INTIMIDAD DE LOS TRABAJADORES Y TRATAMIENTO DE DATOS PERSONALES POR LOS EMPLEADORES*

Alberto Cerda Silva
Abogado y Candidato a Magister en Derecho de la Universidad de Chile.
Investigador del Centro de Estudios en Derecho Informático

SUMARIO: 1.- INTRODUCCIÓN.- 2.- LA LEGISLACIÓN SOBRE TRATAMIENTO DE DATOS PERSONALES.- El bien jurídico protegido: del derecho a la intimidad a la autodeterminación informativa.- Conceptos fundamentales y definiciones legislativas.- Los principios aplicables al tratamiento de datos.- Derechos del titular de datos personales.- 3.- EL TRATAMIENTO DE DATOS PERSONALES DE LOS TRABAJADORES EN LA EMPRESA.- Sobre los datos susceptibles de tratamiento.- Los derechos del titular de los datos personales en la relación laboral.- Terminación del contrato de trabajo y tratamiento de datos personales.- 4.- CONCLUSIONES.-

1.- INTRODUCCIÓN

Al abordar la intimidad de los trabajadores, y particularmente como ella puede verse aquejada frente al tratamiento de los datos personales que a ellos conciernen, parto de un supuesto, cual es que la Ley 19.628, normativa que regula el tratamiento de estos datos entre nosotros, es aplicable en el contexto de las relaciones laborales, prescindiendo de contar con alguna referencia en el Código del Trabajo a su respecto.

No obstante lo precedente, la Ley 19.759, última modificación de envergadura introducida al Código del Trabajo, contempló la incorporación de un nuevo artículo 154 bis, el que a la letra reza *"el empleador deberá mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral"*.[1]

---

* Ponencia pronunciada en el *"Seminario Relaciones Laborales y Tecnologías de la Información"*, organizado conjuntamente por la Facultad de Ciencias Jurídicas de la Universidad de Las Palmas de Gran Canaria y el Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, entre los días 7 y 9 de Agosto de 2002.

[1] Ley 19.759, modifica el Código del Trabajo en lo relativo a las nuevas modalidades de contratación, al derecho de sindicación, a los derechos fundamentales del trabajador y otras materias que indica, publicada en el Diario Oficial el 5 de Octubre del 2001.

Lamentablemente la historia fidedigna de la Ley 19.759, en especial del artículo recién referido, no permite extraer qué tenían en mente los legisladores al imponer tal obligación al empleador.[2] Sin embargo, entiendo que el artículo 154 bis del Código del ramo alude, si bien no en términos explícitos, a los preceptos de la Ley 19.628.

Ahora bien, qué significa que la Ley 19.628 sea aplicable en el marco de las relaciones regladas por el Código del Trabajo. Antes de responder tal interrogante, me parece imprescindible hacer siquiera una breve reseña al alcance de la Ley sobre Protección a la Vida Privada que reglamenta el Tratamiento de Datos Personales, ya que sobre la base de ella discurrirá posteriormente el análisis relativo al procesamiento de tales datos en el marco de las relaciones tejidas al abrigo del Código del Trabajo.

Hecho lo previsto en el párrafo precedente, dividiré mi presentación en tres segmentos atinentes al tratamiento de estos datos en la empresa: en el primero, examinaremos el tipo de datos que caen bajo el ámbito de nuestra legislación, tanto por su contenido como por la forma en que ellos se manifiestan; en el segundo, revisaremos la concreción de algunos de los derechos que la legislación adjudica al titular de los datos personales en el marco de la relación laboral; y, en tercer lugar, dada la relevancia que suele tener para quienes hacen ejercicio del derecho del trabajo, por la incidencia que tiene en las causas judiciales, es establecer sí con relación a éste tratamiento de datos personales pueden llegar a configurarse alguna de las causales de terminación del contrato de trabajo de aquellas previstas en el ordenamiento laboral. Finalmente, a modo de conclusiones, pese a las ventajas que la aplicación de la Ley 19.628 representa para garantizar los derechos fundamentales de los trabajadores, las consideraciones precedentes y otras evidenciarán la insuficiencia de sus previsiones para responder al tratamiento de datos que tiene lugar en el contexto laboral, dejando abierto el desafío para su regulación futura.

[2] La Ley 19.759 procuró innovar en la protección de los derechos fundamentales del trabajador al interior de la empresa, desde que algunos de ellos carecen de una vigencia efectiva en ella, por ejemplo a la hora de ser adoptadas decisiones administrativas en la empresa que colisionan con los mismos; para ello se reforzó el concepto de "ciudadanía laboral", explicitando la plena vigencia de los derechos fundamentales en el marco de las relaciones laborales, mediante modificaciones a los artículos 5, 154 y 154 bis del Código del Trabajo. Sin embargo, la revisión de las actas no consigna discusión legislativa en torno al artículo 154 bis, el que resultó aprobado prácticamente en los mismos términos que contemplaba el Mensaje Presidencial.

2.- LA LEGISLACIÓN SOBRE TRATAMIENTO DE DATOS PERSONALES

2.1. El bien jurídico protegido: del derecho a la intimidad a la autodeterminación informativa

Consideremos en primer término el bien jurídico a que se brinda protección mediante la legislación sobre tratamiento de datos, en nuestro caso la Ley 19.628, el derecho a la intimidad y su evolución hacia una nueva categoría jurídica, la autodeterminación informativa.

Si bien la intimidad es una pretensión que desde antiguo viene afirmada como una necesidad consustancial al desarrollo personal y más de una referencia se contiene a su respecto en la historia, remontándonos a Santo Tomás de Aquino, e inclusive a Aristóteles, la verdad es que jurídicamente cobra relevancia recién hacia fines del siglo XIX.

En efecto, en 1890 Louis Brandeis y Samuel Warren publican en la *Harvard Law Review* el artículo titulado *"The Rigth to Privacy"*, en el cual, con base en el derecho de propiedad y denotando la versatilidad evolutiva del *common law*, esbozaron el derecho a la intimidad como *"the right to be left alone»*.[3] El propósito era cimentar un derecho para hacer frente al hostigamiento por los medios de comunicación social de la época, para guardar reserva respecto de aquel aspecto de la vida personal que legítimamente podía ser excluido de la injerencia de la prensa; una intromisión de la que el propio Brandeis había sido víctima.

Sin embargo, establecer cuáles eran los límites de este derecho a la intimidad suscitó, y sigue haciéndolo, una enorme discusión en la doctrina; cuando menos se han esbozado tres criterios para establecer la extensión del derecho a la intimidad.[4]

Inicialmente se acudió a un criterio geográfico o espacial, en el cual se recurría a los espacios físicos para establecer la extensión del derecho; de tal suerte, es privado lo que tiene lugar entre las cuatro paredes, y público aquello que acontece fuera de ellas. Sin embargo, este criterio presenta ciertas áreas en las cuales resulta difícil establecer si estamos en presencia del derecho a la intimidad o no, tal como la situación de aquello que acontece en un restaurante. Ahora bien, la mayor crítica formulada a esta posición es que limita excesivamente aquello que debe entenderse como amparado por la intimidad, ya que en definitiva queda circunscrito a lo que pasa dentro del marco del hogar y, por analogía, al contenido de las comunicaciones telefónicas y la correspondencia.

[3] BRANDEIS y WARREN, *"The Rigth to Privacy"*, en Harvard Law Review, vol. IV, núm. 5, 1890. Trad., *"El derecho a la intimidad"*, Editorial Civitas, Madrid, 1995.

[4] GARCÍA SAN MIGUEL, Luis *"Reflexiones sobre la intimidad como límite de la libertad de expresión"*, en Estudios sobre el Derecho a la Intimidad, Editorial Tecnos, 1992, pp. 15 – 35.

Ante las insuficiencias del criterio antes expuesto, se elaboró una concepción subjetiva, que atiende más bien a la condición de la persona; en tal caso, será íntimo aquello que realiza una persona privada y público lo que realice un personaje público o una figura pública. Sin embargo, este criterio presenta el inconveniente de la ambigüedad de las categorías en que descansa, el menoscabo a la igualdad a que conduce su extremo –pues bajo su predicamento un personaje público queda sin intimidad alguna–, lo que obligaría a acudir a correcciones, las que evidenciarían aun más sus falencias.

En tercer criterio elaborado por la doctrina descansa en un concepto objetivo, en el cual más que atender a las figuras o a las personas se centra en la conducta desplegada por ellas: si se trata de una conducta destinada a satisfacer necesidades individuales es privada, en tanto que si está orientada a la satisfacción de necesidades de terceros es pública. Con todo, aún este criterio debe admitir hipótesis de conductas que siendo privadas tienen trascendencia pública y, en consecuencia, no podría resguardarse la intromisión a su respecto a partir de la excusa de quedar bajo la protección de la intimidad.

