IMPACTO DE LAS TECNOLOGIAS EN LAS RELACIONES LABORALES

Primera Parte

Prof. Dra. Esc. María José Viega[1]

I) Introducción

Las tecnologías han impactado en todos los ámbitos de nuestra vida, y no es ajeno a ello las relaciones laborales. Uno de los primeros temas que lo pusieron de manifiesto fue el teletrabajo. Pero han ido surgiendo otros aspectos como la protección de datos personales en el ámbito laboral, cuestiones como por ejemplo el manejo de los datos de los postulantes a un empleo, la utilización de las referencias y el impacto de las evaluaciones automatizadas. También vinculado a la privacidad del trabajador no podemos dejar de mencionar la vigilancia electrónica, la utilización del correo electrónico de la empresa y el privado, el uso del chat, de las redes sociales, la hoy muy de moda WhatsApp. Por otra parte, surgen nuevas problemáticas a raíz del uso de los dispositivos personales, como es el fenómeno conocido como Byod (Bring your own device).

---

[1] **Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Profesora de Informática Jurídica, de Derecho Informático y de Derecho Telemático en la UDELAR.** Gerente de la Dirección de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) – Presidencia de la República. Directora del Instituto de Derecho Informático de la Facultad de Derecho de la Universidad de la República (agosto 2010-marzo 2013). Coordinadora del Grupo del Jurisprudencia del Instituto de Derecho Informático de la UDELAR. Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Experta Universitaria en Protección de Datos, UNED (ESPAÑA). Experta Universitaria en Administración electrónica, Universidad Operta de Cataluña (España). Ex - Profesora del curso en línea Derecho del Ciberespacio en la UDELAR. Ex - Profesora de Derecho de las Telecomunicaciones en la Universidad de la Empresa. Ex - Profesora en la Oficina Nacional de Servicio Civil (Presidencia de la República) del Curso Derecho de Internet. Ex - Profesora de los cursos de e-learning “Introducción al Derecho de las TICs”, “Documento y firma electrónica”, “Protección de datos” y “Contratos Informáticos” en Viega & Asociados. Directora del Estudio Jurídico Viega & Asociados (1992-2012). Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico (APADIT). Miembro Fundador del Instituto de Derecho Informático (UDELAR) y de FIADI Capítulo Uruguay. Miembro de la International Technology Law Association. Miembro de la International Association of Privacy Professionals**.** Autora del libro “Contratos sobre bienes y servicios informáticos”. Amalio Fernández, junio 2008 y del e-book “Marketing Comportamental en línea. El desafío de las cookies”. 2012 (publicado en www.viegasociados.com). Co-autora de los Libros: Lecciones de Derecho Telemático Tomo I y II (FCU, abril 2004 y mayo 2009); e-book “Documento Electrónico y Firma Digital. Cuestiones de Seguridad en las Nuevas Formas Documentales (junio 2005); “Marco normativo del Derecho Informático” (julio 2011); “Documento y firma. Equivalentes funcionales en el mundo electrónico”. 2012. Es autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

En general no podemos decir que son temas “nuevos”. Ya en el año 2009 el Dr. Arturo Bronstein, Secretario General de la Sociedad Internacional de Derecho del Trabajo y de la Seguridad Social, dio una conferencia en Montevideo, específicamente el 13 de agosto de 2009, en las que destacó cuatro facetas al referirse a la protección de la vida privada en el lugar de trabajo: la primera de ellas el acopio, tratamiento y posible comunicación a terceros de información relativa a la vida privada de un trabajador o un postulante al empleo, en segundo lugar el uso de cámaras o de otros medios electrónicos para monitorear a trabajadores en el lugar de trabajo o fuera de éste; el tercer lugar el uso personal de Internet y el correo electrónico puestos a disposición por el empleador y por último el monitoreo de las comunicaciones telefónicas hechas por el trabajador.

Para tratar de dar respuestas a las distintas problemáticas que plantean estos temas, vamos a realizar un análisis de documentos con carácter general: desde el ámbito laboral vamos a estudiar el Repertorio de recomendaciones prácticas de la Organización Internacional del Trabajo (OIT) comparándolo con nuestra ley de protección de datos y acción de habeas data N° 18.331 de 11 de agosto de 2008, en segundo lugar un documento del Grupo de Trabajo en Protección de Datos creado por el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 (WP 29), Dictamen N° 55 sobre la “Vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo” y finalmente la Recomendación sobre la protección de datos personales utilizado para fines de empleo del Comité Consultivo de la Convención para la protección de las personas respecto al tratamiento automatizado de datos, de junio de 2014. Pero también vamos a incursionar en el análisis particular, refiriéndonos a la jurisprudencia uruguaya.

