PROTECCIÓN DE DATOS PERSONALES RELACIONADOS CON EL TRABAJO

Dra. Esc. María José Viega[1]

I) Introducción

Quiero comenzar con una apreciación del Dr. Arturo Bronstein, Secretario General de la Sociedad Internacional de Derecho del Trabajo y de la Seguridad Social, quien dio una serie de conferencias en Montevideo 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:

a) Acopio, tratamiento y posible comunicación a terceros de información relativa a la vida privada de un trabajador o un postulante al empleo.

b) Uso de cámaras o de otros medios electrónicos para monitorear a trabajadores en el lugar de trabajo o fuera de éste.

c) Uso personal de Internet y el correo electrónico puestos a disposición por el empleador.

d) Monitoreo de las comunicaciones telefónicas hechas por el trabajador.

Estos aspectos son de trascendental importancia y actualidad y se analizan y pretenden dar respuestas desde diferentes ámbitos. Por un lado la el derecho a la protección de datos personales protege el derecho a la intimidad y privacidad de las personas, haciendo hincapié en diferentes esferas en que existen personas de mayor vulnerabilidad, existiendo estudios sobre la privacidad del trabajador. Por otra parte, desde el Derecho del Trabajo preocupa la manipulación de la información del trabajador en la esfera laboral, la cual se potencializa con el desarrollo de las tecnologías.

Por lo tanto, para realizar un análisis del tema creo interesante analizar dos documentos, uno que proviene del área del Derecho Laboral y es el

---

[1] Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UR). Profesora adscripta de Informática Jurídica y Profesora adjunta de Derecho Telemático. Directora de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). Cursos del Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico. Miembro del Instituto de Derecho Informático (UDELAR) y Coordinadora de la Comisión de Jurisprudencia del mismo Instituto. Co-editora del Boletín Electrónico de Derecho y Tecnologías (www.viegasociados.com). Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

Repertorio de recomendaciones prácticas de la Organización Internacional del Trabajo (OIT) y 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), documento WP 55 sobre la "Vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo".

II) Repertorio de recomendaciones prácticas de la OIT

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:

a) Utilización de técnicas informáticas de recuperación de datos

b) Los sistemas automatizados de información del personal

c) La vigilancia electrónica

d) Los exámenes genéticos y toxicológicos

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

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.

Respecto al 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 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 11 se 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) Documento del Grupo de Trabajo del Artículo 29: WP 55 de 29 de Mayo 2002 relativo a la vigilancia y el control de las comunicaciones electrónicas en el lugar de trabajo

El WP 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) Conclusiones

Es relevante destacar que no solo no existen divergencias entre estos documentos y nuestro derecho positivo en materia de protección de datos, sino que los mismos se basan en los mismos principios, en el amparo y la defensa de este derecho fundamental.

Tanto los principios como los derechos referenciados en el Repertorio y en el Documento WP 55 se hallan contemplados en nuestra Ley de Protección de Datos, encontrándose la protección de datos del trabajador amparado en

esta normativa. La Unidad Reguladora y de Control de Datos Personales es el Órgano que tiene el cometido garantizar el eficaz cumplimiento de la ley, al cual los trabajadores podrán recurrir para realizar consultas y denuncias. También existe la garantía del Habeas Data, que permite que el trabajador concurran ante el Poder Judicial cuando sus derechos hayan sido lesionados.