Publicado en www.relats.org

NUEVAS TECNOLOGÍAS Y PRIVACIDAD DEL TRABAJADOR

Juan Raso Delgue*

Introducción

- Las nuevas tecnologías han tenido un impacto profundo en la privacidad y la salud psicofísica del trabajador.
- Nueva dependencia laboral: subordinación tecnológica: "vigilancia a distancia en términos espaciales y temporales" (Avilés – Roldán) . El País 25 07 2017: *Una empresa estadounidense implantará en algunos de sus empleados unos microchips que facilitan tareas como abrir puertas, acceder a ordenadores, hacer fotocopias, compartir información o pagar compras de máquinas expendedoras. Según publicó el portal tecnológico The Verge, unos cincuenta trabajadores de Three Square Market, una compañía desarrolladora del de software para máquinas expendedoras, se han ofrecido voluntarios para participar en la iniciativa.*
- Se ha desarrollado un verdadero sistema de "trazabilidad" humana: el chip.
- Las tecnologías invaden la vida del trabajador aún fuera de la empresa;
- los ficheros electrónicos guardan datos sobre su imagen, su estructura psicológica, su conducta y salud.

  Pero también es cierto que:

* Catedrático de Derecho del Trabajo y de Relaciones Laborales, Facultad de Derecho, Universidad de la República - Montevideo, Uruguay

“el empleo abusivo de instrumentos tecnológicos de trabajo supone para el empleador un daño económico, lucrum cesans, concretado en el tiempo que el trabajador dedica a cuestiones distintas y ajenas a las propiamente laborales”

- Nosotros – los trabajadores – somos cada vez menos cuidadosos de nuestra privacidad: vamos perdiendo cuotas de pudor. Vivimos una época de exposición del pudor y de la intimidad.
- En definitiva, “la innovación tecnológica plantea distintos desafíos en una dialéctica por otra parte nada novedosa: la que enfrenta al poder de dirección del empresario y los derechos fundamentales del trabajador” (Avilés – Roldán)

Dividiremos la exposición en cuatro partes (necesariamente breves)**: a) elementos conceptuales; b) la opinión de la jurisprudencia nacional: c) la opinión de la Administración; d) el rol de los actores sociales; para luego expresar algunas conclusiones personales.**

A. ELEMENTOS CONCEPTUALES

1) “Privacidad” del **trabajador y contrato de trabajo:** “mezcla explosiva entre la vida profesional y la vida privada”;

2) No es un tema neutro: **cierta dosis de ideologismo;**

3) Estamos ante una **materia en construcción,**

“el desarrollo de las nuevas tecnologías se ha visto acompañado en el tiempo de un paralelo proceso de centralidad del derecho a la intimidad del trabajador, conforme se asumía el riesgo que generan aquéllas en la protección de este derecho” (Aviles – Roldán)

A.1 Los conceptos de privacidad e intimidad

- Conceptos colindantes de ***intimidad*** **y *privacidad*:** conceptos dinámicos en contexto histórico, tecnológico, político y cultural de un país.
- El derecho a la intimidad: (*common law*): el "derecho a ser dejado solo",
- segunda mitad del siglo XX: concepto de privacidad que abarca intimidad, pero se extiende a las relaciones privadas del individuo con terceros.
- La intimidad es un "sentimiento"; la privacidad comprende las actuaciones con relación a la familia, las comunicaciones, los vínculos privados, las orientaciones sexuales, las preferencias literarias, el ejercicio de los derechos religiosos, políticos, sindicales, la salud.
- Art. 54 de la Constitución: "la ley ha de reconocer a quien se hallaré en una relación de trabajo o servicio, como obrero o empleado, **la independencia de su conciencia moral y cívica"**
- **Derechos inespecíficos laborales:** el honor, la dignidad, libertad, igualdad, no discriminación;

A.2. Areas de conflicto entre trabajo y privacidad:

- los procesos de selección de personal,
- las comunicaciones electrónicas: correos, chats, páginas web
- los monitoreos, utilizando cámaras, grabadores, GPS, etc.;
- la protección de los datos personales: obtención, archivo, custodia y transmisión de la información: la empresa puede

solicitar información sobre la salud y la estructura psicofísica del trabajador, que el mismo trabajador puede no conocer o no quiera conocer (por ej., su información genética).