Este derecho a la intimidad, a un cierto margen en que la persona puede mantenerse a buen recaudo de la intromisión de terceros, recién recibe consagración en la Declaración Universal de Derechos Humanos de 1948, a partir de entonces recibe reconocimiento explícito en diversos instrumentos internacionales sobre derechos humanos, así como en constituciones y legislaciones de diversos países.[5]

Ahora bien, a medida que la tecnología y los medios de comunicación fueron extendiendo su alcance e incrementando su potencial el concepto esbozado por Brandeis y Warren, aquél del derecho a ser dejado en paz o derecho a ser dejado solo se mostró insuficiente, pues ya no sólo era necesario excluir a ciertas personas de lo que me acontecía, sino que en cierta forma controlar la información que terceros podían obtener de mi; es así como, tras diversas aportaciones, hacia los años setenta se configura lo que se ha denominado el derecho a controlar la información referente a mí persona: *"the right to control information about oneself"*.[6] Ya no sólo se trata de la imposibilidad que tienen terceros de entrometerse en lo que me sucede, sino en la posibilidad que yo tengo de controlar la información concerniente a mi persona y excluirla del conocimiento de aquellos, con antelación o aún una vez que se ha hecho circular tal información.

Sin embargo, los riesgos que aparejaba el procesamiento de información por los medios de comunicación de masas no guardan proporción con aquellos que resultan del tratamiento auto-

[5] Cf. entre otros instrumentos internacionales, además de la Declaración Universal de Derechos Humanos, el artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966, el artículo 11 de la Convención Americana de Derechos Humanos de 1969, y el artículo 16 de la Convención de Derechos del Niño de 1989.

[6] PARKER, *«A Definition of Privacy»* (1974) y FRIED, Charles, *"An Anatomy of Values"* (1979), cit. por GARCÍA SAN MIGUEL, Luis, *op. cit.*, p. 17.

matizado de los datos personales; el progresivo y exponencial desarrollo de la informática y las telecomunicaciones han originado nuevos peligros para los derechos fundamentales, ya en la celebración de la Conferencia Internacional de Derechos Humanos de Teherán de 1968, organizada por Naciones Unidas, se consideraron los límites que una sociedad democrática debía imponer para proteger los derechos humanos frente al creciente uso de la tecnología. En particular, para hacer frente al tratamiento de datos personales o nominativos, diversas experiencias legislativas se suceden a partir de comienzos de la década del setenta: Land de Hesse (1970), Suecia (1973), Estados Unidos (1974), Alemania (1977), Francia (1978), entre otras.

Inicialmente, la normativa sobre tratamiento de datos personales se construyó a partir del derecho a la intimidad, sin embargo pronto se evidenció la estrechez que tal bien jurídico suponía para los propósitos de tal legislación, pues en rigor más que pretender excluir a determinadas personas de ciertos aspectos de la vida de otra, se confería a ésta la posibilidad de controlar la información concerniente a sí, prescindiendo de si ella decía relación con su intimidad.

Es así como, en 1983 el Tribunal Constitucional Alemán se hace cargo de la insuficiencia antes consignada, al estimar que el número, entidad y agresividad de las preguntas contempladas en la Ley de Censo de 1982, importaba un atentado contra la autodeterminación informativa, esto es, contra la posibilidad efectiva de que el ciudadano pudiera controlar la información que estaba dispuesto a suministrar a los demás legítimamente.[7]

A partir de la construcción formulada por el máximo tribunal alemán, así como de la elaboración de la doctrina –con autores tales como Vittorio Frossini en Italia, Antonio Pérez-Luño y Pablo Murillo de la Cueva en España– se construye lo que se denomina libertad informativa, derecho que tiene un ciudadano cualquiera a controlar la información que le concierne. Este derecho es aquél sobre el cual se asienta la legislación sobre protección de las personas frente al tratamiento de datos personales.[8]

2.2. Conceptos fundamentales y definiciones legislativas.

Antes de proseguir es necesario establecer qué es lo que se ha de entender por dato personal, titular de tal dato y responsable de banco o registro de los mismos.

[7] Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en BJC Boletín de Jurisprudencia Constitucional, número 33, Enero 1984, Publicaciones de las Cortes Generales, Madrid. Trad. Manuel Daranas, pp. 126 – 170.

[8] FROSSINI, Vittorio. *"Los derechos humanos en la sociedad tecnológica"*, Anuario de derechos humanos, número 2, 1983, pp. 101 – 115; PÉREZ-LUÑO, Antonio Enrique. *"Los Derechos Humanos en la Sociedad Tecnológica"*, en Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, 1989, núm. 21, pp. 133 – 213; MURILLO DE LA CUEVA, Pablo Lucas. *"El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática."* Editorial Tecnos. Madrid, 1990.

Entre nosotros la ley concibe el *titular de datos personales* como la persona natural respecto de la cual se predica cierta información.[9] Ahora bien, no solamente es dato personal aquel que está asociado a cierta persona, esto es, a persona determinada, sino también a persona determinable, vale decir, cuando sometido el dato a cierto proceso es posible establecer el sujeto respecto de quien se predica, esto es, basta que esa información sea susceptible de ser asociada a determinado sujeto, de quien la estamos predicando, por ejemplo mediante el empleo de su rol único tributario.[10]

Estos datos personales son objeto de tratamiento, de su incorporación en bancos de datos o registros, lo que nos conduce a otro personaje previsto en la normativa: el responsable del banco de datos, esto es, el sujeto que en definitiva adopta decisiones respecto del contenido y del tratamiento que de esos datos personales se hace, que puede ser una persona natural o jurídica, privada como pública.[11]

Pero, nos resta establecer qué es lo que el legislador concibe como tratamiento de datos. Pues bien, al efecto la legislación ha optado por una definición sumamente amplia, ya que el tratamiento comprende la recogida de información, almacenamiento, procesamiento, transmisión, transferencia, cesión y, en fin, cualquier operación o complejo de operaciones o procedimientos técnicos de carácter automatizado o no que recaiga sobre los datos.[12] El propósito de la Ley 19.628 ha sido incluir toda hipótesis de acciones de que sean objeto los datos personales, a fin de evitar riesgos de elusión normativa.[13]

Pues bien, la legislación sobre tratamiento de datos personales ha experimentado una progresiva evolución y ella ha estado marcada por dos aspectos: por un lado, la disminución en los costes y mayor extensión en el empleo de los sistemas informáticos y, por otro lado, la creciente capacidad de estos para almacenar, procesar información y brindarnos respuesta satisfactoria a nuestros requerimientos.

En un comienzo la normativa surgida allá por los años setenta se limitaba simplemente a reglar las bases de datos de titularidad de organismos públicos, porque entendía que por los costos aparejados a la adquisición de un computador y por la cantidad de tiempo que había que incorporar en el procesamiento de información, los únicos que podían disponer de ellos eran entes públicos –normalmente, los servicios militares y estadísticos de los Estados.[14] Sin embargo, con posterioridad, a medida que los costos de los computadores bajaron y su capacidad de almacenamiento se hizo mayor, ha sido necesario regular también el tratamiento de los datos personales que realizan los privados, hipótesis en la cual habitualmente caen las empresas al verificar tratamiento de datos respecto de los trabajadores.[15]

[9] Vid. Artículo 2 letra fi) Ley 19.628 sobre Protección de la Vida Privada.
[10] Vid. Artículo 2 letra f) Ley 19.628 sobre Protección de la Vida Privada.
[11] Vid. Artículo 2 letra n) Ley 19.628 sobre Protección de la Vida Privada.
[12] Vid. Artículo 2 letra o) Ley 19.628 sobre Protección de la Vida Privada.
[13] Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, 3er Trámite, Diario de Sesiones del Senado, Sesión 18ª (anexo de documentos), p. 2096.
[14] Es el caso de la Ley de Protección de Datos del Land Hesse de 1970 (Alemania) y la Ley de Privacidad de 31 de diciembre de 1974 (Estados Unidos).

Igualmente, la primera legislación en la materia se limitaba al tratamiento automatizado de los datos, vale decir, sólo a aquellos que estaban insertos en un sistema informático. Sin embargo, a mediados de la década pasada se reparó en que tal definición muchas veces permitía que se burlara la normativa, mediante el subterfugio de no tratarse los datos automatizadamente, más aún ciertos registros especialmente sensibles aún se contenían en formato manual, por ejemplo las fichas de tipo médico. Entonces, frente a tal situación, lo que se ha hecho en la legislación comparada es ampliar el ámbito objetivo de protección, incorporando tanto el tratamiento automatizado como el manual, pues de lo contrario se corría el serio riesgo de que se burlasen los derechos de los titulares de tales datos.[16]

En consecuencia, dos definiciones van quedando claras: una, la normativa brinda protección tanto frente al tratamiento de datos personales verificado en forma automatizada como manual; y, segundo, se refiere tanto al tratamiento efectuado por organismos públicos como privados.

