LA VIDEOVIGILANCIA EN EL DERECHO AUSTRÍACO DEL TRABAJO*

[*THE VIDEO SURVEILLANCE IN AUSTRIAN LABOR LAW*]

Sabine Ogriseg

Fecha de recepción: 21 de octubre de 2012
Fecha de aceptación: 11 de noviembre de 2012

Resumen: En tiempos recientes ha habido un notorio incremento en la instalación de vídeo vigilancia por los empresarios dentro de sus centros de trabajo. Tanto si estas cámaras de vigilancia están ocultas como si no, se dirigen esencialmente al mismo objetivo: la protección del negocio empresarial no sólo contra posibles

* Traducción al castellano, desde el alemán original („Videoüberwachung im Arbeitsrecht"), de Jesús Martínez Girón.

intrusos, sino también con sus propios trabajadores. ¿Ésta el derecho a la intimidad del trabajador protegido en su lugar de trabajo?

***Abstract**: In recent years there was a noticeable increase in installation of video surveillance by employers, within their business establishments. Whether these surveillance cameras are hidden or not, they essentially strive toward the same objective: the protection of the employer's business not only against possible intruders, but also against its own employees. Is an employee's right to privacy protected in his work place?*

Palabras clave: Vídeo vigilancia – Lugar de trabajo – Gran hermano – Intimidad – Protección

***Keywords**: Video surveillance – Workplace – Big brother – Privacy – Protection*

* * *

1. Introducción

El desarrollo de la videotecnología, y de la vigilancia frecuentemente aparejada con él, está omnipresente. Se avecina un ascenso continuo de las nuevas tecnologías de la información y de la comunicación, que posibilita el control de las personas en lugares públicos y privados de todo el ámbito empresarial por medio de la videovigilancia. Ahora ya no es posible obviar la presencia de la tecnología moderna. Esto se evidencia, ante todo, en la videovigilancia de espacios públicos[1], por ejemplo, en las estaciones de metro[2]. Sin embargo, según un estudio, el 55 por ciento de los encuestados ha aceptado la omnipresente videovigilancia en Austria como algo acostumbrado[3]. La videovigilancia en lugares públicos por motivos de seguridad se aprueba y se considera apropiada incluso por el 81 por ciento[4].

Pero esta temática también conduce a que se incremente la introducción de medidas de videovigilancia en el mundo laboral. Sólo hace poco se ha avivado la discusión por de la videovigilancia clandestina de trabajadores o, en su caso, clientes de una empresa alimentaria alemana[5]. Por causa de los rapidísimos progresos de la tecnología, también el legislador necesita reaccionar en correspondencia con ellos.

2. Generalidades sobre la videovigilancia

[1] Véase Cuestionario del Ministerio Federal del Interior: Fechado el 1. 1. 2008, videovigilado en Graz, en la Jakominiplatz y en la Estación Principal, al amparo de la norma del parágrafo 54, apartado 5, de la SPG, <http://www.parlament.gv.at/PAKT/VHG/XXIII/AB/AB_03124/fname_104020.pdf> (27. 2. 2013).

[2] Desde 2005 se trata en ese caso de las llamadas "cámaras cúpula", con muy elevada resolución de imágenes. Comunicación de las Líneas de Viena: Comisión de Protección de Datos (DSK) 21. 6. 2005, K507.515–021/0004-DVR/2005; confrontar también *Kunnert*, Big Brother in U-Bahn, Bus und Bim. Videoaufzeichnungen in öffentlichen Verkehrsmitteln aus datenschutzrechtlicher Sicht, juridikum 2006, 42.

[3] <http://www.oekonsult.eu/datensicherheit2008.pdf> (27. 2. 2013).

[4] <http://www.oekonsult.at/bigBrother_gesamtergebnisse_final.pdf> (27. 2. 2013).

[5] Los trabajadores de Lidl, en ese caso, fueron observados durante un período comprendido entre 2006-2008, a través de detectores de carga con vídeocamaras. La autoridad de protección de datos calificó esto como una infracción grave de protección de datos e impuso una multa de 1.462.000 euros. Según Comunicado de Prensa del Ministerio del Interior de Baden-Württemberg, las autoridades de vigilancia de la protección de datos impusieron a Lidl-Vertriebsgesellschaften una multa más elevada, por causa de infracción más grave de protección de datos <https://www.datenschutzzentrum.de/presse/20080911-bw-lidl-bussgeldverfahren.pdf> (27. 2. 2013); confróntese también en relación con ello *Byers*, Die Videoüberwachung am Arbeitsplatz unter besondere Berücksichtigung des neuen § 32 BDSG (2010) 5.

Ante todo, generalmente se asocia con el concepto de videovigilancia un sentimiento de vigilancia y de invasión en la espera privada del individuo. De ahí que me ocupe en lo que sigue de la esfera privada del individuo en conexión con la Ley de protección de datos de 2000 (DSG 2000)[6]. En virtud del parágrafo 50a, apartado 1, inciso último, de la DSG 2000, sólo se aplican las disposiciones sobre videovigilancia cuando no se disponga lo contrario en otras Leyes (principio de subsidiariedad)[7].

2.1. Definición de videovigilancia, según la DSG 2000

El parágrafo 50, apartado 1, de la DSG 2000 define la viodeovigilancia como la constancia sistemática y especialmente continuada de resultados, que afectan a un objeto determinado (objeto vigilado) o a una persona determinada, a través de mecanismos técnicos de grabación de imágenes o de transmisión de imágenes. Según el tenor del parágrafo 50a, apartado 1, de la DSG 2000, se habla de constancia sistemática (...) de resultados. Del requisito «sistemática», se desprende que la constancia de resultados es repetida[8]. De ahí que deba producirse un registro incesante de resultados, que implique «vigilancia», a través de una serie de pasos para utilizar el resultado[9]. De ahí que también se comprenda en la definición legal la vigilancia en tiempo real, esto es, la vigilancia que se agota en la representación en tiempo real, y en la que los resultados ni se almacenan ni se procesan[10].

En relación con el parágrafo 50a, apartado 1, de la DSG 2000, lo siguiente a deducir es que la videovigilancia debe afectar a un objeto determinado o a una persona determinada. La noción de objeto debe entenderse muy ampliamente, aunque al menos debe darse una relación indirecta con una persona. De ahí que se considere suficiente cuando se vigila una parte de un edificio o una zona de servicios de un centro de cálculo, también cuando no hay que contar con que ninguna persona esté en ellos. La noción de «persona» hay que interpretarla en el sentido de persona natural, y sobre la base, en todo caso, de la circunstancia de tratar la grabación de imágenes o, en su caso, la transmisión de imágenes como datos sensibles, en el sentido del parágrafo 4, número 2, de la DSG 2000. Sin

[6] Ley Federal sobre Protección de Datos Personales (Ley de Protección de Datos 2000 – DSG), BGBl I 165/1999 en la redacción de BGBl I 133/2009.