A.3. Ley Nº 18.331: "protección de datos personales y acción de "habeas data"

Artículo 9º. Principio del previo consentimiento informado.- El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse.

A.4. Las principales situaciones que vinculan las tecnologías y la intimidad del trabajador: a) correo electrónico y web; b) **la videovigilancia interna en la empresa**; c) la geolocalización (GPS).

B. LA POSICIÍON DE LA JURISPRUDENCIA

Escasa – especialmente a nivel de Tribunales - pero es tan solo una punta de iceberg - En muchos casos las empresas prefieren pagar despido o o transar.

3.1. Internet, redes sociales, correo electrónico y chats

2002: TAT 3° constituye un caso de NMC "el envío (por parte del trabajador) al personal de la empresa de un mensaje con contenido de sexo explícito a través de correo electrónico utilizando el actor los medios informático del empleador en horario de trabajo".[1].

[1] TAT 3º, Sentencia N° 425 de 16.10.2002, en AJL 2002, c. 454.

2005: TAT 3° el envío de mensajes particulares a través de correo electrónico utilizando el actor los medios informáticos del empleador en horario de trabajo constituye NMC.

2007: TAT 1° → el empleador tiene derecho a revisar el ordenador de la empresa, por ser de su propiedad[2].

2010: TAT 2° hay NMC en el caso de un funcionario que ocupaba un cargo importante porque utilizó el tiempo de trabajo para contactarse a Internet, y acceder en forma más que asidua a páginas pornográficas, lo que se acredita en forma clara con los registros agregados en autos".[3].

2011 TAT 1°: diferencia el uso emails y chats en el lugar de trabajo. NMC de una trabajadora reingresada al trabajo luego haber dado a luz y despedida dentro de los seis meses del período de estabilidad. La trabajadora chateaba en horario de labor con otras personas, agraviando a la empleadora y compañeros de trabajo". El Tribunal distingue el email del Chat y concluye que chatear (es decir una "cyber charla"), es asimilable a una conversación, mientras que la comunicación a través de correo electrónico es un intercambio de correspondencia".

TAT 1° condena la empresa al pago de la IPD en caso de trabajadora - suspendida que ingresa a "Skype", con la clave personal que le dio la empresa mantiene conversaciones con otra funcionaria en términos negativos para la empresa. Además entiende que la empresa al haber revisado la correspondencia de la actora vía "Skype" sin su autorización o presencia, excedió en el ejercicio de su poder de dirección.

---

[2] TAT 1º, Sentencia Nº 103 de 16.4.2007, en AJL 2007, caso 148.
[3] TAT 2º, Sentencia Nº 399 del 22.12.2010, en AJL 2010, c 418.

JLT 21 N° 31 del 20.08.2014:. Trabajadora despedido por NMC por sustracción y utilización para beneficio propio o de terceros de información confidencial y privilegiada de clientes de la empresa. Se hace lugar al reclamo porque la empresa no probó el carácter confidencial de la información, ni el beneficio personal de la trabajadora

3.2. Redes sociales

- **2013: Sobre redes sociales:** la Intendencia Municipal de Montevideo en abril de 2013 instruyó un sumario a cuatro funcionarios que fueron denunciados por subir fotos a Facebook utilizando los equipos informáticos de dependencias municipales. Los funcionarios, pertenecientes de Centro Comunal[4].
- JLT 6 sentencia No. 7 de 24-02-2014 (suma). Acoge demanda y condena al pago de despido. Caso: la empresa despidió al actor por NMC al trabajador porque publicó en Facebook fotos en que el mismo estaba.semidesnudo en los locales de la empresa. EL JLT no condena porque de la prueba surge que era calificado por sus superiores como un excelente trabajador y aplica principio protector.
- TAT 3 sentencia SEF 14-000338/2014 de 30-09-2014: revocatoria de 1ª Inst. Caso: El actor trabajaba en una línea de producción y lo despiden por NMC, imputándoles retrasos por el uso de herramientas informáticas (ingreso en redes, chats, videojuegos). El TAT considera que el uso del trabajador de una computadora de la empresa en horario de trabajo es una inconducta, pero que no puede considerarse NMC. La actora se dedicó a vigilar el trabajador, pero en

[4] Diario El País, Montevideo 9 de abril de 2013.

ningún momento alertándolo o aplicándole una sanción menor (progresividad de la inconducta)

- JLT 6 sentencia No. 7 de 24-02-2014 (suma). Acoge demanda y condena al pago de despido. Caso: la empresa despidió al actor por NMC al trabajador porque publicó en Facebook fotos en que el mismo estaba.semidesnudo en los locales de la empresa. EL JLT no condena porque de la prueba surge que era calificado por sus superiores como un excelente trabajador y aplica principio protector.