II) Análisis comparativo del Repertorio de recomendaciones prácticas de la OIT y la Ley N° 18.331 de 11 de agosto de 2008

El Repertorio de recomendaciones prácticas de la OIT adoptado en Ginebra del 1º al 7 octubre 1996, en una reunión de 24 expertos sobre la protección de la vida privada de los trabajadores, en cumplimiento de una decisión tomada por el Consejo de Administración en su 264ª sesión en noviembre de 1995. Participaron en la reunión ocho expertos designados por consulta previa con los gobiernos, ocho fueron designados por el Grupo de Empleadores y ocho por consulta previa con el Grupo de los Trabajadores del Consejo de Administración. Por Uruguay participó el Escribano Dutra, Director Nacional de Empleo, Ministerio de Trabajo y Seguridad Social.

En la 267ª reunión, realizada en noviembre de 1996, el Consejo de Administración aprobó la distribución del repertorio de recomendaciones prácticas y los comentarios, que fueron revisados a la luz de los debates en la Reunión de expertos.

Los presupuestos que se tienen en cuenta para la realización del referido documento son los siguientes: utilización de técnicas informáticas de recuperación de datos, los sistemas automatizados de información del personal, la vigilancia electrónica y los exámenes genéticos y toxicológicos.

El repertorio no tiene carácter obligatorio y tiene como objetivo proteger la vida privada del trabajador.

Resulta interesante realizar un análisis comparativo de éste con nuestra Ley Nº 18.331 de 11 de agosto de 2008 de Protección de Datos y Acción de Habeas Data[2].

El punto 3 del Repertorio proporciona una serie de **definiciones**, estableciendo lo siguiente:

Datos personales: todo tipo de información relacionada con un trabajador identificado o identificable.

Tratamiento: incluye el acopio, la conservación, la combinación, la comunicación o cualquier otra forma de utilización de datos personales.

Vigilancia: engloba, sin limitarse a ella, la utilización de dispositivos como computadoras, cámaras de fotografía, cine y vídeo, aparatos de grabación sonora, teléfonos u otro material de comunicación, diferentes métodos de identificación y de localización y cualesquiera otros sistemas de vigilancia.

Trabajador: designa a todo trabajador o ex trabajador y a todo candidato a un empleo.

El concepto de trabajador es amplio, siendo interesante el tema de los postulantes y la información que proporcionan en el proceso de selección.

El tratamiento de los datos personales de los postulantes en un concurso público ha sido objeto de consulta a la Unidad de Acceso a la Información Pública (Órgano de Control creado por Ley Nº 18.381 www.informacionpublica.gub.uy), la que

[2] VIEGA, María José. "Protección de Datos Personales relacionados con el trabajo". Publicado en el Libro El trabajo ante las nuevas tecnologías. Fundación de Cultura Universitaria. Agosto, 2010.

adoptó la Resolución Nº 4 de 14 de julio de 2009, en la que se establece que debe entregarse toda la información referente a los postulantes, con excepción de:

a) aquellos datos que no tienen que ver con la situación evaluada, como por ejemplo domicilio, teléfono del postulante y

b) datos de carácter sensible, como por ejemplo evaluaciones sicológicas.

Por otra parte recomienda que se publique el orden de prelación y puntajes globales de todos los participantes en el concurso, y que de solicitarse se muestren los curriculum, previa ocultación de los datos excepcionados.

Las consideraciones en este caso se deben a que estamos ante concurso público y prima el principio de transparencia en la Administración, pero igualmente se reconocen limitaciones.

Diferente sería el caso de un postulante a un trabajo en el ámbito privado, en el cual la empresa debería destruir los curriculum una vez realizada la selección, no pudiendo entregar estos a terceros ni utilizarlo para otros empleos, a no ser que cuente con autorización expresa para ello, porque de lo contrario violaría el principio de finalidad de la recolección de los datos.

Nuestra Ley en el artículo 4º da una serie de definiciones, que entendemos se encuentran alineadas con las analizadas anteriormente:

En el literal d) define los datos personales como la "*información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables*".

En el literal m) se define "*Tratamiento de datos, operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permiten el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias*".

En el punto 4 del Repertorio se prevé el **campo de aplicación**, estableciendo que son tantos los sectores público y privado y que refiere al tratamiento manual o automático de todos los datos personales de un trabajador.

El artículo 3º de la Ley determina su campo de aplicación, estableciendo como Ámbito objetivo el siguiente: "*El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado*".

Siguiendo con el paralelismo entre el documento de la OIT y la Ley Nº 18.331 analizaremos los **principios** contenidos en ambos.

El Repertorio refiere al Principio de licitud y finalidad, mientras que la Ley refiere al Principio de legalidad en el artículo 6º y al principio de finalidad en el art. 8º.

El Repertorio en el punto 5.1 entiende que el tratamiento de los datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita y limitarse exclusivamente a asuntos directamente pertinentes para la relación de empleo del trabajador y en el 5.2 establece que los datos personales deberían utilizarse únicamente con el fin para el cual hayan sido acopiados.

La Ley establece que para que una base de datos sea lícita deberá estar inscripta ante la Unidad Reguladora y de Control de Datos Personales (www.datospersonales.gub.uy), Órgano de Control creado por ésta, y cumplir con la ley y sus reglamentaciones.

Por otra parte, el artículo 8º establece que los datos objeto de tratamiento no pueden ser utilizados para una finalidad distinta a aquella que motivó su recolección.

