PRINCIPALES OPINIONES CONSULTIVAS EMITIDAS EN 2021

I. EN MATERIA LABORAL.

A. VIDEOVIGILANCIA Y COWORKING.

Opinión Consultiva No. 02-2021-JUS/DGTAIPD.

1. "La captación y grabación de datos personales a través de sistemas de videovigilancia constituye un tratamiento de datos personales".

2. El contrato de *coworking* incluye el arrendamiento del local y un contrato de prestación de servicios por el uso y disfrute de servicios como: internet, impresora, salas de reuniones, servicios de recepción, atención de llamadas, recepción de llamadas.

3. En algunos casos el contrato de *coworking* puede incluir el servicio de seguridad del local y control laboral por sistemas de videovigilancia. En estos casos, la empresa arrendataria del espacio de *coworking* actúa como **responsable del tratamiento** y está obligada a informar a sus trabajadores sobre la existencia del control por videovigilancia, conforme al artículo 18 de la Ley 29733; y la empresa arrendadora (espacio de *coworking)* actúa como **encargada de tratamiento**, y debe cumplir con las obligaciones establecidas en la Ley 29733. Ambas entidades deben cumplir con la Directiva 01-2020-JUS/DGTAIPD sobre tratamiento de datos personales sobre sistemas de videovigilancia.

4. El encargo debe estar expresamente contenido en el contrato, el cual debe determinar:

   - "Objeto, duración, naturaleza y finalidad del tratamiento de los datos personales.
   - El tipo de datos personales sujetos a tratamiento.
   - Categoría de los titulares de datos personales: trabajadores, proveedores, clientes.
   - Obligaciones y derechos del responsable del tratamiento (arrendatario).
   - Obligaciones del encargado de tratamiento (arrendador): confidencialidad, realizar el tratamiento conforme a las instrucciones del responsable del tratamiento, subcontratar únicamente conforme a lo establecido en la Ley 29733, suprimir o devolver los datos de carácter personal al responsable una vez finalizado el servicio, demostrar frente al responsable del tratamiento que cumple con la normativa sobre protección de datos personales".

B. SEGURIDAD Y SALUD EN EL TRABAJO.

Opinión Consultiva No. 013-2021-JUS/DGTAIPD

1. La calidad del trabajador como afiliado en el SCTR deviene de la relación laboral.
2. Los resultados de los exámenes médicos realizados en cumplimiento del SCTR son **datos personales sensibles**.

3. En los casos de salud ocupacional aplican las excepciones al consentimiento contenidas en los incisos 5, 6, 9 y 13 del artículo 14 de la Ley 29733, por lo que el empleador podrá realizar el tratamiento sin necesidad de solicitar el consentimiento del titular de los datos personales, siempre que se recopilen los datos necesarios y conforme a las normas autoritativas en materia de salud ocupacional. **La aplicación de las excepciones no libera al empleador de cumplir con el deber de informar en las políticas de privacidad correspondientes.**
4. En materia de salud ocupacional, aplican los principios de proporcionalidad y confidencialidad, por lo que la información médica o clínica de los trabajadores sólo debe ser conocida por el médico ocupacional.
5. El médico ocupacional debe respetar el deber de confidencialidad, por lo que sólo podrá informar al empleador sobre las condiciones generales del estado de salud colectiva de los trabajadores.
6. Las entidades aseguradoras contratadas por el empleador sólo podrán entregar información al médico ocupacional pero no a otros funcionarios del centro laboral.
7. "La información contenida en las historias clínicas de los trabajadores sólo podrá ser conocida por el personal médico y las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse esa información al empleador o a otras personas sin consentimiento expreso y por escrito del trabajador".

C. VIDEOVIGILANCIA CON FINES DE CONTROL LABORAL

Opinión Consultiva No. 045-2021-JUS/DGTAIPD

1. Es válido el uso de los sistemas de videovigilancia si se aplican los criterios de **razonabilidad y proporcionalidad en el tratamiento.**
2. El responsable del tratamiento (empleador) debe cumplir con el deber de informar contenido en el artículo 18 de la Ley 29733. **La existencia de una excepción al consentimiento no exonera al responsable del tratamiento a cumplir con el deber de informar.**
3. La Directiva No. 01-2020-JUS/DGTAIPD, establece que el deber de informar se cumple a través de la colocación de carteles informativos en los espacios videovigilados; si no es posible colocar toda la información contenida en el artículo 18, se debe informar al titular dónde encontrar dicha información.
4. **En el caso de vehículos corporativos se debe colocar el cartel informativo adecuándolo a los espacios disponibles. "Si no existe espacio suficiente, se deberá cumplir con el deber de informar en un documento informativo, el cual puede ser enviado por medios informáticos, digitalizados o impresos".**

II. TELECOMUINCACIONES.

A. ACCIONES DE MONITOREO DE OSIPTEL.

Opinión Consultiva No. 015-2021-JUS/DGTAIPD

1. El artículo 6 del Reglamento General de Supervisión, aprobado por Resolución de Consejo Directivo No. 090-2015-CD/OSIPTEL contempla el monitoreo, "definido como aquellas actividades que realiza el OSIPTEL de manera facultativa, con la finalidad de tomar conocimiento del desempeño de las entidades supervisadas en el mercado de servicios públicos de telecomunicaciones".
2. El proceso de medición efectuado por el OSIPTEL es coordinado de manera previa con el abonado para definir el horario en el cual se llevará a cabo. Para efectuar la medición se utiliza el usuario y contraseña del modem / router brindado por la

empresa operadora, o por el cliente, para poder desactivar momentáneamente la señal Wifi.