[7] Cfr. en relación con ello, por ejemplo, Videoüberwachung im Bereich der Sicherheitspolizei §§ 53, 54 Sicherheitspolizeigesetz (SPG).

[8] *Hattenberger*, Die Bestimmungen des DSG zur Videoüberwachung – Hat sich der Aufwand gelohnt?, en Jahnel (Editor), Datenschutzrecht Jahrbuch 2011 (2011), 117 (120).

[9] Véase ErlRV 472 del Suplemento XXIV. GP. 17.

[10] *Thiele,* Aktuelles zur Videoüberwachung - Erste Erfahrungen nach der DSG Novelle 2010, Parte 2, jusIT 2011/9, 14 (14 ss.).

embargo, se plantea la cuestión de si son «datos sensibles», en el sentido de la DSG 2000, los datos sobre imágenes de video. En el parágrafo 4, número 2, de la DSG 2000, no se enumeran los datos sobre imágenes. El legislador considera los datos comprendidos en la videovigilancia como datos potencialmente sensibles, dado que estas imágenes permiten obtener conclusiones seguras, por ejemplo, sobre el origen étnico o el estado de salud de una persona[11].

Desde el punto de vista del Derecho de la protección de datos, sólo es relevante entonces la videovigilancia cuando se investigan datos relativos a personas. Se desprende del parágrafo 4, número 1, de la DSG 2000 que este requisito se ha cumplido ya cuando es posible la identificación de los afectados por medio de recursos jurídicos[12]. Con este fundamento se explica también la grabación electrónica de caracteres distintivos de un automóvil para la investigación de datos relativos a personas[13].

Como criterio ulterior, hay que considerar el adjetivo «vigilado». De él deduce la doctrina dominante[14] el objetivo de control de la videovigilancia, relevante desde el punto de vista del Derecho de protección de datos. Hay que atender al sentido del objetivo de control, que sólo comprenderá la grabación sistemática de resultados, que sirva a la vigilancia de personas o de objetos. De ahí que no haya que subsumir en el parágrafo 50a de la DSG 2000 las grabaciones artísticas o turísticas, pero tampoco las grabaciones de vídeo con objetivos puramente familiares y personales[15], dado que falta el objetivo de control.

Además, se limita el ámbito de aplicación de la videovigilancia a través de la circunstancia fáctica de la «grabación o transmisión técnicas de imágenes». En consecuencia, la simple percepción u observación está excluida, al igual que la observación intensiva o el recurso técnico tampoco representa videovigilancia, en el sentido del parágrafo 50a, apartado 1, de la DSG 2000.

Según el parágrafo 50a, apartado 5, de la DSG 2000, están expresamente excluidos determinados ámbitos, que se consideran ámbitos vitales muy

[11] *König*, Videoüberwachung (in der betrieblichen Praxis), en Bogendorfer (Editor), Datenschutzgespräche 2011 – Datenschutz im Unternehmen. Das Spannungsfeld einzelner Interessen (2011) 23 (29 ss).

[12] Cfr. en relación con ello DSK 21. 3. 2007, K507.515-023/0002-DVR/2007.

[13] DSK 20. 6. 2008, K600.053-023/0002-DVR/2008.

[14] *Jahnel*, Handbuch Datenschutzrecht (2011) Rz 8/98; *el mismo*, Die DSG-Novelle 2010 im Überblick, jusIT 2010/9, 12 (14); *Souhrada-Kirchmayer* en Jahnel, Datenschutzrecht Jahrbuch 2010, 17, (21); *Löschnigg* en Bergauer/Staudegger, Recht und IT 57, (58 ss.).

[15] Cfr. en relación con ello el parágrafo 45 de la DSG.

personales, como cuartos de baño, vestidores, etc.[16]. Sin embargo, si sólo se relaciona el apartado 5 con el apartado 4, significaría esencialmente que la videovigilancia en ámbitos muy personales en el marco del apartado 3, resulta bastante admisible, por ejemplo, si están implicados intereses vitales muy importantes de la persona, etc.

2.2. Admisibilidad de la videovigilancia, según la DSG

Como baremo para medir la admisibilidad de la videovigilancia, se tomará en cuenta la norma central del parágrafo 16 del ABGB[17]. En el caso de la dignidad de la persona a que se refiere el parágrafo 16 del ABGB, se trata de un concepto jurídico indeterminado, que debe concretarse por aproximación a los preceptos del Derecho Constitucional (en especial, el artículo 8 del CEDH[18] y el parágrafo 1 de la DSG 2000) y del Derecho del Trabajo (en especial, el deber de protección del parágrafo 1157 del ABGB y el párágrafo 18 de la AngG[19]). El Tribunal Supremo (OGH) afirma sobre ello: «la videovigilancia identificadora, sistemática y encubierta, con grabación accesible de imágenes, en virtud del parágrafo 16 ABGB en conexión con el artículo 8 EMRK, representa siempre una noción del derecho protegido al respeto de la espera de la confidencialidad»[20].

En el parágrafo 50a, apartado 2, de la DSG 2000, se mencionan los objetivos respecto de los que resulta admisible la videovigilancia. Según el parágrafo 50a, apartado 2, de la DSG 2000, se mantiene que toda forma de videovigilancia hay que someterla a un examen de admisibilidad en el marco de las disposiciones de los parágrafos 6 a 9 de la DSG 2000. Hay que anotar aquí, en especial, las normas sobre los principios de protección de datos a que se refiere el parágrafo 6 de la DSG 2000, y las normas de admisibilidad del procesamiento y transmisión, y en especial el principio de proporcionalidad a que se refiere el parágrafo 7, apartado 3, de la DSG 2000[21]. El parágrafo 6 de la DSG 2000 contiene, en forma de catálogo, los requisitos esenciales que hay que observar en caso de examen de la admisibilidad del procesamiento de datos, como, entre otros,

[16] *Knyrim*, Datenschutzrecht. Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm^2 (2012) 198; *Ennöckl*, Die DSG-Novelle 2010, ÖJZ 2010/35, 293 (298).

[17] Código Civil General para los Estados Alemanes Reunidos de la Monarquía Austríaca (ABGB), JGS 946/1811 en la redacción de BGBl I 68/2012.

[18] Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales, BGBl 2010/1958 en la redacción de BGBl I 68/2012.

[19] Ley Federal de 11 Mayo 1921 sobre el contrato de servicios de los empleados privados (Ley del Empleado – AngG), BGBl 292/1921 en la redacción de BGBl I 58/2010.

[20] En general sobre afectación de la dignidad humana, véase *Löschnigg*, Datenermittlung im Arbeitsverhältnis (2009) 232.

[21] *König* en Bogendorfer, Datenschutzgespräche 2011, 23 (25).

la lealtad y legalidad, estricta vinculación al objetivo, limitación de la extensión de los datos, veracidad y actualidad, así como la limitación temporal[22].