3.3 GPS

- En un caso de desconexión del GPS, el TAT 2° consideró la configuración de notoria mala conducta, porque el actor utilizó el camíon para efectuar cargas de leña para un tercero (caso AJL 2013 483).
- JLT 4° sentencia N°1 del 3/2/2014; no corresponde el reclamo de horas extra, porque la empresa probó mediante el historial del GPS los horarios trabajados.

3.4: Uso indebido de tarjeta de identificación

TAT 4° sentencia N°1 del 3/6/2014: Confirma acreditación de mala conducta

La trabajadora prestaba su tarjeta personal de registro para que otras personas acccedien a comidas calientes en el comedor de la empresa. La empresa agrega una filmación de la entrevista que le hizo a la trabajadora cuando descubrió el hecho: se debatió la licitud de esa entrevista filmada, y el TAT indicó que dicha filmación era lícita.

C. LA POSICIÓN DE LA ADMINSTRACION: AGESIC

- Monitoreo y controles del trabajador
- Agencia de Gobierno Electrónico y Sociedad de la Información -, organismo que depende de la Presidencia de la República, que funciona con autonomía técnica.
- Procura mejorar los servicios al ciudadano y establecer reglas administrativas, sobre las Tecnologías de la Información y las Comunicaciones.
- Su jurisprudencia administrativa legitima ampliamente el uso de videocámaras, micrófonos y otros elementos de control en los lugares de trabajo.

2. La posición de la URCDP

Entre los casos nacionales más recientes, señalamos la consulta que elevaron a la URCDP funcionarios no docentes del Sindicato Nacional de Trabajadores de la Enseñanza Privada (SINTEP) sobre el sistema de videovigilancia de un instituto de enseñanza privado.

La organización sindical y sus afiliados manifestaron preocupación por “la aparición de cámaras en las áreas de recepción, bedelía y otros sectores, cuya instalación no les fue informada. Asimismo, solicitaron saber si el Instituto inscribió su base de videovigilancia, ya que no se advierte la existencia del logo distintivo y se desconoce la persona responsable del tratamiento de imágenes”.

Ante el referido planteo, la URCDP emitió el Dictamen N° 7/2016 de 6 de abril de 2016 en el que expresa que “la videovigilancia es toda grabación, captación, transmisión,

conservación y almacenamiento de imágenes y en algunos casos de sonidos mediante la utilización de videocámaras u otro medio análogo. Las imágenes y sonidos mencionados constituyen información personal y por tanto es de aplicación la LPDP (*léase* “Ley de Protección de Datos Personales”) y sus normas complementarias”.

En merito a lo expresado, la URCDP dispuso en el Dictamen indicado, que los responsables de las Bases de Datos de videovigilancia deben cumplir con determinadas obligaciones, indicadas a continuación: a) ser responsables por el cumplimiento de la normativa que los regula, sobre todo en lo referido a la protección de datos personales; b) Actuar con la debida reserva o sea adoptar medidas de seguridad para garantizar que solamente las personas autorizadas accedan a la Base de Datos; c) Mantener la información en forma confidencial, por la cual el responsable debe ser el custodio de las imágenes; d) garantizar que el titular de los datos pueda ejercer su derecho de acceso; e) Proceder al registro de las correspondientes Bases de Datos, así como informar a las personas que sus imágenes están siendo captadas, colocando en un lugar visible el distintivo diseñado por la propia URCDP que anuncia la presencia de cámaras.

Agregó el Dictamen en el referido caso, que “en aplicación del principio de veracidad, la captación y registro de sonido se aprecia excesiva en relación con la finalidad de vigilancia por motivos de seguridad locativa”. Luego de recordar que el Centro de enseñanza había presentados diversas bases de datos a la Agencia gubernamental, denominadas “Funcionarios”, “Comunicaciones institucionales”, “Regional Noroeste”, “Facultad de Medicina”, señala que el proceso de inscripción aún está en trámite y no se ha completado.

