente.

Sobre el concepto de intimidad, el Tribunal Superior Español ha mencionado lo siguiente:

> *El derecho a la intimidad, según la doctrina del Tribunal Constitucional, supone "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana", y ese ámbito ha de respetarse también en el marco de las relaciones laborales, en las que "es factible en ocasiones acceder a informaciones atinentes a la vida íntima y familiar del trabajador que pueden ser lesivas para el derecho a la intimidad" (SSTC 142/1993, 98/2000 y 186/2000). De ahí que determinadas formas de control de la prestación de trabajo pueden resultar incompatibles con ese derecho, porque, aunque no se trata de un derecho absoluto y puede ceder, por tanto, ante "intereses constitucionalmente relevantes", para ello es preciso que las limitaciones impuestas sean necesarias para lograr un fin legítimo y sean también proporcionadas para alcanzarlo y respetuosas con el contenido esencial del derecho*[9].

[9] Tomado de www.aranzadi.es/index.php/informacion-juridica/jurisprudencia, junio 2009.

Ahora, en nuestro país el derecho a la Intimidad se encuentra regulado en los numerales 23, 24, y 28 del articulado de la Constitución Política, aunque no de manera expresa.

El artículo 23 la Carta Magna señala:

El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley.

Por su parte, el numeral 24 indica lo siguiente:

Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.

Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

Igualmente, la Ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo.

Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial.

La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos.

Una ley especial, aprobada por dos tercios del total de los diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.

No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación.

A pesar de estas disposiciones, es el artículo 41 de la Constitución Política que, interpretado de una forma amplia, reconoce la protección al derecho a la intimidad recogido, como ya se mencionó, en la interpretación conjunta de varios artículos constitucionales, pues garantiza la reparación de los daños sufridos en la persona, a la propiedad y a los "intereses morales" del individuo; todo lo cual, según lo indica la misma Carta Magna deba garantizar al ciudadano y, en el caso específico del trabajador, que se haga justicia pronta y cumplida en caso que resulten lesionados los derechos ahí establecidos, además de la efectiva reparación de los daños que se hayan logrado determinar.

Hasta este momento, y a pesar de los conceptos ilustrados acerca de una verdadera definición de "intimidad", se coincide con la tesis de algunos sistemas de protección de datos que promulgan que no se trata únicamente de proteger la intimidad, sino algo más que eso, y que en el derecho anglosajón se denomina *privacy*, que en idioma español se traduce como privacidad, concepto que pretende ir más allá y proteger aspectos de la personalidad que, vistos de forma individual, no tienen mayor trascendencia, pero que considerados unos con otros podrían configurar lo que se conoce como el perfil de la persona.

El concepto de privacidad hace remitirnos necesariamente a la idea de intimidad, o más bien, de vida privada. Es precisamente por la influencia de principios que no son

propios de la lengua castellana de donde surge el término, ya que el concepto jurídico tiene un claro origen anglosajón como derivado del precepto *the right to be alone* receptado en el ordenamiento jurídico de los Estados Unidos a fines del siglo XVII. La doctrina sentada por el Juez estadounidense Thomas Cooley en su obra *"The Elements of Torts"*, de 1873 y el trabajo de Warren y Brandeis, "*The Right to privacy"*, dieron forma a una clásica definición del vocablo *privacy*, entendido, genéricamente, como el derecho a estar solo o derecho a la soledad.

> El término *privacy* "*constituye un bien jurídico con proyección social, que enuncia el ejercicio de la libertad humana y, asimismo, impone un límite en la interrelación social. … Si bien el objeto inicial de los ensayos doctrinarios descriptos apuntaba esencialmente a analizar y tratar de encontrar límites para el avance indiscriminado de la prensa sobre la vida privada de los ciudadanos, no podemos discutir que, el avance tecnológico actual, que ha disparado exponencialmente las posibilidades de acceder y disponer de información de cualquier naturaleza, conlleva el potencial peligro de exacerbar la incidencia de tales medios sobre el derecho a la intimidad de las personas"*[10].

En España, el término privacidad fue introducido en el Código Penal de 1995 y se puede definir como la posibilidad del sujeto de decidir qué parte de su intimidad quiere que se conozca (aspecto positivo) y a quien quiere dejar fuera de la misma (aspecto negativo).

Es decir, en aplicación al campo laboral, los trabajadores deben tener el derecho a exigir a sus empleadores que sus datos personales permanezcan en el ámbito de su privacidad.

---

[10] Fernández, Claudio. Privacidad y Derecho a la Información. Artículo publicado en http://www.delitosinformaticos.com/ciberderechos/privacidad.shtm, junio 2009.

1.2 La autodeterminación informativa

El concepto de autodeterminación informativa ha evolucionado paulatinamente de la mano del avance de la teoría de la Protección de Datos y ligado estrechamente al concepto de intimidad y privacidad ya estudiado.

Son muchas las definiciones que existen sobre la llamada autodeterminación informativa, por ejemplo, Murillo de la Cueva define la autodeterminación afirmativa como "*el derecho que toda persona tiene a controlar la información que le concierne, sea íntima o no, para preservar de este modo y en último extremo, la propia identidad, su dignidad y libertad*"[11].

El derecho a la autodeterminación informativa fue llamado por primera vez de esa manera en la sentencia del Tribunal Constitucional Alemán del 15 de diciembre de 1983, que declaró inconstitucionales ciertos aspectos de la Ley del Censo de Población de 1982 de la República Federal Alemana y destacó como contenido del derecho a la personalidad la facultad de decidir por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida. Reconoció, además, que esta facultad requiere de especiales medidas de protección, ya que la interconexión de varias colecciones de datos puede converger en la elaboración de un perfil de la personalidad y puede influir en la autodeterminación del individuo, y en su libertad de decisión. En adelante, la mayoría de las definiciones que en doctrina se pueden encontrar parten de esta base conceptual. Por lo tanto, cuando esta investigación se

[11] Murillo de la Cueva, Pablo Lucas. "El derecho a la autodeterminación informativa". Editorial Tecnos. Madrid, España, 1990. Tomado de www.protecciondedatos.com.ar; julio 2009

refiera a autodeterminación informativa debe hacerse referencia al concepto aquí mencionado.

1.3 El derecho al acceso de los datos personales

Uno de los fines principales que tiene la Teoría de la Protección de Datos es el derecho que debe tener el ciudadano, en este caso el trabajador, de acceder a las bases de datos utilizadas por el empleador, para verificar los datos obtenidos por cualquier medio. Es decir, es la garantía de comprobación de que la información que posee el patrono es veraz, actualizada y necesaria.

Esta es una de las principales cuestiones que deben revisar los empleadores y las empresas que se dedican al reclutamiento y selección de personal, ya que es común que alguna información laboral no sea tan fácilmente accesible y permanezca casi de uso exclusivo del empleador. No obstante, cualquier información del trabajador, obtenida o no con su consentimiento, debe ser facilitada a éste cuando lo solicite. De esta forma podrá revisar y, si es el caso, rectificar desde una simple actualización de la dirección de su domicilio hasta cambios que afecten su estado civil o los datos académicos que posea la empresa previamente.

2. ¿A quiénes protege la protección de datos? Perspectiva laboral

En virtud de los fines para los que se crearon los sistemas de protección de datos, la regulación legal ha sido diseñada, en general, para ser aplicable a los ciudadanos, es decir, a las personas físicas que necesiten un amparo legal que los proteja de las violaciones cometidas en su contra en los más diversos campos que se desarrolla el ser humano. Esta es la premisa de la que parten todos los Estados que han seguido el modelo de protección de datos sensibles del trabajador.

Por ejemplo, la Ley Orgánica de Protección de Datos Personales de España es clara al afirmar que la normativa de protección de datos sólo es aplicable a las personas físicas, ya que el objeto de la ley es garantizar y proteger, "*en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*"[12].

Existen algunas excepciones establecidas por la misma ley española que dejan fuera de la protección citada a los ciudadanos que manipulen datos personales en áreas fuera de lo que podríamos decir la esfera más intima del ciudadano. Por ejemplo, los ficheros de datos mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, como la información contenida en una agenda personal que no ha sido creada con fines comerciales o con ánimo de obtener alguna especie de lucro a través de su gestión.

[12] Información tomada de www.portaley.com/protecciondatos/preguntas.shtml#11, agosto 2008.

Aplicando esta información al campo estrictamente laboral y a la búsqueda del mejoramiento de la conservación de datos por parte de empresas que operan en nuestro país, queda claro que la protección de datos estaría formulada para proteger estrictamente al trabajador, es decir, a aquella persona física que, en estricto apego a lo dicho por la legislación laboral costarricense, es contratada bajo una relación de subordinación para la realización de un servicio a cambio de una remuneración previamente acordada por las partes. Al respecto, véase lo que señala el artículo 4 del Código de Trabajo, que dispone lo siguiente:

> *Trabajador es toda persona física que presta a otra u otras sus servicios materiales, intelectuales o de ambos géneros en virtud de un contrato de trabajo expreso o implícito, verbal o escrito, individual o colectivo.*

Es decir, los empleadores estarían obligados a conservar y proteger la información sensible del trabajador, más allá del tipo de contrato de trabajadores que los ligue, sin importar la duración o la forma de determinación del salario.

CAPÍTULO II. LA REGULACIÓN DE LA PROTECCIÓN DE DATOS DEL TRABAJADOR. ANÁLISIS DESDE EL DERECHO COMPARADO

A. DESARROLLO DEL CONCEPTO DE PROTECCIÓN DE DATOS DEL TRABAJADOR EN EL DERECHO INTERNACIONAL

El avance de los sistemas de protección de datos va de la mano con el desarrollo de la llamada Revolución Tecnológica, caracterizada, principalmente, por el surgimiento de las Nuevas Tecnologías de la Información y de las Comunicaciones. La evolución de la Internet y su influencia en todas las facetas del ser humano; sobre todo en lo económico, social, jurídico, político y cultural; han modificado considerablemente los comportamientos de las personas.

Como señala el especialista español, Juan Carrasco Linares,

> D*esde los años 70, en Europa, juristas, políticos e informáticos desarrollaron una intensa actividad con el objeto de definir el sistema de protección de datos de carácter preventivo que hoy conocemos, dando lugar a la aprobación de varios textos legales en diferentes países europeos. Al mismo tiempo, en el ámbito del Consejo de Europa también encontramos distintos grupos de trabajo, recomendaciones y resoluciones que cristalizan en el Convenio de 28 de enero de 1981, el conocido como Convenio 108*[13].

A continuación se presenta un análisis de la experiencia española y la realidad latinoamericana, como principales – aunque no únicas – fuentes de inspiración de las leyes laborales costarricenses.

[13] Carrasco Linares, Juan. Aspectos Generales de la Protección de Datos. Artículo tomado de www.delitosinformaticos.com/protecciondatos, agosto 2008.

1. La experiencia en Europa

A consideración de este trabajo de investigación, España ha sido uno de los países con más avances en el tema de Protección de Datos, sin que ello implique que otros países como Francia y Alemania hayan avanzado también en sus regulaciones internas. Sin embargo, por la influencia de la doctrina española en nuestro ordenamiento, el caso español merece una mención detallada.

En España, la regulación específica la constituye la Ley Orgánica de Protección de Datos de Carácter Personal, Ley Orgánica número 15/1999. Desde la promulgación de esta ley y la entrada en vigencia de la Agencia Española de Protección de Datos de Carácter Personal, toda persona física o jurídica que trate datos de carácter personal debe proceder a la inscripción del fichero ante esa entidad; por lo tanto, se deben declarar los ficheros utilizados en la fase de selección y reclutamiento de personal para laborar bajo las órdenes de un empleador.

Según las prácticas más comunes en dicha Nación, los departamentos de recursos humanos deben analizar el tipo de información que poseen de sus trabajadores, ya que, en sentido amplio, existen datos personales identificativos, datos académicos, profesionales, económicos, datos formativos, entre otros; y cada uno debe ser tratado de la forma que lo indique la legislación.

A partir de una primera identificación, la información se debe agrupar en función de las finalidades a las que responde, es decir, reviste especial importancia la información que interesa proteger a la ley, es decir, la que está relacionada con cualquiera de las incidencias que se presentan en una relación laboral. Por lo tanto, las

empresas están obligadas a proteger información relacionada con: nóminas, remuneraciones, historia de riesgos laborales, controles de horario, seguridad y vacaciones. Este tipo de información coincide con lo que hasta ahora hemos denominado datos sensibles, cuyo nivel de confidencialidad debe ser valorado por el contratante para cumplir con la normativa de protección de datos de carácter personal.

En el Reglamento de Medidas de Seguridad, emitido mediante Real Decreto Número 999/99 del 11 de junio, se establecen tres tipos de medidas de seguridad diferentes, aplicable a los ficheros en función del tipo de datos que contengan. De esta manera:

> *los ficheros pueden ser de nivel básico, cualquier fichero por el mero hecho de contener datos de carácter personal, de nivel medio, cuando alberga entre otros datos relativos a la administración pública, sanciones administrativas o penales, o de nivel alto, cuando contiene datos de los catalogados como especialmente protegidos, es decir salud, afiliación sindical... etc. A nivel doctrinal (artículo 4.4 del Reglamento de Medidas de Seguridad) se reconoce un cuarto nivel denominado básico cualificado o medio atenuado, aplicable bajo el criterio subjetivo de poseer suficientes datos para extraer un perfil de la personalidad del individuo. Los ficheros que frecuentemente se encuentran en los departamentos de recursos humanos de la empresa suelen ser de nivel básico o básico cualificado, si bien nada obsta a que sean catalogados de nivel alto si concurren en alguno de ellos, cualquiera de los siguientes datos, porcentajes de minusvalías, descuento de la cuota de afiliación sindical, absentismo laboral... etc.*[14].

Es importante mencionar que, según la legislación española, el patrono no solo debe declarar los ficheros digitales, normalmente las bases de datos; sino que también aquellos ficheros no automatizados o en papel, como: el currículo, los resultados de las pruebas realizadas, el reconocimiento médico que se realice a los trabajadores; entre

[14] Información tomada de http://delitosinformaticos.com/protecciondatos/rrhh.shtml, agosto 2008

otros. Si bien es cierto este tipo de información no representa grandes medidas de seguridad física, el patrono está obligado a tomar precauciones para garantizar la confidencialidad de datos.

En la actualidad también otros países del continente europeo cuentan con leyes que regulan el tema de la protección de datos, tal es el caso de: Alemania, Bélgica, Dinamarca, Francia, Irlanda, Luxemburgo, Italia, Países Bajos, el Reino Unido, Austria, Finlandia, Islandia, Grecia[15], Noruega y Suecia.

2. El desarrollo en Latinoamérica

En virtud de la influencia ejercida, principalmente, por los países europeos, y por las propias necesidades de regulación en cada uno de los países del continente latinoamericano; la protección de datos tomó una importante relevancia en los temas legales de las sociedades latinoamericanas. Países como Argentina y Colombia han avanzado más rápidamente en la regulación del tema. A continuación un análisis de la experiencia de dichos países enfocado a temas propios de la relación laboral.

2.1 Argentina

En noviembre del año 2001, el Congreso de la República de Argentina sancionó la Ley número 25 326 de Protección de Datos Personales, también conocida como Ley

[15] Grecia puso en vigencia su Ley de protección de la persona frente al tratamiento de datos personales el 19 de marzo de 1997.

de Habeas Data, con lo cual se puso fin a un proceso iniciado desde el año 1986. Los primeros intentos de regulación en este país se basaban en la conveniencia de regular el derecho a la privacidad, con miras a evitar la intromisión propia de los avances de la informática en materia de la informática en materia de registro de datos. Es así como, a partir de la reforma constitucional del año 1994:

> *…que en el tercer párrafo del nuevo artículo 43, y dentro del marco de la acción de amparo, incluyó una acción especial tendiente a que toda persona pueda tomar conocimiento de los datos a ella referidos y de su finalidad, que conste en registros o bancos de datos públicos, o privados destinados a proveer informes, y exigir su supresión, rectificación, confidencialidad o actualización en caso de falsedad o discriminación*[16].

Esta posición establecida en la legislación argentina en mi opinión es la senda que el resto de países que se han interesado en la protección de datos del trabajador.

B. LA PROTECCIÓN DE DATOS POR MEDIO DEL RECURSO DE HABEAS DATA

[16] Tanús, Gustavo Daniel. PROTECCION DE DATOS PERSONALES. PRINCIPIOS GENERALES, DEBECHOS, DEBERES Y OBLIGACIONES. Artículo publicado en Revista Jurídica El Derecho, 19/06/02, pág. 06. Buenos Aires, Argentina. Tomado de: www.protecciondedatos.com.ar; julio 2009.

Las tesis tendientes a la protección de datos están directamente relacionadas con el concepto de Habeas Data que, en términos generales, consiste en "*una acción constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio*"[17].

A continuación se presenta un análisis detallado de la naturaleza jurídica de esta figura legal y su evolución histórica en el derecho comparado.

1. Evolución del Recurso de Hábeas Data

El hábeas data surge como un proceso constitucional especializado para la protección de ciertos derechos en relación a la libertad informática. Sus antecedentes genéricos básicos podemos remontarlos a los intentos por preservar esferas personales de injerencias o perturbaciones externas no deseadas, a fin de garantizar la privacidad o intimidad personal. De allí se evolucionaría luego hasta llegar a la protección frente a los riesgos del almacenamiento, registro y utilización de datos y, por ende, a la protección de datos personales, entre ellos, los datos personales del trabajador.

En términos generales, el desarrollo conceptual del derecho a la intimidad personal o *right of privac*", tiene lugar en la experiencia de los Estados Unidos y en el Reino Unido desde finales del siglo XIX. Un punto crucial en este itinerario fue la definición del derecho a la privacidad como *the right to be let alone*, es decir, el

[17] Definición tomada de http://es.wikipedia.org/wiki/Habeas_data, julio 2009

"derecho a ser dejado en soledad" (sin ser molestado o perturbado) elaborada por el Juez Cocley y al que se ha hecho referencia líneas atrás. Posteriormente este concepto fue desarrollado por los juristas norteamericanos Warren y Grandeis buscando proteger a la persona frente a datos o actos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado.

Algún tiempo después, aproximadamente desde 1960, y como reacción al vertiginoso desarrollo tecnológico que se traduce en nuevos sistemas informáticos, tanto en los Estados Unidos como en Gran Bretaña, se empiezan a promover proyectos legislativos que, dando un nuevo giro o extensión al concepto de derecho a la privacidad, se refieren a la protección de la libertad y esfera personal frente a posibles excesos del registro informatizado o difusión de datos e informaciones vinculadas a aspectos reservados o íntimos. De esta forma se llegó a la *Privacy Act* norteamericana del 31 de diciembre de 1974, a la *Data Protection Act* británica de 1984, y a la Ley Orgánica mayo de 1992 española, denominada "Regulación del tratamiento automatizada de datos".

A nivel de los textos constitucionales, la Carta de Portugal de 1976 estableció, en su art. 35º, el derecho del ciudadano a:

> a) Conocer las informaciones que le conciernen almacenadas en archivos, su finalidad y la posibilidad de rectificarlas o actualizarlas.
>
> b) A que la información no sea utilizada para el tratamiento de datos "sensibles", referentes a convicciones políticas, religiosas o a asuntos de la vida privada, salvo que se trate de datos no identificables con fines meramente estadísticos.

c) A que no se atribuya a los ciudadanos un número nacional único de identificación.

Por su parte, la Constitución Española de 1978 estableció, en su art. 18.4, que *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".* A su vez, en su artículo 105, b), asegura "*el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de la persona*".

En el ámbito latinoamericano fue la Constitución Brasileña de 1988, en su art. 5º, inc. LXXII, la primera en abordar estos temas, pero sobre todo también la primera en "bautizar" constitucionalmente al instituto del hábeas data. Dicha norma dispone que: "*Se concederá Hábeas Data: a) Para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) Para la rectificación de datos, cuando no se prefiera hacerlo en proceso reservado judicial o administrativo*". El nombre Hábeas Data fue tomado de la Ley 824 del Estado de Río de Janeiro.

Por su parte, la Constitución Colombiana de 1991 establece en su art. 15º que todas las personas tienen derecho a la intimidad personal y familiar y a su buen nombre, con la obligación del estado de respetarlos y hacerlos respetar. Agrega luego: *"De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas".*

La Constitución Argentina, con la reforma aprobada en 1994, regula expresamente en el art. 43º el hábeas data, estableciendo que: *"Toda persona puede interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".*

Estos desarrollos doctrinarios y normativos fueron configurando un nuevo término y una suerte de derecho autónomo conocido como "libertad informática", un derecho que tiene por objeto garantizar la facultad de las personas para conocer y acceder a la información que las concierne, archivada en bancos de datos.