El documento, en los punto 5.4 y 5.5, dispone que los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información, no debería servir para controlar el comportamiento del trabajador y que las decisiones no pueden basarse en un tratamiento exclusivamente informático de los datos personales.

El punto 5.4 lo podemos articular con el principio de finalidad ya mencionado, mientras que la Ley establece en el artículo 16 el Derecho a la impugnación de valores personales, consagrando la posibilidad de impugnar aquellas que se basen en un tratamiento exclusivamente automatizado. Al artículo se le agregó “o no” en la Comisión de la Cámara de Educación y Cultura del Senado, lo que desvirtuó su propósito inicial, el cual tenía como fuentes el artículo 13 de la Ley española denominado Impugnación de valoraciones, el artículo 20 de la Ley argentina llamado Impugnación de valoraciones personales, el artículo 15 de la Directiva 95/46/CE llamado Decisiones individuales automatizadas y el Proyecto MERCOSUR, en el artículo 15 referente a las Decisiones individuales automatizadas.

Por otra parte la OIT hace hincapié en reducir lo más posible el tipo y volumen de los datos personales y que los trabajadores deberían estar informados sobre los datos que se colectan.

En los artículos 7º y 9º de la ley se consagran los Principio de Veracidad y del Previo Consentimiento Informado respectivamente, también del primero de ellos

se desprende el principio de proporcionalidad, al establecer que los datos que se colectan deben ser adecuados, ecuánimes y no excesivos acorde a la finalidad para la cual se recolectan.

La obligación de confidencialidad de quienes manipulan los datos tiene su correlativo en el principio de reserva establecido en el artículo 11 de la ley, por el cual las personas deben utilizar los datos personales a los que tienen acceso en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad. En el inciso 2º se establece que: "*Las personas que, por su situación laboral u otra forma de relación con el titular de la base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. (…)".*

El punto 5.9 refiere a que las personas encargadas del tratamiento de datos personales deberían recibir periódicamente una formación que les permita comprender el proceso de acopio de datos y el papel que les corresponde en la aplicación de los principios enunciados en el presente repertorio.

El punto 5.12 entiende que todas las personas, tales como los empleadores, los representantes de los trabajadores, las agencias de colocación y los trabajadores que tengan acceso a los datos personales de los trabajadores, deberían tener una obligación de confidencialidad, de acuerdo con la realización de sus tareas y el ejercicio de los principios enunciados en el presente Repertorio.

En el punto 5.13 se establece que los trabajadores no pueden renuncian a su derecho a proteger su vida privada. Esto está plenamente consagrado en el artículo 1º de la Ley, en el cual se determina que el derecho a la protección de datos es un derecho inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República.

El punto 6 del Repertorio refiere al acopio de datos personales vinculado al tratamiento que realiza el empleador de los datos del trabajador, a informarlo de su uso y de solicitar su autorización para cederlos a terceros. También establece que los empleadores no deberían recabar datos personales que refieran a:

a) la vida sexual del trabajador,

b) las ideas políticas, religiosas o de otro tipo del trabajador,

c) los antecedentes penales del trabajador.

Respecto a estos aspectos, la Ley establece que los datos facilitados por terceros necesitan el consentimiento, previsto en el artículo 17 denominado comunicación de datos.

También se establece que no deben recabarse datos sensibles, los cuales son definidos en el art. 4º lit. E) como aquellos datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

Respecto a la conservación de los datos, encontramos el Principio de veracidad del artículo 7º, que establece que los datos deben ser exactos y deben estar actualizados y que cuando se constate inexactitud o falsedad de los mismos deberán suprimirlos, sustituirlos o completarlos.

El punto 7.1 del Repertorio establece que: "*los empleadores deberían garantizar, mediante las salvaguardias de seguridad que permitan las circunstancias, la protección de los datos personales contra su pérdida y todo acceso, utilización, modificación o comunicación no autorizados*".

El Capítulo III de la Ley denominado Derechos de los Titulares de los Datos consagra en los artículos 13, 14 y 15 los derechos de información frente a la recolección, de acceso, de rectificación, actualización, inclusión o supresión.

El punto 8 del Repertorio alude a la conservación de los datos personales. A tales efectos entiende que los empleadores deberían evaluar periódicamente sus métodos de tratamiento de datos, con el objeto de reducir lo más posible el tipo y el volumen de datos personales acopiados y mejorar el modo de proteger la vida privada de los trabajadores.

El punto 8.1 establece que la conservación de los datos personales debería limitarse estrictamente a los acopiados de conformidad con los principios enunciados en el repertorio

El punto 8.4 considera que los empleados deberían verificar periódicamente que los datos personales conservados son exactos, actualizados y completos.

El punto 8.5 estima que los datos personales deberían guardarse únicamente durante un período que esté justificado por los fines concretos para los cuales hayan sido recabados, salvo que:

a) El trabajador desee figurar en la lista de candidatos potenciales a un empleo por un período determinado.

b) La legislación nacional disponga que los datos personales deban conservarse.

c) Los empleadores o los trabajadores necesiten estos datos por razones legales para presentar pruebas sobre cualquier cuestión concerniente a una relación de empleo anterior o actual.

