TITULO: La información biométrica inyecta un nuevo riesgo a las firmas mineras				
Nº	**FECHA**	**MEDIO**	**SECCIÓN**	**PÁGINA**
301149	2025-11-17	El Mercurio	Economí-a y Negocios	B 9

Imagen 1/1

Aplicación de la nueva Ley de Protección de Datos Personales:

La información biométrica inyecta un nuevo riesgo a las firmas mineras

Las empresas, debido a las condiciones de trabajo, almacenan datos médicos y biométricos de sus trabajadores, los cuales tienen la categoría más estricta de protección bajo la nueva legislación.

CATALINA MUÑOZ-KAPPES

Un riesgo que había pasado inadvertido surge ahora para la minería por la Ley de Protección de Datos Personales, promulgada a fines del año pasado.

La ley se suele vincular con el deber que las empresas tienen con los datos de sus clientes. Pero hay más. Romina Garrido, abogada de Prieto, afirma que "la empresa tiene la misma responsabilidad que respecto de los datos de sus clientes o usuarios que sobre sus trabajadores, e incluso reforzada". Suele tratarse de un tratamiento forzosos de tales datos, dada la relación laboral. Con todo, "se mantienen los deberes de confidencialidad, seguridad y proporcionalidad en su tratamiento, además de garantías constitucionales de la misma legislación laboral que protegen la información privada de los trabajadores", dice Garrido.

BLOOMBERG

Las mineras emplean cada vez más faenas autónomas, con monitoreos remotos y un uso intensivo de tecnologías avanzadas. Esa digitalización impone un mayor manejo de datos personales.

Los datos médicos

La nueva legislación asigna mayor sensibilidad y más estricto tratamiento a los datos sensibles, también denominados "especialmente protegidos". Corresponde a afiliación política, situación socioeconómica, datos de salud y biométricos, entre otros. Debido a las condiciones de trabajo, las mineras almacenan gran cantidad de estos datos sensibles. "Hacen tratamiento de datos personales de empleados y trabajadores subcontratados, tales como datos biométricos, utilizados para accesos y sistemas de seguridad; datos de salud y condiciones médicas, vinculados al control de faenas; así como datos de monitoreo en tiempo real —incluyendo geolocalización, *wearables* y sensores", indica Carolina Cabrera, socia fundadora de LawTech.

31
infracciones tipificadas tiene la Ley N° 21.719. Las sanciones pueden llegar a $1.390 millones.

"Las características especiales de la industria minera hacen necesario tratar otros datos, como datos de salud, por los exámenes preocupacionales periódicos que se exigen para ir a las faenas. También puede tener que tratar datos biométricos por temas de seguridad e imágenes de los trabajadores captadas por cámaras de circuito cerrado de televisión (CCTV), por nombrar solo algunos", afirma Diego Morandé, asociado sénior de Guerrero Olivos. Tomás Garnham, asociado sénior de Guerrero Olivos, asegura que debido a que los datos de salud son sensibles, "se requiere de un consentimiento especial para su tratamiento adecuado por parte de la empresa y terceros que podrían cumplir tareas administrativas". Para Cabrera, en un escenario de creciente digitalización, donde las mineras emplean faenas autónomas, monitoreo remoto y un uso intensivo de tecnologías avanzadas, es "fundamental garantizar que los datos personales se utilicen de manera segura, transparente y cumpliendo con todas las exigencias de la ley".

Las altas multas

Las multas que arriesgan las mineras pueden ser muy cuantiosas. "En sede de protección de datos son las mismas que para los datos fuera del contexto laboral; la nueva Ley N° 21.719 contempla 31 infracciones tipificadas, clasificadas en leves, graves y gravísimas. Las sanciones van desde la amonestación hasta multas de 1 a 20.000 UTM (entre $70.000 y $1.390 millones), según la gravedad de la infracción y el daño ocasionado", dice Garrido. . Además, si hay reincidencia o infracciones gravísimas, "las multas pueden alcanzar hasta un porcentaje de las ventas anuales de la empresa", dice la abogada. Por otro lado, la responsabilidad por una infracción a la ley no se desvanece si quien almacena los datos es un proveedor, aclaran los expertos. "Cuando una empresa externaliza el tratamiento de datos personales a un proveedor, no transfiere su responsabilidad. El responsable del tratamiento, esto es, la empresa que decide usar al proveedor, sigue siendo jurídicamente responsable", señala Garrido. Morandé resalta que "es muy importante contar con acuerdos de tratamiento de datos con aquellos proveedores".

"En la medida que el responsable adopte las medidas derivadas de las exigencias de la ley no solo evitará las infracciones, podrá también mitigar la responsabilidad en su incumplimiento. Así, reduce riesgos legales y reputacionales, facilita la colaboración con empresas internacionales y demuestra una gobernanza sólida y sostenible", señala Cabrera.