Una de las críticas que reiteradamente se han hecho a los recursos de hábeas data es que se trata de mecanismos reactivos ante el daño que sufre el ciudadano, cuando en realidad se debería configurar toda una estructura tendiente a la protección de la información durante todo el proceso.

Esta crítica es posible plasmarla en los razonamientos que la Comisión de Asuntos Jurídicos de la Asamblea Legislativa de Costa Rica ha brindado con ocasión de la Discusión del Proyecto de Ley número 16 679, denominado "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales", y que se analiza más adelante. En el dictamen de mayoría de dicho proyecto se indica lo siguiente:

> *En realidad, los recursos de hábeas data no son más que instrumentos o mecanismos de garantía procesal que se acuerdan a favor de las personas que han sufrido una lesión en su ámbito de intimidad producto de usos abusivos de sus datos o informaciones. Se trata, en general, entonces, de un derecho procesal reactivo frente a una lesión ya ocasionada. No tienen una vocación*

preventiva de las lesiones y sus efectos son casi siempre acordados a favor del afectado y no tienen efectos extensivos hacia quienes sufren las mismas lesiones [18].

A modo de ilustración se presenta un cuadro comparativo que demuestra la regulación del hábeas data en algunas legislaciones latinoamericanas:

EL DERECHO A LA INFORMACIÓN EN LOS TEXTOS CONSTITUCIONALES

Colombia	**Artículo 15º.-** "Todas las personas tienen derecho (...) a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (...)".
Ecuador	**Artículo 94º.-** "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.

[18] Comisión Permanente de Asuntos Jurídicos de la Asamblea Legislativa de la República de Costa Rica. Ley de Protección de la Persona Frente al Tratamiento de sus datos personales. Expediente número 16 679. Dictamen afirmativo de mayoría del 26 de noviembre de 2008

	La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional". **Artículo 276º.-** "Competerá al Tribunal Constitucional: (...) 3) Conocer las resoluciones que denieguen (...) el hábeas data (...)".
Venezuela	**Artículo 28º.-** "Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley". **Artículo 281º.-** "Son atribuciones del Defensor o Defensora del Pueblo: 4) Interponer las acciones de (...) hábeas data (...)".
Chile	**Artículo 14º.-** "El derecho de presentar peticiones a la autoridad, sobre cualquier asunto de interés público o privado, sin otra limitación que la de

	proceder en términos respetuosos y convenientes". **Artículo 18º.-** "(…) La acción del Estado estará dirigida a garantizar el acceso de todos los habitantes al goce de prestaciones básicas uniformes, sea que se otorguen a través de instituciones públicas o privadas. La ley podrá establecer cotizaciones obligatorias (…)".

19

2. Avances en la tutela de la protección de datos en Costa Rica

En Costa Rica, desde hace algún tiempo se viene hablando de la necesidad de regular el habeas data, discusión que ha sido promovida, entre otros, por el profesor Alfredo Chirino. Sin embargo, el camino hasta convertirse en ley de la República ha sido difícil. A la fecha de esta investigación no se cuenta todavía con la anhelada ley, por ello la protección de datos debe ser revisada en distintas sedes jurisdiccionales, como la vía constitucional e incluso en la vía penal, en lugar de contar con un procedimiento único para tal efecto.

Es así como en el país se han presentado algunas intenciones a nivel parlamentario para la regulación expresa del Hábeas Data, la primera de ellas en el año 1996, proyecto legislativo que naufragó en la corriente legislativa. Posteriormente se presentó, para estudio, el proyecto número 14.778, de fecha 12 de junio de 2002;

[19] Información tomada de www.monografias.com/trabajos50/habeas-data/habeas-data.shtml, agosto 2009.

promovido por los diputados Rocío Ulloa Solano, Carlos Avendaño Calvo y Laura Chinchilla Miranda, el cual fue anunciado ampliamente por diversos medios de comunicación[20].

La intención de los promotores de la ley consistía en una adición a la Ley de la Jurisdicción Constitucional, cuyo texto planteaba algunos artículos directamente provenientes de la teoría de protección de datos hasta ahora expuesta. Para el interés del presente estudio se transcriben algunas de esas propuestas legislativas:

> *Artículo 71: "El recurso de hábeas data tiene por objeto proteger de manera procedimental el derecho de la persona a su intimidad, imagen, honor, autodeterminación informativa y libertad informática en el tratamiento de sus datos personales. Asimismo, es objeto de este recurso garantizar el ejercicio pleno de todos los derechos y las libertades concernientes a los datos y la información de carácter personal.*

> *Artículo 72. El recurso de hábeas data podrá plantearse en los siguientes casos:*

[20] Al efecto, véase la noticia publicada por la periodista Orieta Vargas Cavallini, de fecha 18 de junio de 2002, en la dirección electrónica http://www.tiquicia.com/articulos/derecho/Derecho_Informatico/40asamb180602.asp

a) Toda persona, física o jurídica, podrá plantearlo para conocer lo que conste sobre sí misma o sus bienes en registros, archivos, listados o bancos de datos, sean manuales, mecánicos, electrónicos o informatizados, públicos o privados. No podrán solicitarse datos sobre una investigación judicial por la comisión de algún delito, mientras no haya concluido el proceso investigador.

b) La pretensión del recurso de hábeas data puede consistir en solicitar información sobre la finalidad de los datos personales recogidos, su destino final y su eventual entrega en otros lugares de procesamiento de datos distintos del lugar que, en primera instancia, recolectó los datos.

c) Mediante el recurso de hábeas data podrá requerirse la rectificación, actualización, inclusión, confidencialidad o cancelación inmediata de los datos personales que están en poder del lugar de tratamiento de los datos, ya sea público o privado.

d) El recurso de hábeas data también procederá para solicitar informaciones declaradas secreto de Estado. La Sala en pleno deberá determinar si tales informaciones se ajustan a los requerimientos constitucionales. Para los efectos de esta norma, secretos de Estado son los asuntos en tramitación, de carácter diplomático o referido a operaciones de seguridad nacional pendientes.

e) Podrá plantearse el recurso de hábeas data cuando se haya lesionado alguno de los principios relacionados con el procesamiento de datos personales descritos en el artículo 73.

f) El afectado podrá impugnar, mediante la presentación del recurso de hábeas data, los actos administrativos o las decisiones de carácter particular que impliquen una valoración de su comportamiento, cuya única base sea un tratamiento de datos personales que defina sus características o personalidad.

Artículo 74. El recurso de hábeas data recibirá el trámite establecido para el amparo. Se resolverá con prioridad respecto a otros recursos de amparo, salvo los fundamentados en el derecho de rectificación y respuesta y el de petición. Deberá dictarse sentencia a más tardar cinco días naturales después de recibidas las pruebas del caso.

Artículo 81. Para efectos del recurso de hábeas data, se definen los siguientes conceptos: Datos personales: Información concerniente a personas físicas o jurídicas, identificadas o identificables.

Tratamiento de datos: Operaciones y procedimientos técnicos automatizados o no, que permitan la recolección, la grabación, la conservación, la elaboración, la modificación, el bloqueo y la cancelación de información, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Responsable del fichero: Persona física o jurídica, pública o privada, y órgano administrativo que decida sobre la finalidad, el contenido y uso del tratamiento. Afectado: Persona física o jurídica titular de los datos objeto del tratamiento automatizado o manual.

A pesar del buen intento que pudo significar el proyecto de ley mencionado, diez años después de la primera iniciativa el país continúa sin una regulación específica sobre el tema y con los problemas que representa la no definición de conceptos básicos sobre la protección de datos. Como mencionó el señor Pedro Oller en un artículo publicado en el diario de circulación nacional, La República, en torno a que continúa:

> *…la proliferación de servicios, fuentes y requerimientos que nos exponen a la diseminación indiscriminada de nuestra información y hay muy pocos recursos para protegerse. Hay páginas en línea que permiten conocer además del nombre completo, número de cédula y fecha de nacimiento de un individuo; también, números de teléfono de referencia (así no estén a su nombre pero que han sido suministrados como tales), sociedades anónimas en las que ostenta cargos, empleo, prendas e hipotecas y procesos judiciales pendientes, entre otras cosas*[21].

Ante la falta de regulación sobre la materia, y la poca intención por aprobar el proyecto de inclusión del Recurso de Habeas Datas, se han presentado algunas otras iniciativas que, de forma más amplia, han querido tratar la protección de datos personales ante el avance de la tecnología y su aplicación en diferentes áreas en el país. Una de las más recientes fue propuesta por el Juez Superior del Tribunal de Casación Penal, Carlos Chinchilla, quien propone la necesidad de que la Constitución Política regule, lo que en la doctrina internacional se ha dado en conocer como "Personalidad Jurídica".

[21] Oller, Pedro. Artículo publicado en el Diario la República, de fecha martes 11 de marzo de 2008. Tomado de http://www.larepublica.net/app/cms/www/index.php?pk_artículo=8049

La Personalidad Jurídica es un concepto que ha sido definido como el desdoblamiento del ser humano en su materialidad física y su desmaterialización virtual de información -principio de ubicuidad-, donde esta personalidad virtual, conformada en forma absoluta de información, se encuentra regulada por cada persona y será considera como centro de atribución o imputación de efectos jurídicos. Es decir, que toda persona tiene derecho a tener o no una personalidad virtual y, principalmente, conocer de su presencia, contenido y protección; la cual, por tratarse de información personal, no puede utilizarse con fines discriminatorios en perjuicio de su titular.

En palabras del citado Juez Chinchilla:

> *El Estado debe ser el encargado de garantizar que la información contenida en la personalidad virtual goce de la adecuada seguridad informática y jurídica, con exclusión de terceros no autorizados que pretendan obtenerla. De igual forma, el Estado podrá hacer uso del contenido de la personalidad virtual de las personas, previa autorización de éstas, siempre que se realice en beneficio y provecho de las mismas.*
>
> *El ser humano debe contar con la posibilidad de tener bajo su control y poder dos ámbitos de su personalidad; a- **personalidad material**, protegida en la Constitución Política, donde se reconocen gran cantidad de derechos y garantías fundamentales, como lo son, la libertad (art. 20), vida (art. 21), privacidad (art. 22), intimidad, imagen y secreto de comunicaciones (art. 24), libertad (art. 24, 37 y 48, este último contempla el recurso de Hábeas Corpus), igualdad (art. 33) e integridad física (art. 40), entre otros. b- **personalidad inmaterial o virtual de información**, la que merece efectiva regulación constitucional como un derecho fundamental, debido a la carga sensible de información relevante de cada ser humano, que en forma inadecuada podría ser utilizada en su perjuicio con fines discriminatorios. Esta propuesta es de estudio en muchos países del mundo, pero en ninguno se ha tomado la iniciativa de su regulación constitucional y elevarlo al nivel de derecho fundamental de la quinta generación, identificado como parte de los derechos fundamentales virtuales,*

relacionado con el uso de la tecnología, en el caso particular, la tecnología aplicada a la información[22].

Asimismo, el propio Magistrado Chinchilla manifestó la necesidad de apoyar la gestión de la Personalidad Jurídica con la aprobación definitiva del Recurso de Hábeas Data, en lugar del tradicional recurso de amparo como mecanismo de protección de la intimidad del ciudadano. La nota periodística que contiene dicha manifestación señala:

Por ello, Chinchilla resaltó la importancia del Hábeas Data, recurso que tutela la intimidad de la persona, pues mediante él, el afectado solicita eliminar o modificar la información dentro de un portal Web, de manera que la resolución se dará en un plazo máximo de una semana, por lo cual se convierte en la vía más rápida para resolver una situación que perjudique a la persona[23].

A pesar de lo dicho, en la actualidad existe un proyecto de ley que avanza de forma más rápida que los casos anteriormente expuestos. Se enfoca exclusivamente en mecanismos para la protección de datos sensibles del trabajador. Se trata del expediente número 16 679, denominado "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales".

Al finalizar el mes de octubre del año 2009, el expediente se encuentra en la Comisión de Asuntos Jurídicos, con dictamen afirmativo de mayoría, y dictamen

[22] Chinchilla Sandí, Carlos. Personalidad Virtual: Necesidad de una Reforma Constitucional. Publicado en la Revista de Derecho y Tecnologías de la Información. Nº 3-2005. UNED, Costa Rica. Tomado de www.uned.ac.cr/redti/tercera/documentos/articulo1.pdf. Junio de 2008.

[23] López Arias, Angie. Crearán "personalidad virtual para proteger datos personales". Artículo publicado en el Diario La Prensa Libre, del día 17 de marzo de 2007. Tomado de www.prensalibre.co.cr/2007/marzo/17/abanico08.php

afirmativo de minoría. Por la difusión que ha tenido en los medios de comunicación se puede decir que varios sectores lo esperan.

A continuación se analizan los principales aspectos legales que incluye el citado proyecto de ley.

2.1. El proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales"

El proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales", responde a la necesidad de la sociedad de costarricense por contar con una normativa que regule el tratamiento de la información de los ciudadanos, necesidad que se ha mencionado a lo largo de este trabajo como una de las principales deficiencias del sistema costarricense en este materia.

El objetivo de este proyecto de ley es garantizar a las personas físicas y jurídicas el respeto a la autodeterminación informativa, en relación con su vida o actividad privada y demás derechos de la personalidad y defensa de su libertad e igualdad, respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Es decir, frente a la manipulación intencionada de quienes utilizan información sin estar autorizados para tal efecto, excluyendo de forma expresa las bases de datos de consulta pública en tanto la información no sea utilizada en perjuicio del ciudadano.

En lo que interesa a esta investigación, el proyecto de ley define como datos sensibles los siguientes: datos personales que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida sexual y antecedentes delictivos, operaciones bancarias, registros tributarios, aduaneros o relativos a actividades económicas.

La definición de datos sensibles, anteriormente descrita, coincide plenamente con la definición dada líneas atrás y que, en general, se refieren a la información que de alguna forma pueda ser utilizada de forma indebida para discriminar al candidato a un puesto o al trabajador, sin contar con una razón objetiva que haga desaparecer el carácter discriminatorio de dicha acción.

En términos generales, el proceso que establece el proyecto recoge el sistema mencionado en cuanto a la conservación y utilización de la información, la cual se almacenará en ficheros propiedad del tercero que solicita la información. Así, el artículo 4 del proyecto establece:

> ***ARTÍCULO 4.- Derecho de información en la recolección de los datos***
>
> *Las personas físicas a quienes se soliciten datos de carácter personal y a las personas jurídicas cuyos datos no se les ha dado el carácter de público; deberán ser previamente informados de modo expreso, preciso e inequívoco directamente o por apoderado con poder o cláusula especial; las personas jurídicas por medio de su representante legal o apoderado con poder o cláusula especial:*

a) De la existencia de un fichero automatizado o manual de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se les formulen.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercer los derechos de acceso, rectificación, actualización, cancelación y confidencialidad.

e) De la identidad y dirección del responsable del fichero.

Cuando se utilicen cuestionarios u otros impresos para la recolección, figurarán en los mismos en forma claramente legible, las advertencias a que se refiere el apartado anterior.

No será necesaria la información a que se refiere el apartado a), si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de la circunstancia en que se recaban o de la información derivada de la actividad ordinaria de la institución o de su giro normal; o de la empresa solicitante.

En ningún caso se podrá afectar el secreto de las fuentes de información periodística y el secreto profesional que determinen las leyes correspondientes.

En virtud de que no existe en el proyecto una mención específica a la información solicitada, de un contrato de trabajo, se concluye que, en caso de aprobación del proyecto, las normas aquí mencionadas serán de aplicación también por parte de los empleadores que soliciten información de su personal.

El proyecto de ley también establece la obligación que tiene el interesado, a quien se le solicita la información, de expresar su consentimiento, de forma personal o por medio de representante legal; haciendo constar esto por medio escrito o por otro medio idóneo, sea físico o electrónico.

En cuanto a los datos que pueden ser solicitados, se establece que solamente podrán ser "recolectados, almacenados y empleados … cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimos para los que se han obtenido". Es decir, la cesión de datos que un patrono pretende realizar, por ejemplo, facilitar la base de datos de su personal a un tercero con cualquier otro fin; también debe ser autorizada por el ciudadano, en este caso el trabajador, salvo que se trate de una cesión por motivos amparados en una ley especial.

De lo expuesto en el párrafo anterior se puede afirmar que el patrono solamente estará facultado para solicitar aquella información que, de forma objetiva, pueda tener alguna relación con el empleo o las características del servicio que se pretende contratar. Otras cuestiones personales sin ninguna relación con el tema no podrían ser consultadas de forma válida, evitando así que el candidato o trabajador pueda ser discriminado por una condición personal no relacionada.

En este sentido, el artículo 7 del proyecto, establece la definición de datos sensibles, de la siguiente manera:

ARTÍCULO 7.- Categorías particulares de datos

Los datos de carácter personal de las personas físicas que revelen su origen racial, sus opiniones políticas, sus convicciones religiosas o espirituales, así como los datos de carácter personal relativos a la salud, a la vida sexual y a sus antecedentes delictivos, no podrán ser almacenados de manera automática ni manual en registros o ficheros privados, y en los registros públicos serán de acceso restringido.

Ninguna persona estará obligada a suministrar datos sensibles. Los datos sensibles solo podrán ser recolectados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Sin perjuicio de lo establecido en el párrafo anterior, las asociaciones religiosas, las organizaciones políticas, sindicales y aquellas que agrupen a los individuos de acuerdo con sus preferencias sexuales o ideológicas, podrán llevar un registro de sus miembros, para uso exclusivo de su fin asociativo.

En cuanto a la seguridad de la información de los datos suministrados, el artículo 8 del proyecto dice:

ARTÍCULO 8.- Seguridad de los datos

1.- Todo archivo, fichero, registro o base de datos, público o privado destinado a proporcionar informes debe inscribirse en el Registro de archivos y bases de datos contemplado en el artículo 27 de la presente Ley.

2.- El responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

3.- No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que garanticen plenamente su seguridad e integridad y los de los centros de tratamientos, equipos, sistemas y programas.

4.- Por vía de reglamento, se establecerán los requisitos y las condiciones que deban reunir los ficheros automatizados y los manuales y las personas que intervengan en el acopio, almacenamiento y uso de los datos.

5.- El responsable del fichero y quienes intervengan en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal, están obligados al secreto profesional.

A partir de esta disposición, en caso que la ley sea aprobada, según lo dicho, los patronos deben inscribir ante la Agencia de Protección de Datos, todas sus bases de datos, de forma que el candidato o trabajador tenga derecho al acceso, verificación, rectificación y, eventualmente, a la cancelación de la información personal ahí contenida.

En términos generales se puede decir que la aprobación de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales implicará para los empleadores de nuestro país una serie de nuevas obligaciones que buscan la protección del derecho a la protección de la información de sus trabajadores y, en general, a toda persona que por cualquier razón le fue solicitada información en virtud de un proceso de reclutamiento y selección.

En este sentido se determina que las siguientes serían las principales obligaciones del empleador:

a) Solicitar únicamente la información relacionado con el puesto.
b) Registrar las bases de datos ante la Agencia de Protección de datos que se plantea en el proyecto de ley.
c) Informar al trabajador el motivo por el que se solicita la información y el uso que se hará de ella.

d) Permitir al trabajador la rectificación, actualización, cancelación o eliminación de sus datos personales.
e) Garantizar la confidencialidad de los datos personales recopilados.
f) Utilizar los datos recopilados únicamente con fines relacionados con el empleo.

Asimismo, la persona física o jurídica, de carácter público o privado; incluyendo a los empleadores que incumpla alguna de sus obligaciones, según el tipo de falta, se expondrá a una sanción. Las faltas que menciona el proyecto de ley son las siguientes:

ARTÍCULO 37.- Faltas leves

Serán consideradas faltas leves, para los efectos de esta Ley:

a) La recolección de datos personales para su uso en un archivo o base de datos sin hacer al interesado todas las advertencias especificadas en el artículo 4 de esta Ley.

b) Recolectar, almacenar y transmitir datos personales de terceros por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos.

ARTÍCULO 38.- Faltas graves

Serán consideradas faltas graves, para los efectos de esta Ley:

a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento expreso del titular de los datos, con arreglo a las disposiciones del artículo 4 de esta Ley.

b) Transferir datos personales a otras personas o empresas en Costa Rica en contravención a las reglas establecidas en el artículo 10 de esta Ley.

c) Transferir datos personales a otras personas o empresas radicadas en el extranjero en contravención a las reglas establecidas en el artículo 16 de esta Ley.

d) Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.

e) Negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases de datos, a fin de verificar su calidad, recolección, almacenamiento y uso conforme a esta Ley.

f) Negarse injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco.

ARTÍCULO 39.- Faltas gravísimas

Serán consideradas faltas gravísimas, para los efectos de esta Ley:

a) Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles, según la definición prevista en el artículo 7 de esta Ley.

b) Obtener de los titulares o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.

c) Revelar información registrada en una base de datos personales cuyo secreto estuviere obligado a guardar conforme la ley.

d) Proporcionar a un tercero información falsa a la contenida en un archivo de datos, con conocimiento de ello."