Esto está contemplado en nuestra Ley en los principios, especialmente en lo que refiere a la finalidad y seguridad de los datos.

El punto 9 refiere a la utilización de datos personales y recomienda que debieran ser utilizados de conformidad con los principios del presente repertorio aplicables al acopio, comunicación y conservación de estos datos.

El punto 10 refiere a la comunicación de datos personales, sobre este aspecto ya hicimos mención al artículo 17 de la Ley.

En el punto 11se enumeran los derechos individuales, destacando el derecho a ser informados con regularidad, los trabajadores beberían tener acceso a todos sus datos personales y durante las horas de trabajo, no se le debería cobrar al trabajador por el acceso al expediente o la copia del mismo y el derecho a exigir que se supriman o rectifiquen datos personales inexactos o incompletos.

Por último, en el punto 12 se analizan los derechos colectivos y en el 13 lo referente a la agencias de colocación.

III) Dictamen del Grupo de Trabajo del Artículo 29 N° 55 de 29 de Mayo 2002 relativo a la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo

El Dictamen N° 55 ofrece una orientación y ejemplos concretos sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por parte del empleador. Y parte del supuesto que: "*Los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo. Esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan una parte importante de sus relaciones con los demás. Este derecho debe, no obstante, conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia su empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores. El caso en que el empleador es víctima de un delito imputable a un trabajador constituyen el ejemplo más claro*".

Por tanto, para lograr el equilibrio entre los diferentes derechos e intereses, es fundamental el principio de proporcionalidad.

Hay que considerar el alcance de las medidas de vigilancia y para ello entiende que deben responderse las siguientes preguntas: ¿Es la actividad de vigilancia transparente para los trabajadores? ¿Es necesaria? ¿No podría el empleador obtener el mismo resultado con métodos tradicionales de supervisión? ¿Garantiza el tratamiento leal de los datos personales de los trabajadores? ¿Es proporcional respecto a las preocupaciones que intenta solventar?

El Grupo de Trabajo del Artículo 29 entiende que la prevención debería prevalecer sobre la detección. Por ejemplo, vinculado al uso abusivo de Internet, deberían desplegarse avisos en la pantalla del computador del trabajador cuando intente entrar a lugares que se entiende no corresponden desde su lugar de trabajo o a los cuales no está autorizado, en lugar de monitorear los sitios a los cuales el trabajador ingresa una vez que ya lo ha hecho.

Es esencial que el trabajador esté informado sobre la vigilancia a la que está siendo sometido, sobre los datos que se han recolectado y con qué objetivo se mantienen.

Vinculado al correo electrónico se aconseja que la empresa proporcione al trabajador una cuenta de correo de uso profesional exclusivo y una cuenta de uso privado o autorización de utilizar el correo web, pudiendo ejercerse vigilancia sobre la primera pero no sobre la segunda.

Con relación al punto de la vigilancia en el lugar de trabajo, el WP55 destaca que las condiciones de trabajo han evolucionado, siendo difícil separar el trabajo de la vida privada, sobre todo teniendo en cuenta la “oficina a domicilio” que conlleva a toda la problemática del teletrabajo.

“La dignidad humana de un trabajador prima sobre cualquier otra consideración”, expresa el documento.

En el apartado relativo a la vigilancia y control de las comunicaciones electrónicas en el lugar de trabajo se toma como marco la Directiva 95/46/CE, así como la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

En el documento se entiende que para que una actividad de control sea legal y se justifique, deben respetarse los siguientes principios:

a) Necesidad: deben ser necesario, en casos excepcionales, para obtener prueba de actividades delictivas o para garantizar la seguridad del sistema.

Este principio significa además, que el empleador sólo podrá conservar la información durante el tiempo necesario para lograr el objetivo específico de la actividad de vigilancia.

b) Finalidad: significa que los datos deben recogerse con fines determinados, explícitos y legítimos y no pueden ser tratados posteriormente de manera incompatible con dichos fines.

c) Transparencia: significa que un empleador debe indicar en forma clara y abierta sus actividades. Este principio puede subdividirse en tres aspectos:

    i. La obligación de proporcionar información al interesado: el empleador debe trasmitir a los trabajadores una declaración clara, precisa y fácilmente accesible de su política sobre la vigilancia del correo electrónico y el uso de Internet. Debe tenerse presente aquí la Directiva 2002/14/CE siempre que la empresa figure en su ámbito de aplicación, establece la necesidad de informar y consultar a los trabajadores sobre decisiones que impliquen importantes cambios tanto en la organización del trabajo como en las relaciones contractuales.

    ii. La obligación de notificar a las autoridades de supervisión antes de la aplicación de un tratamiento total o parcialmente automatizado o de un conjunto de tratamientos de este tipo.

    iii. El derecho de acceso que tiene el trabajador sobre todos los datos tratados por el empleador.

d) Legitimidad: el tratamiento de los datos de un trabajador debe ser necesario para la satisfacción del interés legítimo perseguido por el empleador y no perjudicar los derechos fundamentales de los trabajadores, lo que se desprende del artículo 7 de la Directiva 95/46/CE.

e) Proporcionalidad: los datos personales que se utilicen para actividades de control deben ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaban.