En mi opinión, hay que examinar como requisito decisivo el principio de proporcionalidad a que se refiere el parágrafo 7, apartado 3, de la DSG 2000. Este criterio también se expresa en el parágrafo 1, apartado 2, inciso último, de la DSG 2000, según el cual en el caso de restricciones admisibles del concepto, sólo pueden aplicarse al derecho fundamental correspondiente las moderadas que conduzcan al objetivo. Si existe un medio más moderado que la videovigilancia, que también se oriente a conseguir adecuadamente el objetivo pretendido y sea menos agresivo, entonces hay que preferir éste siempre[23]. En ese caso, es concebible la aplicación de chips-espía en las mercancias de las tiendas para prevenir robos, la instalación de puertas de seguridad protegidas, y la aplicación de interfonos o controles de seguridad protegidos con códigos en una cámara acorazada[24], y dar a éstos prioridad frente a la videovigilancia.

El parágrafo 50a, apartado 3 y apartado 4, de la DSG 2000 regulan ese caso, en el que el afectado por la videovigilancia no resulta perjudicado en sus intereses dignos de protección al mantenimiento de la confidencialidad [25].

Según el parágrafo 50a, apartado 3, de la DSG 2000, la videovigilancia sólo está justificada, cuando

— se realiza en interés vital importante de una persona,

— se procesan datos sobre una conducta que indudablemente permiten establecer la conclusión de que se orientaban a una defensa patente, o

— el afectado ha consentido expresamente el empleo de los datos.

A efectos del interés vital importante de una persona, la mayoría de las veces sólo estará justificada la videovigilancia en tiempo real, dado que la defensa del interés vital importante produce necesariamente un impacto inmediato en los resultados. A modo de explicación, se mencionan como ejemplos la transmisión en una unidad de cuidados intensivos, pero también la vigilancia de espacios

[22] *Dohr/Pollirer/Weiss/Knyrim*, DSG[2] § 50a Anm 3.
[23] 62/ME XXIV. GP. 14.
[24] *Thiele,* Aktuelles zur Videoüberwachung – Erste Erfahrungen nach der DSG Novelle 2010, Parte 1, jusIT 2010/107, 219 (220).
[25] *Thanner*, DSG § 50a 145.

carcelarios. En esas circunstancias, se cubren/comprenden sólo esos actos, que sirven directamente al interés vital principal del afectado.

Aparte esto, son comportamientos seguros, en especial en un espacio público, aquellos que pueden ser percibidos por todos, y de ahí que haya que pensar de la misma manera, respecto del consentimiento, acerca que se harán disponibles con carácter general al público. Sobre esto, cuenta ante todo el callejeo o la entrada en escena en el marco de un acto. El mero moverse en la calle no cumple estas circunstancias.

El consentimiento expreso hay que equipararlo al principio de autodeterminación informativa. Se deja a la autodecisión del afectado lo que hace con sus datos. De ahí que pueda dar al comitente el consentimiento para el empleo de sus datos. En ese caso, sin embargo, hay que ponderar dos aspectos. De un lado, el consentimiento requiere una declaración de voluntad del afectado, con conocimiento del verdadero estado de cosas. En el marco de la declaración de su consentimiento, debe ser evidente para el afectado qué datos serán procesados en relación con qué objetivos. De otro lado, el consentimiento debe ser revocable en todo momento, y la revocación tiene como consecuencia la inadmisibilidad de un nuevo proceso[26].

En virtud del parágrafo 50a, apartado 4, de la DSG 2000, también es admisible la videovigilancia en espacios privados, si es

— para la protección del objeto vigilado o de la persona vigilada ante ataques peligrosos (número 1),

— para el cumplimiento de deberes especiales de cuidado relativos a la protección del objeto vigilado o de la persona vigilada (número 2), o

— para la protección del cuerpo, de la vida o de la propiedad del comitente a través de la vigilancia en tiempo real (número 3).

Según el parágrafo 50a, apartado 4, de la DSG 2000, a diferencia del apartado 3, es necesaria una ponderación de intereses en el espacio privado. En este caso, es fundamental tener en cuenta que los datos afectados por la videovigilancia son potencialmente datos sensibles, porque las imágenes suministran ordinariamente informaciones sobre el estado de salud o el origen étnico (color de la piel) del afectado. Pero la videovigilancia no está primariamente dirigida al

[26] *König* en Bogendorfer, Datenschutzgespräche 2011, 23 (27 ss.).

registro de tales datos, sino que estos se producen como «productos de la casualidad»[27].

El parágrafo 50a, apartado 4, número 1, de la DSG posibilita al comitente la videovigilancia para la protección del objeto vigilado o de la persona vigilada ante ataques peligrosos. En el número 1, pueden subsumirse también concretos peligros para los secretos del negocio y de la empresa, así como, en todo caso, el concreto peligro de una violación administrativa grave. La videovigilancia a que se refiere el número 1 también puede comprender la videovigilancia preventiva en relación con un concreto peligro para el objeto vigilado o la persona vigilada. Esto también es posible si aún no ha ocurrido ningún ataque peligroso a este objeto o a esta persona[28].

Requisito del número 2 es que se impusieran al comitente deberes especiales de cuidado para la protección del objeto vigilado (o la persona vigilada)[29]. Para cumplir los correspondientes deberes de cuidado, puede aplicarse la videovigilancia. Pero en la videovigilancia aplicada debe utilizarse siempre un medio apropiado y moderado[30].

El número 3 regula la videovigilancia de una persona o de un objeto a través de la vigilancia en tiempo real. Como ya se dijo brevemente antes, en el marco de la vigilancia en tiempo real, los datos no serán ni almacenados ni ulteriormente procesados de forma especial. A través de ello, no puede conseguirse el objetivo de aseguramiento de la prueba, únicamente la introducción de medidas inmediatas para el objetivo de protección de la correspondiente persona/correspondiente objeto. Objetivos permitidos son la protección del cuerpo, de la vida o de la propiedad del comitente. Si se persigue la protección ajena a través de la vigilancia en tiempo real, ésta no resulta subsumible en el número 3[31].

Aparte esto, el parágrafo 50, apartado 6, de la DSG regula también cómo hay que proceder con los «casos de azar». Con ello se alude a las grabaciones de datos que exceden el objetivo de uso regulado (parágrafo 50a, apartados 2 a 4, de la DSG 2000). Según decisión libre del comitente, el uso de la grabación y la transmisión sólo resultan posibles a un ulterior comitente:

[27] 62/ME XXIV. GP. 15.
[28] 62/ME XXIV. GP. 16.
[29] Cfr. en relación con ello, por ejemplo, parágrafo 1319a del ABGB, y parágrafo 19 de la Ley del ferrocarril.
[30] *König* en Bogendorfer, Datenschutzgespräche 2011, 23 (32 ss.).
[31] 62/ME XXIV. GP. 16.

— cuando es una autoridad o tribunal competente, si existe sospecha fundada en el comitente de que los datos documentan un acto penal perseguible de oficio. Ordinariamente, sólo surgirá la sospecha fundada a través de denuncia de terceros (por ejemplo, comunicación de que una persona ha estado hurtando carteras ante la empresa, en el espacio comprendido en la vigilancia del escaparate)[32];

— cuando son funcionarios de seguridad, si hubiese que utilizar los datos a que se refiere el parágrafo 53, apartado 5, de la SPG[33] (por ejemplo, para la defensa ante un ataque peligroso o para la búsqueda de personas[34])[35].