La comisión de alguna de las faltas descritas expondrá en este caso al patrono, alguna de las siguientes sanciones:

a) Para las faltas leves, una multa hasta cinco salarios base, conforme a la Ley N.º 7337.

b) Para las faltas graves, una multa de cinco a veinte salarios base, conforme a la Ley N.º 7337.

c) Para las faltas gravísimas, una multa de 15 a 30 salarios base, conforme a la Ley Nº 7337; y la suspensión para el funcionamiento del fichero de uno a seis meses.

Se considera necesario indicar que la ley que se propone vendría a resolver un tema que ha ocasionado confusiones en su aplicación y la posibilidad que algunos empleadores utilicen la información sensible del trabajador para fines no relacionados con el empleo. Incluso, este mismo criterio se expresa en la exposición de motivos de la Comisión de Asuntos Jurídicos de la Asamblea Legislativa, en el dictamen de mayoría, como una de las consideraciones más importantes señala lo siguiente:

> *Hoy más que nunca, las informaciones adquieren un enorme valor económico. Esto es particularmente cierto en el caso de las transacciones bancarias y financieras en general, pero sobre todo en aquellos ámbitos en donde es posible construir una imagen de los ciudadanos a partir de su interacción con la sociedad y con los medios tecnológicos dispuestos para garantizar el acceso a los datos e informaciones que requiere para realizar su plan de vida y los objetivos que se haya planteado*[24]*.*

La propuesta se basa, principalmente, en la necesidad de regular la protección de datos del ciudadano a partir de los inconvenientes que se han generado con el manejo que muchas entidades bancarias, a nivel nacional, han venido dando a la información de sus clientes, reconociendo la problemática como "*un verdadero riesgo vital en una sociedad profundamente marcada por la necesidad de intercambiar datos e informaciones"*[25]*.*

Sin embargo, la ley no resolverá el tema en definitiva si, tanto los empleadores como los trabajadores de nuestro país, no incluyen la protección de datos sensible del

[24] Comisión Permanente de Asuntos Jurídicos de la Asamblea Legislativa de la República de Costa Rica. Ley de Protección de la Persona Frente al Tratamiento de sus datos personales. Expediente número 16 679. Dictamen afirmativo de mayoría del 26 de noviembre de 2008.
[25] Ídem,

personal como uno de sus valores que se expresen en las políticas de las organizaciones.

Los mecanismos para violentar la norma siempre existirán, en realidad se trata de un tema de conciencia por el respeto de los derechos de los trabajadores.

TÍTULO SEGUNDO: LA PROTECCIÓN DE DATOS DEL TRABAJADOR DURANTE LA RELACION LABORAL

CAPÍTULO I. LÍMITES AL MONITOREO DEL TRABAJADOR

A. GARANTÍAS PARA EL TRABAJADOR

1. Límites que debe respetar el empleador

La Protección de Datos del trabajador implica un régimen de protección, respeto y de algunos valores o bienes jurídicos a los que la sociedad brinda un amparo especial. Como tal, esta regulación debería, además, implicar el derecho de los trabajadores al respeto de tales garantías y, consecuentemente, la obligación de la contraparte, es decir, del patrono, a respetar y hacer cumplir esos deberes.

En una relación laboral, el patrono, como parte solicitante de información necesaria para la contratación del trabajador, está obligado a respetar algunos límites que no son otros que los derechos que le corresponden al trabajador en cuanto a la disposición y el uso de sus datos personales, y que, en la opinión de quien ejecuta este trabajo de investigación, se resumen en los siguientes tópicos: el consentimiento del uso de la información personal y la pertinencia de los datos solicitados.

1.1. El consentimiento para el uso de datos personales

El consentimiento para el uso de datos personales constituye el requisito básico para que la recopilación de información y, su posterior uso dentro de los parámetros permitidos por la ley, sea considerado como válido.

A modo de ejemplo, la ya citada norma argentina de Ley de Protección de Datos, habla de consentimiento informado, como "*aquel que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural*"[26].

En España, la regla general es que para realizar cualquier tratamiento de datos de una persona se precisa su consentimiento. Sin embargo, existen algunas excepciones como la establecida en el artículo 6.2 de la Ley Orgánica de Protección de Datos, que establece que "*no será necesario el consentimiento cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*". Por ejemplo, podrían ser considerados como necesarios los datos de los trabajadores para gestionar su vinculación laboral con la empresa o bien los datos para llenar las planillas de pago o de seguridad social.

Si bien no es necesario un consentimiento expreso del trabajador, la empresa debe cumplir con el deber de comunicar al trabajador sobre la existencia de un fichero de información enviado a las autoridades administrativas correspondientes (en nuestro país, por ejemplo, la Caja Costarricense de Seguro Social o el Instituto Nacional de

[26] Al respecto, véase el artículo número 6 de la Ley de la República de Argentina número 25.326.

Seguros), ya que éste tiene derecho a consultar dicha información y solicitar la rectificación de la misma en caso de ser necesario.

En Costa Rica no existe una disposición expresa que regule el tema aplicado a la realidad laboral. Sin embargo, el proyecto para la "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" establece algunas reglas que, en caso de aprobarse, deberán ser observadas por el patrono.

Por ejemplo, el artículo 5 de dicho proyecto de ley establece como necesario el consentimiento del interesado para que la información solicitada forme parte de los registros o las bases de datos. Establece además la posibilidad de que el trabajador revoque en cualquier momento el consentimiento, lo cual, más que una revocación, será una nueva manifestación del trabajador, en este caso, dirigida a la eliminación de dicha información.

A su vez, el proyecto de ley plantea algunos casos en los que no sería necesario el consentimiento expreso del ciudadano, en este caso, del trabajador. Estos supuestos se establecen en el artículo 5 del proyecto, que en lo que interesa dispone:

No será necesario el consentimiento cuando:

b) *Exista orden motivada, dictada por autoridad judicial competente.*
c) *Los datos se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limite a nombre, documento nacional de identidad y fecha de nacimiento, u otros datos que por ley especial tengan la misma condición.*

La posibilidad de buscar información en registros de acceso público ha sido aceptada, incluso, por la Sala Constitucional de la Corte Suprema de Justicia, que al efecto ha señalado:

> *Alega el recurrente que durante casi veinte años ha laborado como funcionario público destacado en diferentes oficinas, que ha procurado proteger de la mejor manera a sus hijos y aquellas persona que forman parte de su vida, motivo por el cual, ha tratado de que su información personal no sea divulgada de manera innecesaria en beneficio de sus seres queridos. No obstante, la semana pasada, se enteró de que el Tribunal recurrido dispuso otorgar un acceso directo en su página Web, en donde, cualquier persona tiene la posibilidad de consultar no solo los datos de filiación de cualquier costarricense y la edad, sino también los datos básicos de las personas con las cuales han estado casados cada uno de ellos. Además, es posible consultar el nombre de los hijos de estas personas y los datos del lugar en donde votan, lo que de manera indirecta fija un perímetro de donde pueden ser ubicados. En razón de lo anterior, el 03 de setiembre de este año, se presentó a las oficinas centrales del Tribunal recurrido a fin de que se le dieran las explicaciones pertinentes del caso, para lo cual, en la Oficina de Información de dicho Tribunal se le dieron varios motivos. Con base en las consideraciones dadas en la sentencia, se declara sin lugar el recurso*[27]*.*

A partir de esta disposición, la recomendación inicial para los empleadores se refiere a la obligación de advertir a los trabajadores que la información brindada durante su proceso de contratación es únicamente para efectos laborales con el empleador, o bien, que podría ser adjuntada a bases de datos a las que accedan otras compañías. El trabajador debe consentir esto y, preferiblemente, dejar prueba escrita de su decisión libre y voluntaria.

[27] Voto Número 3346 – 09. Sala Constitucional de la Corte Suprema de Justicia.

En otras áreas de control del trabajador, referidas a la seguridad de la información, es también necesario el consentimiento del trabajador. Por ejemplo, si bien los empleados pueden ser informados en el contrato de trabajo de que van a ser monitoreados a través de un equipo de circuito cerrado a la entrada del edificio, accesos, pasillos, entre otros; es recomendable que se informe a través de las políticas corporativas, incluso, colocando carteles que recojan las medidas a las que anteriormente se ha hecho referencia.

Siguiendo la posición de la corriente proteccionista argentina, se puede concluir que el empleador encuentra un límite esencial en el derecho del trabajador a consentir el conocimiento y tratamiento informático o no de sus datos personales. Es decir, se trata de la "*facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo*"[28].

1.2. La pertinencia de los datos solicitados al trabajador

Toda la información que recolecte un empleador, con respecto a un trabajador, debe ser consecuente con el puesto y las funciones que desempeñará para la compañía. Esto es conocido a nivel doctrinario como "Principio de Pertinencia" que, aplicado al ámbito laboral, debe ser entendido, sin más, como el límite que encuentra el empleador de solicitar únicamente aquella información que es verdaderamente relacionada con el puesto.

[28] Tomado de: www.protecciondedatos.com.ar; agosto 2008.

Por ejemplo, ¿para qué se necesitaría saber si un trabajador posee una condición que no es necesaria para el puesto al que inicialmente se contrata? El empleador debe limitarse a condiciones realmente necesarias para el desempeño del puesto y, en el mejor de los casos, a otro tipo de datos que sean necesarios para el crecimiento del trabajador dentro de la organización, con lo cual se cumpliría el requisito de pertinencia mencionado, es decir, no se permite incluir más (…) *datos que aquellos que sirvan o puedan servir para la consecución de la finalidad que justifica dicho tratamiento, que debió determinarse en el momento de la obtención del consentimiento, o que sirve para presumir la concurrencia de éste en los supuestos en que se establecen presunciones legales de su otorgamiento"*[29].

En síntesis, se trata solamente de solicitar información personal que tenga una relación directa con el puesto que se pretende contratar, pero, además, que obedezca a motivos objetivos que no sean utilizados como elementos de discriminación; por ejemplo, relacionados con el padecimiento de enfermedades o cuestiones médicas que afecten las habilidades técnicas del solicitante a un puesto.

[29] Salom, Jaiver Aparicio, "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Editorial Aranzadi. Pamplona, España, 2000, p. 95.

2. Los derechos del trabajador frente a las posibilidades de recolección y uso de datos por parte del empleador

Una vez definidos los derechos inherentes al trabajador y los límites que debe respetar el patrono, en cuanto al uso de datos del trabajador, resulta procedente analizar cuáles son los mecanismos o herramientas legales con los que cuenta el trabajador contratado para reclamar y buscar el resarcimiento, en aquellos casos en los que se han visto violentados los derechos que como ciudadano le corresponden. Antes de analizar las posibilidades legales que implicarían un litigio, se deben tomar en cuenta algunas recomendaciones prácticas, con la intención de evitar un conflicto administrativo o judicial.

2.1. Algunos derechos del trabajador

A partir del fundamento doctrinario de la teoría de protección de datos, existen algunos derechos del ciudadano que pueden traerse al campo del derecho laboral y que, además, resultan aplicables al caso:

Derecho de oposición: Es la posibilidad del titular de los datos personales a negarse a facilitar un dato de carácter personal, en caso que no sea obligatorio hacerlo. Es decir, durante todo el proceso de contratación y, más allá, durante el desarrollo de la relación laboral, el empleador debe advertir al trabajador que tiene la posibilidad de decidir qué información proveer, además de las consecuencias de no facilitar dicha información.

A modo de ejemplo, durante la solicitud de trabajo o en la entrevista que se aplique al trabajador se le debe indicar que tiene la posibilidad de no contestar alguna pregunta que puede causarle algún perjuicio. Este breve cuidado, si bien no garantiza que la información obtenida se utilice para otros fines, puede ser considerado como una manifestación de buena fe entre las partes, principio que, como en todo acuerdo negocial, debe imperar con especial preponderancia en las relaciones obrero patronales.

Existe alguna información que será necesaria conocer por parte del patrono. Por ejemplo, si se contrata un chofer saber si cuenta con licencia de conducir y record al volante; pero, por el contrario, no es necesario conocer si tiene o no deudas en el sistema bancario nacional. En este caso, el trabajador podría oponerse a brindar esa información o, en su defecto, reclamar los perjuicios que pueda sufrir cuando sea utilizada por medios no autorizados por el trabajador.

Derecho de información: El trabajador tiene derecho a que se le informe, con anterioridad, la finalidad de los datos recopilados por el empleador y quiénes pueden ser sus destinatarios. Asimismo, debe conocer donde se almacenará dicha información, tanto en medios físicos como electrónicos, teniendo la posibilidad de accesarlos en cualquier momento para verificar si existe alguna información que ha dejado de ser la vigente al momento de la revisión.

2.2. Acciones legales del trabajador

El trabajador tiene la posibilidad de buscar en la ley la rectificación de los datos que posea el empleador y, eventualmente, el derecho a buscar una indemnización en caso de producirse un grave perjuicio para él. En nuestro país, ante la falta expresa de legislación, el trabajador, como cualquier ciudadano costarricense, tendría derecho a acudir a los tribunales de justicia para buscar el reparo que le corresponda, principalmente, a través de dos vías: el recurso de amparo en sede constitucional y la vía judicial en sede laboral.

2.2.1. El recurso de amparo

En Costa Rica, el derecho a la intimidad, la privacidad, y con ello a la autodeterminación informativa que conlleva la protección de datos, encuentra el fundamento legal en las regulaciones ya mencionadas en la Constitución Política. Por ello, deben ser tutelada por medio del Recurso de Amparo, tal y como se tutelaría cualquier derecho de con rango constitucional.

Esto es así porque el artículo primero de la Ley de la Jurisdicción Constitucional establece lo siguiente:

> *Artículo 1.- La presente Ley tiene como fin regular la jurisdicción constitucional, cuyo objeto es garantizar la supremacía de las normas y principios constitucionales y del Derecho Internacional o Comunitario vigente en la República, su uniforme interpretación y aplicación, así como los derechos y*

libertades fundamentales consagrados en la Constitución o en los instrumentos internacionales de derechos vigentes en Costa Rica.

En igual sentido, el artículo 29 de la Constitución Política establece que es el recurso de amparo la vía idónea para la protección del derecho a la intimidad, relacionado con la protección de datos de un trabajador. Establece el citado artículo:

Artículo 29.- El recurso de amparo garantiza los derechos y libertades fundamentales a que se refiere esta ley, salvo los protegidos por el de hábeas corpus.

Procede el recurso contra toda disposición, acuerdo o resolución y, en general, contra toda acción o simple actuación material no fundada en un acto administrativo eficaz, de los servidores y órganos públicos, que haya violado, viole o amenace violar cualquiera de aquellos derechos.

El amparo procederá no sólo contra los actos arbitrarios, sino contra las actuaciones u omisiones fundadas en normas erróneas interpretadas o indebidamente aplicadas.

En un material de investigación preparado en la Facultad de Derecho de la Universidad de Costa Rica sobre el tema, se indica que:

…la Sala Constitucional de la Corte Suprema de Justicia, el 23 de mayo de 1995, ante un recurso de amparo presentado contra el Organismo de Investigación Judicial, manifestó que una persona, erróneamente incluida en el Archivo de Criminales, tiene todo el derecho a que su nombre sea eliminado de él y a recibir el pago de daños y perjuicios que le hubiere ocasionado tan errónea inclusión. En un sentido similar, la misma Sala ha reconocido el secreto

y confidencialidad de ciertas informaciones, como por ejemplo, un caso importante es la protección del secreto profesional. En el voto 2251-91, del 5 de noviembre de 1991, la Sala rechazó un pedido de un ciudadano de tener acceso a «documentos que la Junta Directiva de la C.C.S.S. conoce el resolver gestiones.» Para son ejemplos claros de lo que resolvería la Sala Constitucional en un recurso de Habeas Data, con la importante salvedad de un plazo, sin duda alguna, más expedito [30].

Concluyendo este punto se debe hacer referencia a la propuesta establecida en el proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales", el cual establece un recurso administrativo que el ciudadano afectado con la divulgación no autorizada de sus datos sensibles podrá interponer ante la Agencia de Protección de Datos.

Este recurso se encuentra establecido en el artículo 12 del citado proyecto de ley, y dispone lo siguiente:

ARTÍCULO 12.- Garantías efectivas

1.- Todo interesado tiene derecho a un recurso administrativo sencillo y rápido ante la Agencia de Protección de Datos, con el fin de ser amparada contra actos que violen sus derechos fundamentales reconocidos por esta Ley. Lo anterior sin perjuicio de las garantías jurisdiccionales generales o específicas que la Ley establezca para este mismo fin.

[30] Informacion tomada de www.derecho.ucr.ac.cr./~gapmerayo/cursos/cursoDI/trabajosclase/habdata/habdata, junio 2008.

2.- Toda persona tiene derecho a controlar que sus datos personales existentes en ficheros públicos o particulares cumplan con las reglas previstas en esta Ley, y a obtener en su caso la correspondiente indemnización por los daños y perjuicios que hubieren sido ocasionados en su persona o intereses debido al uso de sus datos personales.

2.2.2. El reclamo en sede laboral

La posibilidad de reclamar frente a los abusos del patrono puede, en algunos casos, implicar denuncias en la sede laboral ordinaria, "*solicitando la extinción del contrato de trabajo por modificación sustancial de las condiciones de trabajo que redunden en perjuicio de su dignidad. Y ello sin menoscabo de la posibilidad de acudir a la vía penal si la conducta del empresario fuese constitutiva de delito o falta*"[31].

El caso específico que interesa analizar es la posibilidad del trabajador de dar por finalizada la relación laboral cuando el patrono incumpla de forma grave sus obligaciones. El trabajador dejaría una condición donde le resulta imposible continuar una relación laboral.

La legislación laboral en Costa Rica establece diferentes formas de terminación de la relación laboral, entre las que se encuentran las siguientes:

- Renuncia del trabajador.
- Despido con o sin justa causa.

[31] Información tomada de http://www.weblaboral.net/aop/aop0014.htm. junio 2009.

- Rompimiento unilateral del trabajador.
- Causas ajenas a la voluntad de las partes.
- Incapacidad (después de 3 meses), jubilación o muerte del trabajador.
- Fuerza mayor y caso fortuito.
- Insolvencia, quiebra, incapacidad o muerte del patrono.
- Cumplimiento de obligaciones legales que impidan la prestación del servicio o arresto del trabajador.

El caso que se analiza tiene que ver con la posibilidad del trabajador de romper de forma unilateral el contrato de trabajo, situación prevista en el artículo 83 del Código de Trabajo que, literalmente, dispone lo siguiente:

Artículo 83.-

Son causas justas que facultan al trabajador para dar por terminado su contrato de trabajo:

a) Cuando el patrono no le pague el salario completo que le corresponda, en la fecha y lugar convenidos o acostumbrados. Quedan a salvo las deducciones autorizadas por la Ley;

b) Cuando el patrono incurra durante el trabajo en falta de probidad u honradez, o se conduzca en forma reñida con la moral, o acuda a la injuria, a la calumnia o a las vías de hecho contra el trabajador;

c) Cuando un dependiente del patrono o una de las personas que viven en casa de éste, cometa, con su autorización expresa o tácita, alguno de los actos enumerados en el inciso anterior contra el trabajador;

d) Cuando el patrono directamente o por medio de sus familiares o dependientes cause maliciosamente un perjuicio material en las herramientas o útiles de trabajo del trabajador;

e) Cuando el patrono o su representante en la dirección de las labores acuda a la injuria, a la calumnia o a las vías de hecho contra el trabajador fuera del lugar donde se ejecutan las faenas y en horas que no sean de trabajo, siempre que dichos actos no hayan sido provocados y que como consecuencia de ellos se haga imposible la convivencia y armonía para el cumplimiento del contrato;

f) Cuando el patrono, un miembro de su familia, o su representante en la dirección de las labores u otro trabajador esté atacado por alguna enfermedad contagiosa, siempre que el trabajador deba permanecer en contacto inmediato con la persona de que se trate;

g) Cuando exista peligro grave para la seguridad o salud del trabajador o de su familia, ya sea por carecer de condiciones higiénicas el lugar de trabajo, por excesiva insalubridad de la región o porque el patrono no cumpla las medidas de prevención y seguridad que las disposiciones legales establezcan;

h) Cuando el patrono comprometa con su imprudencia o descuido inexcusable, la seguridad del lugar donde se realizan las labores o de las personas que allí se encuentren;

i) Cuando el patrono viole alguna de las prohibiciones contenidas en el artículo 70; y

j) Cuando el patrono incurra en cualquier otra falta grave a las obligaciones que le imponga el contrato.

La regla que contiene el párrafo final del artículo 81 rige también a favor de los trabajadores.