    Establece el documento que: "*Si es posible, el control del correo electrónico debería limitarse a los datos sobre tráfico de los participantes y a la hora de una comunicación más que al contenido, si ello es suficiente para satisfacer las necesidades del empleador".*

f) Exactitud y conservación de los datos: este principio requiere que todos los datos legítimamente almacenados por un empleador deberán ser precisos y actualizarse y no podrán conservarse más tiempo del necesario. El WP 29 entiende que los empleadores deberían especificar el tiempo de conservación y que normalmente es difícil imaginar que pueda justificarse un período de conservación superior a tres meses para la conservación de mensajes electrónicos.

g) Seguridad: este principio consta de un doble aspecto, por un lado la obligación del empleador de aplicar medidas técnicas y organizativas adecuadas para proteger los datos personales en su poder y por otra parte, su derecho a proteger sus sistemas contra virus, lo que puede implicar el análisis automatizado de mensajes electrónicos y del tráfico en la red. El Grupo de Trabajo entiende que no constituyen una violación a la privacidad del trabajador las búsquedas automatizadas en los correos electrónicos y destaca la importancia del administrador del sistema en cuanto a la responsabilidad en la protección de los datos.

IV) Recomendación sobre la protección de datos personales utilizado para fines de empleo del Comité Consultivo de la Convención para la protección de las personas respecto al tratamiento automatizado de datos

El Comité Consultivo de la Convención para la protección de las personas respecto al tratamiento automatizado de datos (T-PD del Convenio 108), del cual Uruguay es parte, aprobó por unanimidad en la 31° Reunión Plenaria realizada en Estrasburgo (Francia) entre 2 y 4 de junio de 2014 la Recomendación sobre la protección de datos personales utilizados para fines de empleo, que revisa la Recomendación Nº 89 (2) sobre este tema y tiene presente los "Principios rectores para la protección de las personas físicas en lo que respecta a la recogida y tratamiento de los datos por medio de video vigilancia", adoptada por el Comité Europeo de Cooperación Jurídica (CDCJ) del Consejo de Europa en mayo de 2003.

La Recomendación se basa en la toma de consciencia de la creciente utilización de las nuevas tecnologías y los medios de comunicación electrónica en las relaciones entre empleadores y empleados, y las ventajas correspondientes de los mismos y entendiendo que el uso de las tecnologías debe realizarse basado en principios diseñados para reducir al mínimo cualquier riesgo que tales métodos

podrían suponer para los derechos de los trabajadores y las libertades fundamentales, en particular su derecho a la intimidad.

La Recomendación se aplica a los datos tratados con fines de empleo tanto en ámbitos públicos como privados. La recomendación define los datos personales, el tratamiento de datos y los sistemas de información, interesándonos en este caso concreto las siguientes definiciones:

Empleador: cualquier persona física o jurídica, autoridad pública o agencia que tiene una relación laboral con un empleado o futuro empleado y tiene la responsabilidad legal de la empresa y/o establecimiento.

Empleado o potencial empleado: cualquier persona física de que se trate contratado por un empleador en virtud de una relación laboral.

El **principio 2** establece que: “El respeto por la dignidad humana, la intimidad y la protección de los datos personales debe ser salvaguardada en el tratamiento de datos personales con fines de empleo, en particular para permitir el libre desarrollo de la personalidad de los empleados, así como las posibilidades de relación individual y social en el lugar de trabajo”.

El **principio 3** trata de la aplicación de los principios del procesamiento de datos.

La recogida y almacenamiento de datos se encuentra regulado en el **principio 4** que tiene en cuenta los siguientes aspectos:

1. Los empleadores deberían recabar los datos personales directamente del titular de los datos. Cuando sea necesario y legal para procesar datos obtenidos de terceros, por ejemplo, para obtener referencias profesionales, el interesado deberá ser informado debidamente por adelantado.

2. Los datos personales recogidos para fines de empleo deben ser pertinentes y no excesivos, teniendo en cuenta el tipo de empleo.

3. Los empleadores deberían abstenerse de pedir a un empleado o posible empleado acceso a la información que comparte con otros en las redes sociales.

4. Los datos de salud solo se podrán recoger para los fines establecidos en el principio 8.2 de la presente Recomendación

5. El almacenamiento de los datos personales para fines de empleo sólo se autorizará si los datos han sido recogidos en forma legítima y sólo durante

el tiempo necesario para alcanzar el objetivo legítimo de la tramitación. Cuando los datos de evaluación guardan relación con el desempeño o potencial de un empleado, tales datos sólo deben basarse a los efectos de evaluar las competencias profesionales.