Además, el comitente no puede negar a una autoridad o a un tribunal la entrega de videodatos, si éstos lo exigen como medio de prueba en el curso de un procedimiento, y disponen[36] de las correspondientes posibilidades de coacción[37].

En el parágrafo 50a, apartado 7, de la DSG 2000, el legislador regula la llamada prohibición de análisis en relación con la videovigilancia. Los datos de los afectados conocidos por medio de videovigilancia no pueden ser respaldados, en cuanto que criterio de selección de datos sensibles, con otros datos de imágenes registradas o almacenadas. A través de ello, debe excluirse la búsqueda de apoyo automatizada de personas no afectadas. Por lo demás, también es inadmisible la búsqueda según criterios sensibles en el sentido del parágrafo 4, número 2, de la DSG 2000 (por ejemplo, color de la piel, limitaciones de salud)[38].

2.3. Deberes del comitente

El comitente también tiene que cumplir deberes ciertos en el marco de la videovigilancia. Estos son

— El deber de comunicar la videovigilancia.

---

[32] *König* en Bogendorfer, Datenschutzgespräche 2011 – Datenschutz im Unternehmen, 23 (34).

[33] Ley Federal sobre la Organización de la Administración de Seguridad y el Ejercicio de la Policía de Seguridad (Ley de la Policía de Seguridad – SPG), BGBl 566/1991 en la redacción de BGBl I 50/2010.

[34] ErlRV 472 del Suplemento XXIV. GP. 19.

[35] Véase en relación con ello, también, *Jahnel*, Datenschutzrecht, Rz 8/105.

[36] ErlRV 472 der BlgNR XXIV. GP. 19; *Bergauer*, Änderungen der strafrechtsrelevanten Bestimmungen des DSG 2000 durch die Novelle 2010, en Jahnel (Editor), Datenschutzrecht Jahrbuch 2010 (2010) 73 (90 ss.); *Thanner*, DSG § 50a 148.

[37] En los materiales prácticos se menciona la posibilidad de realización subsiguiente como aseguramiento de la prueba.

[38] 62/ME XXIV. GP. 17.

— El deber de identificar los datos de la videovigilancia.

— El deber de protocolizar.

— El deber de cancelación.

— El deber de satisfacer los derechos del afectado (en especial, el derecho de información).

2.3.1. Deber de comunicación y procedimiento de registro

Los datos de videovigilancia están sujetos, en virtud de los parágrafos 17 y siguientes de la DSG 2000, al deber de comunicarlos a la DSK y al registro de procesamiento de datos. No resulta obligado realizar electrónicamente las comunicaciones sujetas a control previo, por medio de una aplicación de internet. Éstas se examinarán con apoyo automatizado y se registrarán inmediatamente si no tienen errores. Las disposiciones especiales sobre el procedimiento de registro, a que se refiere el parágrafo 50c de la DSG 2000, establecen que esas comunicaciones, por causa de su muy elevado potencial de peligro, en atención al frecuentemente amplio círculo de afectados y al uso potencial de datos sensibles[39], se sujetan a un control previo[40]. Aparte esto, la vigilancia en tiempo real[41] no está sujeta a comunicación[42].

Del deber de comunicación al registro de proceso de datos, con base en el Reglamento estándar y el Reglamento modelo[43], están exceptuados, además:

— Bancos,

— Joyerías, el comercio de antigüedades y objetos de arte, talleres de oro y plata,

[39] Véase en relación con ello ErRV 472 BlgNR XXIV. GP. 18.

[40] *Jahnel*, jusIT 2010/9, 12 (14).

[41] La misma existe cuando la vigilancia se agota en una mera repetición y los datos comprendidos no pueden ser almacenados ni procesados, véase parágrafo 50a, apartado 4, número 3, de la DSG.

[42] Véase también *Hattenberger* en Jahnel, Datenschutzrecht Jahrbuch 2011, 117 (131).

[43] Reglamento del Canciller Federal sobre las aplicaciones estándar y modelo, según la Ley de Protección de Datos de 2000 (Reglamento Estándar y Modelo 2004 – StMV 2004), BGBl II 312/2004 en la redacción de BGBl II 255/2009, BGBL II 152/2010, BGBl II 105/2011 y BGBl II 306/2012; detalladamente en relación con ello véase *Thiele*, Neues zur Datenermittlung im Konzern, Videoüberwachung & Co – Neuerliche Änderung der Standardanwendung SA032, jusIT 2012/85, 178.

— Estancos

— Gasolineras

— Terrenos privados edificados (con entrada a la casa y garaje),

— Autoridades representativas extranjeras y organizaciones internacionales.

Dichas excepciones se critican por *Hattenberger*[44], dado que a través de ellas se potencia directamente el aumento de videovigilancias.

Las imitaciones de cámaras no deben comunicarse, dado que no tiene lugar la grabación. Sin embargo, el OGH ha expresado en una decisión[45], que a pesar de todo, el montaje de una imitación de cámara puede resultar inadmisible, en virtud del parágrafo 16 del ABGB, en conexión con el artículo 8, apartado 2, del CEDH, dado que el control continuo por medio de una cámara representa un menoscabo de la esfera privada.

Además, por principio, el dispositivo de videovigilancia sólo puede ser instalado en la empresa cuando se ha concluido el procedimiento de registro, es decir, cuando se ha producido el registro de procesamiento de datos dentro de los dos meses siguientes al depósito del anuncio (el llamado procedimiento de control previo). Si se instala antes la videovigilancia en la empresa, esto representa una infracción administrativa, y puede ser sancionada con una multa de hasta 10.000 euros[46].

En caso de videvigilancia en la empresa, el parágrafo 50a, apartado 1, inciso último, de la DSG 2000 establece que también hay que presentar durante la tramitación del procedimiento de registro los eventuales acuerdos de empresa que se hayan celebrado (sobre esto, véanse más detalles en 3.3.1.f).

2.3.2. Deber de protocolización, deber de cancelación y deber de identificación

[44] *Hattenberger* en Jahnel, Datenschutzrecht Jahrbuch 2011, 117 (132).

[45] OGH 19. 12. 2005, 8 Ob 108/05y = ecolex 2006/167, 385 = JBl 2006, 447 = RdW 2006/253, 273 = Zak 2006/125, 74.

[46] *Knyrim*, Datenschutzrecht[2], 202.

En virtud del parágrafo 50b, apartado 1, de la DSG 2000, cabe observar que todo proceso de aplicación de videovigilancia hay que protocolizarlo íntegramente, exceptuándose de ello solamente la videovigilancia constante.

En relación con la videovigilancia, tiene una importancia esencial el criterio de la limitación temporal. Según *Dohr/Pollirer/Weiss/Knyrim*[47], en lo posible, el almacenamiento debe mantenerse poco tiempo.