Como se desprende de la lectura de la lista de causales de solicitud de terminación de la relación laboral por parte del trabajador, no existe – al menos de forma expresa – ninguna posibilidad que el trabajador solicite la terminación del contrato de trabajo en el caso que el empleador utilice de forma indebida la información suministrada voluntariamente o de alguna forma recopilada y relacionada directamente con el trabajador. Incluso, los artículos 70 y 71 del Código de Trabajo establecen una serie de obligaciones y prohibiciones para el patrono y ninguna se relaciona con la protección de datos sensibles del personal.

La Sala Segunda de la Corte Suprema de Justicia se ha referido a la posibilidad del trabajador de dar por finalizada la relación laboral, estableciendo una clara diferencia entre la renuncia del trabajador y el despido sin responsabilidad patronal que puede ejercer el patrono ante una falta grave. Así una importante sentencia de esta órgano judicial señala lo siguiente:

> **III.- ACERCA DE LA FINALIZACIÓN DE LA RELACIÓN LABORAL POR LA VOLUNTAD UNILATERAL DEL TRABAJADOR:** Antes de entrar a examinar el caso en estudio, deben hacerse algunas consideraciones de orden teórico y jurisprudencial sobre la materia. No debe confundirse la renuncia al trabajo con el rompimiento o disolución justificada del contrato, por parte de la persona

asalariada. Resulta fundamental distinguir entre las dos figuras, pues aunque ambas dependen de la voluntad del trabajador, las indemnizaciones que se derivan de cada modalidad varían. Así, cuando el empleado renuncia, no se hace acreedor del pago del preaviso y del auxilio de cesantía, mientras que, en caso de ruptura justificada del contrato, sí existe responsabilidad patronal (artículo 83 del Código de Trabajo). La renuncia es una típica manifestación de la autonomía de la voluntad, consciente y unilateral, que encuentra amparo en el artículo 28 del Código de Trabajo, mediante la cual la parte trabajadora extingue el vínculo jurídico que la une a su patrona, sin más obligación que la de otorgarle el preaviso o la de pagarle la indemnización sustitutiva. Por tratarse de un acto jurídico unilateral, no requiere del concurso de otro –aceptación– ni de la existencia de una causa justa para ser plenamente eficaz, y lo es desde el momento mismo en que se expresa y se comunica, salvo, claro está, que se haga depender de alguna condición o término. Aunque nada impide que pueda existir, también, una aceptación de la renuncia, es lo cierto que la negativa del empleador o de la empleadora a admitirla, no la deja sin efecto (consultar los Votos N°s. 66 de las 9:20 horas del 27 de febrero y 120 de las 10:00 horas del 6 de mayo, ambos de 1998). La segunda figura, por su parte, también conocida como despido indirecto o autodespido, previsto, en lo fundamental, por el numeral 84, en concordancia con el 83 ibídem, consiste en *"la disolución del contrato de trabajo por iniciativa del trabajador, basándose en las que califica de justas causas para ello debidas al patrono o al empresario. Para Russomano, se está ante un acto del empresario por el cual se crean condiciones que imposibilitan la continuidad de la prestación de servicios. El patrono no declara la rescisión contractual, pero, al violar sus deberes legales y contractuales, coloca al trabajador, so pena de perjuicios morales y económicos, en el trance de no poder proseguir sus tareas en la empresa."* (CABANELLAS (Guillermo), Compendio de Derecho Laboral, Tomo I, Bibliográfica Omeba, Buenos Aires, 1968, p. 778). Al respecto, la Sala ha resuelto:

> *"Sin duda, un acto de esa naturaleza constituye una modalidad de despido, es decir, un acto del empleador, que se manifiesta, en la realidad, como encubierto o velado. Por su medio, el patrono ubica al trabajador en una difícil posición: mantener su trabajo a costa de la vulneración de sus derechos o concretar, en la práctica, lo que aquél no ha tenido la deferencia de hacer. En estos casos, la resolución del contrato laboral no es, entonces, imputable al trabajador, aunque sea una acción suya la que le haya dado efectividad, sino que tiene su causa en la voluntad unilateral del empresario, exteriorizada irregularmente. Se trata, pues, de un típico cese patronal que es evidentemente contrario a la buena fe, que debe imperar siempre en toda relación jurídica y más aún en las laborales."* (Voto N° 141 de las 16:00 horas del 4 de julio de 1997).

> Ahora bien, cuando la persona asalariada decide romper la relación con plena responsabilidad patronal, ″necesariamente″ debe comunicárselo así a su contraparte, indicándole, también, los hechos en que se fundamenta. De igual modo, considerando tanto la necesaria estabilidad del contrato de trabajo, su contenido ético y los principios de buena fe y de equidad, que resultan consustanciales a los vínculos jurídicos laborales o de servicio, como la envergadura de la máxima medida a la que puede recurrir la parte afectada por un despido encubierto, la jurisprudencia ha sido conteste en señalar que, por regla general, de previo a ejecutarla, es preciso procurar el agotamiento de las vías conciliatorias (ver, sobre el particular, los votos N°s. 88 de las 9:30 horas del 21 de abril de 1992; 21 de las 10:00 horas del 21 de enero, 31 de las 15:10 horas del 26 de enero, 284 de las 10:10 horas del 30 de setiembre, los tres de 1994; 80 de las 14:00 horas del 1° de marzo de 1995; 281 de las 9:00 horas del 14 de noviembre de 1997; 131 de las 14:50 horas del 27 de mayo y 318 de las 9:30 horas del 23 de diciembre, ambos de 1998; y 354 de las 10:10 horas del 12 de noviembre de 1999). En definitiva, la parte asalariada no puede recurrir a las vías de hecho y romper el contrato de trabajo, unilateralmente y con responsabilidad patronal, sin el indispensable y oportuno requerimiento a su contraparte. Además, a efecto de evitar que se incurra en abusos, con perjuicio directo para la parte empleadora, las causas que originan esa medida deben ser diáfanas y han de tener un adecuado sustento probatorio, recayendo la carga de la prueba en el trabajador (ver el Voto N° 184 de las 14:10 horas del 14 de julio de 1999). En materia de carga probatoria, se ha señalado que, en el Derecho Procesal Laboral, normalmente, es el patrono demandado, sobre quien recae una mucho mayor responsabilidad –no toda–, en cuanto a la aportación de la prueba relacionada con las particularidades de la relación de trabajo; por cuanto, al ser la parte más fuerte de la contratación, tiene mayor facilidad de preconstituir, durante el transcurso de la relación, la tendente a demostrar los normales hechos aducidos, en un juicio de tal naturaleza laboral. Sin embargo, también está claro que, esa mayor responsabilidad del patrono está referida, precisamente, a los elementos normales de una contratación de ese tipo y, además, que ello no puede implicar, jurídica ni legítimamente, una liberación total, para el trabajador, de su propia e ineludible carga probatoria; pues, respecto de ciertos hechos, sobre él pesa, siempre y necesariamente, aquel determinado ″onus probandi″. (Sobre este tema puede consultarse PASCO COSMÓPOLIS (Mario), Fundamentos de Derecho Procesal del Trabajo, Editorial AELE, segunda edición, 1997). [32]

La falta de regulación específica que en mi concepto existe en el campo laboral, hace que existan trabajadores que no hayan ejercido ningún reclamo en contra de sus

[32] Resolución número 784 – 2000. Sala Segunda de la Corte Suprema de Justicia.

patronos, toda vez que podría considerarse necesario para la aceptación de la demanda la demostración de un daño tangible que sufrido por el trabajador.

En casos donde el empleador utilice o manipule la información del trabajador sin causar perjuicio deberían considerarse también como violaciones al tratamiento confidencial de la información personal del trabajador. Por ejemplo, el encargado de Recursos Humanos que facilita una hoja de vida a otro contacto fuera de la empresa, a criterio de esta investigación, claramente está utilizando la información para un fin diferente haya o no producido un perjuicio para el trabajador.

En las condiciones actuales un reclamo interpuesto por este motivo resultaría difícil que se declare a favor del trabajador, aunque haya lesionado su privacidad, lo cual entonces limita la posibilidades de poder controlar en qué medida, en nuestro país, se están presentado inconvenientes en este sentido.

Resulta diferente el caso en que el trabajador demuestre que el uso ilegítimo de la información, por parte de su patrono, ha resultado en una acción injusta que modifica claramente sus condiciones laborales. Por ejemplo, en el caso de un trabajador que es descartado de un proceso de reclutamiento y selección, de un ascenso no otorgado a un trabajador en virtud de una información obtenida sin su autorización, o bien, una acción disciplinaria impuesta a partir de información desactualizada o que claramente no tiene relación con el puesto que desempeña el trabajador.

En casos como este habría que distinguir entre dos situaciones distintas: primero, si se trata de un candidato que es descartado de un proceso de selección la

única opción para el afectado es acudir a la vía constitucional e interponer un recurso de amparo (habeas data) por la lesión causada a uno de sus derechos fundamentales, en este caso, la autodeterminación informativa. Esto es así, porque al no haber existido todavía una relación laboral, la jurisdicción del trabajo no sería aplicable al caso en particular.

Si la relación laboral se encuentra vigente y claramente existe una afectación para el trabajador, este podrá acudir a la vía ordinaria de trabajo donde planteará su acción. A criterio de esta investigación, a pesar del principio general que ordena que la carga de la prueba en materia laboral le corresponde al patrono, el resultado del juicio dependerá mucho de la posibilidad de poder demostrar, en la vía judicial, una relación directa entre el uso no autorizado de datos sensibles y la afectación sufrida por el trabajador. Más adelante se analizará el valor de la prueba en sede judicial, en casos como el que se plantea a modo de ejemplo.

B. FORMAS DE CONTROL DE DATOS DEL TRABAJADOR

El contrato de trabajo se caracteriza porque el trabajador realiza sus labores dentro del ámbito de organización y dirección del empresario, es decir, una relación de subordinación, lo que se traduce en la posibilidad del empleador de dar órdenes e instrucciones de carácter general o particular a su personal, las cuales debe respetar el trabajador. Esto es lo que en teoría se llama el poder de dirección del patrono.

Ese poder de dirección no es un derecho absoluto sino que está sometido a una serie de limitaciones, entre las que se derivan la obligación del empresario de respetar la intimidad y las consideraciones debidas a la dignidad de los trabajadores en todas y cada una de las etapas que componen el desarrollo de una relación laboral, desde la etapa precontractual hasta la extinción del contrato de trabajo.

Es por ello que, en atención a los procesos para el control de datos del trabajador, existen algunos elementos que deben ser considerados para que los procesos internos que establezca una empresa se encuentren dentro de un marco de legalidad y se protejan los más íntimos derechos del trabajador.

1. Requisitos de validez para el control de datos del trabajador

Una vez delimitados los bienes jurídicos que debe proteger un empleador en cuanto a la recopilación y uso de datos personales del trabajador, se considera que existen algunos aspectos que se pueden llamar de validez y parecen necesarios para la validez de los procedimientos internos que implemente un empleador en su empresa. Son los siguientes:

1.1. Comunicación oportuna de los procedimientos

La comunicación previa, al personal, de una organización en relación a los procedimientos mediante los que el empleador puede obtener, antes y durante la relación laboral cualquier dato sensible del trabajador, es uno de los principales

requisitos de legalidad para la aplicación y aceptación de tales formas de control y registro de datos.

Comunicar oportunamente al trabajador estos procedimientos representa cumplir con la buena fe que corresponde, en este caso al empleador, en cuanto a la aplicación de sistema y niveles de seguridad de protección de la información que he mencionado a lo largo de este trabajo de investigación. No solamente basta la comunicación oportuna sino que, además, sería considerado como un requisito de legalidad para la formación de archivos y bases de datos, sobre todo si finalmente resultara aprobado el proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales", en cual señala que debe existir, además de un simple consentimiento del trabajador, un consentimiento realmente informado para que el trabajador conozca las reglas que regirán el uso de su información personal.

En síntesis, se trata de establecer reglar claras, amparadas por normas y procedimientos internos que regulen la aplicación de procesos de control de datos y que deben ser comunicadas desde el inicio de la relación laboral, o desde el momento de su puesta en práctica cuando ya ha iniciado el contrato de trabajo; por lo que es recomendable que se firme una hoja de conformidad una vez leída y comprendida la política del empleador en esta materia. De esta forma, se lograría que los procesos de obtención, verificación y uso de información definidas por el patrono no puedan ser considerados como arbitrarias.

1.2. Obligación de confidencialidad aplicada a la protección de datos sensibles

En términos generales, la obligación de confidencialidad aplicada a la protección de datos sensibles puede ser definida como la obligación del patrono de respetar y garantizar la confidencialidad de la información del trabajador obtenida en cualquiera de las fases del proceso de contratación y que, en algunos casos, deberá subsistir aun después de finalizada la relación laboral. Este deber de confidencialidad responde a la finalidad de evitar que la información salga del círculo de personas a quienes está destinada, es decir, el uso para fines laborales que debió ser autorizado por el trabajador previamente.

El proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" establece la obligación que le correspondería al empleador como usuario de dicha información. De forma específica, el artículo 9 del citado proyecto establece:

> ***ARTÍCULO 9.- Deber de confidencialidad***
>
> *El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto después de finalizada su relación con el archivo de datos. El obligado podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.*
>
> *Las comisiones legislativas que por disposición constitucional y reglamentarias les confiera atribuciones de investigación, tendrán acceso a los archivos y bases*

de datos, siempre que se enmarquen estrictamente en el ámbito de las competencias asignadas.

Esta obligación de confidencialidad conlleva la necesidad, para el empleador, de instaurar procesos de seguridad internos con el fin de limitar el libre acceso a la información del personal, salvo casos previamente justificados, como sería por orden judicial o por situaciones de salubridad claramente definidas. Es decir, el patrono debe asegurarse que la información, sea que conste en medios físicos o electrónicos, se encuentre claramente resguarda, conservada en un lugar seguro y que sea accesada únicamente por las personas que requieran su consulta para la toma de decisiones de carácter estrictamente laboral.

El tema de la confidencialidad, tan en boga en nuestra actualidad, ha dejado de ser una simple forma de protección de algunas empresas interesadas en resguardar sus más íntimos secretos comerciales e industriales y, afortunadamente, poco a poco se convierte en una obligación que opera para ambas parte de la relación laboral, ya que son ahora más los casos en los que la empresa se compromete a resguardar la información personal del trabajador. Por ejemplo, desde octubre del 2005, en Argentina se publicaba un artículo periodístico que señala que cada vez más *"en las empresas aparte del contrato de trabajo existirá una tendencia a que se firmen contratos de confidencialidad"*[33].

En Costa Rica, la situación es similar: cada día las empresas se protegen más y cuentan con esquemas para la protección de información confidencial. Sin embargo,

[33] Información tomada de: www.infobaeprofesional.com/notas/20352-Bases-de-datos-empresas-deberan-firmar-acuerdos-de-confidencialidad.html; julio 2009.

se ha quedado en una protección de información que solamente es propiedad del empresario, definida por criterios estrictamente comerciales.

Al respecto se sugiere es que estos procesos de confidencialidad apunten a la inclusión de la información de los trabajadores, clasificándola de carácter altamente sensible. Se considero que debe existir un cambio en la visión de las empresas, ya que en la actualidad la información del trabajador no representa mayores niveles de seguridad.

Es posible que en caso de aprobarse la regulación específica sobre el tema y al verse las empresas expuestas a sanciones económicas, empiecen de forma progresiva a incluir las protecciones necesarias para el cumplimiento de la norma constitucional que asegura la protección de la información confidencial del trabajador.

2. Algunos ejemplos del control de datos del trabajador

Son muchos los sistemas, políticas o procedimientos internos que puede implementar una empresa relacionados con el control de datos del trabajador. Es imposible dar una lista única, ya que depende de la actividad de la empresa y también de los avances de la tecnología aplicable a cada sector de la producción.

Es por esta imposibilidad de definir un proceso único aplicable a todas las empresas, que se recomienda que los empleadores cumplan con los requisitos de legalidad propuestos en esta tesis, y que respeten los derechos legales y

constitucionales examinados en esta investigación, es decir, la intimidad, dignidad y autodeterminación informativa de todos sus trabajadores.

La legislación laboral costarricense no contiene una norma clara y precisa que señale expresamente las obligaciones y derechos del trabajador, pero principalmente del empleador. Sin embargo, se considera que los patronos no deberían aprovecharse de este vacío legal para utilizar de forma indebida, por desconocimiento o mala fe, la información que de forma voluntaria fue suministrada por el trabajador. La obligación del operador jurídico es hacer una lectura cuidadosa e integral de la legislación aplicable, partiendo de las disposiciones de la Constitución Política que puedan ser de aplicación al ámbito laboral, y que deberían ser la primera guía para el respeto de los valores y principios constitucionales que regulan la materia.

Lo ideal sería llegar a una regulación expresa en el tema laboral, tal y como lo hace ahora la legislación española, la cual contiene indicaciones expresas que regulan los límites que debe respetar el empleador en cuanto a la aplicación de procesos de control de datos. Así, el artículo 18 del Estatuto de los Trabajadores de España señala lo siguiente:

> *Art 18.-Inviolabilidad de la persona del trabajador*
>
> *Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un*

representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

La intención del legislador es señalar que el patrono puede, dentro de los límites permitidos, establecer los procedimientos que considere adecuados, los cuales está obligado a cumplir el trabajador, siempre que con ello no se le cause ningún perjuicio. Con más detalles, el artículo 20 del Estatuto de los Trabajadores de España, señala lo siguiente:

Art 20.-Dirección y control de la actividad laboral

1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien éste delegue.

2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe.

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

Es así como, a partir de los deberes y obligaciones, tanto del patrono como del trabajador, y en aplicación a la realidad de nuestro país, se incluye un análisis de algunas formas de monitoreo y control, principalmente en los casos que se obtiene algún nivel de apropiación de la información personal del trabajador por parte del empleador.

2.1. El control del correo electrónico

El uso de un correo electrónico corporativo, propiedad del empleador y facilitado al trabajador como una mera herramienta de trabajo, dio lugar a que muchos empleadores instauren la práctica de controlar los datos enviados y recibidos a través de este procedimiento y que, en muchas ocasiones, contiene información que va más allá de lo estrictamente laboral.

En su momento, esta situación generó toda una polémica a nivel internacional y, pese a las diferentes posiciones, no se ha podido establecer una, debido al roce que existe con la protección de la intimidad del trabajador. Por ejemplo, en Estados Unidos la vigilancia de las comunicaciones electrónicas y telefónicas de los trabajadores es una realidad para tres cuartas partes de la fuerza laboral, y si bien los grupos de defensa de los derechos civiles llevan varios años elevando sus protestas contra los abusos a los que puede prestarse el sistema, el Congreso de esa Nación ha introducido varias iniciativas legislativas que, lejos de anular o limitar la práctica corporativa de vigilar los *emails* de sus empleados, obligan a las empresas informar acerca de su política de vigilancia.

En esta misma línea, en Inglaterra, además de oficializar el uso de programas de espionaje y pese a la oposición de los sindicatos británicos, el gobierno del Primer Ministro Blair dispuso una norma que permitió que los empresarios controlen el correo electrónico y las llamadas telefónicas que realicen sus empleados desde su lugar de trabajo, siempre que existan razones justificadas. Esta iniciativa coincide con otra que obligó a las empresas prestadoras de servicios de acceso a Internet a reportar a la policía todos los movimientos que realicen en la red las personas que se encuentren sospechadas de cometer alguna actividad delictiva[34].

En Argentina, los tribunales de Justicia han sido claros al señalar que el empresario debe delimitar las condiciones de uso de la herramienta de trabajo, dentro de los límites legales y siempre que no se perturbe la intimidad del trabajador. Así se desprende del siguiente extracto de una resolución judicial de aquel país:

> *... las condiciones de confidencialidad de acceso por parte del empleador al "correo-herramienta", otorgado al trabajador como consecuencia de una relación laboral deben ser amplias, y ello encuentra sustento en que no se prive al trabajador de verdaderas herramientas tecnológicas imprescindibles para el desarrollo de cualquier trabajo. Si una empresa no tiene una política clara en el uso de esta herramienta, no advirtiendo al empleado que dicho uso debe ser realizado exclusivamente en función de su actividad laboral y haciéndole conocer el derecho de la compañía a controlar el correcto uso del e-mail, podría crear una falsa expectativa de privacidad.* (CNTrabajo, Sala VII de la Corte Suprema de Justicia, República de Argentina. "Pereyra, Leandro Ramiro c/ Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. s/ Despido". 27/03/2003)[35].

[34] Tanús, Gustavo Daniel. Alguien te está mirando. Artículo publicado en Information Technology, revista editada por Mind Opener S.A. Edición Nº 50 - Noviembre 2000, pág. 144. Buenos Aires, Argentina. Tomado de //www.protecciondedatos.com.ar; julio 2009.
[35] Información tomada de http://www.protecciondedatos.com.ar, agosto 2008

A pesar de lo dicho, en Argentina, el 04 de julio de 2008 entró en vigencia la ley 26.388 sobre delitos informáticos que penaliza con prisión, de hasta seis meses, a quien acceda sin autorización o desvíe un correo electrónico que no le esté dirigido, con lo cual se reafirma todavía más la prohibición del empleador de leer correos electrónicos enviados o recibidos por sus trabajadores.