Hay otros puntos en los cuales no existe pleno consenso en el derecho comparado, por ejemplo si la protección debe hacerse extensiva sólo a las personas naturales, o también al tratamiento de datos concernientes a personas jurídicas. En el caso de nuestra normativa derechamente se optó por el concepto de que eran las personas naturales las que merecían protección; sin embargo, bien podría extenderse el ámbito subjetivo de tutela y, de hecho, en algunas latitudes así se ha optado.[17]

Otra de las definiciones centrales de la normativa sobre esta materia es si se establecen mecanismos de autocontrol o se adoptan medidas de heterocontrol. A este respecto debemos

[15] Entre otras, la Ley Alemana Federal de Protección de Datos de 1977 y la de 1990 (República Federal Alemana), la Ley 1998/204 sobre Protección de Datos de Carácter Personal (Suecia), la Ley de Informática, Ficheros y Libertades de 1978 (Francia), la Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal, LORTAD y Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (España), la Ley 25.326 protección de los datos personales de 2000 (Argentina) y la Ley 675 de 1996 sobre la tutela de las personas y otros sujetos respecto al tratamiento de datos personales (Italia).
[16] Es la situación de la Directiva 95/46/CE del Parlamento Europeo y el Consejo de 24 de Octubre de 1995 relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y de los Estados miembros de la Unión Europea que han traspuesto a su derecho interno las disposiciones de ella, tal como Inglaterra, Suecia, España y Francia, entre otros.
[17] Es el caso de la Ley 25.326 protección de los datos personales de 30 de octubre de 2000 (Argentina), la Ley 27.489 que regula las centrales privadas de información de riesgos de protección al titular de la información de 28 de junio de 2001 (Perú) y la Ley 675 del 31 de diciembre de 1996 sobre la tutela de las personas y otros sujetos respecto al tratamiento de datos personales (Italia).

formular una precisión inicial: todos los países del mundo entienden que frente a una infracción a los derechos del titular de los datos personales este puede acudir a los tribunales y pedir amparo, protección o resguardo a sus derechos, vale decir, el control ex-post en sede judicial es indiscutible. El eje de la discusión a este respeto radica en la necesidad o no de que el Estado adopte una institucionalidad que vele ex - ante por el cumplimiento de la normativa sobre tratamiento de datos personales y que tal cometido no quede entregado tan sólo a la gestión de los propios agentes intervinientes.

En Estados Unidos, la *Privacy Act de 1974* ha optado por un sistema de protección que carece de mecanismos de heterocontrol, es así como junto al imprescindible control jurisdiccional, encontramos el ejercicio de sus derechos por el propio titular de los datos y, eventualmente, la adopción de códigos deontológicos por las empresas que tratan datos personales, éstas son normas de conducta o de buenas prácticas adoptadas por las propias entidades que tratan datos, que no le son impuestas por el Estado, sino que, al contrario, son expresión de regulación autonómica.

En oposición a la política norteamericana se encuentra la de los países integrantes de la Unión Europea, los que estiman que es insuficiente dejar entregado el cumplimiento de esta normativa a la propia gestión del responsable del banco de datos o registros así como al ejercicio de los derechos del titular ante los tribunales, de modo que han generado una instancia de control de carácter administrativo –que desarrolla un rol similar al que entre nosotros desempeña la Dirección del Trabajo en la legislación laboral, pero en este caso referido a la legislación sobre datos personales–, una entidad que no solamente se encargara de controlar que se cumpla con la norma, sino que también de promoverla, asesorar, asistir, fiscalizar, eventualmente sancionar o cuando menos abogar ante tribunales por la sanción de las infracciones.[18] Es el caso, por ejemplo, de la Agencia de Protección de Datos en España, del Comisario de Control de Datos en Inglaterra y, en general, de todos los países integrantes de la Unión, ya que su normativa comunitaria gira sobre la constitución en el derecho interno de los Estados miembros de un ente que se encarga de realizar tareas de promoción y velar por el cumplimiento de las normas.

Cuando se examina la historia fidedigna de la Ley 19.628, particularmente los informes y discusiones parlamentarias, se podrá reparar en que los legisladores entendieron que estaban asumiendo en lo fundamental la normativa europea, aún cuando progresivamente el énfasis estuvo en la impronta de la legislación española de 1992, la Ley Orgánica sobre Regulación del Tratamiento Automatizado de Datos Personales

[18] Vid. Directiva 46/95/CE del Parlamento Europeo y el Consejo de 24 de Octubre de 1995 relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En Latinoamérica, es el caso de Argentina y, con matices bastante acentuados, el de Perú.

(LORTAD),[19] pero a la hora de definirse por un órgano de control, el legislativo adscribió derechamente la doctrina norteamericana y optó por entregar la fiscalización en el cumplimiento de la normativa a las propias partes involucradas y no hacer intervenir al Estado, salvo en cuanto al rol que compete a los tribunales de justicia. No cabe duda que tal opción ha significado socavar profundamente la eficacia de la pretendida protección a las personas ante el tratamiento de datos nominativos que les conciernen.[20]

Otra de las definiciones centrales de una normativa sobre la materia es la opción entre un *modelo de tutela estático o dinámico.* El primero de ellos atiende fundamentalmente a la naturaleza de un dato –así por ejemplo, dentro de la normativa habrá datos personales y, a su vez, entre ellos ciertos datos que revestirán mayor protección, los denominados datos sensibles, los que de circular por doquier nos significarían un detrimento para nuestra intimidad o nos harían quedar expuestos a eventuales actos de discriminación.

Para quienes son laboralistas, recordarán que el artículo 2 del Código del Trabajo establece una serie de circunstancias por las cuales no se puede discriminar a la hora de contratar, las que, en lo fundamental, se corresponden con el concepto de datos sensibles. Estos datos son, entre otros, los relativos a la adscripción ideológica, ya sea política o religiosa, al comportamiento sexual y a la condición étnica; en fin, esos datos en principio no puede ser objeto de tratamiento, salvo con el consentimiento del titular de los datos y demás hipótesis de excepción prevista en la Ley 19.628.[21] Se trata de datos que merecen una especial protección, porque eventualmente alguien puede ser discriminado y no ser contratado por su origen racial, por sus antecedentes criminales, por pertenecer a determinado partido político, o abrigar determinadas convicciones religiosas o ideológicas, todas situaciones que el legislador repudia.

[19] Entre las diversas materias a que se refería la moción parlamentaria inicial se encontraba el tratamiento de datos personales, punto en que el proyecto manifestaba haberse fundado en la Ley 78-17, del 6 de enero de 1978, sobre informática, ficheros y libertades, de Francia; la ley de 14 de junio de 1984, sobre protección de datos, de Gran Bretaña; y, la ley N°48, de 9 de junio de 1978 sobre registro de datos personales, de Noruega. Consigna también haber tenido presente los artículos 18 numeral 4 de la Carta Fundamental de España y 35 de la Constitución de Portugal. Cf. Diario de Sesiones del Senado, Sesión 20 (anexo de documentos), pp. 3081 – 3082. En la tramitación posterior del proyecto dé ley, fue cobrando relevancia la Ley Orgánica 5/1992, de 29 de octubre de ese año, sobre regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), de España. Cf. Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, en Diario de Sesiones del Senado, Sesión 63ª (anexo de documentos), p. 7483.

[20] En el mismo sentido CUMPLIDO, Francisco, *"Análisis del Anteproyecto de Ley sobre Protección de Datos Personales elaborado por el Ministerio de Justicia (1990 – 1994)"*, en Ius et Praxis, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, Año 3 N°1, 1997, pp. 201 – 207, refiriéndose al proyecto elaborado por el Ministerio de Justicia, el cual contemplaba procedimientos de protección administrativo y judicial, un servicio al que se denominaba "Servicio Nacional para la Protección de Datos" y un "Registro General para la Protección de Datos".

[21] Vid. Artículo 10 Ley 19.628 sobre Protección de la Vida Privada.

Sin embargo, un modelo de protección estático tiene sentido hasta en tanto no sea factible verificar cruzamiento de bancos de datos, esto es, mientras el desarrollo de la informática era incipiente y la telemática –o sea, la transmisión de información de un lugar a otro del mundo a través de la red– era precaria, pero una vez desarrolladas suficientemente sucede que es posible confrontar el banco de datos de una gran multitienda, con el banco de datos de la administradora de tarjeta de crédito o aquél de la entidad administradora de cuenta corriente bancaria, y con ellas saber el tipo de lencería que compra determinada persona, la clase de locales que frecuenta por las noches, el tipo de publicaciones que adquiere y, a partir de ello disponer no de una fotografía, pero si de un perfil relativamente claro de su opción sexual, sin siquiera haberle preguntado cuál es ella. Es lo que en doctrina se denomina la *teoría del mosaico*, que no importa renunciar a cierta categoría de datos sensibles, pero admitiendo que datos que inicialmente parecen inocuos pueden devenir en una fuente de riesgo similar según las funcionalidades o usos a que sean destinados, lo que conduce al diseño de un modelo de tutela dinámico, en que cobrarán relevancia, entre otros, las condiciones de transmisión de los datos, la regulación del flujo transfronterizo de los mismos, los sistemas de seguridad y resguardo que debe adoptar el responsable del banco.

