



# **Alcances y límites** de la **facultad de fiscalización:** la protección de datos personales

*Jorge Toyama Miyagusuku*

*Abril, 2021*



# AGENDA

- 1. Datos personales**
- 2. La protección de datos personales en el ámbito de la fiscalización laboral**
- 3. Recomendaciones finales**

# Datos personales



# Datos personales

Domicilio

Teléfono

E-mail

Nombres y apellidos

Fecha de nacimiento

RUC

Huella digital

Imagen

Voz



**Cualquier información que permite identificar a una persona.**

# Datos sensibles

Datos personales que requieren especial protección.



Salarios e ingresos económicos



Religión



Origen racial o étnico



Salud



Afiliación política



Sindicalización



Orientación sexual

Los antecedentes policiales, penales o judiciales no son calificados como datos sensibles de manera expresa, pero reciben el mismo tratamiento. Se requiere consentimiento, salvo excepción o sea necesario.

# Tratamiento de datos personales: ¿qué está permitido?

- Recopilar
- Clasificar
- Ordenar
- Almacenar
- Procesar
- Comparar

- Usar
- Transferir
- Analizar
- Actualizar
- Intercambiar
- Otros

# La protección de datos personales en el ámbito de la **fiscalización** **laboral**





# Límites a la facultad de fiscalización en materia de datos personales

## Datos personales

toda información recopilada por cualquier medio que permite identificar a una persona natural.

## Límites de fiscalización



### Principios de proporcionalidad y finalidad:



Debe existir proporcionalidad entre el fin que se persigue lograr y la intensidad de la intervención de la medida. La finalidad debe ser determinada, explícita y lícita

### Principio de legalidad:



Todo tratamiento de los datos personales debe efectuarse en respeto de las normas vigentes y demás principios previstos en ley.

### Deber de informar:



El empleador debe informar al trabajador en forma detallada, sencilla, expresa, inequívoca y de manera previa a la recopilación de datos personales sobre el tratamiento de estos (art. 18 LPDP).

### Principio de consentimiento:



El tratamiento de datos personales del trabajador requiere de consentimiento informado y previo, salvo que sea necesario para la ejecución del servicio o se encuentre en otra excepción legal.

# Principios adicionales para el tratamiento de datos personales

## Principio de calidad



Los datos deben ser veraces, exactos, adecuados y conservados por el tiempo necesario.

## Principio de seguridad



Se deben adoptar medidas necesarias y apropiadas para garantizar seguridad y confidencialidad.

**Toda fiscalización debe garantizar la seguridad, confidencialidad y calidad de los datos personales.**

# Clasificación de los Datos Personales - Consentimiento

Tipo de información	Para el cumplimiento de obligaciones laborales (necesidad y proporcionalidad)	Encargatura de obligaciones a terceros	Transferencia de información para otros fines
Datos personales	No	No	Sí
Datos sensibles	No	Sí	Sí

# Formas de fiscalización y datos personales:



## Medios informáticos proporcionados por el empleador:

- Computadoras, tablets, celulares y similares (incluyendo archivos que contienen)
- Correo institucional
- Otras plataformas institucionales proporcionadas por el empleador (teams, zoom, etc.)
- Plataformas de trabajo colaborativo proporcionadas por la empresa (Miró, OneDrive, Asana, etc.)

**Criterio vigente del TC:** Previa **autorización judicial**.

**Práctica vigente:** **expectativa de privacidad + razonabilidad y proporcionalidad**



Consentimiento o información de fiscalización y revisión de contenidos del medio informático del trabajador:

- Al inicio de la relación laboral
- Al momento de entrega del medio

Se precisan los medios de control de manera **clara y previa**.



Proporcionalidad y razonabilidad en la forma de fiscalización (no poder irrestricto): se aplica la medida **menos intrusiva y se justifica su uso**.

# Formas de fiscalización y datos personales:



## Medios informáticos proporcionados por el empleador:

### ¿Qué no se puede hacer?



Revisión de chats o comunicaciones del trabajador desde sus redes personales (no institucionales), a pesar de que haya usado el medio proporcionado por el empleador.



Control sin restricciones de los medios proporcionados, si es que no es necesario para la prestación del servicio.