3. La ANPDP concluye que es desproporcional que "el OSIPTEL obtenga de forma previa a la coordinación con el abonado, el usuario (código asignado al dispositivo) y la contraseña del modem/router, puesto que es evidente que podrá solicitarlos directamente al abonado al momento de coordinar lo que requiera para llevar a cabo la supervisión del servicio"; siendo que también representa un riesgo para la "confianza digital", la cual tiene como componente a la protección de datos, transparencia, seguridad digital y protección del consumidor en el entorno digital, conforme a lo establecido en el Decreto de Urgencia 007-2020.
4. La ANPDP dejó constancia que su postura no "constituye un impedimento para el ejercicio de la función supervisora del OSIPTEL, toda vez que el organismo supervisor cuenta con opciones para realizar la desactivación de la señal Wifi sin vulnerar el principio de proporcionalidad".

B. ENTREGA DE DATOS Y CONVENIO DE BUDAPEST

Opinión Consultiva No. 040-2021-JUS/DGTAIPD

1. La consulta estuvo orientada a solicitar opinión de la ANPDP respecto a si en virtud del Convenio de Budapest, que entró en vigencia en nuestro país el 01 de diciembre de 2019, los representantes del Ministerio Público se encuentran facultados para requerir la información de abonados (identidad de titulares de números telefónicos y titulares de IP) a las empresas concesionarias de servicios de telefonía, sin necesidad de contar con autorización judicial, en el marco de investigaciones penales.
2. La ANPDP determinó lo siguiente:
   - Para realizar transferencia de datos personales, se debe verificar si dicho tratamiento se encuentra dentro de las excepciones establecidas en la Ley 29733 en cuyo caso aplican los principios de proporcionalidad y finalidad; de lo contrario, corresponde solicitar dicho consentimiento, de forma previa, expresa, informada y libre.
   - "El Convenio de Budapest no habilita legalmente al Ministerio Público a obtener, de manera inmediata y sin autorización judicial, la información de abonados (identidad de titulares de números telefónicos y titulares de IP) por parte de las empresas concesionarias de servicios públicos de telecomunicaciones.
   - No puede tomarse la normativa de protección de datos personales como un obstáculo para obtener la información de abonados, siendo necesario realizar una adecuación de la legislación penal, en el marco de la cooperación internacional regulada en el Convenio de Budapest y a efectos del cabal cumplimiento de las funciones de los representantes del Ministerio Público para combatir la ciberdelincuencia"
   - El Ministerio Público debe evaluar la necesidad de la adecuación legislativa y ejercer iniciativa legislativa, conforme a lo establecido en la Constitución Política del Perú, para dar cuenta de los vacíos o defectos de la legislación actual.

C. METADATOS.

Opinión Consultiva No. 041-2021-JUS/DGTAIPD

1. Los metadatos son "datos que describen otros datos", o "conjunto de datos estructurados que describen otros datos, que proporcionan a semántica para entender al dato al definirlo entender sus relaciones, referencias de uso, e incluso sus valores permitidos, con la finalidad de garantizar su disponibilidad,

accesibilidad, conservación e interoperabilidad con otros sistemas". **Por ejemplo: datos de tráfico (números de origen y destino de una llamada, nombre y dirección de los abonados, fecha de inicio y fin de la llamada, servicio telefónico utilizado, IMSI e IMEI), y localización.**

2. La Ley 29733 define al dato personal como "aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados."
3. Los metadatos que revelen información sobre una persona identificada o identificable están protegidos por la Ley 29733.
4. Las empresas de telecomunicaciones con las titulares de los bancos de datos personales de sus clientes, incluyendo los metadatos, por lo tanto, se sujetan a lo establecido en la Ley y a las normas sectoriales.

III. FLUJO TRANSFRONTERIZO DE DATOS.

Opinión Consultiva No. 043-2021-JUS/DGTAIPD

Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales o, por lo menos, un nivel equiparable a lo previsto por la LPDP o por los estándares internacionales en la materia.

Esa Opinión Consultiva establece criterios relacionados con las transferencias internacionales de datos y del principio de nivel adecuado de tratamiento. Así, la ANPDP considera que un país cuenta con un nivel adecuado de tratamiento si cuenta con:

1. Regulación en materia de protección de datos personales.
2. Procedimientos y medios mediante los cuales el titular de datos pueda ejercer sus derechos de acceso, rectificación, cancelación u oposición al tratamiento de los datos personales.
3. Régimen de responsabilidades, obligaciones y deberes para los responsables y encargados de tratamiento.
4. Régimen sancionador en caso de incumplimiento.
5. Una agencia de protección de datos personales con independencia técnica y que cuente con potestad sancionadora y de tutela de derechos.

Para cualquier consulta en materia de protección de datos personales, comuníquese con martinserkovic@esola.com.pe, carolquiroz@esola.com.pe o andreazanusso@esola.com.pe.

MARTIN SERKOVIC
Socio

CAROL QUIROZ
Asociada Senior

ANDREA ZANUSSO
Asociada