Finalmente, otra de las decisiones relevante es establecer si la normativa de tratamiento de datos personales va a ser una ley general aplicable bajo toda circunstancia y respecto, o bien se adoptará una serie de leyes especiales para cada contexto en el cual se realice tratamiento de datos personales. En este sentido, la Ley 19.628 ha optado por un régimen jurídico general, aplicable por cierto al tratamiento de datos verificado en el contexto de una relación laboral, lo cual es reafirmado por la modificación introducida al Código del Trabajo por la Ley 19.759 al incorporar el nuevo artículo 154 bis, a cuyo respecto ya nos abocaremos a examinar algunas de las interrogantes que resultan de tal aplicación de la ley.[22]

La generalidad de los países europeos ha configurado una normativa general, pero, a su vez, ha generado normas de carácter específico, ya sea legales o reglamentarias, referidas concretamente al tratamiento de los datos personales en el contexto de una relación laboral, en el entendido de que las normas generales resultan insuficientes y demandan una adecuación

[22] En este sentido, merece considerarse que Estados Unidos rechaza la técnica legislativa *omnibus* (normativa general) en el tratamiento de datos personales, acusando a los Gobiernos que recurren a su empleo de esgrimir la defensa de los derechos fundamentales para levantar barreras comerciales. En tanto, la Unión Europea repudia la técnica de legislación sectorial por dejar abandonados ciertos sectores, con lo cual no garantiza los derechos de los afectados, junto con carecer de una entidad que brinde tutela a los afectados y uniforme pareceres. Cf. ESTADELLA YUSTE, Olga *"La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales"*, Editorial Tecnos, Madrid, 1995, pp. 35 – 37, 40 – 43.

cuando tal tratamiento tiene lugar en el marco de la relación entre empleador y trabajadores.[23] De hecho, ya al final de mi exposición, podrán reparar en cuan razonable es adoptar una opción similar, ya que la normativa nacional presenta vacíos e inconsistencias ante ciertas hipótesis que se pueden suscitar en el marco de las relaciones laborales.[24]

2.3. Los principios aplicables al tratamiento de datos.[25]

Habiendo examinado las principales definiciones que competen al legislador a la hora de diseñar una ley sobre tratamiento de datos personales, y antes de entrar a considerar algunos problemas que nos representa tal normativa a la hora de proyectar sus efectos al tratamiento de tales datos que tiene lugar en la empresa, parece necesario examinar siquiera brevemente los principios que informan la materia y los derechos que la ley atribuye al titular de los datos personales.

Entre los principios rectores del tratamiento de datos personales deben destacarse los principios de calidad de los datos, consentimiento del titular, seguridad en las operaciones de tratamiento y, quizá si el más relevante de ellos, el principio de la finalidad; examinemos que implican cada uno de tales principios.

El *principio del consentimiento del titular* constituye la piedra angular sobre la cual se cimientan todas las legislaciones en la materia, e importa que siempre que se desee tratar datos personales de un sujeto cualquiera debe mediar el consentimiento informado del mismo, sin perjuicio de una serie de excepciones previstas en la ley, las que, tratándose de nuestra Ley 19.628, por su extensión menoscaban el propósito de brindar protección frente al tratamiento de datos nominativos.

[23] Cf. Data Protection Working Party, *"Opinion 8/2001 on the processing of personal data in the employment context"*, adopted on 13 September 2001. Una situación particular la representa Italia, ya que la tardanza en adoptar una legislación sobre protección de las personas respecto del tratamiento de sus datos personales, condujo a elaborar la protección frente al tratamiento de datos realizados en el contexto de las relaciones laborales a partir de disposiciones del Estatuto de los Trabajadores (Ley de 20 de mayo de 1970, nº30). Cf. LOSANO, Mario, *"Un proyecto de ley sobre la protección de los datos personales en Italia"*, en Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, 1989, núm. 21, pp. 61 – 94. La OIT también se inclina por la elaboración de disposiciones específicas aplicables a la utilización de datos personales de los trabajadores, cf. Número 1 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997.

[24] Cf. CERDA, Alberto, *"Relaciones Laborales y Nuevas Tecnologías"*, Revista Chilena de Derecho Informático de la Facultad de Derecho de la Universidad de Chile, número 1, año 2002, pp. 51 – 63.

[25] Para una revisión de los principios que han de informar el tratamiento de datos, cf. *"Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronteras de datos personales"*, adoptada por el Consejo de Ministros de la Organización de Cooperación y Desarrollo Económicos (OCDE) el 23 de septiembre de 1980, y *"Principios rectores para la reglamentación de los ficheros computarizados de datos personales"*, adoptados por la Asamblea General de la Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990.

De conformidad con el *principio de calidad de los datos*, es responsabilidad del responsable de la base contener datos actualizados, que se correspondan efectivamente con aquello que dicen representar y, a su vez, siempre para velar porque los datos sean expresión fiel de la realidad, el titular de los mismos dispondrá del derecho de rectificación, cancelación o bloqueo, según las diversas hipótesis previstas por la ley.

Por su parte, el *principio de seguridad en el tratamiento de los datos* se refiere a la adopción de medidas de diversa índole conducentes a resguardar la información contenida en los datos. En doctrina se distinguen tres tipos de medidas de seguridad susceptibles de ser adoptadas al respecto: físicas, que recaen sobre la infraestructura en la cual se contiene el banco de datos; lógicas, aquellas que operan sobre los medios técnicos de tratamiento; y, jurídicas, que son las suministradas por el ordenamiento jurídico.

Respecto de los medios lógicos, uno de los órganos consultivos de la Unión Europea acaba recientemente de proponer la adopción en el tratamiento de los datos personales en el marco de las relaciones laborales de cuando menos las siguientes medidas de seguridad: a) el empleo de login y password, esto es, nombre y clave de acceso a los sistemas informáticos; b) la generación de copias de respaldo periódicamente; y, c) la encriptación de mensajes o contenidos de datos personales, especialmente si estos van a ser transmitidos fuera de la empresa.[26]

Ahora bien, el *principio de la finalidad* es quizá el más relevante de los principios rectores en el tratamiento de datos personales, ya que estos pueden ser objeto de tratamiento en forma legítima sólo en cuanto respondan a una finalidad concreta y determinada, además de que las operaciones que recaigan sobre ellos no excedan de aquella.

Las recomendaciones elaboradas por la Oficina Internacional del Trabajo, que han debido informar el trabajo del legislativo, aunque a decir verdad la historia fidedigna de la ley nada consigna al respecto, contiene una amplia gama de criterios que serán de bastante utilidad, particularmente a la hora de incorporar cláusulas contractuales para salvaguardar los derechos de los trabajadores en instrumentos colectivos de trabajo, entre las cuales se presta gran atención a la finalidad del tratamiento de datos en un contexto laboral. De este modo, su artículo quinto se encarga de precisar que el tratamiento de datos personales de los trabajadores solamente es legítimo en cuanto responda a una finalidad concreta en el contexto de una relación laboral, así, por ejemplo, durante el proceso de selección de personal será legítimo acopiar antecedente en tanto sean pertinentes para efectos de calificar la idoneidad laboral del candidato, mientras que durante la relación el tratamiento será legítimo cuando los datos

[26] Cf. Data Protection Working Party, *"Opinion 8/2001 on the processing of personal data in the employment context"*, adopted on 13 September 2001, p. 22.

tengan por objetivo dar cumplimiento a las normas laborales, de seguridad social, u otras cargas impuestas por la ley.[27]

Ahora, sentado que todo tratamiento debe ajustarse a una finalidad, cabe preguntarse qué sucede cuando se hace un empleo de los datos que excede a aquella. La respuesta es inequívoca, el tratamiento deviene en ilegal y el responsable del banco de datos o registros, o quien trate los datos por su encargo, habrá de asumir la responsabilidad que le competa.[28]

Veamos algunos casos al respecto, tomados de jurisprudencia extranjera, ya que la nacional aún no nos los proporciona. No me extenderé sobre ellos y los diversos ribetes de relevancia jurídica que evidencian, pues entiendo serán objeto de análisis por otros de los panelistas que participan de este seminario.

En España se suscitó la situación de que un sindicato votó e hizo efectiva la huelga, sin embargo no todos los trabajadores participaron de ella, mas la empresa se sirvió de los datos relativos a afiliación sindical –los que habían sido suministrados para efectuar el descuento de la cuota sindical y posterior ingreso de tales sumas al sindicato– para descontar a los afiliados su ausencia originada en la huelga. Esta situación fue representada judicialmente, pues la operación de tratamiento era ilícita, ya que el uso que se hizo de los datos excedió la finalidad, lo que resultaba evidente al ser descontado de sus remuneraciones a algunos trabajadores que no habían participado efectivamente en la huelga, pese a encontrarse afiliados a la organización.[29]

Otra situación en que se exceden las finalidades se ha presentado en Italia, donde una empresa instaló un sistema de tarjetas de registro con el propósito de velar por la seguridad de las instalaciones, de este modo cada trabajador disponía de una tarjeta y clave numérica que le brindaba acceso a diversas secciones de la empresa, a la par que la empresa procesaba los datos de quiénes, por cuánto tiempo y cuántas veces había ingresado, también almacenaba en sus registros el número de ocasiones en que cada empleado hacia uso de la tarjeta para abrirse paso por sus dependencias. Pues bien, la empresa no solamente empleó los datos para efectos de velar por la seguridad de la misma, sino que llegó a establecer que había un trabajador relativa-

[27] Cf. International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997. Puede verse igualmente la Recomendación sobre las agencias de empleo privadas, R188, adoptada por la Conferencia General de la Organización Internacional del Trabajo, convocada en Ginebra por el Consejo de Administración de la Oficina Internacional del Trabajo, y congregada en dicha ciudad el 3 de junio de 1997, en su 85ª reunión.

