



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

OPINIÓN CONSULTIVA N° 035-2022-DGTAIPD

ASUNTO : Consulta sobre instalación de software con finalidad de prevención de comisión del delito de pornografía infantil

REFERENCIA : a) Hoja de Trámite N° 154639-2022MSC
b) Hoja de Trámite N° 277239-2022MSC

FECHA : 13 de octubre de 2022

I. ANTECEDENTES

1. Mediante el documento a) de la referencia, se remitió a esta Dirección General la consulta respecto a si la instalación de un software que tiene como finalidad prevenir la comisión de delitos de pornografía infantil (en adelante, el "Software") en las computadoras de una empresa, contraviene alguna disposición de la normativa de protección de datos personales.
2. Particularmente, el administrado consulta lo siguiente:

"(...) En caso existan indicios de la comisión de un delito de pornografía infantil, el empleador pueda intervenir dichas computadoras y verificar la existencia de estas conductas a través del Software y, de ser el caso, abrir un procedimiento disciplinario al trabajador responsable.

Bajo este escenario, les traslado las siguientes consultas:

- *¿La instalación y uso del Software en la computadora del trabajador podría contravenir alguna disposición de la Ley? Lo anterior en el entendido que: (i) el Software será instalado en la computadora (de propiedad del empleador) asignada al trabajador en el marco de su relación laboral; y, (ii) el empleador le informará al trabajador, de manera previa, que la compañía cuenta con mecanismos para prevenir y detectar el uso indebido de sus computadores.*
- *¿El empleador deberá obtener el consentimiento específico del trabajador para el uso del Software que sería instalado en la computadora que ha sido asignada a cada trabajador en el marco de su relación laboral? O, al ser el Software una medida para el control laboral y prevención del delito, podría encausarse en la excepción establecida en el artículo 14 de la Ley, siendo únicamente suficiente que el empleador cumpla con informar al trabajador conforme lo establece el artículo 18 de la Ley.*
- *¿La instalación y uso del Software podría requerir alguna medida de seguridad específica?"*

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

 **Siempre
con el pueblo**



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

II. MARCO NORMATIVO DE ACTUACIÓN

3. El artículo 32 de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, la "LPDP"), crea la Autoridad Nacional de Protección de Datos Personales (en adelante, "ANPD"), que se rige por dicha ley, su reglamento y las normas pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado mediante Decreto Supremo N° 013-2017-JUS (en adelante, ROF del Minjusdh).
4. Entre las funciones de la ANPD, previstas en el artículo 33 de la LPDP, se encuentra la de absolver consultas sobre protección de datos personales y emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la cual es vinculante¹.
5. Por su parte, el ROF del Minjusdh, establece en su artículo 70 que la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la "DGTAIPD") es el órgano de línea encargado de ejercer la ANPD, por lo que tiene entre sus funciones absolver consultas sobre protección de datos personales y emitir opinión técnica respecto de proyectos normativos que se refieran a los ámbitos de su competencia.²
6. Por ende, esta Dirección General, en su calidad de órgano de línea del Ministerio de Justicia y Derechos Humanos sobre el que recae la ANPD, emite la presente Opinión Consultiva en el ámbito de la interpretación abstracta de las normas y no como mandato específico de conducta para un caso en concreto.

¹ Ley N° 29733, Ley de Protección de Datos Personales

"Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales"

La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

(...)

10. Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.

11. Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante.

(...)"

² Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos

"Artículo 71.- Funciones de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales"

Son funciones de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales las siguientes:

(...)

d) Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los ámbitos de su competencia. En materia de protección de datos personales la opinión técnica es vinculante.

e) Absolver las consultas que las entidades o las personas jurídicas o naturales le formulen respecto de la aplicación de normas de transparencia y acceso a información pública; así como sobre protección de datos personales.

(...)"