### ¿Qué se puede hacer?

- Instalación de software de bloqueo de acceso a redes sociales o páginas no permitidas por la empresa.
- Controlar uso de medios en la medida que es necesario para la prestación del servicio. P. ej.: trabajadores sujetos a fiscalización durante jornada laboral.

### ¿Qué se debe hacer?

- Garantizar que los medios de control sean razonables, adecuados y legales.

# Formas de fiscalización y datos personales:



## Cámaras y videovigilancia:

- Únicamente para fiscalizar **actividades laborales en el centro de trabajo**, salvo que medie consentimiento o sea necesario para la prestación del servicio.
- **Principio de proporcionalidad.**
- **Respeto a la intimidad:** prohibido grabar espacios privados y personales.
- **Deber de información y confidencialidad.**



## GPS:

- **Principio de proporcionalidad.**
- **Deber de información y confidencialidad.**

# Formas de fiscalización y datos personales:



## Polígrafo:

**Exp. 273-  
2010-PA/TC**

1. Es voluntaria del trabajador.
2. Debe informarse de manera expresa y clara al trabajador del propósito de la prueba;
3. El trabajador debe tener conocimiento de la naturaleza y el procedimiento de la prueba;
4. El trabajador debe ser informado de que puede contar con la presencia de un abogado o una persona de su confianza durante la prueba y tener la libertad de elegirlo; y,
5. El trabajador debe obtener un ejemplar de los resultados del examen.

**No se permite su uso para:** (i) determinar acceso al empleo; (ii) determinar una falta laboral; o; (iii) sancionar al trabajador por no someterse a la prueba.



**TC reconoce su uso para casos de:** (i) sospecha razonable de la intervención del trabajador en un incidente que ha ocasionado un grave perjuicio financiero y económico a la empresa; o, (ii) se haya puesto en grave peligro la existencia misma de la organización del empleador.



## Derecho comparado.

- ▶ Solo podrán utilizarse cámaras para supervisar el home office de manera extraordinaria o cuando las funciones lo requieran. (México). Para capturar imagen del trabajador, es **NECESARIO** su consentimiento expreso e informado. (Costa Rica). Si no existe fin necesario, puede configurar acoso laboral. (Colombia)
- ▶ La huella dactilar **DEBE** procesarse utilizando sistema de cifrado. (España)
- ▶ Si un empleador monitorea llamadas telefónicas y mensajes de correo de voz del celular del empleado, ya sea propio o de la compañía, **PUEDE** ser demandado. (Estados Unidos)
- ▶ El control de los movimientos del trabajador **REQUIERE** acuerdo entre empleador y trabajador, de lo contrario, el trabajador puede desactivar la geolocalización. (España)
- ▶ No puede obligarse a un trabajador que use dispositivos propios a instalar software de control de su actividad; pero si pertenecen a la empresa, solo se le deberá informar; **SIN NECESIDAD** de obtener consentimiento. (España y Costa Rica). También se le puede obligar si en la etapa de reclutamiento se le informó que constituía un requisito de contratación. Una negativa podría ser causal de sanción despido. (Costa Rica)



# Recomendaciones finales



# Recomendaciones finales

Elaborar formatos de **consentimiento e información sobre el tratamiento de datos personales**.

**Adecuación de los contratos** del personal y con terceros proveedores relacionado con el tratamiento.

**Adecuación de los sistemas de gestión o aplicaciones**, de los procesos del negocio.

Elaborar **políticas y normativas** del tratamiento de datos personales.

Revisar con **periodicidad** la efectividad de las medidas de seguridad adoptadas.

Llevar un **control y registro** de personas con acceso a los BDP.

**Validar legalmente los mecanismos y sistemas** de fiscalización de datos personales.

Establecer un **sistema de control sobre encargados de Compliance**.

**RESPETAR EN TODO MOMENTO LOS PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES**

# Planeamiento estratégico: compliance laboral





Vinatea  
& Toyama

Tel . (511) 706 4200  
[www.vinateatoyama.com](http://www.vinateatoyama.com)

Para cualquier consulta  
relativa a esta presentación,  
por favor contactar a:



**Jorge Toyama**  
[jtoyama@vinateatoyama.com](mailto:jtoyama@vinateatoyama.com)