[28] Entre nosotros, la Ley 19.628 establece disposiciones bastante generales aplicables al tratamiento de datos personales por mandato en su artículo 8.

[29] Tribunal Constitucional de España, sentencias 11/1998, de 13 de enero de 1998; 105/1998, de 18 de mayo de 1998; y 124/1998, de 15 de junio de 1998.

mente torpe, ya que usaba la tarjeta y digitaba su clave de acceso cuatro o cinco veces antes de ingresar a un mismo lugar, a raíz de lo cual tomó la medida disciplinaria del despido. El caso muestra un uso de los datos personales que excede los propósitos previstos inicialmente por la propia empresa.[30]

Tomemos un ejemplo en nuestra normativa para graficar cómo opera el principio de la finalidad y, de otra parte, las dificultades que nos puede originar establecer hasta que oportunidad resulta legítimo el tratamiento de los datos de un trabajador fundado en la relación laboral, ya que una vez que el dato ha sido empleado para la finalidad que legitimaba su tratamiento la empresa debía proceder a su cancelación o eliminación; sin embargo, el problema es que no siempre resulta sencillo establecer cuándo borro o elimino esos datos personales.

En el caso de las horas extras, por ejemplo, uno podría pensar que el procesamiento de información relativa a las horas de sobretiempo que labora una persona queda justificado para efectos del cálculo del sobresueldo, de manera que pagado este, normalmente a fin de mes, debe suponerse agotada la finalidad que legitimaba el tratamiento de tales datos y la empresa debía proceder a la eliminación de ellos. Sin embargo, el pago de sobresueldo no es la única circunstancia que justifica el tratamiento de datos relativos a las horas de trabajo de una persona, él resultará lícito en tanto sea pertinente contar con tales datos para efectos probatorios, o bien hayan transcurrido los términos de prescripción de las prestaciones u obligaciones que se originan de la circunstancia consignada en los datos. En el caso de las horas extras, podríamos suponer que siendo el plazo de prescripción de las acciones de cobro de seis meses contados desde su exigibilidad, una vez transcurrido tal plazo el tratamiento deviene en ilegítimo. No obstante, tampoco parece sea la respuesta correcta, pues si consideramos que la remuneración sobre las horas extraordinarias de trabajo forman parte de la base de cálculo de las cotizaciones previsionales, hemos de aceptar que, siendo el lapso de prescripción de la acción de cobro previsional de cinco años contados desde el término de la relación laboral, sólo después de transcurrido tal plazo la empresa carecería de causa que justificase el procesamiento de datos al respecto y, en consecuencia, debía proceder a eliminar los datos.[31]

[30] Al respecto la OIT ha recomendado que los datos personales reunidos con el objeto de garantizar la seguridad y buen funcionamiento de los sistemas automatizados no debía servir para controlar el comportamiento de los trabajadores. De igual modo, recurriendo al principio de la finalidad, la OIT acepta la utilización de datos sobre calificaciones o rendimientos de los trabajadores a efectos de ser utilizados para adoptar decisiones relativas a la introducción de nuevas ventajas sociales, como sucede con aquellos relativos a la facturación de clientes, pero repudia su empleo para fines disciplinarios. Cf. Número 5 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997.

[31] En similar sentido se ha pronunciado la Dirección del Trabajo en su dictamen 3677/189, de 6 de noviembre del 2002, de conformidad con el cual la conservación y exhibición de la documentación que sustenta el pago de las gratificaciones -como obligación específica del empleador- puede exigirse dentro del plazo de cinco años, contados desde el término de los respectivos servicios, por ser tal plazo, a lo menos, el de prescripción de mayor extensión concebido por la legislación, cual es, el aplicable a los derechos y obligaciones previsionales. Consignemos, claro está, que en caso alguno la Dirección del Trabajo hace cita a las disposiciones sobre tratamiento de datos personales.

2.4. Derechos del titular de datos personales.

Finalmente, antes de entrar a los tres tópicos propuestos al comenzar esta exposición, es necesario referirse a los principales derechos que asisten al titular de datos personales respecto de aquellos que le conciernen: el derecho a la información, el derecho de acceso y el derecho de rectificación, cancelación o bloqueo.[32]

El derecho a la información supone que el titular de los datos personales debe ser informado en el momento mismo en que son recogidos los datos de quién, para qué y porqué se requiere la información, así como sobre el carácter facultativo u obligatorio que tienen las respuestas del titular. Para efectos de resguardar al titular indicándole quiénes y qué categorías de datos tratan, así como otros antecedentes relacionados, el legislador ha dispuesto un sistema registral público, de responsabilidad del Servicio de Registro Civil e Identificación, aún cuando circunscrito únicamente a los bancos de datos de organismos públicos;[33] en consecuencia, las empresas, por lo general, no están en la hipótesis de verse obligadas a precisar el tratamiento de datos personales que efectúan sobre aquellos que conciernen a los trabajadores. Indudablemente la limitación del registro constituye una cortapisa para que el trabajador –y, en general, para que toda persona– pueda efectivamente ejercer los derechos que les irroga la ley, pues desconocen en varios extremos los antecedentes relativos a tal tratamiento.

Un segundo derecho que la Ley 19.628 reconoce a las personas es el derecho de acceso, por medio del cual el titular puede obtener del responsable del banco de datos o registro la indicación precisa de aquellos incluidos en ellos y que le conciernen; dicha entrega puede verificarse con periodicidad prevista en la ley, gratuitamente y en condiciones que aseguren su comprensión.

Ahora bien, una vez que se ha accedido a los datos que corresponden al titular, este puede reparar en que algunos de ellos son abusivos, no se justifica su tenencia, o bien son erróneos, circunstancias que conducen a un tercer derecho conferido al titular de los datos: el derecho de rectificación, cancelación o bloqueo. Cada uno de estos derechos opera en circunstancias precisas previstas por la ley y tienen por propósito poner término a un tratamiento ilegítimo de los datos personales que conciernen a su titular.

[32] Todos ellos merecen reconocimiento en el artículo 12 de la Ley 19.628; en cambio, nuestra legislación no prevé el derecho del titular de los datos a no ser objeto de decisiones de relevancia jurídica fundadas únicamente en el tratamiento de los datos que le conciernen, el que suele preverse en el derecho comparado.

[33] Vid. Artículo 22 Ley 19.628 sobre Protección de la Vida Privada.

El ejercicio de los derechos que la ley irroga al titular de los datos se verifica directamente ante el responsable del banco o registros de datos, o sea, ante el sujeto que adopta decisiones respecto del contenido de ellos. Sin embargo, si el responsable del banco desconoce los derechos del titular de los datos, la ley le asegura un medio procesal para el resguardo de los mismos: el *habeas data*, una acción por la cual se pretende reestablecer el derecho del titular afectado por el tratamiento ilícito de datos personales referidos a él. En nuestra legislación, el *habeas data* tiene lugar solamente en una instancia judicial que se sustancia ante los juzgados de letras en lo civil o ante la Corte Suprema, según las diversas hipótesis previstas por la ley; en cambio, otras experiencia de derecho comparado contemplan una instancia administrativa, ante la autoridad de control, por la cual se evita la judicialización inmediata del asunto.[34]

3.- EL TRATAMIENTO DE DATOS PERSONALES DE LOS TRABAJADORES EN LA EMPRESA.

Hecha ésta somera revisión respecto del alcance general de la ley que regula el tratamiento de datos personales, nos abocaremos a los tres temas anticipados: los datos personales susceptibles de tratamiento en el contexto de las relaciones laborales, el ejercicio de los derechos del titular de los datos personales en tal circunstancia y la posibilidad de fundar la terminación del contrato de trabajo en eventos acaecidos en relación con el tratamiento de datos.

3.1. Sobre los datos susceptibles de tratamiento.

Antes de proseguir, debemos puntualizar que los amplios términos con que la Ley conceptualiza los datos personales permiten afirmar que ella se refiere no sólo a contenidos en formato alfanumérico, sino que comprende documentos en formato de imagen y sonido, con tal que transmitan información concerniente a personas susceptibles de ser determinadas.[35] Inclusive, debe calificarse como tales a los datos relativos a dirección de correo electrónico, más

[34] Vid. Artículo 16 Ley 19.628 sobre Protección de la Vida Privada.