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

III. ANÁLISIS

Sobre la facultad de fiscalización y control laboral de los empleadores

7. El poder de dirección empresarial se encuentra regulado en el artículo 9 del Texto Único Ordenado del Decreto Legislativo N°728, Ley de Productividad y Competitividad Laboral, aprobado mediante Decreto Supremo N°003-97-TR (en adelante, la "Ley de Productividad y Competitividad Laboral"):

"Artículo 9.- Por la subordinación, el trabajador presta sus servicios bajo dirección de su empleador, el cual tiene facultades para normar reglamentariamente las labores, dictar las órdenes necesarias para la ejecución de las mismas, y sancionar disciplinariamente, dentro de los límites de la razonabilidad, cualquier infracción o incumplimiento de las obligaciones a cargo del trabajador.

El empleador está facultado para introducir cambios o modificar turnos, días u horas de trabajo, así como la forma y modalidad de la prestación de las labores, dentro de criterios de razonabilidad y teniendo en cuenta las necesidades del centro de trabajo".

En virtud de este poder de dirección, derivado del derecho constitucional a la libertad de empresa, el empleador tiene la facultad de emitir disposiciones generales y de obligatorio cumplimiento para la organización y funcionamiento de la empresa, dictar instrucciones a los trabajadores para la ejecución de las prestaciones laborales y establecer funciones, modificar de forma unilateral las circunstancias y límites de la prestación laboral, controlar el efectivo cumplimiento de las obligaciones laborales y aplicar sanciones disciplinarias.

8. Resulta oportuno mencionar que en atención al principio de buena fe laboral todo trabajador está obligado al cumplimiento adecuado de sus obligaciones, lo que incluye hacer un uso correcto de los instrumentos y/o herramientas provistas por el empleador para la ejecución de sus actividades. En este sentido, la Ley de Productividad y Competitividad Laboral contempla la posibilidad de sanción como falta grave este tipo de incumplimientos:

"Artículo 25.- Falta grave es la infracción por el trabajador de los deberes esenciales que emanan del contrato, de tal índole, que haga irrazonable la subsistencia de la relación. Son faltas graves:

- a) *El incumplimiento de las obligaciones de trabajo que supone el quebrantamiento de la buena fe laboral, la reiterada resistencia a las órdenes relacionadas con las labores, la reiterada paralización intempestiva de labores y la inobservancia del Reglamento Interno de Trabajo o del Reglamento de Seguridad e Higiene Industrial, aprobados o expedidos, según corresponda, por la autoridad competente que revistan gravedad (...);*
- c) *La apropiación consumada o frustrada de bienes o servicios del empleador o que se encuentran bajo su custodia, así como la retención o utilización indebidas de los mismos, en beneficio propio o de terceros, con prescindencia de su valor;*

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sqd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sqd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

 **Siempre
con el pueblo**



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

(...)"

9. Es en el ejercicio de este poder de dirección que el empleador se encuentra legitimado a efectuar control y vigilancia de la ejecución de las actividades laborales de sus trabajadores sin su consentimiento. Entre estas medidas de supervisión y control, el empleador, en su calidad de administrador de los bienes de su propiedad, como son las computadoras que entrega como herramientas de trabajo a sus empleados, puede disponer la instalación de sistemas informáticos y/o software para resguardar un uso adecuado de los mismos.
10. Sin embargo, el ejercicio de esta facultad legal de fiscalización y/o de control laboral del empleador respecto de las funciones y desempeño de labores, así como del uso correcto de las herramientas de trabajo entregadas a sus trabajadores no puede ser desmedido ni avasallador respecto al derecho a la protección de datos personales de estos últimos. Consecuentemente, esta Dirección General considera que si bien el poder de dirección y/o de control laboral se ampara en una finalidad legítima de supervisión de cumplimiento de obligaciones laborales, los mecanismos y/o herramientas que permitan llevar a cabo dicho control deben ser adecuados y no excesivos para el cumplimiento de una finalidad específica, siendo en el presente caso, fiscalizar el correcto uso de las computadoras, a efectos de detectar y/o evitar la comisión del delito de pornografía infantil .