El Dictamen concluye (y esto es lo que más importa a los efectos de la presente nota):

“Respecto de la consulta sobre el sistema de videovigilancia, deberá estarse a lo dispuesto por el Dictamen Nº 10, de 16 de abril de 2010 y la Resolución Nº 989, de 30 de julio de 2010”.

No existe en el Dictamen del 2016 una censura a la actuación del empleador, sino algunas consideraciones a los efectos que la videovigilancia se ajuste a los criterios establecidos en el año 2010, posición invariablemente sostenida por la *URCDP,* que como veremos no es distante de la jurisprudencia de la Gran Cámara de Estrasburgo.

Examinemos pues la posición de la URCDP, ya expresada en el año 2010, a raíz de un planteo de la Dirección Directora de Derechos Ciudadanos, que solicitaba se indicara como debía regularse en Uruguay la videovigilancia de acuerdo con la Ley N° 18.331 del 11 de agosto de 2008.

La Unidad Reguladora en el referido dictamen, luego de definir la videovigilancia en los términos consignados también en el caso planteado por SINTEP, expresaba que la misma “tiene como principales finalidades la protección de las personas físicas, del derecho de propiedad, la tutela del orden público, la detección y prevención de delitos, así como otros intereses legítimos”. La premisa consignada pues en el dictamen es que existe equivalencia entre bienes jurídicos tales como la protección de la persona física y el derecho de propiedad, sin perjuicios de la existencia de “otros intereses legítimos”.

El Dictamen de 2010, reiterado en el 2016, afirma que en determinadas situaciones es legítimo apartarse de la normativa vigente en materia de protección de datos personales y a continuación enumera las diversas situaciones que así lo autorizan:

a) Cuando se utilizan éstos (v.g., los datos personales) con fines de seguridad pública, defensa del Estado o para el ejercicio de actividades del Estado en el ámbito penal, excepción que se encuentra contenida en el artículo 3° literal b de la LPDP.

b) A las operaciones de tratamiento realizadas por personas físicas dentro de su ámbito personal o doméstico de acuerdo con lo establecido en el artículo 3° literal a) de la LPDP y artículo 15 literal b del Decreto 414/009, de 31 de agosto de 2009.

c) Cuando se utilicen con fines periodísticos o de expresión artística o literaria, realizándose un juicio de ponderación entre el derecho a la privacidad de las personas y la libertad de información, ambos derechos constitucionales, éste último regulado en la Ley N° 16.099, de 4 de diciembre de 1989.

Lo que más importa del Dictamen es la referencia a los principios previstos en el art. 5 de la Ley 18.331 de 11.8.2008, que así enumera y explicita:

a. **Principio de la legalidad**, que indica que el tratamiento debe ser acorde a la normativa vigente, con lo cual las bases de datos deben inscribirse en el Registro de Base de Datos Personales a cargo de la Agencia y no tener finalidades violatorias de derechos humanos o contravengan la moral pública;.

b. **Principio de "finalidad"**, que indica que los sistemas de videovigilancia deben tener consignado por escrito u otro medio análogo las finalidades para los que se utiliza. La regla agrega que deberán adoptarse políticas de privacidad y el uso de las videocámaras deberá estar estrictamente limitado a las finalidades expresamente consignadas.

c. **Principio del consentimiento informado**: es necesario contar con el referido consentimiento del titular de los datos, excepto los casos de seguridad pública, que tienen una regulación

específica y en los cuales del juicio de ponderación debe resultar de mayor relevancia la seguridad pública.

d. **Principio de veracidad**: los sistemas de videovigilancia deben ser subsidiarios y sólo pueden ser utilizados cuando no exista otro medio menos lesivo de la intimidad de las personas.

e. **Principio de seguridad**: los responsables de las Bases de Datos deben garantizar la seguridad de las imágenes y evitar su adulteración, pérdida, tratamiento o acceso no autorizado.

f. Plazo de conservación: con relación al plazo de conservación de las imágenes incide asimismo el principio de finalidad, por el cual una vez agotada la finalidad por la se estableció el sistema de videovigilancia, se debe proceder a la eliminación de los registros realizados.