[35] En el mismo sentido, Article 29 – Data Protection Working Party, *"Opinion 8/2001 on the processing of personal data in the employment context"*, adopted at Bruselas on 13 Septembre 2001, pp. 2 – 3. La opinión citada revirtió la interpretación de la doctrina, que fundada en el artículo 33 de la Directiva 95/46/EC sobre tratamiento de datos personales, y prescindiendo de una concienzuda lectura de los considerandos 14º a 17º de la misma, sostenía que sería tarea de la Comisión estudiar la aplicabilidad de la mencionada directiva al tratamiento de datos de imagen y sonido. Vid. HEREDERO HIGUERAS, Manuel. *"La Directiva Comunitaria de Protección de Datos de Carácter Personal"*, Editorial Aranzadi, Pamplona, 1997, pp. 232 – 233; y, SUÑE LLINÁS, Emilio, *"Tratado de Derecho Informático. Volumen I: Introducción y Protección de Datos Personales"*, Universidad Complutense Madrid, España. 2000, pp. 103 – 104. Entre nosotros, es el parecer de CEA EGAÑA, José Luis, *"Los derechos a la intimidad y a la honra en Chile"*, en Ius et Praxis, Universidad de Talca, Facultad de Ciencias Jurídicas y Sociales, Año 6 N°2, 2000, p. 159.

conocidos como e-mail.[36] De modo que, desde que el dato puede ser asociado a una persona, la condición de identificación queda satisfecha.[37]

A efectos de establecer las condiciones que legitimen el tratamiento de datos, nuestra ley ha distinguido cuando menos dos categorías fundamentales: los datos personales en general y aquellos de éstos que son especialmente sensibles. El tratamiento en los datos personales en general se justifica cuando el titular confiere su consentimiento al respecto, o bien el legislador autorice a prescindir de él; la misma Ley 19.628 contempla diversas hipótesis que autorizan a obrar de tal modo.[38] Tratándose de los datos sensibles, de los que ya antes hemos hablado, su tratamiento puede tener lugar en tres circunstancias: cuando el titular consienta en ello, cuando la ley así lo permita y cuando fuere menester para la determinación u otorgamiento de prestaciones de salud.[39]

Pues bien, de aquellos datos que la ley califica de sensibles, dos merecen una consideración por el uso que de los mismos se hace en el contexto de una relación laboral: los datos de salud y los datos de carácter ideológico, ya sea se refieran a convicciones políticas o religiosas.

Respecto de los datos de salud, merece destacarse las más recientes innovaciones habidas en nuestro medio en la materia. En efecto, los formularios adoptados y la normativa actualmente vigente de la Superintendencia de Seguridad Social y de la Superintendencia de ISAPRES se adecuan de mejor forma a las recomendaciones de la Organización Internacional del Trabajo,[40] en orden a que el tratamiento de los datos de salud deben de disgregarse, ya que en caso de la licencia médica es justificable que el empleador tenga acceso a la información por lo que respecta al período de cese y eventualmente la determinación de si la condición de salud del titular es compatible o

[36] Entre nosotros ha prescindido de tal carácter la Dirección del Trabajo, en su dictamen 0260/0019 de 24 de enero de 2002, cuando al pronunciarse sobre las facultades de reglar y controlar el uso del correo electrónico por los trabajadores dependientes ha prescindido de considerar los efectos que en ello ocasiona la naturaleza de tales datos. Cf. CERDA, Alberto, *"Comentario al Dictamen de la Dirección del Trabajo: Uso del Correo Electrónico por los Trabajadores"*, en *Revista Chilena de Derecho Informático*, del Centro de Estudios en Derecho Informático de la Universidad de Chile, número 1, 2002, pp. 155 - 161.

[37] Cf. BIBENT, Michel, *"Informática, Personas y Libertades. El proyecto de ley español y la experiencia francesa"*, en Encuentros sobre Informática y Derecho, Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1992 – 1993, pp. 58 y 59, quien pasa revista a una serie de hipótesis que la autoridad de control de Francia, la Comisión Nacional de la Informática y las Libertades, ha calificado como datos nominativos sujetos a tratamiento automatizado, tales como dispositivos de identificación electrónica empleados en el desplazamiento dentro de la empresa, las comunicaciones de mensajería electrónica, datos de abonados gestionados por la televisión por cable, entre otros.

[38] Vid. Artículos 4 y 20 Ley 19.628 sobre Protección de la Vida Privada.

[39] Vid. Artículo 10 Ley 19.628 sobre Protección de la Vida Privada.

[40] Cf. Circular conjunta Nº 68 y 2020 de 27 de septiembre de 2002, de las Superintendencia de Isapres y de la Superintendencia de Seguridad Social que imparte instrucciones respecto del uso del nuevo formulario de licencia médica a contar del 1º de octubre de 2002; y, Resolución Exenta Nº 790, del Ministerio de Salud, que aprobó el nuevo formulario de licencia médica, impreso en la Casa de Moneda de Chile (Diario Oficial, 27 de septiembre de 2002).

no con el desarrollo de la prestación laboral; sin embargo, nada justifica que el empleador tenga derecho a acceder al diagnóstico en sí, no obstante lo cual hasta no hace mucho tal recomendación carecía de adecuado resguardo jurídico y práctico.[41] Se comprenderá la razonabilidad de una previsión como la sugerida por la OIT, si consideramos el atentado a la intimidad del trabajador que importa develar su estado de salud ante el empleador, sino peor aún al exponerlo a eventuales actos de discriminación arbitraria en su contra fundada precisamente en tales datos.

En cuanto a los datos de connotación ideológica, es decir, aquellos que se refieren a convicciones políticas, religiosas u otras creencias, el artículo 2º del Código del Trabajo prohíbe los actos de discriminación y califica como tales aquellos fundados en distinciones, exclusiones o preferencias basadas, entre otras, en motivos de religión u opinión política; como consecuencia de ello, nuestro legislador excluye el empleo de datos de tal naturaleza para condicionar la contratación de una persona. Sin embargo, esta no es una solución uniforme en derecho comparado ni en la doctrina, ya que tratándose de las denominadas *"empresas de tendencia"* –aquellas en las cuales existe un cierto compromiso ideológico del trabajador con la empresa–, se admite el tratamiento de datos de develen la ideología del candidato.[42] En Chile, cuando menos en términos teóricos, el legislador impide que el empleador pueda recabar tales antecedentes o en función de ellos condicionar su contratación. Ahora bien, la doctrina española ha mitigado el alcance de una excepción tal, pues le admite tan sólo cuando la naturaleza del cargo suponga la adscripción ideológica del trabajador para con los fines de la empresa, mas no cuando en la calificación laboral del mismo carezca de sentido su compromiso al respecto.[43]

En el mismo orden, hemos de considerar también en este breve examen, la reciente modificación introducida por la Ley 19.812 al artículo 2º del Código del Trabajo, prohibiendo que la contratación laboral quede condicionada a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial, ni exigir declaración ni certificado alguno en este sentido, salvo tratándose de trabajadores respecto de los cuales el empleador debe abrigar un grado de confianza superior, sea por las facultades que le son conferidas o por el cometido que les es confiado, con lo que se pretende poner freno al uso indiscriminado de datos personales de carácter patrimonial para efectos de calificar la idoneidad laboral de las personas.[44]

[41] Cf. Organización Internacional del Trabajo, Recomendación número 171 sobre servicios de salud en el trabajo, 1985. En similar sentido, respecto del tratamiento de datos médicos de los trabajadores, cf. Número 10 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997.

[42] Cf. Número 6.5 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997, en que admite, por vía de ejemplo, considerar las ideas políticas en la contratación de un periodista por un periódico afiliado a un determinado partido político.

[43] Sobre el tratamiento de datos personales de los trabajadores tratándose de las denominadas *"empresas de tendencia"*, cf. FERNÁNDEZ VILLAZÓN, Luis Antonio, *"Tratamiento automatizado de datos personales en los procesos de selección de trabajadores"*, en *Revista Relaciones Laborales*, Tomo I, 1994, pp. 510 – 538.

[44] Ley 19.812 modifica la Ley Nº19.628, sobre Protección de la Vida Privada (Diario Oficial, 13 de junio de 2002).

Al respecto, cabe destacar que ni los documentos de la comunidad económica europea ni los de la Organización Internacional del Trabajo consignan siquiera una sola referencia a los antecedentes comerciales, por cuanto tal práctica resulta ajena a la experiencia internacional, ya que el recurso de los antecedentes comerciales para calificar la idoneidad profesional en el proceso de selección laboral constituye una perniciosa costumbre nacional, que precisamente la Ley 19.812 ha pretendido erradicar.

Algo similar acontece con el requerimiento de los antecedentes penales de los candidatos: mientras en nuestro medio constituye un elemento mediante el cual se pretende calificar la aptitud laboral de las personas, en otras latitudes es una práctica rechazada, la que sólo por excepción logra ser admitida, en aquellos casos en los cuales por la naturaleza del trabajo sea necesario precaverse de ellos,[45] lo cual se aviene por lo demás con el pretendido carácter resocializador de las penas, pues no se ve como pueda emplearse los certificados de antecedentes para condicionar la contratación de una persona sin que ello signifique desconocer tal fin a la sanción penal. En este punto la Ley 19.628 ha establecido alguna cortapisa, pues ha prohibido a los organismos públicos que someten a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, salvo excepciones.[46]

3.2. Los derechos del titular de los datos personales en la relación laboral.

La Ley confiere al titular de los datos personales –según antes hemos visto- un haz de facultades para resguardar el derecho a la autodeterminación informativa, para permitirle controlar la información que le concierne, ya que el propósito es que el tratamiento de datos personales suponga el consentimiento de su titular.