Sobre el uso del software y la observancia de la normativa de tratamiento de datos personales

11. Desde el punto de vista de la LPDP, el tratamiento de datos personales del empleador para fines de control y fiscalización laboral se exceptúa de la obligatoriedad de la obtención previa del consentimiento por parte del titular del dato personal (trabajadores) por estar enmarcado en la ejecución de una relación contractual. En tal sentido, la LPDP, artículo 14, numeral 5, establece que no se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento *"cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento."*
12. El hecho de que el empleador pueda tratar datos personales de sus trabajadores para fines laborales (como es la supervisión del cumplimiento de sus actividades laborales y adecuado uso de las computadoras que les entrega para ello), sin el consentimiento de los mismos, no lo exime de la obligación de informar acerca de la existencia de esta herramienta y/o software de detección de actividades ilícitas, así como los supuestos en los que el mismo se activa y qué datos personales e información respecto al trabajador en dicha situación el empleador tendría acceso,

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

así como los encargados de tratamiento de ser el caso, y los alcances previstos para dicho tratamiento.

13. El detalle de información respecto al empleo y uso de este software para la prevención y detección de la comisión del delito de pornografía infantil permitirá a los empleados no contar con expectativas de privacidad que resguarden cualquier tipo de actividad que realicen mediante el uso de las computadoras que le fueron asignadas, en tanto la facultad de fiscalización laboral se encuentra debidamente legitimada en los casos de sospechas razonables y/o indicios de la comisión de este tipo de conducta ilícita.
14. Este tipo de información debe estar contenida en la cláusula informativa que todo empleador debe poner de conocimiento a sus trabajadores y para la cual debe observar el artículo 18 de la LPDP³.
15. Para el caso particular, es necesario evaluar si la medida de instalación del software resulta proporcional a la finalidad legítima de ejercicio de fiscalización y control laboral desarrollada para fines de detección y prevención del delito de pornografía infantil por parte de alguno de los trabajadores. El principio de proporcionalidad se encuentra contemplado en el artículo 7 de la LPDP y establece que "todo

³ Artículo 18 de la LPDP:

"Artículo 18. Derecho de información del titular de datos personales

El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

En el caso que el titular del banco de datos establezca vinculación con un encargado de tratamiento de manera posterior al consentimiento, el accionar del encargado queda bajo responsabilidad del Titular del Banco de Datos, debiendo establecer un mecanismo de información personalizado para el titular de los datos personales sobre dicho nuevo encargado de tratamiento

Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento".

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."





PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados."

16. Respecto al uso del Software, este debe ser adecuado y no excesivo en relación con la finalidad de su instalación, debiendo esta ser expresada de forma clara y precisa. En este sentido, este Despacho opina que el empleador solo podría acceder a la información del trabajador respecto al uso de la computadora asignada a través del Software en caso existan motivos concretos (indicios y/o sospecha razonable de la comisión del delito de pornografía infantil por parte de un trabajador) que justifiquen esta necesidad de acceso a la computadora por parte del empleador y siempre que la información obtenida esté vinculada únicamente a la comisión del delito, omitiendo toda información de carácter personal y familiar. Dicho esto, a criterio de este Despacho un tratamiento contrario al principio de proporcionalidad sería el uso del Software de forma indiscriminada por parte del empleador, por ejemplo, escoger aleatoriamente a un grupo de trabajadores (de los cuales no se tienen indicios y/o sospechas razonables) y monitorear abiertamente y de forma constante sus carpetas e historiales de visita online a través del Software.
17. Finalmente, respecto a la instalación y uso del software es importante traer a colación la observancia del principio de seguridad regulado en el artículo 9, complementado con el artículo 16 de la LPDP, que establece que, independientemente, del tipo de tratamiento que realicen los responsables del tratamiento, es obligación de los mismos establecer y mantener medidas técnicas, organizativas y legales necesarias y suficientes para garantizar la seguridad de los datos personales en su máxima expresión, evitando su alteración, pérdida, tratamiento o acceso no autorizado.
18. En tal sentido, dependiendo del uso de medios automatizados o no para el tratamiento de los datos personales, el Reglamento de la LPDP (aprobado mediante el Decreto Supremo N° 003-2013-JUS), en sus artículos 39 al 46, desarrolla medidas de seguridad mínimas de obligatorio cumplimiento para todo titular de banco de datos personales, las cuales se recomienda sean revisadas por el desarrollador y/o proveedor del Software a efectos de dotar del mismo de los resguardos mínimos indispensables, inclusive mejorar la efectividad de dichas medidas.
19. Sin perjuicio de la revisión de los artículos antes referidos, dependiendo del desarrollo específico del Software y su funcionamiento, como punto de partida respecto a la seguridad del tratamiento de la información digital, se tiene en el artículo 39 del Reglamento de la LPDP la obligación de implementar a los controles de acceso y registro sobre la interacción de los datos para fines de trazabilidad lo siguiente:

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

 **Siempre
con el pueblo**



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

"Artículo 39.- Seguridad para el tratamiento de la información digital.

Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:

1. *El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario-contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad.*

2. *Generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones relevantes. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.*

Asimismo, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales."

20. Asimismo, es necesario tener en cuenta el deber de confidencialidad establecido en el artículo 17 de la LPDP:

"Artículo 17. Confidencialidad de datos personales

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.

El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional."

21. El empleador, en cumplimiento del principio de confidencialidad, así como de la implementación de medidas de seguridad en el software, ante una situación de investigación para la detección del delito de pornografía infantil y/o en el marco de un procedimiento disciplinario, debe custodiar la información obtenida. Por este motivo, únicamente podrá compartir dicha información con aquellas personas que se encuentren debidamente legitimadas a conocer sobre el caso (las autoridades

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

 **Siempre
con el pueblo**



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

fiscales persecutoras del delito), por lo cual debe mantener la reserva frente al resto de trabajadores y/o terceros.

IV. CONCLUSIONES

1. La instalación y uso del Software en las computadoras de la empresa que son asignadas a sus trabajadores no requiere de consentimiento en tanto el tratamiento de datos personales del empleador para fines de control y fiscalización laboral se exceptúa de la obligatoriedad de la obtención previa del consentimiento por parte del titular del dato personal (trabajadores), por estar enmarcado en la ejecución de una relación contractual (numeral 5 del artículo 14 de la LPDP)
2. No obstante, el empleador se encuentra obligado a informar de manera clara y expresa acerca de la existencia de esta herramienta y/o software de detección de actividades ilícitas, así como los supuestos en los que el mismo se activa y qué datos personales e información respecto al trabajador en dicha situación, el empleador, y el encargado de tratamiento, de ser el caso, tendrían acceso, así como los alcances previstos para dicho tratamiento, conforme a lo señalado en los considerandos 12, 13 y 14 del presente documento.
3. El empleador puede utilizar el software como una forma de ejercicio de su poder de dirección y de control/fiscalización laboral siempre que el tratamiento de los datos personales vinculados al uso del mismo sea proporcional a la finalidad del tratamiento, la cual debe ser expresada de forma clara y precisa.
4. Corresponde a cada responsable de tratamiento de datos personales cumplir con las obligaciones previstas en la LPDP y su reglamento, partiendo especialmente de la interpretación de los principios rectores de finalidad, proporcionalidad, seguridad y confidencialidad, para efectos de la implementación y ejecución de medidas informáticas de control y/o fiscalización laboral.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

 **Siempre
con el pueblo**



PERÚ

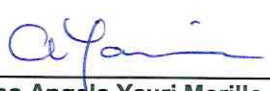
Ministerio de Justicia y Derechos Humanos

Despacho Viceministerial de Justicia

Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"

- 5. El desarrollo de la presente consulta se encuentra limitado únicamente al supuesto consultado de prevención del delito de pornografía infantil, no debiendo extenderse como una regla general para justificar cualquier acción que pueda ser ejercida por los empleadores en virtud de su poder de dirección.

Aprobado por:	Aprobado por:
<hr/> Eduardo Luna Cervantes Director General Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales	 <hr/> Liliana Angela Yauri Morillo Directora (e) de la Dirección de Protección de Datos Personales

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sqd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sqd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