El proyecto del Gobierno[48] y el borrador del Ministerio[49] preveían aún, en el parágrafo 50b, apartado 2, de la DSG 2000, la cancelación de los datos conocidos por videovigilancia a las 48 horas. Sin embargo, la Ley sólo prevé la cancelación tras 72 horas. Pero este deber de cancelación se enfrenta en la práctica a la crítica, dado que el mismo se mantiene muy poco tiempo. En diversas tomas de posición sobre enmiendas a la DSG de 2010[50], se propuso reiteradamente el deber práctico de almacenamiento de hasta una semana. El Comité procedimental llegó a la conclusión de que, en caso de cancelación, es posible plantear la necesidad de información en aproximadamente 48 horas. De ahí que se decidiese fijar la duración del almacenamiento admisible en 72 horas, por motivos prácticos (fines de semana, festivos)[51].

Complementariamente, se atenúa la breve duración del almacenamiento, por referencia al parágrafo 33, apartado 3, de la AVG[52]: si el final del plazo cae en sábado, domingo, festivo legal o Viernes Santo, entonces es el último día del plazo es el siguiente día laboral.

La prolongación de la duración del almacenamiento es ciertamente posible, en principio. Sobre ello, debe expresarse en la comunicación al registro de proceso de datos qué motivos especiales hay para pretender ese objetivo (por ejemplo, la lucha contra el fraude en el sector bancario)[53].

[47] *Dohr/Pollirer/Weiss/Knyrim*, DSG^2 § 50a Anm 3, con notas sobre la DSK.

[48] RV 472 BlgNR XXIV. GP. 4.

[49] 62/ME XXIV. GP. 17.

[50] Cfr. en relación con ello la toma de posición del Club de Periodistas Austríacos (40/SN-62/ME); toma de posición de la Cámara de Médicos Austríacos (56/SN-62/ME); de la toma de posición de la Comisión de Protección de Datos (57/SN-62/ME) hay que deducir que la duración del almacenamiento debía ascender a 96 horas.

[51] AB 531 de los Suplementos a los Protocolos Estenográficos del Consejo Nacional XXIV. GP. 4.

[52] Ley del Procedimiento Administrativo General de 1991 – (AVG), BGBl 51/1991 en la redacción de BGBl I 33/2013.

[53] *König* en Bogendorfer, Datenschutzgespräche 2011, 23 (37).

El comitente tiene también el deber de identificación, en virtud del parágrafo 50d de la DSG 2000. Este deber de identificación se considera lex specialis, respecto del deber de información del parágrafo 24 de la DSG 2000. De ahí que el comitente de la videovigilancia deba identificarla consecuentemente, para informar de la videovigilancia a las personas (potencialmente) afectadas. Esto se remarca usualmente por medio de la palabra «videovigilado» o de un pictograma (por ejemplo, DIN 33450)[54]. A través de ello, debe darse a los afectados la posibilidad de recibir informaciones sobre la identificación de la videovigilancia, esto es, sobre el comitente[55].

2.3.3. Deber de información

El parágrafo 50e de la DSG 2000 completa el deber de información general del parágrafo 26 de la DSG 2000. En el deber de información, no se trata como en los deberes antes mencionados de un deber explícito, sino de una forma implícita de deber del comitente, que sólo debe cumplir a exigencia del que pide la información. El comitente sólo tiene que dar información al que la pide sobre los datos procesados sobre su persona, cuando ésta fue posiblemente afectada en un período por la videovigilancia, así como sobre el lugar en que posiblemente ha ocurrido. Requisito fundamental para el que solicita la información es el de que el solicitante debe realizar su petición dentro del plazo de grabación (72 horas); en caso contario, debe darse una información negativa. La información tiene que darse en el formato técnico habitual, por medio del envío de una copia de los datos de imágenes relativos a la persona[56]. Pero supuesto que la información basada en intereses justificados preponderantes de un tercero no pueda ser consecuentemente enviada, el solicitante de la información tiene derecho a una descripción por escrito de la conducta grabada por la vigilancia o a la información desfigurada de las otras personas[57]. En una decisión del DSK[58], se indica sobre ello que existe en el solicitante de la información un elemento adicional, especial, extraordinario y con derecho a la protección de datos. Pues «supuesto que el comitente no ha valorado la identificación del video, no sólo conoce los datos “clasificables” — ciertamente los ha investigado y guardado en su “ámbito de dominio” y de ahí que sea “comitente”, pero no puede tomar de él ningún elemento, a no ser que se interfiera objetivamente un motivo de evaluación, que fuese reconocido en el procedimiento

[54] *Schrems*, Private Videoüberwachung (2010) 94.

[55] Ya hubo una primera sanción por causa de una identificación insuficiente, aunque lamentablemente el juicio correspondiente no está hasta ahora disponible, véase *Knyrim*, Datenschutzrecht[2], 203.

[56] *König* en Bogendorfer, Datenschutzgespräche 2011 (2011) 23 (46).

[57] 62/ME XXIV. GP. 18.

[58] DSK 5. 12. 2008, K121.401/0009-DSK/2008.

de registro como caso de existencia de un interés predominante y justificado a la evaluación».

El derecho a la información no existe en caso videovigilancia constante, dado que los datos no se almacenan.

3. La videovigilancia en el Derecho del Trabajo

3.1. Generalidades

En el ámbito del mundo del trabajo, con el objetivo de videovigilar, se aducen a menudo motivos expresos como «incremento de la seguridad», «control del desarrollo de la producción» y hasta «protección ante daños a la propiedad del empresario». En él, se diferencian la mera «autoprotección» (por ejemplo, propiedad, integridad corporal propia) y la protección ajena (protección de terceros). En la valoración de la autoprotección, se opone a menudo al derecho fundamental a la protección de datos otro derecho fundamental, como, por ejemplo, el derecho a la propiedad. Aquí hay que prestar atención a que no ocurra una ampliación desproporcionadamente excesiva del derecho de propiedad[59]. Sin embargo, si está en primer plano la protección de terceros (protección ajena), se plantea especialmente la cuestión de en qué medida el empresario tiene que cargar sobre el trabajador el derecho o la obligación que tiene de garantizar la protección de terceros.

Pero, por principio, dichos sistemas de control, como la videovigilancia, también suministran datos «accesorios», que pueden ser puestos en determinadas circunstancias bajo el control del trabajador[60]. La conducta del trabajador puede ser verdaderamente protocolizada de modo íntegro a través de dicho sistema de control. Según *Grillberger*[61], «la esfera privada de las personas se ahueca cada vez más». Los controles directos en Derecho del Trabajo[62] se caracterizan por una cierta ambivalencia: de un lado, está la relación laboral, caracterizada directamente

[59] Críticamente *Kunnert*, juridicum 2006, 48.

[60] *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsverhältnis, en Resch (Editor), Die Kontrolle des Arbeitnehmers (2005) 13 (15).