Pues bien, precisamente la primera observación que suele hacerse respecto del tratamiento de datos en el contexto de una relación laboral dice relación con tal supuesto, pues caben dudas en cuanto a la existencia de un consentimiento libre e informado por parte del trabajador al tratamiento de datos por el empleador –a lo cual nuestra Ley 19.628, en un exceso de celo condenado al desuetudo, ha agregado que ha de constar por escrito–, riesgo mayor durante la etapa de selección de personal, tanto por la posición que ocupa el candidato, como por la recogida de información suministrada por terceros prescindiendo siquiera de su conocimiento.

[45] Cf. Article 29 – Data Protection Working Party, *"Opinion 8/2001 on the processing of personal data in the employment context"*, adopted at Bruselas on 13 Septembre 2001, pp. 16 –17. En igual sentido, número 6.5 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997.

[46] Vid. Artículo 21 Ley 19.628 sobre Protección de la Vida Privada.

La circunstancia de que la relación laboral suponga un vínculo de subordinación y dependencia del trabajador respecto del empleador, llamada la atención de la doctrina, que apunta hacia la *"desmitificación del papel del consentimiento"* con pretensiones de expreso y escrito que el trabajador ha de prestar para el tratamiento de los datos que le conciernen por su empleador.[47]

En consecuencia, ante la relativa libertad en el consentimiento del trabajador, parece razonable adoptar medidas de resguardo para el tratamiento de los datos en un contexto laboral, que bajo otras condiciones resultaría innecesario, punto que queda entregado –ante la decidía legislativa– a la regulación autonómica, particularmente mediante instrumentos colectivos de trabajo, sin perjuicio del rol que compete a la Dirección del Trabajo en la materia. Ya luego, al examinar la terminación del contrato de trabajo fundada en el tratamiento de datos personales, podremos apreciar a qué conduce aceptar que el consentimiento del trabajador experimenta un menoscabo en la relación laboral.

A este respecto, nuestro legislador ha omitido conferir a los representantes de los trabajadores algún rol para contribuir a la protección de los derechos de sus representados, más aún de aplicarse lisa y llanamente la Ley 19.628 hemos de aceptar que alguno de tales derechos no admiten siquiera la interposición de dichos representante. Huelga decir que la experiencia en derecho comparado es otra, por ejemplo imponiendo a las empresas un acuerdo con la representación de los trabajadores antes de la introducción de mecanismo de control alguno en ella, admitiendo la asistencia al trabajador en ejercicio de los derechos que le competen como titular de los datos que le conciernen, e inclusive haciendo extensivo a los representantes de los trabajadores los deberes de confidencialidad previstos para quién trata datos nominativos por sí o mediante encargo.[48]

Con todo, ya antes hemos precisado que la ley autoriza el tratamiento de datos personales prescindiendo del consentimiento del titular en determinados casos. Esta hipótesis es recurrente en el procesamiento de datos efectuados por el empleador, tal como sucede con los registros de asistencia y remuneraciones, previstos en los artículos 33 y 62 del Código del Trabajo, respectivamente. En cambio, a diferencia de nuestra Ley 19.628, la Directiva 95/46/CE nos ofrece una solución más pragmática, al referirse a los principios relativos a la legitimación del tratamiento de datos, ha impuesto a los Estados miembros que éste sólo pueda efectuarse con el consentimiento inequívoco del interesado, o, entre otras excepciones, se prescindirá de aquél cuando el tratamiento es necesario para la ejecución de un contrato en el que el interesado sea parte, cuya es la hipótesis relativa al tratamiento de datos personales de los trabajadores por la empresa originada con motivo del contrato de trabajo.[49]

Para garantizar la transparencia en el tratamiento de los datos personales de los trabajadores, las recomendaciones de la OIT no se limitan a contemplar el derecho de acceso de aquellos a los datos procesados por el empleador, sino que sugieren imponer a este la obligación de suministrar regularmente a los trabajadores información general respecto de tal tratamiento, el tipo de datos conservados, a quienes son comunicados y el empleo dado a los mismos;[50] con tales medidas, las recomendaciones procuran empoderar a los trabajadores a efectos de hacer ejercicio de sus restantes derechos, sin las limitaciones que supondría hacer exigencia de acceso a los datos que les conciernen.

Por último, debemos consignar las dificultades que tiene concretar el derecho de rectificación respecto de los denominados "datos apreciativos", aquellos que comprenden juicios, apreciaciones o valoraciones subjetivas que se predican de una persona determinada o determinable, frecuentes a efectos de evaluación de los trabajadores. Sobre el particular somos de la opinión de que tales datos quedan afectos al régimen jurídico previsto en la Ley 19.628.[51] Sin embargo, nuestra normativa evidencia serias deficiencias frente al tratamiento de tales datos; de hecho, su empleo ilegítimo puede encubrir un medio para eludir el cumplimiento de los principios que informan el tratamiento de los datos personales, como resultaría del procesamiento de datos de calificación crediticia formulados a partir de datos de carácter patrimonial caducos. En el derecho comparado se adoptan algunos resguardos a su respecto, por ejemplo, admitiendo el derecho de réplica por parte de aquel

[47] CARDONA, Ma. Belén, *"Informática y Contrato de Trabajo"*, Tirant lo blanch, Valencia, 1999, p. 155.

[48] Sobre el particular, la OIT ha recomendado que toda actividad de acopio de datos, así como las reglas que le gobiernan y los derechos deben ser informados a los trabajadores y sus representantes, que estos deben cooperar conjuntamente con los empleadores en la protección de los datos personales y en la elaboración de políticas empresariales que respeten la vida privada de los trabajadores y extiende la confidencialidad en el tratamiento de tales datos a los representantes de estos; admite la designación por los trabajadores de un representante o compañero de labores que los ayude en el ejercicio de su derecho de acceso; y la necesidad de informar y consultar a los representantes de los trabajadores sobre la instalación o modificación de sistemas automatizados de tratamiento de datos y sistemas de vigilancia electrónica, así como de la finalidad, contenido, aplicación e interpretación de cuestionarios y pruebas relativos a datos personales de los trabajadores, entre otros. Cf. Números 5, 11.5 y 12 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997.

[49] Cf. Artículo 7 de la Directiva 95/46/CE del Parlamento Europeo y el Consejo de 24 de Octubre de 1995 relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[50] Cf. Números 8 y 11 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997.

[51] En sentido contrario, MAGLIONA, Claudio, *"Habeas data y protección de datos personales en Chile"*, en http://www.adi.cl/pdf/magliona2.pdf (visita 16 de enero 2003), p. 2.

a quien concierne, criterio propugnado por la OIT, que se materializaría permitiéndole consignar su propia versión respecto de los juicios que se emiten a su respecto.[52]

3.3. Terminación del contrato de trabajo y tratamiento de datos personales.

Para establecer si con motivo del tratamiento de datos personales de los trabajadores efectuado por la empresa puede configurarse alguna de las causales de terminación de contrato de trabajo previstas en nuestra legislación, debemos considerar cuando menos dos hipótesis: por un lado, el tratamiento ilegítimo del empleador a datos de sus dependientes y, por otro lado, la negativa o falsedad en que incurra el trabajador a la hora de suministrar datos que le conciernen a su empleador.

Antes de avanzar, conviene anticipemos que nuestro Código del Trabajo no establece una causal explícita que vincule el tratamiento de datos personales de los trabajadores con alguna de las causales de terminación contempladas en él. En consecuencia, y puesto que nuestro régimen de cese laboral es reglado, debemos recurrir a la doctrina que nos ayudará a asociar alguna infracción en la materia con alguna de las causales de terminación del contrato previstas en nuestra codificación.

En primer lugar, consideremos si las infracciones en que incurra el empleador en el tratamiento de datos pueden configurar una causal de término del contrato. Al respecto, habiendo dejado sentado que la incorporación del nuevo artículo 154 bis introducido por la Ley 19.759 al Código del Trabajo impone al empleador la obligación de reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral, hemos de considerar, por consiguiente, si la infracción a tal obligación legitima al trabajador para desahuciar el contrato, mediante el denominado *despido indirecto*, que resulta del concurso de los artículo 171 y 160 número 7 del Código del ramo, en virtud de los cuales se faculta al trabajador para poner término al contrato con derecho a indemnización, y eventualmente a los incrementos legales, si quien incurriere en incumplimiento grave de las obligaciones que impone el contrato fuere el empleador.