De aquí entonces que (*…) el contenido de tal prohibición no es otro que la violación del derecho a la privacidad del trabajador, facultad que no comporta un elemento configurativo del débito contractual y que, por ello, hace a la indiscutible e impenetrable dignidad y autodeterminación que como sujeto titulariza el trabajador* [36].

La doctrina internacional suele decir que los casos más controvertidos en la materia surgen del derecho español, en particular, de los fallos del Tribunal Superior de Justicia de Cataluña. Por ejemplo, la sentencia de fecha 14 de noviembre de 2000 en la demanda instaurada por un empleado del *Deutsche Bank*, quien había sido despedido por haber enviado 140 *e-mails* personales en cinco semanas a través de los servidores de la empresa cuando estaba explícitamente prohibida por la normativa del banco. El Tribunal entendió que no correspondía proceder a indemnizar al mismo pues "*concurre así un acreditado incumplimiento laboral del trabajador sancionado", ya que su actitud "supone la pérdida de tiempo de trabajo efectivo, tanto del trabajador al confeccionar y enviar los mensajes como de sus compañeros al recibirlos y leerlos"*.

[36] Durrieu, Roberto. El e – mail y el derecho a la intimidad. Artículo publicado en la edición digital de El Periódico La Nación de Argentina, el 20 de julio de 2008.

De igual forma, el Tribunal Supremo español, señaló en un interesante caso lo siguiente:

> ***Tercero.-*** *Estas consideraciones muestran que el artículo 18 del Estatuto de los Trabajadores no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral. El artículo 18 del Estatuto de los Trabajadores establece que "sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo", añadiendo que en la realización de estos registros "se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible". El supuesto de hecho de la norma es completamente distinto del que se produce con el control de los medios informáticos en el trabajo. El artículo 18 está atribuyendo al empresario un control que excede del que deriva de su posición en el contrato de trabajo y que, por tanto, queda fuera del marco del artículo 20 del Estatuto de los Trabajadores. En los registros el empresario actúa, de forma exorbitante y excepcional, fuera del marco contractual de los poderes que le concede el artículo 20 del Estatuto de los Trabajadores y, en realidad, como ha señalado la doctrina científica, desempeña –no sin problemas de cobertura– una función de "policía privada" o de "policía empresarial" que la ley vincula a la defensa de su patrimonio o del patrimonio de otros trabajadores*

de la empresa. … Tanto la persona del trabajador, como sus efectos personales y la taquilla, forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores. Por el contrario, las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario "como propietario o por otro título", y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste, que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador.

De ahí que los elementos que definen las garantías y los límites del artículo 18 del Estatuto de los Trabajadores no sean aplicables al control de los medios informáticos. En primer lugar, la necesidad del control de esos medios no tiene que justificarse por "la protección del patrimonio empresarial y de los demás trabajadores de la empresa", porque la legitimidad de ese control deriva del carácter de instrumento de producción del objeto sobre el que recae. El

empresario tiene que controlar el uso del ordenador, porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales. … El control de los ordenadores se justifica también por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores (pedidos, relaciones con clientes...), por la protección del sistema informático de la empresa, que puede ser afectado negativamente por determinados usos, y por la prevención de responsabilidades que para la empresa pudieran derivar también algunas formas ilícitas de uso frente a terceros. En realidad, el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores.

En segundo lugar, la exigencia de respetar en el control la dignidad humana del trabajador no es requisito específico de los registros del artículo 18, pues esta exigencia es general para todas las formas de control empresarial, como se advierte a partir de la propia redacción del artículo 20.3 del Estatuto de los Trabajadores. En todo caso, hay que aclarar que el hecho de que el trabajador no esté presente en el control no es en sí mismo un elemento que pueda considerarse contrario a su dignidad.

En tercer lugar, la exigencia de que el registro se practique en el centro de trabajo y en las horas de trabajo tiene sentido en el marco del artículo 18, que se refiere a facultades empresariales que, por su carácter excepcional, no pueden ejercitarse fuera del ámbito de la empresa. Es claro que el empresario no puede registrar al trabajador o sus efectos personales fuera del centro de trabajo y del tiempo de trabajo, pues en ese caso sus facultades de policía privada o de autotutela tendrían un alcance completamente desproporcionado[37].

En Estados Unidos, el problema tiene aristas interesantes que evidencian el conflicto generado por la superposición intersubjetiva de derechos. Una investigación realizada por la *American Management Asociation* (Asociación de Administraciones Empresarias de los Estados Unidos), de Nueva York, que incluyó a 1626 pequeñas y medianas empresas norteamericanas, descubrió que casi el 80% de ellas habitualmente controla el correo electrónico de sus empleados, así como sus llamadas telefónicas y sus conexiones a Internet.

El fundamento esgrimido, en general, apunta a que los correos electrónicos pueden llegar a obstruir el sistema de telecomunicaciones de una compañía y cierto material sexualmente explícito o de otra índole inapropiada extraído de Internet puede provocar reclamos referidos a un ambiente laboral hostil. Esta realidad habla de una ilusoria privacidad en los lugares de trabajo si se tiene en cuenta que la legislación norteamericana no obliga a las empresas a informar a sus dependientes respecto de los controles que se realizan. La tendencia jurisprudencial que se evidencia en los tribunales estadounidenses al respecto lleva a una ostensible mayoría de fallos a favor de los empleadores[38].

[37] Resolución tomada de www.aranzadi.es/index.php/informacion-juridica/jurisprudencia, junio 2008.
[38] Fernández, Claudio. Privacidad y Derecho a la Información. Artículo publicado en http://www.delitosinformaticos.com/ciberderechos/privacidad.shtm, junio 2009.

En Costa Rica, los casos que se presentan son similares y las discusiones y puntos de vistas de los diferentes operadores jurídicos también. Ponen en evidencia la lucha por conciliar el poder de control que tiene el empresario de sus medios de producción y la obligación de cumplir con el respeto de derechos constitucionales del trabajador. Como resultado de esto, los Tribunales de Justicia, y en especial, la Sala Constitucional de la Corte Suprema de Justicia, ha resuelto varios casos definiendo, como punto esencial, la necesidad del equilibrio entre ambas posiciones a partir de comportamientos de buena fe, de ambas partes, de una relación laboral.

Así por ejemplo, la Sala Segunda de la Corte Suprema de Justicia, máximo tribunal costarricense en materia laboral, realizando el análisis sobre la validez de un despido sin responsabilidad patronal aplicado por el empresario en virtud de un mal uso del computador y del correo electrónico, ambos propiedad de la empresa, por parte de una trabajadora, en el voto número 797 de las 15:00 horas del 18 de diciembre de 2003, sostuvo el siguiente criterio:

> *La utilización, no expresamente autorizada, de los medios informáticos y de comunicación de la empresa con fines estrictamente personales constituye un incumplimiento de los deberes laborales y una vulneración de la buena fe contractual, lo que es suficiente para que quien incurra en ella pueda ser sancionado incluso con el despido. Dicha utilización y su ocasional sanción nada tienen que ver ni con el derecho a la intimidad personal ni con el derecho a la protección de datos de carácter personal, ni consecuentemente con los espacios de privacidad que puedan existir en la empresa, ya que ésta es, por su propia naturaleza y por definición legal, "una unidad productiva con organización específica", es decir, los medios, instrumentos y herramientas puestos por la dirección a disposición de los trabajadores lo son en orden a la producción de bienes y servicios y* ***no para su uso particular y personal****.*

> *… En este sentido, el empleado no tiene una expectativa razonable de intimidad en la comunicación del correo electrónico, hecha voluntariamente sobre un sistema de correo provisto por la compañía. El patrono tiene la potestad, dentro de sus poderes de dirección, de fiscalizar el uso que sus empleados hagan de las herramientas de trabajo que se ponen a su disposición, dentro de las cuales se encuentra el correo electrónico. En este sentido, el derecho a la intimidad personal e inviolabilidad de las comunicaciones cede frente la potestad que tiene todo empresario a proteger sus medios organizativos patrimoniales y a dirigir y controlar la actividad laboral de sus trabajadores (* El resaltado no es original).

En primer término, la Sala Segunda de la Corte Suprema de Justicia toma como punto de partida que los equipos informáticos, provistos por el empleador, para el desempeño de las funciones propias del puesto del colaborador son considerados como herramientas de trabajo. Por lo que, como consecuencia de dicha naturaleza (instrumentos puestos a la orden de la producción de bienes y servicios y no para el uso particular), el empleador tiene la potestad, dentro de su poder de dirección, de fiscalizar que su depositario, el trabajador, haga uso de este instrumento con fines eminentemente laborales y no para realizar actividades ajenas a las encomendadas por el empleador; actos que podrían significar entre otras cosas el abandono de labores por parte del trabajador, daño a la imagen de la empresa, fuga de información confidencial, vulneración a la seguridad del equipo de computo o de la información almacenada en él.

En este mismo sentido, la Sala Segunda de la Corte Suprema de Justicia considera que al ser el computador y el correo electrónico herramientas informáticas puestas a las órdenes de la producción de bienes y servicios el trabajador no puede tener una expectativa de derecho a la intimidad, en virtud, que al considerarse la computadora una herramienta de trabajo, ésta *“debe ser utilizada exclusivamente para*

fines productivos, a menos que el empleador consienta expresamente en su uso para fines personales"[39]*,* de ahí que la expectativa de privacidad sea inexistente. Es decir, el derecho a la intimidad debe ceder de cara a *"la potestad que tiene todo empresario a proteger sus medios organizativos patrimoniales y a dirigir y controlar la actividad laboral de sus trabajadores"*[40]*.*

Como consecuencia, a criterio de este órgano jurisdiccional, el patrono podría realizar inspecciones o revisiones sobre los medios informáticos entregados al trabajador para el desempeño de sus funciones, sin que esto implique una violación a la intimidad, ya que el trabajador no puede tener una expectativa de privacidad sobre medios informáticos los cuales están destinados a la producción. Lo anterior es válido siempre y cuando al trabajador se le haya apercibido de la posibilidad de las inspecciones y de que las herramientas informáticas, únicamente, podrán ser utilizadas para fines laborales.

Lo anterior debe conciliarse con el criterio externado por la Sala Constitucional de la Corte Suprema de Justicia que, en un reciente fallo, ordenó la prevalencia del derecho del trabajo al respeto de su intimidad:

> *En el asunto bajo examen quedó debidamente acreditado que el Ministro de Comercio Exterior, por oficio No. DM-0019-5 del 6 de enero del 2005, despidió a la amparada del cargo de Directora de Negociaciones Comerciales Internacionales. A partir de esa fecha, el Ministro recurrido ordenó el respaldo de toda la documentación que constaba en la computadora de la amparada e impidió que ésta tuviera acceso a los archivos y comunicaciones almacenados en su disco duro con el fin de garantizar la continuidad de las funciones que ésta*

[39] Voto número 797 de las 15:00 horas del 18 de diciembre de 2003, Sala Segunda de la Corte Suprema de Costa Rica.
[40] Ídem.

ejercía. Con ello estima la Sala que se ha quebrantado el artículo 24 de la Constitución Política. En primer término, es preciso señalar que el correo electrónico y los documentos electrónicos almacenados en la computadora que utilizaba la recurrente, aunque sea un bien público, están protegidos por el derecho fundamental al secreto de las comunicaciones y nunca podría realizarse un control de los mismos con garantías inferiores a las establecidas por el mencionado precepto. Asimismo, el hecho que la computadora sea propiedad del Ministerio de Comercio Exterior, no significa que la amparada haya renunciado completamente a la garantía de inviolabilidad de las comunicaciones privadas, por cuanto, como se indicó anteriormente, la garantía del derecho fundamental no depende de la titularidad del medio sino que es independiente de la titularidad del soporte (En este sentido, puede verse la sentencia del Tribunal Europeo de Derechos Humanos de 24 de agosto de 1998 No. 872/1997, caso Lambert c. Francia). Los trabajadores no renuncian a la esfera de privacidad y a la protección de datos por ejercer una función pública, sino que, por el contrario, esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan una parte importante de sus relaciones con los demás. En otros términos, la circunstancia que al funcionario o empleado se le suministre un equipo para el cumplimiento y ejercicio de sus funciones –de propiedad de la Administración o empleador-, no excluye que el mismo sea soporte de información confidencial o personal cubierta por el secreto o reserva de las comunicaciones y, en general, por el derecho a la intimidad. Este derecho debe, no obstante, conciliarse con otros derechos e intereses legítimos del empleador – sea público o privado -, en particular, su derecho a administrar con cierta eficacia, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones irregulares de los trabajadores o funcionarios. La apertura por el empleador de los mensajes electrónicos de la cuenta del funcionario o trabajador sólo es justificable en circunstancias muy limitadas ya que el acceso a este tipo de datos no es necesario para satisfacer un interés legítimo del empleador, debiendo prevalecer por el contrario el derecho fundamental al secreto de las comunicaciones [41].

En este mismo sentido, la Sala Constitucional, en otra ocasión, resolvió de la siguiente forma:

Alega el recurrente que cuando se reintegró a su cargo como Jefe del Área de Gestión de Bienes y Servicios del Hospital San Rafael de Alajuela, el pasado primero de junio de 2009, al cesar la aplicación de una medida cautelar decretada en su contra, se percató que el computador que tenía asignado al momento de su separación del cargo, no estaba. Acusa que cuando indagó para

[41] Voto número 15063-2005 de las a las quince horas con cincuenta y nueve minutos del primero de noviembre del dos mil cinco, Sala Constitucional de la Corte Suprema de Justicia.

determinar la ubicación de este implemento - el cual contenía documentos de trabajo así como información personal -, pudo constatar que los archivos que tenía grabados fueron borrados, ello por orden de la persona que ocupó su lugar mientras se encontraba fuera, y quien actualmente labora en el Área de Regulación y Evaluación de la Gerencia de Logística de la Caja Costarricense del Seguro Social. Se declara con lugar el recurso. Se ordena al Director General del Hospital San Rafael de Alajuela, realizar las gestiones que estén dentro del ámbito de sus competencias, a efectos de que dentro del plazo de quince días contado a partir de la notificación de esta sentencia, se brinde al tutelado copia de la información de índole personal que existía en su computador institucional previo a ser suspendido de su cargo [42].

En resumen, la recomendación general es que los empleadores deben contar con acuerdos firmados entre la empresa y sus empleados, en los cuales se regule la política corporativa para la utilización de los correos electrónicos. En tales supuestos no debería existir violación a la intimidad del trabajador, fundamentalmente, porque una de las partes en la comunicación, el trabajador, ha dado su consentimiento previo para el acceso de su correspondencia electrónica estrictamente relacionado con el empleo a los órdenes de su patrono. Es decir, la empresa no hace más que incluir disposiciones corporativas para el manejo de las comunicaciones realizadas por sus trabajadores que, además, ocurren a través de un servidor central de su propiedad, y mediante una cuenta de *e-mail* con dominio corporativo.

Por último, estos acuerdos de revisión no podrían incluir los *e-mails* privados, como los que proveen dominios en Internet como Yahoo, Hotmail, Messenger o Gmail; los cuales merecen una protección constitucional diferente al caso de las direcciones de correo de corporativas, ya que poseen características de protección de privacidad más acentuadas y para su funcionamiento se requiere un prestador de servicio, el

[42] Voto número 13818 del año 2009, Sala Constitucional de la Corte Suprema de Justicia.

nombre de usuario y un código o contraseña de acceso que impide el acceso de terceros a él. Es decir, el ámbito de operación de este tipo de cuentas de correo electrónico va más allá del poder de control que le corresponde al patrono, porque se trata de una de las esferas más íntimas del trabajador como son sus comunicaciones personales.

Regresando al tema de los correos corporativos, existen casos donde se hace necesario realizar una auditoría o inspección del correo electrónico corporativo de un trabajador. Esta posibilidad debe estar prevista en los procedimientos internos de la compañía, pero, en la medida de lo posible, es conveniente que exista una causa objetiva que justifique la inspección más allá, incluso, de una simple formalidad establecida en un procedimiento interno.

Estas causas objetivas, como se las denomina en esta investigación, se pueden originar en los más diversos motivos, por ejemplo:

- Pérdida de rendimiento y productividad en el puesto de trabajo.

- Acceso no autorizado a páginas Web de contenido de pago.

- Existencia de virus y software maliciosos en correos electrónicos y navegaciones inseguras por Internet.

- Desprestigio de la imagen pública de la empresa a través de contenidos recibidos o enviados a través del correo electrónico corporativo.

- Fuga de información corporativa, confidencial, que haya o pueda poner en peligro los intereses de la empresa.

Ahora bien, en caso de proceder una inspección de esta naturaleza, lo conveniente será que la misma se realice en las oficinas de la compañía y en horario laboral con la presencia del propio trabajador, del representante de los trabajadores o, en su defecto, de cualquier otro trabajador de la empresa que pueda rendir testimonio sobre los datos recopilados durante el proceso, de forma que se cumpla con la buena fe que, como se ha indicado, debe privar en el desarrollo de la relación laboral.

2.2. El resguardo de la información medica

En este apartado corresponde hacer un análisis sobre la conservación de datos médicos que pueda obtener un empleador y no sobre si es legalmente posible hacerlo. Es decir, parte del hecho de exámenes médicos realizados con base en la legislación ordinaria y no de aquellos realizados afectando la dignidad y privacidad del trabajador.

Se debe recordar que hay pruebas médicas que son expresamente permitidas por la ley, o bien, actividades donde las propias empresas están obligadas a ofrecer a los trabajadores un reconocimiento médico con el fin de controlar el estado de salud de un trabajador. Esas pruebas deben contar con un fundamento legal y ser conocidas previamente por el trabajador como requisito de validez.

En España, por ejemplo, el Tribunal Constitucional, en una sentencia del 15 de noviembre del año 2004, anuló el despido, por parte de la empresa de aviación Iberia, de una trabajadora a la que se le detectó consumo de *cannabis* tras un análisis de orina, ya que, en criterio de ese tribunal, las pruebas realizadas a la empleada vulneraron su derecho a la intimidad porque "*no se le comunicó ni por la empresa ni por sus servicios médicos cuál era la información buscada con los análisis médicos y, en concreto, no se le informó de que se analizaría su consumo de estupefacientes*". Según ese tribunal, "*Iberia tenía la obligación de informar expresamente a la trabajadora de esa analítica, toda vez que ... tenía como objeto datos sensibles, pues el hecho de haber consumido en algún momento algún género de drogas, pese a que ... es una conducta impune, provoca a menudo un juicio social de reproche*". Además, afirma que: "*no habrá vulneración del derecho a la intimidad si el trabajador puede tener acceso, de solicitarlo, al conocimiento del contenido y alcance de la detección, tipo de pruebas que le vayan a ser practicadas y sus efectos, sus contraindicaciones y riesgos*".

En Costa Rica, también la Sala Constitucional de la Corte Suprema de Justicia ha resuelto casos relacionado con la recopilación y custodia de información médica del ciudadano. Por ejemplo, en una sentencia de este año indicó lo siguiente:

> *Acusa la recurrente la violación, en perjuicio de la amparada, de lo dispuesto en el artículo 24 de la Constitución Política, ya que solicitó ante la Sala Constitucional, que se eliminara de la página web del Poder Judicial, los datos confidenciales que constan en el registro digital de un expediente en donde figura como recurrente, en donde no sólo le garantizó el compromiso de todo el personal de la Sala Constitucional en resguardar los datos confidenciales de quienes figuren como partes en los asuntos sometidos a su conocimiento, sino también, que se había subsanado la información que sobre su caso estaba*

disponible en internet. Sin embargo, por consulta electrónica realizada el 19 de mayo del año en curso, constató que los datos confidenciales acerca de su estado de salud, aún están a disposición de cualquier persona que acceda a internet. Se declara con lugar el recurso. Se ordena al Jefe del Departamento de Tecnología de Información, bajo pena de desobediencia que en forma inmediata gire las órdenes necesarias y tome las medidas pertinentes que estén dentro del ámbito de sus atribuciones y de sus competencias para la exclusión del expediente 08-002159-0007-CO - por ser de índole confidencial- de las páginas de Internet del Poder Judicial y de la Sala Constitucional de la Corte Suprema de Justicia [43].