[61] *Grillberger*, Rechtliche Grenzen der Ermittlung von Arbeitnehmerdaten im Arbeitsrecht und Datenschutz-gesetz, en Festschrift Floretta (1983) 373.

[62] Sobre los controles en el Derecho del Trabajo véase *Binder*, Detektiveinsatz und Arbeitnehmerkontrolle, en Festschrift Tomandl (1998) 11.

por la dependencia personal[63], que implica control cierto, incluso sometimiento a control de la conducta del trabajador. El empresario, en el marco de su deber de asistencia, tiene el deber de proteger la vida y la salud del trabajador, así como defender los intereses materiales e inmateriales del trabajador. En relación con ello, debe tener a disposición los datos correspondientes sobre el trabajador[64]. De otro lado, el control del empresario, por ejemplo, a través de la vigilancia continua, no debe interferir con fuerza en la esfera privada del trabajador.

3.2. Videovigilancia de trabajadores desde la perspectiva de la DSG 2000

Desde la perspectiva de la protección jurídica de datos, para la aplicación de la videovigilancia en el puesto de trabajo resulta decisivo el parágrafo 50a, apartado 5, de la DSG 2000. En principio, se prohíbe a través de él la videovigilancia con el propósito de control del trabajador «en los lugares de trabajo». Pero de ello se excluyen, por ejemplo, la vigilancia de las cajas, de los almacenes o de rampas de carga, con el objetivo de protección de la propiedad. En los materiales prácticos[65], se pone de relieve que cabe encontrar un medio moderado de control de los trabajadores, en base a una intervención profunda. La DSK ha alertado en su toma de posición sobre el borrador del Ministerio[66], acerca de que en el texto de la Ley debería ponerse en claro, al menos en los comentarios a la misma, que sólo el control de la prestación del trabajador por videovigilancia está prohibido, y, en cambio, que debería excluirse de la prohibición el control del ambiente de trabajo con otros objetivos, como la protección del trabajador ante peligros especiales (por ejemplo, en el ámbito de una máquina peligrosa, unidad de cuidados intensivos de un centro hospitalario).

En este contexto, se plantea primeramente la cuestión de lo que hay que entender bajo el concepto «lugares de trabajo». ¿Se trata aquí de la empresa, de una parte del centro de trabajo o sólo de un concreto puesto de trabajo? ¿Cuenta a esos efectos, como lugar de trabajo, un espacio para fumadores fuera de las instalaciones de la empresa? Además, se plantea la cuestión de si también el aparcamiento para los trabajadores o la entrada para el aparcamiento de trabajadores pertenecen al centro de trabajo. A través de todo ello, el empresario podría vigilar cuándo vienen los trabajadores al trabajo y cuándo estos vuelven a abandonarlo.

[63] En relación con ello véase *Löschnigg* en Löschnigg (Editor), AngG Band I[9] § 1 Rz 8 (2012).

[64] *Oberhofer*, Datenschutz und Arbeitsrecht, en Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht (2009) 457.

[65] 62/ME XXIV. GP. 16.

[66] Toma de posición de la Comisión de Protección de Datos (57/SN-62/ME).

El problema es que hay que ver si se entiende el concepto de lugares de trabajo de modo estricto, dado que si, por ejemplo, sólo se comprenden en él los edificios de la empresa, el trabajador sólo está protegido dentro de las instalaciones. De ahí que pueda el empresario videovigilar al trabajador en el aparcamiento de trabajadores o en el espacio de fumadores que está fuera de los edificios de la empresa, y el trabajador no estaría protegido. También se plantean cuestiones en el ámbito de la «home-office»[67]. Como consecuencia de ello, debe partirse de un concepto amplio de lugares de trabajo, para proteger adecuadamente al trabajador. Sería perfectamente concebible un concepto de centro de trabajo en el sentido de la ArbVG[68] (parágrafo 34 de la ArbVG), o el concepto de lugares de trabajo en el sentido de la Ley de Protección del Trabajador[69] (parágrafo 2, apartado 3, de la ASchG), para orientarse. En virtud del parágrafo 34 de la ArbVG, se considera centro de trabajo todo lugar de trabajo, que constituye una unidad organizativa y donde se desarrolla un objetivo empresarial unitario. De ahí que este concepto amplio de lugares de trabajo también comprenda el recinto de la empresa y se adecuaría, en consecuencia, al objetivo de protección de la Ley, y también debería así ser expuesto. En caso contrario, se burlaría el objetivo de protección, que se persigue por el parágrafo 50a, apartado 5, de la DSG 2000. Precisamente en base a la relevancia práctica del problema, resultará evidente a medio plazo la necesidad de actuación del legislador.

Löschnigg[70] y, siguiéndole, *Hattenberger*[71] ven la problemática de la disposición legal también en relación con el «trabajador»[72]. Es cuestionable si el concepto de trabajador es igual a la definición de empleado. Mi opinión es que debió el legislador aclarar el concepto de trabajador. Naturalmente, debería producirse como ulterior consecuencia un ajuste legislativo.

3.3 Videovigilancia de trabajadores desde la perspectiva de la ArbVG en relación con la AVRAG

[67] Véase también con carácter general sobre esta temática *Melzer-Azodanloo*, Telearbeitsrecht (2001).

[68] Ley Federal de 14 diciembre 1973 relativa a la organiación del trabajo (Ley de Organización del Trabajo – ArbVG) BGBl 22/1974 en la redacción de BGBl I 111/2010.

[69] Ley Federal sobre Seguridad y Protección de la Salud en el Trabajo (Ley de Protección de Trabajadoras y Trabajadores – AschG), BGBl 450/1994 en la redacción de BGBl I 118/2012.

[70] *Löschnigg* en Bergauer/Staudegger, Recht und IT, 57 (63).

[71] *Hattenberger* en Jahnel, Datenschutzrecht Jahrbuch 2010, 29 (33).

[7272] Para consideraciones detalladas sobre el concepto de trabajador véase *Löschnigg* en Bergauer/Staudegger, Recht und IT, 57 (63 ss.); es cuestionable si "trabajador" es comparable al concepto de "empleado" o si, en su caso, persona asimilada a trabajador, prestador libre de servicios o trabajador cedido pueden subsumirse en la noción de trabajador.

Junto a las disposiciones de la DSG 2000, que en lo esencial están más bien concebidas desde la perspectiva jurídica individual, tienen también importancia especial para la videovigilancia de los puestos de trabajo las normas jurídicas sobre organización de la empresa de la ArbVG[73].