El **principio 5** de la Recomendación refiere al uso interno de los datos, y de los aspectos referidos interesa destacar que: los empleadores deben respetar el principio de finalidad, deberían adoptar políticas de protección de datos para el uso interno de los datos, cuando el tratamiento se utilice para una finalidad diferente –en situaciones excepcionales- los empleadores deben tomar las medidas adecuadas para evitar el mal uso de los datos en un contexto diferente, e informar al empleado y cada cambio sustantivo de los datos por modificaciones a nivel empresarial debe ser comunicado a los empleados.

El **principio 6** trata los aspectos de la comunicación y uso de las TIC con el propósito de representación de los trabajadores, estableciendo que solo podrán ser comunicados por el empleador a los representantes de los empleados en la medida en que tales datos son necesarios para permitir que éstos representan adecuadamente los intereses de los empleados de que se trate, o si los datos son necesarios para la realización y supervisión de las obligaciones establecidas en convenios colectivos. Para ello deben existir acuerdos previos que establezcan la transparencia en la comunicación de los datos y medidas de seguridad que garanticen la confidencialidad.

En el **principio 7** se considera la comunicación externa de los datos del trabajador en los siguientes términos:

7.1 Los datos personales recogidos para fines de empleo sólo se deben comunicar a los organismos públicos que actúen en sus funciones oficiales (excepción prevista en la Ley N° 18.331), y para los efectos de llevar a cabo, y sólo dentro de los límites de las obligaciones legales de los empleadores o de acuerdo con otras disposiciones de la legislación nacional.

7.2. La comunicación de datos personales a los organismos públicos para otros fines o a terceros que no sean entidades públicas, incluidas las entidades de un mismo grupo, sólo debe llevarse a cabo:

a. cuando sea necesario para fines de empleo y los efectos no sean incompatibles con los fines para los que los datos fueron originalmente recogidos y se les informa de esto de antemano ya sea al empleado en cuestión o sus representantes; o

b. con el consentimiento expreso e informado del trabajador individual; o

c. si la comunicación está prevista en la legislación interna a los efectos de la ejecución de obligaciones legales o convenios colectivos.

7.3. En lo que respecta al sector público, por las disposiciones que rigen la divulgación de datos personales para asegurar la transparencia del gobierno u otra autoridad pública, siempre proporcionando las adecuadas garantías para el derecho del individuo a la privacidad y protección de datos personales.

7.4. Los empleadores deben tomar las medidas apropiadas para garantizar que los datos publicados en línea, sean relevantes, precisos y actualizados.

El tratamiento de los datos sensibles, se trata en el **principio 8** de la Recomendación y remite al artículo 6 del Convenio 108 que establece que este tratamiento sólo se permite en casos particulares, en que es indispensable para la contratación de un empleo determinado, o para cumplir las obligaciones legales relacionadas con el contrato de trabajo dentro de los límites establecidos por la legislación nacional y de conformidad con las salvaguardias apropiadas, las que tendrán por objeto la prevención de los riesgos que el tratamiento de estos datos puede presentar a los intereses, los derechos y libertades fundamentales del trabajador, en particular el riesgo de discriminación. El tratamiento de los datos biométricos es posible bajo las condiciones establecidas en el Principio 17 de la presente Recomendación.

A un empleado o futuro empleado solo se le pueden pedir datos de salud cuando haya dudas sobre la idoneidad para el empleo, para cumplir con los requisitos de la medicina preventiva, para garantizar una rehabilitación apropiada, para salvaguardar los intereses vitales del interesado o de otros empleados, para acceder a los beneficios sociales o para satisfacer los procedimientos judiciales.

El tratamiento de los datos genéticos está prohibido para determinar, por ejemplo, la idoneidad profesional de un empleado o futuro empleado, incluso con el consentimiento de la persona interesada. Este tratamiento podría concederse excepcionalmente si es proporcionada por el derecho interno y con sujeción a las salvaguardias adecuadas, en particular para evitar cualquier perjuicio grave para la salud de la persona afectada o de terceros.

Los datos de salud amparados por la obligación del secreto médico sólo deberían ser accesibles y procesados por personal que están obligados por el secreto médico u otras normas del secreto profesional o la confidencialidad. Cuando estos datos sean comunicados a los empleadores, este tratamiento debe ser realizado

por una persona debidamente autorizada, como el personal con derecho a la administración, la salud y la seguridad en el trabajo.

Los datos de salud cubiertos por el secreto médico y los datos genéticos, se deben almacenar por separado de otras categorías de datos personales, debiéndose tomar las medidas de seguridad técnicas y organizativas necesarias para evitar que personas ajenas al servicio médico autorizado tenga acceso a ellos.

El **principio 9** regula la transparencia del proceso. La información relativa a los datos personales en poder de los empleadores debe estar disponible ya sea para el trabajador afectado, directamente o por intermedio de sus representantes. Los empleadores deben proporcionar a los empleados la siguiente información: las categorías de los datos personales que son procesados y una descripción de los objetivos de los tratamientos; los destinatarios o categorías de destinatarios de los datos personales; los medios que los empleados tienen de ejercer los derechos establecidos en el principio 10 de la presente recomendación y cualquier otra información necesaria para garantizar el tratamiento leal y lícito.