Las empresas que realizan pruebas médicas, voluntarias y comunicadas, y autorizadas previamente por el trabajador, podrían recopilar una serie de datos identificativos del paciente demostrando que el empleado es apto o no para realizar su trabajo, sin revelar la enfermedad o dolencia que lo incapacita para ello. En la creación y el uso de este fichero debe mediar la debida confidencialidad, lo mismo que adoptar las medidas de seguridad para asegurarlas. Un caso, por ejemplo, que justifica la creación de un fichero de datos de esta naturaleza, es el suministro de la información, a la Dirección General de Hacienda, para beneficiarse de las bonificaciones destinadas a aquellas empresas que contratan personas con algún tipo de incapacidad física. El tratamiento debe ser cuidadoso, ya que podría dar lugar a discriminaciones en el empleo. Por ejemplo, en España, el Tribunal Constitucional *Ordenó a la entidad bancaria BCH a destruir un fichero con datos de salud de sus trabajadores contenido en su base de datos laborales, por entender que violaba el derecho a la intimidad reconocido por los artículos 18.1 y 18.4 de la Constitución. Este fichero se utilizaba para controlar el absentismo de los empleados, y recogía gran cantidad de datos,*

[43] Voto número 12434 de 2009, Sala Constitucional de la Corte Suprema de Justicia.

excesivos en opinión del Tribunal Constitucional, ya que albergaba incluso datos médicos de trabajadores ya jubilados[44].

En síntesis, la revisión de los procesos de protección de los datos médicos del trabajador tiene importancia porque esa información no sólo incide sobre aspectos de la "privacidad" del individuo, sino porque "*de los datos obtenidos puede deducirse de forma aproximada cuestiones como la vida sexual del trabajador, sus hábitos, su régimen alimenticio y de descansos, etc., de forma tal que el empresario puede inmiscuirse en la vida extralaboral de su personal, transponiéndola al ámbito de la empresa a los efectos de determinar ciertas inclinaciones o propensiones y, consiguientemente"* [45] y, a partir de ello, hasta tomar decisiones que van más allá de cuestiones relacionadas con el papel del trabajador en la empresa, es decir, de su rendimiento laboral y los resultados obtenidos, que es lo que finalmente interesa a casi todas las empresas.

[44] Gargía Noguera, Noelia. Artículo tomado de Revista Digital Portalley.com. www.portaley.com/empresa/revista24042002.shtml julio 2008.
[45] Cuervo, Jose. La intimidad informática del trabajador. Artículo tomado de http://www.informatica-juridica.com., junio 2008.

CAPÍTULO II. LA LEGALIDAD DE LA PRUEBA OBTENIDA A PARTIR DE DATOS DEL TRABAJADOR

A. OBLIGACIONES DEL EMPLEADOR DURANTE LA FASE DE RECLUTAMIENTO Y SELECCIÓN DE TRABAJADORES

La información tiene, en la actualidad, una gran importancia en el proceso de contratación laboral. La obtención de datos del trabajador, así como su conservación, es lo que hace importante analizar el tema para complementar esta información.

La selección de unos trabajadores y no de otros es un acto empresarial que requiere de información, de datos personales de los candidatos; sin embargo, ello también implica la obligación de garantizar el derecho a la intimidad del trabajador. Se considera que esto es lo que algunas empresas prefieren olvidar, lo cual implica a su vez un peligro para todas las partes ya que "*esa búsqueda de datos puede llegar más lejos de lo necesario hasta alcanzar aspectos de la vida de los solicitantes que no son relevantes para la determinación de su aptitud*"[46].

[46] Cuervo, Jose. La intimidad informática del trabajador. Artículo tomado de http://www.informatica-juridica.com., junio 2009.

1. Los datos que puede exigir el empleador

Son muchos los documentos que un contratante, público o privado, puede solicitar o, de alguna forma, obtener durante el proceso de contratación e incluso durante el desarrollo de la relación laboral, por ejemplo, la actualización anual de la información contenida en su archivo laboral. Por ello, no existe una lista taxativa de cuáles son esos documentos, aunque todos los procesos suelen iniciar con la presentación del llamado *curriculum vitae,* o bien, hoja de vida, que contiene la información básica del candidato, como: nombre, número de cédula de identificación, estado filial, dirección del domicilio, atestados académicos y antecedentes laborales.

Muchas empresas creen que, por haber sido remitido voluntariamente por el candidato, existe un consentimiento tácito del trabajador para ser utilizado como la empresa considere, lo cual no es cierto ni preciso en todos los casos. Por lo tanto, aunque las personan envíen su información personal de forma voluntaria, lo recomendable es que sean informados del uso que la empresa puede dar y, además, indicar de forma expresa si son cedidos a terceros con fines laborales o de cualquier otro tipo.

Se recomienda en este punto que, al momento de la entrega de la información por parte del solicitante, se informe solicitante éste sobre las condiciones o si se trata de enviarlo por un medio electrónico, como por ejemplo, un sitio en la Web de la empresa. La compañía debe contar con una política clara que defina el tratamiento y que pueda ser consultado por el propio candidato interesado en el puesto.

Por último, en relación con los datos de los candidatos, es recomendable imponer la obligación de mantener los datos actualizados por el propio interesado que remite su *curriculum vitae*. En caso que no se decida contar con los servicios del oferente, sería recomendable indicar las políticas para la conservación de la información, ya que el paso del tiempo es suficiente para que los datos varíen considerablemente.

Es común que muchas empresas apliquen diferentes *test* psicotécnicos y de personalidad, incluso hasta pruebas de caligrafía que sirven para evaluar a un candidato para un puesto de trabajo. Si bien en la legislación laboral existe un vacío sobre el tema, está claro que la información obtenida debe ser protegida y considerada como estrictamente confidencial, por cuanto podría proporcionar más datos de los necesarios para el empleo, lo cual, cuando es utilizado para fines distintos a la vinculación en una determinado empresa, podrían afectar en forma directa la intimidad o la dignidad del solicitante. Se ha mencionado, de forma insistente, que el candidato tiene derecho a solicitar que la información no sea divulgada ni utilizada más que para efectos laborales al interior de la empresa interesada en su contratación.

La información solicitada por el empleador debe ser información basada en criterios objetivos, relacionados directamente con el puesto, y no que pueda dañar al trabajador, en caso de no ser seleccionado por la empresa. Un caso de esta naturaleza fue recientemente resuelto por la Sala Segunda de la Corte Suprema de Justicia, que señaló lo siguiente:

Aduce el recurrente que adquirió una tarjeta de crédito con el Banco Popular la cual no pudo pagar por razones de solvencia, tampoco pudo hacer abonos al saldo deudor. En consecuencia, cayó en cobro judicial el 26 de abril de 2005, la cual fue cancelada el 15 de febrero de 2008 y el 26 de febrero siguiente el Banco le entregó un documento en el cual solicitó el levantamiento de embargos. Posteriormente, el 19 de marzo de 2008, la empresa Manpower de Costa Rica S.A., donde laboraba, lo despidió argumentando que su desempeño no era satisfactorio, sin embargo, es de su conocimiento que esa empresa hace estudios de su personal para constatar que su historial crediticio no esté manchado e incluso tuvo que explicar a sus superiores que lo visto en pantalla no correspondía a la realidad de los hechos, pues la deuda estaba satisfecha. Agrega que lo que más le preocupa, es que su condición crediticia todavía se encuentra manchada, ya que realizó un trámite ante la Empresa Cero Riesgo, donde todavía aparece en trámite el cobro judicial de su deuda ante el Banco Popular, cuando en realidad está cancelada y más bien hay un saldo a su favor. Hasta ese momento no había entendido por qué razón todas las empresas donde había solicitado trabajo, le habían insistido en la entrevista sobre cuentas pendientes y deudas, incluso le señalaron que eso era condición necesaria para poder contratarlo, encontrarse libre de toda mancha delictiva o crediticia. Considera que esa mancha crediticia le ha impedido encontrar trabajo, y considera que hay falta de seriedad del Banco Popular al no realizar el levantamiento dentro de las 24 horas posteriores a la cancelación. Alega que ha sido llamado a laborar y luego es cesado por cuestiones judiciales, con lo que se ha lesionado su derecho al trabajo y su integridad moral, emocional y económica. Se declara parcialmente con lugar el recurso. Se condena a "Cero Riesgo Información Crediticia Digitalizada Sociedad Anónima" al pago de las costas, daños y perjuicios causados con los hechos que sirven de fundamento a esta declaratoria, los que se liquidarán en ejecución de sentencia de lo civil [47].

Además de lo dicho, el patrono debe estar regido por el criterio de confidencialidad para la protección de los datos suministrados por el trabajador durante una entrevista de trabajo, en el entendido que el patrono únicamente podría almacenar y utilizar información con fundamento legal.

Es decir, no puede, bajo ningún argumento, utilizar información, por ejemplo, sobre el estado de embarazo de una trabajador, o bien, la pertenencia a una

[47] Voto número 10705 del año 2009. Sala Segunda de la Corte Suprema de Justicia.

organización sindical, ya que esta información puede ser utilizada con fines discriminatorios.

1.1. La protección de datos del trabajador cuando se utilizan empresas de selección y reclutamiento

En muchos casos, la selección de personal es realizada por empresas especializadas que realizan el trabajo de recopilación, almacenamiento y tratamiento de datos personales de los aspirantes al empleo. Con ello surge la posibilidad que estas empresas especializadas, a partir de los datos a los que van teniendo acceso en el desarrollo de su actividad, creen fondos o bancos de información con el fin de emplearlos en futuros procesos de selección o, incluso, de cederlos a otros empleadores que realicen el reclutamiento de sus empleados, pero que busquen información sobre ellos.

Es aquí donde podrían presentarse algunos problemas, principalmente, porque no existe regulación expresa sobre el tema, pero también por la falta de precisión y, en algunos casos, el desinterés por parte de las empresas que realizan esas actividades.

En España, por ejemplo, esta situación parece estar prohibida por el artículo 27 de la Ley de Regulación del Tratamiento Automatizado de Datos que con el título de "Prestación de servicios de tratamiento automatizado de datos de carácter personal" indica:

1. Quienes , por cuenta de terceros, presten servicios de tratamiento automatizado de datos de carácter personal no podrán aplicar o utilizar los obtenidos con fin

distinto al que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación, a otras personas.

2. Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se presten tales servicios, porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años".

En palabras del Tratadista, José Cuervo, "*Las empresas de selección tienen como fin específico la selección de trabajadores para otras empresas que acuden a sus servicios, no al tratamiento automatizado de datos por cuenta de terceros"*[48].

Una empresa de selección no podría emplear, con otros fines, la información obtenida para un reclutamiento en particular, tampoco cederla a otras empresas de la misma naturaleza o bien a otros empleadores distintos al que inicialmente contrató los servicios. Ello supondría una contradicción, al principio de finalidad, estudiado líneas atrás, según el cual los datos personales no deben ser usados para fines distintos de los que fueron recopilados.

Esta situación también ha sido propuesta en el proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" que, de forma expresa, establece una regulación para la cesión de la información, la cual podría resultar de aplicación para este caso en particular.

[48] Cuervo, Jose. La intimidad informática del trabajador. Artículo tomado de http://www.informatica-juridica.com., junio 2009.

El artículo 10 del proyecto de ley establece lo siguiente:

ARTÍCULO 10.- Cesión de datos

Los datos de carácter personal conservados en archivos o bases de datos públicos o privados, solo podrán ser cedidos a terceros para fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado, en los términos del artículo 5 de esta Ley.

El consentimiento para la cesión podrá ser revocado pero la revocatoria no tendrá efectos retroactivos.

Lo anterior es aplicable a cualquier fichero independientemente de su titularidad pública o privada.

El consentimiento no será exigido cuando:

a) Así lo disponga una ley.

b) Se trate de la cesión de datos personales al Estado o una institución pública de salud o de investigación científica en el área de la salud, relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

c) Se trate de la cesión de datos personales al Estado o a una institución pública en materia de seguridad pública, siempre y cuando la cesión resulte necesaria para fines de esta seguridad pública y de la persecución de delitos sin perjuicio de lo establecido en el artículo 24 de la Constitución Política.

d) Se trate de cesión de datos personales referente a estadísticas y censos poblacionales para fines específicos.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y este responderá solidariamente y conjuntamente por la observancia de los mismos ante la Agencia de Protección de Datos y el titular de los datos.

La regulación legal propuesta es atinada, por cuanto arroja una primera guía para las empresas que se dedican a esta actividad: deben contar con el consentimiento de la persona que voluntariamente cede la información; pero, a criterio de esta investigación, este consentimiento informado implica la obligación de indicar al cedente de la información, que la misma será facilita a los empleadores interesados en contar con sus servicios.

En este mismo sentido, este mismo proyecto de ley se establece una condición que, de forma amplia, podría aplicarse a las empresas de Selección y Reclutamiento, propuesta de normativa que dispone:

ARTÍCULO 16.- Transferencia de datos personales. Regla general

Las personas públicas y privadas encargadas del manejo de bases de datos y los archivos físicos, estarán imposibilitadas para transferir datos que hayan recibido directamente de los titulares de la información o de terceros.

Se exceptúan de la prohibición contenida en el párrafo anterior las transferencias ocurridas con absoluto arreglo a alguna de las siguientes reglas:

a) Que la Agencia para la Protección de Datos Personales autorice la transferencia a la persona o institución receptora, pública o privada, por corroborar que con dicho traslado no están siendo vulnerados los principios rectores del manejo de datos personales, descritos en esta Ley.

b) Que el titular de la información haya autorizado expresa y válidamente tal transferencia y que no haya sido notificada la revocatoria a la Autoridad encargada del fichero.

c) Si se trata de una persona o institución pública o privada domiciliada en el extranjero, dicha transferencia solo podrá ser llevada a cabo si, además de las condiciones antes mencionadas, dicho receptor está domiciliado o tiene como base un país que ofrezca un nivel de protección de los datos personales, igual o superior al establecido en Costa Rica, salvo que el titular de los datos personales autorice expresamente su transferencia, la cual se hará sin más trámite.

Según esta norma, las empresas de selección y reclutamiento serán de las principales obligadas a registrar su actividad comercial y cumplir con el registro de sus bases de datos ante la Agencia de Protección de Datos, de conformidad con lo que dispone la regulación contenida en el artículo15 del proyecto de ley que dispone:

"ARTÍCULO 15.- Protocolos de actuación

Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, almacenamiento y uso de datos personales, podrán emitir un protocolo de actuación, en el cual establecerán los pasos que deberán seguir, en la recolección, almacenamiento y manejo de los datos personales, de conformidad con las reglas previstas en esta Ley.

Para ser válidos, los protocolos de actuación deberán ser inscritos ante el Registro de archivos y bases de datos. La Agencia de Protección de Datos Personales podrá, en cualquier momento, verificar que el titular del archivo esté cumpliendo cabalmente con los términos de su código de conducta.

La manipulación de datos con base en un protocolo de actuación inscrito ante la Agencia hará presumir (iuris tantum) el cumplimiento de las disposiciones contenidas en esta Ley, para los efectos de autorizar la cesión de los datos contenidos en un archivo o base.

El tratamiento automatizado de datos en los procesos de selección y reclutamiento para fines posteriores a un proceso de reclutamiento en particular, exigirá el consentimiento del candidato, pues se encuentra fuera del marco de una relación laboral, es decir, la información deja de ser necesaria si la contratación del trabajador en la empresa que acordó el servicio no llega a buen término. En este sentido, es adecuada la regulación que, de forma inicial, establece el proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" y que podría ser aplicado a este tipo de empresas.

2. ¿Cómo se debe proteger la información?

La protección de datos del trabajador, por parte de su empleador, implica una serie de obligaciones que no solamente se refieren a la garantía de respetar la privacidad del personal y utilizarlos para fines autorizados por el trabajador. Implica además, la protección, mediante mecanismos eficaces, que asegure el acceso restringido a las bases de datos que se crean en una organización para fines laborales.

En general, las bases de datos creadas por el empleador, durante los procesos de selección y reclutamiento, deben ser utilizados para fines relacionados con el empleo en dicha organización, salvo que el candidato o, en su defecto, el trabajador que resulte contratado haya autorizado el uso para fines distintos que, a su vez, debieron ser previamente explicados al cedente de la información.

Una vez recopilada la información y utilizada para alimentar las bases de datos del empleador, este debe garantizar la seguridad de los datos aplicando, como medida general, un buen control del acceso a dicha información para evitar fugas, secuestros de documentos y la posibilidad de copiarlos y utilizarlos para fines distintos a los que fue creado.

En este sentido, el artículo 8 del proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales" establece lo que serían las bases de la seguridad de la información. Señala el artículo citado:

ARTÍCULO 8.- Seguridad de los datos

1.- Todo archivo, fichero, registro o base de datos, público o privado destinado a proporcionar informes debe inscribirse en el Registro de archivos y bases de datos contemplado en el artículo 27 de la presente Ley.

2.- El responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

3.- No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que garanticen plenamente su seguridad e integridad y los de los centros de tratamientos, equipos, sistemas y programas.

4.- Por vía de reglamento, se establecerán los requisitos y las condiciones que deban reunir los ficheros automatizados y los manuales y las personas que intervengan en el acopio, almacenamiento y uso de los datos.

5.- El responsable del fichero y quienes intervengan en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal, están obligados al secreto profesional.

Las disposiciones establecidas en el anterior artículo podrían ser suficientes para garantizar la conservación de los datos. Sin embargo, el proyecto de ley plantea la inquietud sobre si los empleadores deberán inscribir necesariamente sus bases de datos ante la Agencia de Protección de Datos.

A criterio de la investigación, no necesariamente deberían cumplir con esta disposición en tanto los datos sensibles del trabajador o del candidato sean utilizados para fines internos y no para la confección de informes que puedan llegar a terceros.

Pese a esta inquietud, se considera que las reglas generales de conservación de la información sí pueden ser utilizadas por las empresas como una guía para cumplir adecuadamente con la protección de la información de sus trabajadores.

Además de lo mencionado, los sistemas de conservación de datos del personal deben garantizar al trabajador la posibilidad de verificar la existencia de los registros que posee el patrono y, por supuesto, la posibilidad de rectificar los datos recopilados

estableciendo un mecanismo que permita la actualización constante y la oportunidad de solicitar la eliminación de información que no se encuentre vigente.

Según lo mencionado durante toda esta investigación, el trabajador debe tener la posibilidad de conocer, de forma anticipada y clara, las políticas que en esta materia haya establecido el patrono.

La información que un trabajador provea a un empleador, para un proceso de selección, no debe ser utilizada en otro proceso de contratación, incluso de la misma empresa, si el trabajador no autorizó expresamente tal situación. De lo contrario, el trabajador podría quedar imposibilitado de modificar en cualquier sentido la información suministrada haciéndola más atractiva para un puesto al que inicialmente no concursó.

B. OBLIGACIONES DEL EMPLEADOR EN LA EJECUCIÓN DE LA RELACIÓN LABORAL. LEGALIDAD DE LA PRUEBA OBTENIDA

1. La intención de conservar datos del trabajador durante la relación laboral

Se considera que, además de la comunicación efectiva al trabajador, los empleadores de nuestro país deberían plantearse cuestiones más allá de los requisitos de legalidad que deben observar en cuanto a la protección de datos del trabajador y delimitar con claridad cuáles son los datos que realmente necesitan conocer del trabajador durante la relación laboral y que, por ese motivo, deban considerar como necesarios para la correcta prestación del servicio contratado.

Está claro que durante la relación laboral, las condiciones iniciales de contratación pueden cambiar por diversos motivos: cambios en el organigrama de la organización, diversidad del negocio, la propia capacitación del trabajador, así como el crecimiento que el trabajador pueda tener dentro del organigrama de la empresa,. Todas ellas situaciones que implican la toma de decisiones respecto a las condiciones del trabajador, y que solo podrían aplicarse en beneficio del trabajador.

El control de datos del trabajador debe ir más allá de una simple fuente de información para la toma de acciones disciplinarias, como puede suceder en muchos casos. Por el contrario, la oportunidad de actualizar la información que consta en el expediente personal del trabajador y, en general, en cualquiera de los registros que el patrono haya escogido para la conservación de la información; debe ser ofrecido como una oportunidad para el trabajador de mejorar su condición laboral, esto, además, como cumplimiento de la posibilidad del trabajador de revisar y actualizar la información que posee su patrono.

Siguiendo la tesis del profesor español, José Cuervo, el acceso a los datos personales del trabajador que conserva la empresa podría generar aspectos tan positivos como los siguientes:

- Mayor capacidad de combinación con la formación de "perfiles" más completos, avanzándose en la configuración del denominado "trabajador transparente".
- Mayores posibilidades de transmisión de información a otros niveles de la compañía.

- Mayor perdurabilidad de la información.
- Mayor posibilidad de actualización de la información del trabajador.
- La oportunidad de crear el denominado "clima psico-sociológico de control y transparencia", esto es, de conciencia en los trabajadores de poder ser conocidos en todos sus aspectos, con la certeza de que toda la información fue obtenida con su consentimiento

Los patronos deben plantearse lo siguiente: ¿para qué se conserva la información del trabajador? La respuesta a esta inquietud debe ir más allá del mero valor comercial que representa la posibilidad de contar con una base de datos de trabajadores y, en general, de personas que de alguna forma participaron de un proceso de selección. Además debe responder a motivos objetivos pero que contribuyan al mantenimiento del trabajador en la organización y, eventualmente, potenciar su crecimiento.