3.3.1. Videovigilancia al amparo del parágrafo 96a, apartado 1, número 1, de la ArbVG

La videovigilancia en el centro de trabajo, en virtud del parágrafo 96a de la ArbVG, puede representar la introducción de sistemas de tratamiento de protección automatizada y transmisión de datos de carácter personal del trabajador, que sólo resulta posible con el consentimiento del comité de empresa. La «introducción» no comprenderá sólo la instalación estricta, sino también la aplicación, modificación y el cambio de lugar[74]. Además, debe existir un «sistema», que represente por lo general una unidad de instalaciones de maquinaria (hardware) con programas determinados (software). Con respecto al concepto «protección automatizada», hay que tener en cuenta la norma del parágrafo 4, número 7, de la DSG 2000. En ella, hay que comprender la aplicación mecánica y controlada por ordenador de los datos[75]. Por último, también deben estar comprendidos los «datos del trabajador de carácter personal», que exceden de la transmisión de datos generales sobre la persona y condiciones especiales[76]. El concepto de datos de carácter personal hay que interpretarlo de modo amplio, de modo que todas las informaciones que estén en conexión con el trabajador o que podrían ser utilizadas en conexión con él, como, por ejemplo, el nombre, la fecha de nacimiento, grado académico, sexo, nivel de inteligencia, patrimonio, creencias religiosas, etc., están comprendidas en ello[77]. Se opina que también los log-files, supuesto que al ordenador del trabajador en su puesto de trabajo se le pidan el nombre de usuario y la contraseña, si están asignados al trabajador[78]. *Löschnigg*[79] habla incluso de datos de carácter personal, supuesto que la asignación no pueda efectuarse con seguridad, sino con alta probabilidad.

[73] *Hattenberger* en Jahnel, Datenschutzrecht Jahrbuch 2010, 29 (30).

[74] *Preiss* en Cerny/Gahleitner/Preiss/Schneller (Hrsg), Arbeitsverfassungsrecht Volumen 3[4] § 96a Erl 5 (2009).

[75] *Preiss* en Cerny/Gahleitner/Preiss/Schneller, ArbVG 3[4] § 96a Erl 5.

[76] *Reissner* en Neumayr/Reissner (Editores), Zeller Kommentar zum Arbeitsrecht[2] § 96a ArbVG Rz 16 (2011).

[77] *Oberhofer* en Bauer/Reimer, Handbuch Datenschutzrecht, 457 (460).

[78] *Sacherer*, Datenschutzrechtliche Aspekte der Internetnutzung von Arbeitnehmern, RdW 2005/221, 173 (174).

[79] *Löschnigg*, Datenschutz und Kontrolle im Arbeitsverhältnis, DRdA 2006, 459 (461).

En virtud del parágrafo 96a, apartado 2, de la ArbVG, el consentimiento del comité de empresa también puede reemplazarse por decisión del órgano de conciliación. En el parágrafo 50c, apartado 1, inciso último, de la DSG 2000, se contiene una referencia explícita a la norma del parágrafo 96a de la ArbVG.

3.3.2. Videovigilancia al amparo del parágrafo 96, apartado 1, número 3, de la ArbVG

Pero a través de ello también es posible que la videovigilancia en el centro de trabajo deba introducirse por medio del acuerdo de empresa a que se refiere el parágrafo 96, apartado 1, número 3, de la ArbVG, dado que frecuentemente hay que calificarla como introducción de medidas de control y de sistemas técnicos para el control de los trabajadores, que afectan a la dignidad humana[80]. Naturalmente, es cuestionable en este contexto cuándo existe «afectación de la dignidad humana» y cómo hay que interpretarla, a efectos de comentar la ArbVG[81], para esclarecer el «espacio de límites angostos» entre perjudicar la dignidad humana y las medidas que no tocan la dignidad humana. En relación con esto, el legislador parte de un concepto triple o dual[82]:

— Medidas de control que no afectan en absoluto a la dignidad humana: la mayoría de las veces se trata en ese caso de preceptos de ordenación (por ejemplo, preceptos generales sobre vestimenta, reglas relacionadas con fumar), que hay que calificar en el sentido del parágrafo 97, apartado 1, número 1, de la ArbVG[83].

— Medidas de control que dañan la dignidad humana: en ellas, se comprenden, por ejemplo, escuchar conversaciones telefónicas, sin informar al trabajador; cámaras de vigilancia en los cuartos de baño.

— Medidas de control que afectan a la dignidad humana.

De ahí la importancia de la intensidad del control, dependiente de la forma del control (control por medio de personas o de técnica), de la duración temporal (duradero o sólo puntual), del alcance del control (ligado a datos

[80] *Risak,* Betriebliche Mitbestimmung bei der Mitarbeiterkontrolle en Brodil (Editor), Datenschutz im Arbeitsrecht. Mitarbeiterüberwachung vs Qualitätskontrolle (2010) 35; detalladamente sobre el tema de la afectación de la dignidad humana, véase *S. Mayer,* Videoüberwachung ¿también sin consentimiento del comité de empresa? Überlegungen zum „Berühren der Menschenwürde“ im Sinne des § 96 Absatz 1 Ziffer 3 ArbVG, wbl 2009, 217.

[81] ErlRV 840 BlgNR XIII. GP. 22.

[82] *Binder* en Tomandl (Editor), Arbeitsverfassungsgesetz § 96 Rz 62 (2010).

[83] Véase también *Löschnigg,* Arbeitsrecht[11] (2011) 806.

diferentes) y, en ese caso, los datos comprendidos (sensibilidad)[84]. En las medidas de control, hay que comprender la vigilancia sistemática de cualidades, acciones o la conducta general de los trabajadores por el dueño de la empresa[85]. De ahí que pueda afectarse la dignidad humana, en el sentido del parágrafo 96, apartado 1, número 3, de la ArbVG, a través de la gran densidad del control, que sobrepase la dimensión necesaria para alcanzar el objetivo del control[86]. Según el punto de vista del OGH[87], no existe control que afecte a la dignidad humana en el sentido del parágrafo 96, apartado 1, número 3, de la ArbVG, en el caso del trabajador que en el marco de todo un día de trabajo es observado por poco tiempo y de manera no continuada en una pantalla, sólo durante una parte de la ejecución de su trabajo (cargar un camión).

El OGH[88] llega a la conclusión de que el legislador quiere conseguir con la conexión a la dignidad humana del parágrafo 96, apartado 1, número 3, de la ArbVG, que el libre desarrollo de la personalidad del trabajador no padezca ninguna intervención excesiva.

En los centros de trabajo en los que no existe comité de empresa, se requiere el consentimiento de cada concreto trabajador para introducir la videovigilancia, en virtud del parágrafo 10 de la AVRAG[89]. A través de él, debe asegurarse que en los centros de trabajo sin comité de empresa la introducción de medidas de control, que afecten a la dignidad humana, resulte inadmisible sin el consentimiento del trabajador[90].

3.4. Relación entre la DSG 2000 y la ArbVG

[84] Véase *Löschnigg*, Biometrische Daten und Arbeitsverhältnis. Zur Zulässigkeit betrieblicher Zutrittskontroll-systeme mittels biometrischer Daten, ASoK 2005, 37 (42); *Preiss* en Cerny/Gahleitner/Preiss/Schneller, ArbVG 3[4] § 96a Erl 7.

[85] OGH 20. 12. 2006, 9 ObA 109/06d = ARD 5754/1/2007 = ASoK 2007, 139 = DRdA 2008/26, 326 (*Mosler*) = infas 2009, 139 (*Heilegger*).