En la hipótesis esbozada en el párrafo precedente nos inclinamos por la afirmativa, esto es, una infracción al deber de reserva, más aún a alguno de los deberes que la Ley 19.628 impone al empleador en cuanto responsable de banco de datos o registros, faculta al trabajador afectado para poner término al contrato. Sin embargo, no ha de tratarse de una infracción

[52] Vid. número 11.12 de International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997. En otras se ha negado la posibilidad de proyectar mediante los datos apreciativos el contenido de datos ilegítimamente tratados, o bien se admite la adopción de ciertas restricciones en la materia por la autoridad llamada a preservar el cumplimiento de la legislación, es el caso de la facultad conferida a la Inspección de Datos para adoptar medidas correctivas prevista en la Ley 1998/204 sobre Protección de Datos de Carácter Personal de 29 de abril de 1998 (Suecia).

cualquiera, pues, según la jurisprudencia judicial reiterada, el Código del Trabajo exige que tal incumplimiento revista gravedad tal que permita fundar en él la terminación de la relación laboral.[53]

Por lo demás, esta ponderación judicial de las infracciones no ha de resultarnos ajena en el contexto de la Ley 19.628, ya que esta misma contempla entre sus disposiciones ciertos casos de contravenciones, de muy diversa gravedad, las cuales sanciona con multas de monto variable;[54] vale decir, tanto la Ley sobre Protección a la Vida Privada como el Código del Trabajo hacen suponer que no toda infracción a las disposiciones de uno y otro cuerpo normativo ameritan una sanción similar o de igual gravedad, sino que ella debe ser aquilatada judicialmente.

En segundo lugar, hemos de considerar si la negativa o falsedad en que incurriere el trabajador al suministrar a su empleador datos que le conciernen puede dar lugar a la terminación del contrato de trabajo por despido; situaciones que Dávara a dado en llamar el *fraude de la información* y la *huelga de los datos*.[55] Al respecto, podemos considerar la concurrencia de las causales previstas en los numerales 1, 5 y 7 del artículo 160 del Código del Trabajo, las cuales pasamos a examinar en los sucesivos párrafos.

Eventualmente, la falsedad en que incurriere el trabajador a la hora de proporcionar datos que le conciernen a su empleador podría ser calificada como una *falta de probidad*; sin embargo, tras la reciente modificación introducida al artículo 160 número 1 para configurar tal causal de despido es además necesario que tal falta del trabajador haya tenido lugar en el desempeño de sus funciones, circunstancia de difícil ocurrencia tratán-

[53] La Jurisprudencia de nuestros tribunales es conteste en manifestar que no toda infracción al contrato de trabajo reviste la gravedad necesaria para fundar la terminación del mismo, en este sentido: Corte de Apelaciones de Valparaíso, 27.01.2000, Rol número 191-99: *"el adjetivo 'grave' para calificar la dimensión que debe revestir el incumplimiento de sus obligaciones por parte de alguno de los contratantes al describir la causal, lo cual de inmediato da a entender que no cualquier incumplimiento la configura porque la gravedad implica cierta magnitud o importancia, o sea, debe entenderse por grave la falta que sea grande, de mucha envergadura, en lo que constituye la esencia o forma de una cosa y ello ocurrirá 'cuando implique la comisión de un delito, de algún acto fraudulento o de abuso de confianza en su caso, en este sentido, el requisito de gravedad que la falta debe revestir debe entenderse proyectado, en cierto modo, sobre la obligación misma cuya infracción se denuncia"*; Corte de Apelaciones de San Miguel, 09.03.2000, Rol número 364: *"No basta cualquier incumplimiento para despedir a un trabajador, sino, que este debe ser de tal magnitud, naturaleza e importancia que permita al sentenciador dar lugar al término de la relación laboral, sin el pago de las indemnizaciones"*; Corte de Apelaciones de Concepción, 04.09.1999, Rol número 270: *"Para que exista la gravedad exigida por la ley al fijar las condiciones de procedencia de la causal invocada para justificar el término de la relación contractual, es necesario que se manifieste en situaciones tales que importen una falta de cuidado o descuido grave que puedan equivaler al dolo como lo precave el inciso 1° del artículo 44 del Código Civil"*.

[54] Vid. Artículos 16 y 19 Ley 19.628 sobre Protección de la Vida Privada.

[55] DÁVARA, Miguel Angel, *"Manual de Derecho Informático"*, Aranzadi Editorial. Pamplona, 1997, pp. 101.

dose de la entrega de datos que le competen, con lo cual fundar el despido en tal hipótesis se nos presenta como improbable.[56]

La segunda causal en la cual puede asilarse el despido de un trabajador con motivo del tratamiento de sus datos personales puede tener cobijo en el número 5 del artículo 159; sin embargo, para configurar tal causal no bastará con un acto, omisión o imprudencia temeraria de parte del dependiente a la hora de suministrar datos de sí, sino que será necesario establecer un vínculo entre tal conducta y la afectación de la seguridad o funcionamiento del establecimiento, la seguridad o la actividad de los trabajadores, o a la salud de los mismos. En consecuencia, las exigencias que supone la aplicación de esta causal tornará muy marginal su empleo, sólo imaginable en situaciones en que la omisión o falsedad en que haya incurrido el titular de los datos suscite una afectación de aquéllas previstas por el legislador.

Finalmente, una tercera hipótesis normativa a la cual se podrá acudir frente a la omisión o falsedad en que incurra el trabajador al proporcionar datos personales que le correspondan es la prevista en el numeral 7 del artículo 160, esto es, *incumplimiento grave de las obligaciones que impone el contrato*. Sin embargo, hemos de formular tres reparos por lo tocante a un despido fundado en tal causal: primero, la disposición en examen no admite el despido frente a cualquier infracción en que incurra el trabajador respecto del contrato, sino que ella ha de revestir *gravedad*, circunstancia que, como ha quedado antes dicho, debe ser sopesada por los tribunales de justicia;[57] segundo, del tenor de la disposición hemos de suponer que ella no operaría tratándose de las faltas en que incurriere el trabajador al entregar datos que le conciernen durante el proceso de selección de personal, ya que, por un lado, la causal opera con respecto a obligaciones que se originan en el contrato y, por otro lado, no existe un genérico deber de veracidad que recaiga sobre el titular de los datos que le sea exigible en esta sede; y, tercero, refrendando lo señalado en primer término, y ciñéndonos a las recomendaciones de la OIT, las respuestas inexactas o incompletas del trabajador a preguntas contrarias a ciertos principios sustentados en el propio repertorio –tales como aquellas derivadas del tratamiento de datos que excedan los directamente pertinentes a la relación laboral, aquellos que pudieren conducir a una discriminación ilícita en materia de empleo, o aquellos correspondientes a los denominados datos sensibles–, no deberían quedar sancionadas por una terminación de la relación de empleo ni comportar ningún tipo de medida disciplinaria.[58]

[56] El artículo 160 número 1 del Código del Trabajo fue reemplazado por el numeral 23 del artículo único de la tantas veces mencionada Ley 19.759.
[57] Cf. Nota número 52 *supra*.
[58] Cf. Número 6.8 International Labour Organization, *"Protection of workers' personal data"*. Ginebra, Suiza. 1997.

4.- CONCLUSIONES.

El cúmulo y la calidad de la información nominativa relativa a los trabajadores susceptible de ser acopiada, procesada y transmitida por el empleador puede guardar proporciones sin parangón respecto de otros organismos responsables de bancos o registros de datos, tanto por el carácter de tracto sucesivo que reviste el contrato de trabajo, como por la naturaleza de la relación que se teje entre las partes: sujeta a subordinación y dependencia, de un lado, y dotada de poder de control y vigilancia, de otro.

En este sentido, la aplicación de la Ley 19.628, así como el artículo 154 bis del Código del Trabajo, contribuyen a brindar amparo a los derechos fundamentales de los trabajadores, por la vía de garantizar la autodeterminación informativa del titular de los datos y, a su vez, reforzar otras garantías y libertades públicas, anticipando criterios para la solución de problemas jurídicos que aún no se han suscitado, cuando menos judicialmente.

Con todo, la normativa antes referida no resulta suficiente para prever soluciones jurídicas apropiadas respecto de la protección al afectado por el tratamiento de datos personales en el contexto de las relaciones de trabajo. Así, entre otras, la concreción de principios como el consentimiento y finalidad, el tratamiento de datos personales relativos a convicciones ideológicas en las empresas de tendencia, el empleo regular de datos relativos a condenas por delitos e infracciones, la adopción de resguardos ante el tratamiento de datos apreciativos, y el rol de los sindicatos o representantes de los trabajados en la protección de los datos personales de sus representados. Más aún, aspecto sobre el cual no nos hemos detenido, es necesario esclarecer la extensión de las facultades interpretativas, fiscalizadoras y sancionadoras de la Inspección del Trabajo frente a la obligación del artículo 154 bis del Código del Trabajo, máxime si se considera que la propia Ley 19.628 no contempla autoridad de control alguna que se haga cargo de tal cometido con un abanico similar de atribuciones al detentado por tal organismo.

En consecuencia, parece ser necesario introducir modificaciones legales para hacer frente a algunos de los problemas que resultan de la aplicación de la Ley 19.628 al tratamiento de datos personales de los trabajadores por su empleador, ya que su carácter general constituye un obstáculo para la plena vigencia de los derechos conferidos al titular de los datos.