Existe información personal que, en principio, no sufrirá ninguna modificación, por ejemplo, el número de cédula de identidad nacional. Sin embargo, sería necesario actualizar esta información cuando se trate, por ejemplo, de un trabajador de nacionalidad extranjera, de modo que se pueda conocer la vigencia de su estatus migratorio en el país.

Como se ve en el caso planteado, la solicitud de actualización de esta información básica y consecuentemente la obligación del trabajador de proporcionar la información solicitada no responde a una situación antojadiza sino más bien al deber de la empresa de contar con personal que, a su vez, posea las condiciones mínimas

legales. De cumplirse esta situación, el empleador no se expone a la imposición de sanciones por contratar trabajadores ilegales en el país y, a su vez, el trabajador se evita cualquier inconveniente con las autoridades migratorias del país. Estas situaciones sustentan lo planteado con anterioridad en esta investigación, de que las razones para la solicitud de información deben corresponder a cuestiones objetivas y de ninguna forma que perjudiquen la situación laboral dentro de la compañía.

En otro ejemplo también se aprecia lo mismo, al interrogar: ¿Por qué se solicitan los datos sobre el número de hijos del trabajador? Un empleador debería estar en la capacidad de responder a esta pregunta indicando, por ejemplo, que es necesario para hacer partícipe al trabajador de algunos beneficios que son exclusivos para los padres de familia, o, que conocer el número de menores de edad es necesario para ampliar la cobertura que brinda la empresa. De ninguna manera la respuesta debería ser para conocer las expectativas de la vida personal del trabajador, situación que podría representar algún práctica discriminatoria, principalmente, en el caso de las mujeres a las que frecuentemente se les consulta sobre su intención de tener hijos, como frecuentemente ocurre en algunas empresas que terminan en medio de un proceso judicial por este motivo.

Existen casos que se pueden considerar más fáciles de contestar que otros, porque se trata de solicitudes de información sobre datos que tienen relación directa con el empleado. Por ejemplo, la actualización del permiso de conducir para un chofer, el permiso de portación de armas de un empleado de seguridad, o la tenencia de la licencia de médico de un doctor contratado en una empresa de servicios médicos.

Aquí existe un criterio objetivo para la solicitud y actualización de datos del trabajador, ya que se trata de condiciones necesarias para la prestación del servicio que el patrono debe estar en capacidad de garantizar.

Otros ejemplos típicos se refieren, por ejemplo, a la aportación de títulos que acreditan la formación académica del trabajador con la clara intención de promover el desarrollo en la organización; sin embargo, en este caso, aunque resultaría ilógico pensarlo en sentido contrario, el trabajador debe estar en capacidad de aportar la información de forma voluntaria. Lo mismo sucede cuando el trabajador es sujeto de evaluaciones constantes con el objeto de medir su desempeño y decidir el otorgamiento de aumentos de salario o bonos propios del esquema de compensación, con la particularidad, además, que el trabajador debe tener acceso a dicha información para verificar que fue calificado a partir de información actualizada y principalmente correcta. En caso que no sea así, el trabajador debe tener la posibilidad de rectificar la información, aportando la documentación que posea para demostrar su posición.

En síntesis, la información del trabajador que el empleador conserve durante la relación laboral debe responder a interrogantes que permitan contribuir a la objetividad que un patrono debería procurar para evitar situaciones discriminatorias, basadas en situaciones subjetivas o personales.

A pesar de lo dicho existen casos donde la información recopilada por el trabajador no solamente se utiliza para procurar el mejoramiento de las condiciones de la relación laboral, sino todo lo contrario: se utiliza para ejercer acciones disciplinarias, tema que con más claridad se analiza en el siguiente punto.

2. El uso de datos del trabajador como fundamento del poder disciplinario

Cualquier decisión que toma el patrono se basa en la información que posea del trabajador. Cuando esta información no conviene a los intereses de la empresa o se utiliza para tomar acciones disciplinarias, debe hacerse a partir del registro de información y datos que, además, puedan ser demostrados de forma contundente en un proceso administrativo o judicial. Esta obligación corresponde en general al patrono producto de que en materia laboral le corresponde al patrono la carga de la prueba, lo cual ha sido reiterado de forma clara por la Sala Segunda de la Corte Suprema de Justicia, quien en un fallo reciente mencionó:

> ***VI.- LA CARGA PROBATORIA EN MATERIA LABORAL:*** *En relación con el tema de la carga de la prueba, el artículo 317 del Código Procesal Civil establece: "La carga de la prueba incumbe: 1) A quien formule una pretensión, respecto de las afirmaciones de los hechos constitutivos de su derecho. / 2) A quien se oponga a una pretensión, en cuanto a las afirmaciones de hechos impeditivos, modificativos o extintivos del derecho del actor". Según se desprende de la norma citada, la cual resulta de aplicación en el proceso laboral con los matices que a continuación se expondrán y de conformidad con el artículo 452 del Código de Trabajo, el problema del "onus probandi" -o de la carga probatoria- surge cuando los hechos no han logrado demostrarse; debiéndose, entonces, determinar sobre cuál de las partes ha de pesar las consecuencias de una omisión en probar determinado hecho. Parte de la doctrina ha entendido que el empleador demandado es, normalmente, quien debe aportar los elementos probatorios respectivos para desvirtuar los hechos indicados por el demandante; pues, al ser la parte más fuerte de la contratación, tiene mayor facilidad de pre-constituir, durante el transcurso de la relación de trabajo, la prueba tendiente a demostrar los normales hechos aducidos en un proceso de naturaleza laboral. Así, se ha indicado que: "En sentido estricto, al proceso común deben aplicársele dos principios, que están traducidos en sendos aforismos: 'Quien afirma algo está obligado a demostrarlo' y 'Si el demandante no prueba, el demandado será absuelto'. De acuerdo a ello, la carga probatoria es siempre del peticionante, quien está en la necesidad y en la obligación de acreditar con elementos de convicción que los hechos que alega son ciertos. / En el Derecho Procesal del Trabajo este criterio es deliberadamente quebrantado, subvertido: el trabajador, que es normalmente el actor o demandante, es exonerado en lo sustancial de la obligación de probar su*

dicho; el onus probandi recae en lo básico sobre el empleador, usualmente el demandado. La demanda goza, por decirlo así, de una presunción de veracidad, se le reputa cierta a priori, presunción juris tantum que debe ser destruida por el empleador con su prueba". (PASCO COSMOPOLIS, Mario. Fundamentos de Derecho Procesal del Trabajo, Editorial AELE, segunda edición, 1997, p. 67). Ahora bien, aunque, de conformidad con lo anterior, se entiende que sobre el empleador recae una mayor responsabilidad en cuanto a la aportación de la prueba, debe tenerse claro que ello no implica una liberación total del trabajador de su carga probatoria; pues, respecto de ciertos hechos, sobre él pesa siempre y necesariamente aquel "onus probandi." Así, en cuanto a la acreditación del despido, se ha considerado que la carga probatoria corresponde al trabajador, debiendo entonces el empleador comprobar la causal que medió para aplicar dicha sanción. En consecuencia, al trabajador únicamente le corresponde acreditar el despido y el empleador debe demostrar, sin que medie duda alguna, que el primero incurrió en una causal de despido o en faltas de tal gravedad que hicieron imposible la continuación de la relación de trabajo.[49]

Si el patrono toma alguna decisión de carácter sancionatorio, ya sea con base en la información que ya posea del trabajador o a partir de datos específicos sobre una situación particular, recopilados con la intención de tomar alguna represalia en contra del trabajador, por ejemplo, por la comisión de una falta grave; debe estar en la capacidad de asumir una posición válida frente a los siguientes cuestionamientos: ¿la información es precisa?, ¿se comunicó al trabajador previamente el motivo de la recopilación de la información? ¿Los datos que posee el empleador fueron obtenidos por medios válidos desde el punto de vista probatorio?

Estos cuestionamientos obligan a considerar que no solamente se trata de preguntas como las mencionadas, sino relacionadas a la forma en que recopiló la información y las personas que han tenido acceso a la información personal del trabajador.

[49] Resolución número 549 2009. Sala Segunda de la Corte Suprema de Justicia.

Aquí nuevamente se debe señalar que los medios de obtención debieron comunicarse previamente al trabajador y que, durante todo el proceso que se instaure para la investigación del hecho, debe primar la voluntariedad del suministro de información y la protección de confidencialidad, ya que no existiría ninguna razón para que esto sea conocido por un tercero, salvo en casos de revisión ante una autoridad administrativa o judicial que deba enterarse de la situación personal del trabajador que plantea una acción legal para reclamar la violación de alguno de sus derechos relacionados con la privacidad, tanto por cuestiones de forma como de fondo.

En materia laboral, el trabajador que considere haber sufrido alguna violación a las condiciones de trabajo y que termine en un despido sin responsabilidad patronal, estará en la posibilidad de acudir a la sede judicial para buscar la reparación del daño sufrido. Es entonces que, en virtud del principio de carga de la prueba, el patrono demuestre que su accionar fue legítimo.

Cuando la decisión que toma el patrono se fundamente en datos del trabajador, debe entenderse en su sentido más amplio. Por ejemplo, cuando en la utilización de un circuito cerrado se descubre un fraude o una falta grave cometida por el trabajador que faculta su despido sin responsabilidad patronal. Sin embargo, esta prueba obtenida, mediante un sistema de vigilancia, solo debería ser considerada como válida si el sistema de monitoreo es previamente conocido por el trabajador y, además, es acorde con la teoría de protección de datos que se ha tratado de explicar en este trabajo y, de forma específica, aplicada al campo laboral.

En este tema, el laboralista español Jose Luis Goñi Sein, señala que

> *Debe haber una adecuación o correspondencia de las imágenes así adquiridas y la finalidad de la instalación de tal sistema de grabación con la medida disciplinaria, o, de no haberla, ha de tratarse de incumplimientos especialmente graves, porque las imágenes y sonidos que constituyen un subproducto no querido, una consecuencia meramente accidental de la utilización de los sistemas de videovigilancia, no deben servir – como se señala con anterioridad – para legitimar medidas disciplinarias o para acusar a un empleado de una falta disciplinaria menor" [50].*

La recomendación del citado tratadista está relacionada con el sentido de pertinencia de la recopilación de datos, es decir, si llevamos el ejemplo de los datos obtenidos mediante un sistema de vigilancia por circuito cerrado, se debe decir que su utilización debió estar ampliamente justificada, por ejemplo, en la necesidad de resguardar los bienes del patrono.

Además, para respaldar su legalidad, al menos desde la perspectiva de esta investigación, la aplicación del sistema de monitoreo debió responder a una cuestión objetiva, es decir, de aplicación general para todo el personal y no solamente para el trabajador al que se pretendía sancionar. De lo contrario, se podría estar en presencia de lo que en doctrina laboral se conoce como persecución laboral, siendo una de sus manifestaciones la recopilación de pruebas mediante sistemas que solamente se aplican a un trabajador y no a la generalidad.

[50] GOÑI SEIN, Jose Luis: LA VIDEOVIGILANCIA EMPRESARIAL Y LA PROTECCION DE DATOS PERSONALES, Primera Edición. Editorial Aranzado, 2007, p. 222.

En este sentido, señala Roqueta Buj, lo siguiente:

> *Por último, a la empresa le corresponde acreditar todos los hechos relevantes para determinar el alcance de la infracción. Así, debe probar las llamadas telefónicas que hace el trabajador de índole particular, si se hacen dentro de su jornada laboral o fuera de ella, número de ellas, el tiempo al que alcanzan e importe de las mismas. En los casos de navegación por Internet, a la empresa le corresponde la prueba no sólo de navegación en determinadas páginas web (páginas visitas y tiempo utilizado para su visión), sino también que ésta no tiene relación alguna con el trabajo. Por lo demás, la determinación de estos hechos deberá figurar previamente en la carta de despido …*[51].

En tesis de principio, las pruebas obtenidas mediante cualquier sistema de captación de datos, por ejemplo: videos, fotografías, registros de accesos a Internet, entre otros; podrían ser aceptados en sede judicial laboral en el tanto se hayan respetado los derechos fundamentales del trabajador, en este caso, relacionados con su privacidad y la posibilidad de haber exigido la garantía de su cumplimiento. Cualquier mecanismo de obtención de información debe ser rechazado por un tribunal laboral si su obtención implica una lesión a tales derechos del trabajador.

[51] Roqueta Buj, Remedios: Uso y Control de los Medios Tecnológicos, Primera Edición. Editorial Tirant Lo Blanch, 2005, p. 111.

3. Efectos de la prueba ilícita

En materia laboral procesal, una vez que se determina que un patrono fundamentó una acción disciplinaria en una prueba ilícita, podrían darse dos posiciones:

a. Que la sanción disciplinaria se mantenga al margen de la posible calificación de ilícita, en el caso que la falta del trabajador se demuestre por otros medios; o
b. Que la calificación de la prueba afecte también la calidad del despido o como ha mencionado Goñi Sein en un trabajo sobre este tema "*en tanto que la prueba se instrumenta a la consecución de un fin específico, cual es la acreditación de una causa justa para despedir, la vulneración de derechos y libertades fundamentales en la obtención de la misma, que implica su ilicitud, debe viciar de nulidad, igualmente, el instituto jurídico al que se vincula"* [52]

En Costa Rica, la posición de los tribunales laborales parece ser la segunda, es decir, considerar que la declaración de ilegalidad de la prueba implica la declaración de nulidad del despido con el consecuente pago de prestaciones a favor del trabajador. Sin embargo, diferente sería el caso en que la acción disciplinaria se logra demostrar por otros medios, en cuyo caso debe darse la valoración de cada uno de ellos,

[52] GOÑI SEIN, Jose Luis: LA VIDEOVIGILANCIA EMPRESARIAL Y LA PROTECCION DE DATOS PERSONALES, Primera Edición. Editorial Aranzado, 2007, p. 235.

atendiendo a los principios de la sana crítica y a la conciencia con que el Juez de Trabajo debe analizar las pruebas para la aplicación de una sanción en perjuicio del trabajador. Así ha sido aceptado por la Sala Segunda de la Corte Suprema de Justicia que al efecto ha mencionado:

> quien juzga debe valorar los elementos de convicción traídos a los autos y, además, debe aplicar las reglas de la sana crítica y la razonabilidad, pues esa norma no contempla un régimen de íntima o de libre convicción. A la luz de los parámetros de constitucionalidad, esa concreta norma fue analizada en la sentencia de la Sala Constitucional número 4.448, de las 9:00 horas del 30 de agosto de 1996, en la cual se estimó que no resulta inconstitucional la facultad de los jueces laborales de apreciar la prueba en conciencia, siempre y cuando se dicte un fallo fundamentado en aplicación de las reglas de la sana crítica y la razonabilidad. Con base en lo anterior, se impone determinar si los integrantes del tribunal incurrieron o no en los supuestos errores de valoración acusados por el recurrente, a efecto de determinar si, efectivamente, en el caso bajo examen, resultaba procedente el pago de los extremos reclamados por el actor. [53]

C. LA PROTECCIÓN DE DATOS DEL EX TRABAJADOR

1. Vigencia de la Protección de Datos

En este punto, nuevamente se presenta la disyuntiva que representa la falta de regulación en el país, que implica, de manera insistente, la falta de claridad en cuanto al plazo que un patrono puede mantener en sus bases de datos la información personal de un trabajador y hasta cuándo podría hacer un uso lícito de ella.

En legislaciones de otros países existe lo que comúnmente se conoce como el "derecho al olvido" o "principio de limitación en el tiempo", esto implica que los datos deben desaparecer del archivo o base de datos una vez que se haya cumplido el fin

[53] Resolución número 246 – 2009. Sala Segunda de la Corte Suprema de Justicia.

para el que fueron recabados y que, para efectos de este estudio, sería la terminación de la relación laboral.

Por ejemplo, en la empresa que suministra datos de un trabajador a una base de datos de empleo y brinda la información recopilada, en su momento, referente a un grado académico que el trabajador años más adelante ha superado ampliamente. Sin duda, esa información no actualizada puede dejar por fuera de un nuevo proceso de reclutamiento al trabajador, lo cual le afecta directamente.

En Argentina, donde existe legislación específica sobre el tema, el inciso 7 del artículo 4º de la Ley de Protección de Datos señala que los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. De igual forma:

> *…refuerza este principio lo establecido por el párrafo tercero del artículo 4 del Decreto 1558/2001 que al reglamentar su ejercicio indica que "el dato que hubiera perdido vigencia respecto de los fines para los que se hubiese obtenido o recolectado debe ser suprimido por el responsable o usuario sin necesidad de que lo requiera el titular de los datos* [54]*.*

Los datos personales de los trabajadores deben ser adecuados a las finalidades para las cuales fueron recabados, en este sentido y dependiendo de la finalidad que la empresa haya informado a sus trabajadores, tratará los datos conforme a este principio o no.

[54] Información tomada de www.protecciondedatos.com.ar; agosto 2008

La doctrina española sobre el tema suele considerar que la conservación de datos en poder de la empresa debe ir aparejada a la utilidad o vigencia del contrato que los origina. Es decir, "*en la medida en que la relación entre el empleado y la empresa está vigente, se entiende justificado el mantenimiento de todos los datos que pudieran recabarse durante dicha relación contractual*"[55].

Con carácter general, la empresa conserva los datos de los trabajadores al día, puesto que éstos deben comunicar a la empresa, por su propio interés, las modificaciones producidas en su situación personal, estado civil, hijos, entre otros; por ejemplo, para beneficiarse de las ventajas fiscales que establece la ley, específicamente, de gastos deducibles del impuesto de renta.

En lo que se refiere a la eliminación de datos, según la legislación española, se estima que los datos deben ser bloqueados cuando se extingue la relación laboral, y conservados, en todo caso, por un plazo no superior a cuatro años. Este plazo incluiría los posibles reclamos que se puedan hacer por: infracciones relativas al tratamiento de los datos (3 años), las derivadas del contrato laboral (1 o 3 años, en caso de sucesión de empresas) o las derivadas de aspectos sociales (4 años).

En Costa Rica tampoco existe una norma expresa que resuelva esta situación. Sin embargo, el artículo 6 del proyecto del proyecto de "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales", se indica que los datos de carácter personal serán conservados solamente por el tiempo que permita, de forma efectiva, la identificación de la persona con los fines para los que se creó la base de

[55] Información tomada de http://delitosinformaticos.com/protecciondatos/rrhh.shtml, agosto 2009

datos, y "*en ningún caso serán conservados los datos personales que puedan de cualquier modo afectar a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición legal en contrario*"[56].

Ante la falta de regulación específica, el patrono debería conservar los datos personales del trabajador, por lo menos un año después de finalizada la relación laboral, plazo que la ley laboral costarricense establece como el período con el que cuenta el trabajador para reclamar los derechos devenidos de una relación laboral. Sin embargo, en virtud de que son muchas las situaciones que se pueden presentar y que podrían interrumpir dicha prescripción, se considera que un plazo de cuatro años es un período razonable.

Existe otro tipo de información que puede ser almacenada por un plazo mayor de hasta de diez años. Se refiere a todos los datos relacionados con la remuneración del trabajador que podrían ser solicitados por la Caja Costarricense de Seguro Social,

[56] Artículo 6: 1. Solo podrán ser recolectados, almacenados y empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimos para los que se han obtenido. 2. Los datos de carácter personal objeto de tratamiento automatizado o manual no podrán utilizarse para finalidades distintas de aquellas para los cuales los datos hubieren sido recogidos. 3. Dichos datos serán exactos y puestos al día, de forma que respondan con veracidad a la situación real del interesado. 4. Si los datos de carácter personal registrados resultaren ser inexactos en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por el responsable del fichero por los correspondientes datos rectificados, actualizados o complementados. Igualmente serán cancelados si no mediare un consentimiento legal y legítimo o estuviere prohibida su recolección. 5. Los datos de carácter personal serán cancelados por el responsable del fichero cuando hayan dejado de ser pertinentes o necesarios para la finalidad para la cual hubieren sido recibidos y registrados. **No serán conservados en forma que permita la identificación de la persona en un período que sea superior al necesario para los fines con base en los cuales hubieren sido recabados o registrados. Sin embargo, en ningún caso serán conservados los datos personales que puedan de cualquier modo afectar a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición legal en contrario. 6. Serán almacenados de forma tal que se garantice plenamente el derecho de acceso por la persona interesada. 7.** Es obligatoria la cancelación de datos por el fallecimiento o deceso confirmado de la persona, y se define un año como plazo para tal efecto. 8. Se prohíbe el acopio de datos por medios fraudulentos, desleales o ilícitos. 9. Los archivos de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública.

en este plazo. Esta misma tendencia es seguida por la legislación argentina y así fue puesto de manifiesto en una resolución de sus Tribunales de Justicia que establece:

> *A nuestro entender, el término de 10 años es razonable (art. 28 CN.), pues el plazo es más que suficiente para darle un valor útil a la información y además no se coloca al recolector de información en una situación desigual frente al registrado si se le permite tener ese dato por un plazo determinado. A nuestro juicio se trata de la fijación de límites temporales para el ejercicio de un derecho que en forma alguna vulnera la igualdad constitucional*[57].