El Dictamen del 2010 establece también responsabilidades y pautas de conducta de quienes emplean bases de datos de videovigiliancia (en el caso, que nos ocupa, el empleador):

a) Ser responsables por el cumplimiento de la normativa que los regula, sobre todo en lo referido a la protección de datos personales.

b) Actuar con la debida reserva o sea adoptar medidas de seguridad para garantizar que solamente las personas autorizadas accedan a la Base de Datos.

c) Mantener la información en forma confidencial, por la cual el responsable debe ser el custodio de las imágenes.

d) Garantizar que el titular de los datos pueda ejercer su derecho de acceso.

e) Proceder al registro de las correspondientes Bases de Datos así como informar a las personas que sus imágenes están siendo captadas.

f) colocar distintivos que deben especificar ante quién (responsable, con su respectivo domicilio) se podrán ejercer los derechos consagrados en la Ley N0 18.331.

Si bien una primera lectura del Dictamen del 2010 permite pensar que existen muchas limitaciones para la colocación de aparatos de videovigilancia, la lectura del mismo nos permite concluir – en material laboral – que el empleador tiene facultades para instalar instrumentos de monitoreo en los lugares e instrumentos de trabajo, en la medida que existan razones que lo justifiquen y que el trabajador haya sido previamente informado. Las razones pueden ser variadas, desde motivos de seguridad a controles para asegurar la calidad del producto, hasta necesidades de evitar el ingreso de virus a las computadoras. Aunque en el pronunciamiento de 2010 se aluda al "principio del consentimiento informado", veremos que no es indispensable requerir la aprobación por parte del trabajador.

Para confirmar nuestra opinión en el sentido que los criterios administrativos nacionales legitiman un amplio uso de controles digitales sobre los trabajadores, destacamos el Dictamen 19/2011, que se pronuncia sobre un caso muy puntual: las eventuales consecuencias jurídicas que tendría contratar el servicio de videovigilancia ofrecido por ANTEL, a efectos de instalar la cámara en la cocina-comedor del domicilio particular donde realiza sus tareas la niñera contratada para el cuidado de los hijos menores de edad.

En el referido dictamen la URCDP expresa que la evolución producida en materia de derecho a la intimidad y a la privacidad ha llevado a plantear situaciones "donde se entrecruzan varios derechos de raigambre constitucional, desde una perspectiva que enfatice en esta nueva concepción". En el caso concreto – indica el

Dictamen -, **no es necesario obtener el consentimiento de la persona afectada por el sistema de videovigilancia**[5], porque el art. 9 de la Ley N° 18.331, Numeral D, indica que no se requiere recabar el consentimiento de una persona, si los datos refieren a una relación contractual y son necesarios para su desarrollo o cumplimiento de la misma". En el caso que se analiza – expresa el Dictamen – "puede considerarse que este tratamiento es necesario para el adecuado desenvolvimiento de la relación laboral referida al cuidado de los niños". La URCDP concluye afirmando que – aunque no se requiere el consentimiento de la trabajadora – **"de todos modos deberá informarse expresamente y en forma anticipada a la misma, porque la videovigilancia pasará a formar parte de la propia relación laboral y deberán respetarse los espacios privados de la trabajadora (baños, dormitorios o vestuarios), pues la videovigilancia en estos casos afecta su intimidad y privacidad"**[6].

D. CONCLUSIONES:

- toda actitud invasiva de la privacidad del trabajador debe estar legitimada en un propósito legítimo y objetivo de la empresa;
- proporcionalidad: debe existir una razonable proporcionalidad entre el objetivo legítimo y la intrusión en la privacidad del individuo;
- como se afirma en el derecho anglosajón, importa el ***be fair***: ser limpio, ser leal; un propósito legítimo no justifica una actitud ilegal o persecutoria;
- principio de la no discriminación: el empleador no puede sancionar a unos trabajadores y no sancionar a otros, que

[5] *negritas del autor*
[6] *negritas del autor*

incurren en una misma eventual inconducta (por ejemplo, abusar de la página web);

- principio de la transparencia: los trabajadores deben ser informados sobre las políticas de la empresa que invaden la privacidad
- Ponderación de los fines y derechos tutelas (Avilés y otro)
- Una vuelta al **principio de la razonabilidad**, que se expresa en la breve y clásica definición de Plá Rodríguez: el ser humano, en sus relaciones laborales, debe proceder conforme a la razón