zegarra & schipper
abogados consultores

LA ANPDP PUBLICÓ UNA OPINIÓN CONSULTIVA QUE PRECISA LA FACULTAD DE LOS EMPLEADORES DE INSTALAR *SOFTWARES* EN LAS COMPUTADORAS DE SUS TRABAJADORES CON LA FINALIDAD DE DETECTAR LA COMISIÓN DE ACTIVIDADES ILÍCITAS

La Autoridad Nacional de Protección de Datos Personales (en adelante, la "ANPDP") publicó en su página web la Opinión Consultiva N° 035-2022-DGTAIPD de fecha 13 de octubre de 2022, la cual tiene por finalidad precisar si existe alguna posible afectación a la Ley N° 29733 - Ley de Protección de Datos Personales (en adelante, la "LPDP") por parte de los empleadores, al instalar *softwares* en las computadoras de sus trabajadores que permitan detectar y/o evitar la comisión del delito de pornografía infantil, o en general para fiscalizar el uso correcto de las computadoras como herramientas de trabajo. En tal sentido, a continuación desarrollaremos los aspectos más importantes de la Opinión Consultiva N° 035-2022-DGTAIPD.

1. USO DEL *SOFTWARE* Y LA OBSERVANCIA A LA LPDP

La LPDP faculta a los empleadores para que puedan instalar un *software* en las computadoras de sus trabajadores que tenga por objetivo tratar sus datos personales sin que se solicite su consentimiento, siempre que dicho *software* sea utilizado para fines de control y fiscalización laboral.

Entre las medidas de supervisión y control, el empleador, en su calidad de administrador de los bienes de su propiedad –como serían las computadoras que utiliza el trabajador para realizar sus labores–, puede disponer de la instalación de un *software* para resguardar un uso adecuado de los mismos.

Esta facultad se desprende de lo señalado en el Texto Único Ordenado del Decreto Legislativo N° 728 - Ley de Productividad y Competitividad Laboral, aprobado mediante el Decreto Supremo N° 003-97-TR; y, se encuentra en el marco de una excepción al consentimiento establecida en la LPDP[1], la cual dispone que no será necesario solicitar el consentimiento del titular de datos personales para todo aquel tratamiento que sea realizado para la ejecución de una relación contractual.

Por otra parte, si bien no sería necesario solicitar el consentimiento del trabajador para la instalación del *software*, lo cierto es que el empleador se encuentra sujeto a otras obligaciones enumeradas en la LPDP y su Reglamento, tales como:

- Informar de manera clara y expresa acerca de la existencia de un *software* de detección de actividades ilícitas, así como precisar qué información se estaría

[1] **Ley N° 29733 - Ley de Protección de Datos Personales:**
"Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. 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.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.
12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley".

tratando (deber de información). Ello podrá ser informado en una cláusula que se encuentre en el contrato de trabajo suscrito por los trabajadores.

- El uso del *software* debe ser adecuado y no excesivo con relación a la finalidad de su instalación (deber de proporcionalidad y finalidad). En atención a lo indicado por la ANPDP, el empleador sólo podría acceder a la información del trabajador a través del *software* en caso existan motivos concretos –indicios o sospecha razonable– que justifiquen la necesidad de acceso.

- Establecer y mantener medidas de seguridad técnicas, organizativas y legales necesarias y suficientes para garantizar la seguridad de los datos personales, evitando su alteración, pérdida, tratamiento o acceso no autorizado (deber de seguridad). Por ejemplo, se deben implementar controles de acceso al banco de datos, generar y mantener registros que provean evidencia sobre las interacciones con los datos para fines de trazabilidad, entre otros.

2. COMENTARIO

La consulta formulada se encuentra enmarcada en la posible instalación de un *software* que permita al empleador detectar si el trabajador accede a páginas web de pornografía infantil a través de las computadoras de la empresa. Al igual que en oportunidades anteriores, la ANPDP reconoce la plena facultad de dirección del empleador, lo que incluye la posible fiscalización con fines de control laboral y que, como es evidente, no exime del uso de mecanismos tecnológicos como son los *softwares* de registro de acceso a páginas web.

La ANPDP también reconoce que el tratamiento de datos personales para fines laborales se encuentra considerado entre las causales de excepción del consentimiento señaladas en el artículo 14 de la LPDP. No obstante lo anterior, la ANPDP pone de manifiesto la absoluta obligatoriedad de cumplir con todas demás obligaciones adicionales al simple consentimiento.

De esta forma, sobre este control laboral a través de un *software* se indica que debe ser para fines específicos y no ser invasivo, a fin de cumplir con principio de proporcionalidad. En igual medida, se debe cumplir con el deber de información, así como el deber de seguridad, los cuales forman parte del marco normativo básico de la protección de los datos personales de los trabajadores.