Este mismo término de diez años ha sido reconocido por la Sala Constitucional de la Corte Suprema de Justicia, en relación a casos que estrictamente tienen que ver con la Protección de Datos del Trabajador, así por ejemplo:

> *Señala el recurrente que en el sistema del Consejo de Seguridad Vial, tanto en la página en Internet como en los registros físicos, aparecen los registros de multas sin plazo alguno, incluyendo las superiores a 10 años, así como los registros de multas por las cuales el infractor resultó absuelto de toda pena y responsabilidad. También señala que solicitó a ese órgano borrar del sistema al menos las infracciones que tenían más de 10 años, fundamentado en la jurisprudencia constitucional sobre la prohibición de penas a perpetuidad y el derecho al olvido, pero se le indicó que los votos citados se aplican al Ministerio de Seguridad Pública y no al MOPT. Se declara parcialmente con lugar el recurso y, en consecuencia, se ordena a la Directora Ejecutiva, así como al Jefe del Departamento de Infracciones, ambos del Consejo de Seguridad Vial, que de inmediato ejecuten las acciones pertinentes dentro del ámbito de sus competencias a fin de que se cancele de toda base de datos de acceso público, Internet u otros, los datos del amparado relativos a las boletas de Tránsito No. 1420804 1998, 146550 1997, 297639 1997 y 368885 1997* [58].

[57] Palazzi, Pablo. El habeas data y el derecho al olvido. Artículo publicado el 11 de mayo de 2006. Tomado de http://www.habeasdata.org/olvido, junio 2008.

[58] Voto 12973 del año 2009. Sala Segunda de la Corte Suprema de Justicia.

CONCLUSIONES

Una vez realizado este trabajo de investigación son varias las conclusiones a las que se ha podido arribar y las cuales se expresan a modo de enunciados que, por sí mismos, permitan formar una idea del resultado de la investigación:

- La protección de datos puede definirse como el amparo que deben recibir los trabajadores contra la posible utilización de sus datos personales por personas no autorizadas o que, estando autorizadas, realicen un uso indebido de dicha información y que trasgreda su privacidad. Esta protección debe garantizarla el empleador durante todos los procesos de recopilación de datos, su almacenamiento y su posterior cesión, es decir, todas las operaciones y procedimiento técnicos de carácter automatizado o no, que permitan: la recopilación, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones, y transferencias.

- Por datos de carácter personal se suele entender la información que, en un sentido muy amplio, pueda pertenecer al trabajador. En general se trata de toda información: numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable. Sin embargo, existen otros datos considerados como especialmente sensibles, que como criterio final de esta investigación, son los que principalmente debe proteger el empleador y conservarlos de forma confidencial. Se refiere a los datos de

carácter personal que revelen información del trabajador sobre: su ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual y comisión de infracciones penales o administrativas. Sin embargo, en atención al espíritu de las teorías de protección de datos, se considera que no debería existir una lista taxativa, siendo tan variadas las formas en las que un trabajador podría sentirse afectado por el mal uso de su información personal.

- La Organización Internacional del Trabajo ha señalado algunas recomendaciones tendientes a la protección de datos del trabajador, indicando que únicamente debería recopilarse aquella información que es estrictamente necesaria para la prestación del servicio contratado al empleado, o bien, cuando existan normas legales que obliguen a ello, por ejemplo, para alimentar los reportes que se hagan a instituciones de seguridad social.

- La información de un trabajador puede almacenarse y conservarse a través de diversos sistemas que pueden ir desde los más sofisticados a nivel tecnológico hasta las más sencillas formas de archivo de información. A nivel doctrinario, estas bases de datos son denominados ficheros, sin importar la forma o modalidad de su creación, almacenamiento, organización y acceso.

- En los países donde existe una regulación expresa, como por ejemplo España y Argentina, los patronos están obligados a registrar en las instituciones u organizaciones, que corresponda, todas aquellas bases de datos o ficheros

utilizados en las etapas del proceso de selección y reclutamiento del desarrollo de la relación laboral y, en algunos casos, una vez finalizada.

- Todos los procesos de protección de datos del trabajador, durante cualquier etapa de la relación laboral, deben estar ligados con la garantía de conservación del derecho la intimidad del trabajador, entendido como un derecho al control de la información referente a uno mismo. Este autocontrol de la propia intimidad ha sido denominado también como "autodeterminación informativa". Es la posibilidad del trabajador, del ciudadano en general, de decidir qué información suministrar al patrono, pero, además, tener un control sobre el estado, uso y conservación de sus propios datos personales.

- La empresa debe garantizar al trabajador el acceso a su información personal, cualquiera que esta sea, con el fin de verificar, corregir e incluso, solicitar la anulación de datos que no tienen relación con el trabajo.

- Los empleadores, públicos o privados, tanto personas físicas como jurídicas, deben establecer niveles adecuados de protección de datos de sus trabajadores a través de procedimientos internos, claramente establecidos, apegados a la legislación vigente que regula la materia. Los niveles de seguridad que instaure el empleador y los procedimientos internos que se deben cumplir para garantizar dicha protección dependen, en gran medida, del nivel de la información, es decir, de su carácter más o menos sensible. En cuanto más sensible sea la

información del trabajador, más rigurosos deben ser los procedimientos de seguridad.

- El recurso de hábeas data es un instrumento para controlar la calidad de la información recopilada, corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su posible transmisión. Este tema ha sido regulado debidamente por varios países; sin embargo, en Costa Rica, los esfuerzos legislativos no han sido suficientes y continúa la necesidad de una protección especializada que ayude a controlar el abuso que pueda presentarse. De momento se debe continuar acudiendo al recurso de amparo tradicional.

- La implementación de procesos de control de datos del trabajador, en cualquiera de sus manifestaciones, desde la más avanzada forma de monitoreo informático hasta la más rudimentaria verificación de información; debe estar amparada en un fin lícito que, de ninguna forma, busque la discriminación del trabajador o su descalificación por motivos personales. Para ello es necesario el establecimiento de reglas claras, escritas y previamente informadas al trabajador, de lo cual el empresario debería conservar un registro que permita demostrar su comunicación oportuna. A la hora de plantear estos procesos, las empresas y patronos, en general, deben tener en consideración tres criterios esenciales: idoneidad, necesidad y proporcionalidad; ya que probablemente estos serán tomados en cuenta por los tribunales de justicia para la resolución de cualquier conflicto.

- Además de la vía constitucional, el trabajador tiene la posibilidad de dar por terminado el contrato de trabajo cuando la violación de sus datos represente un perjuicio claramente demostrado. Sin embargo, se considera que esta no es la herramienta legal idónea para estos casos, porque ello conlleva la terminación de la relación laboral, dejando imposibilitado al trabajador de continuar con su servicio para la organización, con las consecuencias económicas que ello representa.

- Los sistemas de recopilación de datos pueden ser utilizados como medios de prueba pericial, en tanto exista una proporcionalidad entre los derechos fundamentales de los trabajadores y las sanciones impuestas como medidas disciplinarias, cuando en utilización de dichos sistemas se detecte la comisión de una falta.

RECOMENDACIONES

- La información que solicita el empleador de un trabajador y, en general, la que obtiene por cualquier medio, debe ser utilizada para fines estrictamente laborales con la compañía interesada en su contratación. Si el patrono tiene la intención de utilizar esa información y compartirla con terceros, debe contar con una autorización expresa, el consentimiento informado, del trabajador, lo cual debe estar en condición de demostrar en cualquier momento. Sin embargo, está claro que debe existir una conexión entre la información personal del trabajador y el objetivo para el que se solicita, ya que existen casos, como por ejemplo, el reporte de salarios a las instituciones de seguridad social, donde no existe un motivo para solicitar el consentimiento del trabajador. Sin embargo, en aras de preservar el principio de buena fe que debe regir las relaciones laborales, el patrono debe instaurar medidas de seguridad y control para asegurar la confidencialidad de la información, más allá de los fines del reporte que está obligado a realizar. Por ejemplo, debe proteger como confidencial la información personal de los trabajadores a nivel interno de la compañía.

  Todos los patronos debe revisar sus operaciones y procedimientos relacionados con la recolección, conservación y destrucción de datos personales de sus trabajadores, lo mismo que contar con políticas claras sobre la cesión a terceros de toda la información que ha sido puesta en su custodia. Se trata entonces de adecuar las informaciones obtenidas en los procesos de contratación, y los que se ejecutan durante la relación laboral, a las necesidades estrictamente

necesarias para el puesto que desempeña el trabajador. Todo ello, en estrecha relación con la finalidad para la cual se recopila la información, es decir, para ser utilizada durante la relación laboral.

- La empresa que requiere la contratación de un trabajador debe ejercer una tarea más preponderante en cuanto al control de los flujos transfronterizos de información, es decir, debe detenerse a analizar si los medios de donde se obtuvo son confiables, legales y, principalmente, si durante su obtención se respetaron los derechos del trabajador.

- En cuanto al acceso de datos enviados o recibidos por el trabajador a través de un correo corporativo, la recomendación general es suscribir acuerdos entre el trabajador y la empresa, al inicio de la relación laboral, que se fundamente en políticas internas claras y precisas. En estos acuerdos, el empleado debe prestar su conformidad para que el correo corporativo, no las cuentas de correo personal privada, que le asignan como herramienta de trabajo pueda ser controlada y vigilada por la compañía.

- En cuanto al uso del correo corporativo, desde el punto de vista del trabajador, y en vista de la falta de claridad de la legislación actual costarricense, las principales recomendaciones deben enfocarse en intentar que el contenido de sus correos sea serio y con fines estrictamente laborales. Evitar mensajes a direcciones compartidas por varias personas, las famosas cadenas de correos, y

notificar la recepción a los encargados en la empresa sobre la recepción no deseada de información que no ha sido solicitada o que no tiene ninguna relación con el trabajo.

- Para finalizar, los empleadores deben cumplir con la protección de datos de sus trabajadores y, en general, de todas aquellas personas que de forma directa o indirecta hayan participado de sus procesos de contratación. Así se evitarán sanciones económicas y morales, principalmente contribuirán al anhelo de todos: el respeto de los derechos de privacidad que le corresponde a las personas.

BIBLIOGRAFÍA

- BLÁZQUEZ ANDRÉS, Mª Consuelo; CARRASCOSA LÓPEZ, Valentín**;** *"Intimidad personal y limitaciones",* Informática y Derecho nº 4, UNED, Editorial Aranzadi, Centro Regional de Extremadura, Mérida, 1994.
- CABANELLAS DE TORRES, Guillermo; Diccionario Jurídico Elemental. Décimo cuarta edición, Buenos Aires, Argentina. Editorial Heliasta S.R.L., 2000
- CAMPUZANO TOMÉ, Hermidia. "Vida Privada y Datos Personales. Su protección Jurídica frente a la sociedad de la información". Madrid, España. Editorial Tecnos S.A. 2000.
- CANTERO RIVAS, Roberto**.** *"*Los derechos inespecíficos de la relación laboral: libertad de expresión, libertad ideológica y derecho a la intimidad*",* La Ley nº 4402, viernes, 24 octubre 1997
- CARDONA RUBERT, Ma. Belen. *"*Informática y Contrato de Trabajo". Valencia, España. Editorial Tirant Lo Blanch. 1999.
- CHIRINO SÁNCHEZ, Alfredo y HASSEMER, Winfried. "El Derecho a la Autodeterminación Informativa y Los Retos del Procesamiento Automatizado de Datos Personales. Buenos Aires, Argentina. Editores del Puerto S.R.L. 1997.
- CHIRINO SANCHEZ, Alfredo. "Informática y Derecho a la Intimidad. Perspectiva de Política Criminal". San José, Costa Rica. Editorial Mundo Gráfico. 1991.
- GOÑI SEIN, José Luis. "La Videovigilancia Empresarial y la Protección de Datos Personales". Primera Edición, Pamplona España. Editorial Aranzadi S.A. 2007

- PALAZZI, Pablo. "La Transmisión Internacional de Datos Personales y la Protección de la Privacidad". Buenos Aires Argentina. Primera Edición. Editorial Ad-Hoc. 2002.
- PIERINI, Alicia. "Habeas Data. Derecho a la Intimidad". Buenos Aires Argentina. Editorial Universidad. 1999.
- ROQUETA BUJ, Remedios. "Uso y Control de los Medios Tecnológicos de información y comunicación en la empresa." Valencia, España. Editorial Tirant Lo Blanch. 2005
- SALOM, Javier Aparicio, "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Editorial Aranzadi. Pamplona, España, 2000.

Artículos de Internet

- www.aranzadi.es/index.php/informacion-juridica/jurisprudencia, junio 2009.
- http://delitosinformaticos.com/protecciondatos/rrhh.shtml, agosto 2009
- http://es.wikipedia.org/wiki/Habeas_data., julio 2009.

- http://www.habeasdata.org/Carranza_Torres_Derecho_a_la_Imagen, julio 2009.

- http://www.microsoft.com/spain/empresas/asesoria/control_medios.mspx, junio 2009.

- www.habeasdata.org/PedroDubieProteccionDeDatosAmericaLatina, junio 2009.

- Aparisi, Angela. Nuevas tecnologías y contratos de trabajo. Artículo tomado de http://es.catholic.net/abogadoscatolicos/435/2085/articulo.php?id=36842, junio 2009.
- Carrasco Linares, Juan. Aspectos Generales de la Protección de Datos. Artículo tomado de www.delitosinformaticos.com/protecciondatos, agosto 2009.
- Chinchilla Sandí, Carlos. Personalidad Virtual: Necesidad de una Reforma Constitucional. Publicado en la Revista de Derecho y Tecnologías de la Información. Nº 3-2005. UNED, Costa Rica. Tomado de www.uned.ac.cr/redti/tercera/documentos/articulo1.pdf. Junio de 2009.
- Cuervo, José. La intimidad informática del trabajador. Artículo tomado de http://www.informatica-juridica.com., junio 2009.
- Durrieu, Roberto. El e – mail y el derecho a la intimidad. Artículo publicado en la edición digital de El Periódico La Nación de Argentina, el 20 de julio de 2009.
- Gargía Noguera, Noelia. Artículo tomado de Revista Digital Portalley.com. www.portaley.com/empresa/revista24042002.shtml julio 2009.
- López Arias, Angie. Crearán "personalidad virtual para proteger datos personales". Artículo publicado en el Diario La Prensa Libre, del día 17 de marzo de 2007. Tomado de www.prensalibre.co.cr/2007/marzo/17/abanico08.php
- Fernández, Claudio. Privacidad y Derecho a la Información. Artículo publicado en http://www.delitosinformaticos.com/ciberderechos/privacidad.shtm, junio 2009.
- Oller, Pedro. Artículo publicado en el Diario La República, de fecha martes 11 de marzo de 2008. Tomado de

http://www.larepublica.net/app/cms/www/index.php?pk_articulo=8049, junio 2009.

- Palazzi, Pablo. El habeas data y el derecho al olvido. Artículo publicado el 11 de mayo de 2006. Tomado de http://www.habeasdata.org/olvido, junio 2009.
- RIVERO SÁNCHEZ, Juan Marcos, Identidad virtual. Artículo tomada del sitio web: http://ww.virtualrights.org/NuevaFigura.doc, junio 2009.
- Santopino, Sabrina. Bases de Datos: Empresa deberán firmar acuerdos de confidencialidad. Artículo tomado de: www.infobaeprofesional.com/notas/20352-Bases-de-datos-empresas-deberan-firmar-acuerdos-de-confidencialidad.html; julio 2009.
- Tanús, Gustavo Daniel. Alguien te está mirando. Artículo publicado en Information Technology, revista editada por Mind Opener S.A. Edición Nº 50 - Noviembre 2000, pág. 144. Buenos Aires, Argentina. Tomado de: www.protecciondedatos.com.ar; julio 2009.
- Tanús, Gustavo Daniel. PROTECCION DE DATOS PERSONALES. PRINCIPIOS GENERALES, DEBECHOS, DEBERES Y OBLIGACIONES. Artículo publicado en Revista Jurídica El Derecho, 19/06/02, pág. 06. Buenos Aires, Argentina. Tomado de: www.protecciondedatos.com.ar; julio 2009.
- Vargas Cavallini, Orieta. Presentan Proyecto de Habeas Data. Noticia tomado de:www.tiquicia.com/articulos/derecho/Derecho_Informatico/40asamb180602.asp. Junio de 2009.
- www.agpd.es/portalweb. Sitio web oficial de la Agencia Española de Protección de Datos.

- www.asamblea.go.cr/actual/boletin/1998/set98/01set98.htm, junio 2009.
- http://www.weblaboral.net/aop/aop0014.htm. junio 2009.
- www.contraloriachiapas.gob.mx/transparencia/inicio/glosario3.php, julio 2009
- www.jus.gov.ar/dnpdpnew/. Sitio web oficial de la Dirección Nacional de Protección de Datos Personales de Argentina.
- www.monografias.com/trabajos50/habeas-data/habeas-data.shtml, agosto de 2009.
- www.portaley.com/protecciondatos, agosto 2009.
- www.protecciondedatos.com.ar/, agosto 2009.
- www.derecho.ucr.ac.cr./~gapmerayo/cursos/cursoDI/trabajosclase/habdata/habdata, junio 2009.
- www.tiquisia.com/editorial/index64.asp. Editorial titulado: El Habeas Data, fechado 15 de julio de 2002.

Artículos de Períodico

- Ruíz Ramón, Gerardo. “Diputados crearán agencia para la Protección de Datos Personales”. Períodico La Extra. Martes 30 de diciembre de 2008.
- Vizcaíno, Irene. “Corte restringirá acceso a datos contenidos en sentencias”. Periódico La Nación, Costa Rica. Lunes 26 de febrero de 2009.

Legislación Costarricense

- Código Civil
- Constitución Política de Costa Rica
- Ley de Jurisdicción Constitucional de Costa Rica

- Código de Trabajo de Costa Rica. Ley No.2. de 26 de agosto de 1943.
- Proyecto de Ley de Protección de la Persona Frente al Tratamiento de sus datos personales. Expediente número 16 679. Dictamen afirmativo de mayoría del 26 de noviembre de 2008.

Legislación Internacional

- Estatuto de los trabajadores, España
- Ley Orgánica de Protección de Datos de Carácter Personal, Ley Orgánica número 15/1999
- Ley de Protección de Datos de Argentina.

Jurisprudencia

Sala Constitucional de la Corte Suprema de Justicia

- Resolución número 05958 de las 14 horas 54 minutos del 19 de agosto de 1998 de la Sala Segunda de la Corte Suprema de Justicia.
- Resolución número 797 de las 15:00 horas del 18 de diciembre de 2003 de la Sala Segunda de la Corte Suprema de Costa Rica.
- Voto 15063-2005 de las a las quince horas con cincuenta y nueve minutos del primero de noviembre del dos mil cinco, Sala Constitucional de la Corte Suprema de Justicia.

- Voto número 4336 del año dos mil nueve, Sala Constitucional de la Corte Suprema de Justicia.
- Voto 5607 del veintiséis de abril de dos mil seis, Sala Constitucional de la Corte Suprema de Justicia.
- Voto 17380 del veintinueve de noviembre de 2006, Sala Constitucional de la Corte Suprema de Justicia.
- Voto 11054 del treinta y uno de julio de 2007, Sala Constitucional de la Corte Suprema de Justicia.
- Voto 11274 del año 2009, Sala Constitucional de la Corte Suprema de Justicia.
- Voto número 12434 de 2009, Sala Constitucional de la Corte Suprema de Justicia.
- Voto número 12537 de 2009, Sala Constitucional de la Corte Suprema de Justicia.
- Voto número 12683 de 2009, Sala Constitucional de la Corte Suprema de Justicia.
- Voto 12973 del año 2009. Sala Segunda de la Corte Suprema de Justicia.

Sala Segunda de la Corte Suprema de Justicia

- Resolución número 784 – 2000. Sala Segunda de la Corte Suprema de Justicia.
- Resolución número 94 – 2008. Sala Segunda de la Corte Suprema de Justicia.
- Resolución número 670 – 2008. Sala Segunda de la Corte Suprema de Justicia.

- Resolución número 246 – 2009. Sala Segunda de la Corte Suprema de Justicia.
- Resolución número 549 2009. Sala Segunda de la Corte Suprema de Justicia.