En este contexto, debe proporcionarse una descripción clara y completa del tipo de datos personales que pueden ser recogidos por las TIC, incluyendo video-vigilancia y su posible uso. La información debe proporcionarse en un formato accesible y antes de que un empleado lleve a cabo la actividad o acción en cuestión.

En el **principio 10** se realizan recomendaciones respecto a derecho de acceso y rectificación. Un empleado debe ser capaz de obtener, previa solicitud, a intervalos razonables y sin demoras excesivas, la confirmación del procesamiento de los datos personales referentes a él. La comunicación debe ser en forma inteligible, incluir toda la información sobre el origen de los datos, así como cualquier otra información que se requiera para garantizar la transparencia de los tratamientos, especialmente la información proporcionada en el principio 9.

Un empleado debe tener derecho a que sus datos personales rectificados, bloqueados o borrados, si son inexactos y/o si los datos se han elaborado en contravención de la ley o los principios enunciados en la presente recomendación. También debe tener derecho a oponerse en cualquier momento al tratamiento de sus datos personales a menos que el procesamiento sea necesario para fines de empleo o de otra manera prevista por la ley.

El derecho de acceso también debe estar garantizado con respecto a los datos de evaluación, incluso cuando tales datos se refieren a las evaluaciones del rendimiento, la productividad o la capacidad del empleado, y sin perjuicio del

derecho de defensa de los empleadores o terceros involucrados. Aunque estos datos no pueden ser corregidos directamente por el empleado, las evaluaciones puramente subjetivas deben ser objeto de recurso en la forma prevista en el derecho interno. Este derecho se encuentra expresamente regulado en nuestra Ley N° 18.331.

Se permiten excepciones a estos derechos cuando sean proporcionados por la ley y constituyan una medida necesaria en una sociedad democrática, para proteger la seguridad del Estado, la seguridad pública, importantes intereses económicos y financieros del Estado o la prevención y represión de las infracciones penales, la protección del interesado o de los derechos y libertades de los demás. Por otra parte, el ejercicio de estos derechos puede, en el caso de una investigación interna llevada a cabo por los empleadores, ser aplazada hasta el cierre de la investigación, si el ejercicio de esos derechos puede amenazar la investigación.

El **principio 11** refiere a la Seguridad de los datos. Los empleadores o entidades, que pueden procesar los datos en su nombre, deben aplicar las medidas técnicas y organizativas adecuadas en respuesta a las revisiones periódicas de las políticas de evaluación de riesgos y seguridad de la organización, actualizadas según corresponda. Tales medidas deben ser diseñadas para garantizar la seguridad y confidencialidad de los datos personales tratados para fines de empleo.

El **principio 12** regula la conservación de los datos. Los datos personales no deben ser conservados por los empleadores por un período más largo del que se justifica por los fines de empleo señaladas en el Principio 1 bis.

Los datos personales presentados en apoyo de una solicitud de trabajo normalmente se deben eliminar tan pronto como se pone de manifiesto que no se hará una oferta de empleo.

Cuando se almacene dicha información con miras a una oportunidad de trabajo adicional, el interesado debe ser informado a su debido tiempo y de sus datos debe suprimirse si así lo solicita la persona.

Cuando sea necesario almacenar los datos presentados con el fin de defender acciones judiciales o cualquier otro propósito legítimo, deben ser almacenados sólo durante el tiempo necesario para el cumplimiento de la finalidad.

Los datos personales tratados con el fin de una investigación interna llevada a cabo por los empleadores, que no ha dado lugar a la adopción de medidas negativas en relación a cualquier empleado, deben suprimirse transcurrido un plazo razonable, sin perjuicio del derecho de acceso del trabajador hasta el momento en la que se eliminan.

La segunda parte de la Recomendación refiere a formas particulares de procesamientos y en el **principio 13** refiere a los sistemas de información y tecnologías para el control de los trabajadores, incluida la vigilancia de vídeo.

No se debe permitir la introducción y el uso de sistemas y tecnologías con el propósito directo y principal de seguimiento de la actividad y el comportamiento de los empleados. La introducción y el uso de sistemas y tecnologías de la información para proteger la producción, la salud, la seguridad o la organización del trabajo tiene como consecuencia indirecta la posibilidad de supervisar la actividad de los empleados, lo que debe estar sujeto a las salvaguardias adecuadas establecidas por el principio 20, y en particular a la consulta de los representantes de los trabajadores.

Los sistemas de información y tecnologías deben ser, en cualquier caso diseñados y ubicado específicamente a fin de no socavar los derechos fundamentales de los trabajadores. El uso de video vigilancia para el seguimiento de incidencias en los lugares que forman parte de la zona más personal de la vida de los empleados no está permitido en cualquier situación.

En caso de controversia o procedimiento legal, los empleados deben ser capaces de obtener copias de la grabación realizada cuando proceda y de conformidad con el derecho interno. El almacenamiento de la grabación realizada debe ser limitado en el tiempo.