[86] *Rauch*, Zur privaten Nutzung des PC und Telefons im Arbeitsverhältnis. Der Arbeitgeber kann Einschränkungen vereinbaren und in bestimmten Grenzen Kontrollen durchführen, ASoK 2007, 169 (171).

[87] Departamento de Conciliación de Viena 24. 4. 1986, II Re 61/86, Arb 10.518.

[88] OGH 20. 12. 2006, 9 ObA 109/06d = ARD 5754/1/2007 = ASoK 2007, 139 = DRdA 2008/26, 326 (*Mosler*) = infas 2009, 139 (*Heilegger*).

[89] Ley de Adaptación del Derecho del Contrato de Trabajo – (AVRAG), BGBl 459/1993 en la redacción de BGBl I 152/2011.

[90] *Reissner* en Neumayr/Reissner, Zeller Kommentar[2] § 10 AVRAG Rz 2.

Según *Löschnigg*[91], se cumplirán ordinariamente de modo estricto, en el ámbito de la videovigilancia en el centro de trabajo, las circunstancias del parágrafo 96, apartado 1, número 3, de la ArbVG, al igual que las del parágrafo 96a, apartado 1, número 1, de la ArbVG. Esto permite motivar que la videovigilancia en el centro de trabajo haya que calificarla la mayoría de las veces como una vigilancia duradera. La videovigilancia es un control de la esfera privada del trabajador, que expresa el sentido de una vigilancia (potencial) duradera[92]. El consentimiento del comité de empresa no es necesario, supuesto que no sobrepase el cumplimiento de los deberes para un uso previsto u objetivo de los datos, que se deprendan de la Ley, de las normas de regulación jurídica colectiva y del contrato de trabajo[93].

De ahí que no resulte comprensible por qué la disposición del parágrafo 50c, apartado 1, inciso último, de la DSG 2000 sólo menciona el parágrafo 96a, apartado 1, número 1, de la ArbVG, y que tampoco se remita al parágrafo 96, apartado 1, número 3, de la ArbVG.

En relación con esto, hay que anotar que la disposición del parágrafo 79e de la BDG[94], en relación con el parágrafo 29n de la VBG[95], representa la limitación más poderosa, dado que la introducción y uso de medidas de control y sistemas técnicos resulta, con carácter general, inadmisible[96].

También según *Hattenberger*[97], es distinto el ámbito de protección a que se refiere la ArbVG, en comparación con la DSG 2000. La DSG 2000 persigue el objetivo de que debe introducirse siempre el medio moderado, y la medida ya no resulta proporcionada cuando excede el objetivo. Entre tanto, la ArbVG puede introducir perfectamente dicha medida por medio del consentimiento del comité de empresa.

[91] *Löschnigg* en Bergauer/Staudegger, Recht und IT, 57 (66).

[92] También así básicamente *Burgstaller/Neußl*, Videoüberwachung und Zutrittskontrolle am Arbeitsplatz, ecolex 2011, 82.

[93] Cfr. *Preiss*, en Arbeitsverfassungsrecht Volumen 3[4] § 96a Erl 6, 7; *Löschnigg*, Datenermittlung, 202.

[94] Ley Federal de 27 Junio 1979 sobre el Derecho de Servicios de los Funcionarios (Ley del Derecho de Servicios de los Funcionarios 1979 – BDG), BGBl 333/1979 en la redacción de BGBl I 77/2009.

[95] Ley Federal de 17 Marzo 1948 sobre el Derecho de Servicios y Retributivo de los Servidores Contractuales de la Federación (Ley de los Servidores Contractuales 1948 – VBG), BGBl 86/1948 en la redacción de BGBl 35/2012.

[96] *Löschnigg*, Arbeitnehmerdatenschutz, en Jahnel/Mader/Staudegger (Editores), IT-Recht[3] (2012) 497 (512 ss.).

[97] *Hattenberger* en Jahnel, Datenschutzrecht Jahrbuch 2010, 29 (37).

4. Conclusión

Con carácter general, cabe decir compendiadamente que el control por el empresario se incrementa enormemente si ocurre igualmente por medio de videovigilancia, del registro de datos telefónicos o por el uso de GPS. Esto permite afirmar que el trabajador puede escaparse cada vez más del control por el empresario, con base en la gran movilidad y flexibilidad que son inmanentes a las nuevas exigencias del mundo laboral. El cambio (futuro) hacia modelos de trabajo móviles[98], pondrá muchos más desafíos al Derecho del Trabajo, pero también a la DSG 2000.

El legislador se ocupa crecientemente de la problemática de la videovigilancia. En mi opinión, el legislador observa, sin embargo, el problema de la videovigilancia —como muestra el parágrafo 50a de la DSG 2000— aisladamente. Establece ciertamente la disposición normativa de que está prohibida la videovigilancia con el objetivo del control del trabajador en los lugares de trabajo, aunque en ese caso se prescindirá de las normas jurídico-laborales. Los conceptos que el legislador utiliza en el parágrafo 50a, apartado 5, de laDSG 2000 se trasladan dificultosamente con armonía a los conceptos del contexto jurídico-laboral. Como arriba ya se explicó, debe partirse de un concepto amplio de lugares de trabajo, que se oriente hacia el parágrafo 34 de la ArbVG o al parágrafo 2, apartado 3, de la ASchG. Sólo a través de ello puede establecerse con seguridad una protección adecuada del trabajador ante la videovigilancia en el puesto de trabajo.

También hay que indagar críticamente la remisión del parágrafo 50c, apartado 1, de la DSG 2000 «sólo» al parágrafo 96a de la ArbVG. En mi opinión, también deben comunicarse a la DSK, para su control previo, los acuerdos de empresa que se concluyan al amparo del parágrafo 96, apartado 1, número 3, de la ArbVG, por analogía con el parágrafo 50c, apartado 1, de la DSG 2000. A pesar de los objetivos de protección diferenciados de la ArbVG y de la DSG 2000, no se excluyen los ámbitos jurídicos[99]. La observación aislada de los dos ámbitos jurídicos conduce a que las disposiciones de la ArbVG infiltren los objetivos de protección de la DSG 2000. De lege ferenda sería deseable, entre otras cosas,

[98] *J. Müller*, Der Arbeitsplatz der Zukunft: Ein Mitarbeiter, sechs Endgeräte, zwei Drittel Schreibtisch <http://www.citrix.com/news/announcements/sep-2012/der-arbeitsplatz-der-zukunft--ein-mitarbeiter--sechs-endgeraete-.html> (27. 2 2013).

[99] Con otra perspectiva *Burgstaller/Neußl*, ecolex 2011, 82 (85); llegan a la conclusión de que la videovigilancia y las medidas de control pueden armonizarse los trabajadores, por lo que hay que valorarlas en consecuencia, por un lado, según las normas del Derecho del Trabajo, y por otro lado, según las disposiciones del Derecho de protección de datos.

regular expresamente la exclusión de controles de la prestación a través de la videovigilancia.