El **principio 14** trata sobre el mecanismo de información interna. Cuando los empleadores están obligados por la ley o las normas internas para implementar mecanismos de información internos, tales como líneas telefónicas, deben garantizar la protección de los datos personales de todas las partes involucradas. En particular, los empleadores deben garantizar la confidencialidad del empleado que informa sobre la conducta ilegal o poco ético (por ejemplo, un denunciante). Los datos personales de las partes involucradas deben ser utilizados exclusivamente para los fines de los procedimientos internos apropiados en relación con el informe, la ley u orden judicial.

En circunstancias excepcionales, los empleadores pueden permitir la denuncia anónima. Las investigaciones internas no deben llevarse a cabo únicamente sobre la base de una denuncia anónima, excepto cuando sea debidamente circunstanciada y se refiere a infracciones graves.

En el **principio 15** se regula el uso de Internet y las comunicaciones electrónicas en el lugar de trabajo. Los empleadores deben evitar interferencias injustificables e irrazonables con el derecho del empleado a la vida privada. Este principio se extiende a todos los medios técnicos y las TIC utilizadas por un empleado. Las

personas interesadas deben estar debidamente informadas y de forma periódica, a través de una política de privacidad clara y de acuerdo con el principio 9 de la recomendación. La información proporcionada debe mantenerse actualizada y debe incluir el propósito del procesamiento, la preservación o el período de copia de seguridad de los datos de tráfico y el archivado de mensajes electrónicos.

En relación con el posible tratamiento de datos personales relativos a Internet o Intranet, páginas visitadas por el empleado, se debe dar preferencia a la adopción de medidas preventivas, como el uso de filtros que impidan determinadas operaciones.

El acceso a la comunicación electrónica profesional de los empleados, que han sido informados previamente de la existencia de esa posibilidad, sólo puede ocurrir cuando sea necesario para la seguridad u otra razón legal. En el caso de los empleados ausentes, los empleadores deben tomar las medidas necesarias y prever los procedimientos apropiados encaminados a permitir el acceso a los mensajes de correo electrónico profesional sólo cuando dicho acceso sea por necesidad profesional. El acceso debe realizarse de la manera menos intrusiva posible y sólo después de haber informado a los trabajadores afectados.

El contenido, el envío y recepción de la comunicación electrónica privada en el trabajo no deberán ser monitoreados.

Cuando un empleado deja la organización, los empleadores deben adoptar las medidas organizativas y técnicas necesarias para desactivar automáticamente la cuenta del empleado a su salida. Si los empleadores necesitan recuperar el contenido de la cuenta del empleado para la buena marcha de la empresa, lo harán antes de la salida del empleado y, cuando sea posible, en su presencia.

El **principio 16** refiere al uso de un equipo que revele la ubicación de los empleados. Un equipo que revele la ubicación de los empleados debe introducirse sólo si resulta necesario para alcanzar el fin legítimo perseguido por el empleador y su uso no deberá dar lugar a un seguimiento continuo de un empleado. En particular, la vigilancia no debe ser el objetivo principal, sólo una consecuencia indirecta de las acciones necesarias para proteger la producción, la salud, la seguridad o la organización del trabajo. Dado el potencial de violar los derechos y libertades de las personas por el uso de estos dispositivos, los empleadores deben asegurar todas las garantías necesarias para el derecho del empleado a la privacidad y protección de datos personales, incluyendo las garantías adicionales previstas en el principio 20. De acuerdo con principios 3 y 4, los empleadores deberán prestar especial atención a la finalidad para la que se utilizan estos dispositivos y con los principios de minimización y proporcionalidad.

El **principio 17** refiere al procesamiento de los datos biométricos. La recogida y posterior tratamiento de los datos biométricos sólo pueden ser realizadas cuando es necesario para proteger los legítimos intereses de los empleadores, empleados o terceros, únicamente si no existen otros medios menos intrusivos disponible y sólo si acompañados de salvaguardias apropiadas, incluido el garantías adicionales previstas en el principio 20.

El tratamiento de los datos biométricos debe basarse en métodos científicos reconocidos y estará sujeto a requisitos de seguridad estrictos y al principio de proporcionalidad.

El **principio 18** regula los test psicológicos, análisis y procedimientos similares.

Las pruebas, análisis y procedimientos similares realizados por profesionales especializados, con sujeción a la confidencialidad profesional, que están diseñados para evaluar el carácter o personalidad de un empleado o futuro empleado, sólo debe permitirse si es legítimo y necesario para el tipo de actividad que se realiza en el trabajo, proporcionando las debidas garantías.

El empleado o futuro empleado deben ser informados con antelación del uso que se hace de los resultados de estas pruebas, análisis o procedimientos similares y, posteriormente, del contenido del mismo.

El **principio 19** prevé garantías para otros procedimientos que puedan significar riesgos para los empleados y el **principio 20** establece garantías adicionales, recomendando consultar, de conformidad con el derecho interno, a las autoridades nacionales competentes en el tratamiento de datos personales.