LAS CONSECUENCIAS DEL TELETRABAJO PARA LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

Autor: Daniel Villanueva Plasencia
Asociado Sr. de Baker McKenzie Abogados

Hoy el teletrabajo es una realidad, pero hace algunos años quizás no era algo tan común en México, aunque según algunos estudios en México miles de personas y empresas ya utilizaban esta modalidad de empleo desde hace varios años. Sin embargo, de manera similar a otras actividades en nuestra vida diaria, la pandemia de COVID-19 aceleró la implementación del teletrabajo. Nuestra nueva realidad de tener que trabajar de manera remota ha puesto a más personas que nunca, trabajando fuera de sus oficinas, de su infraestructura y resguardo. Quizás como consecuencia de dicha aceleración, muchas empresas e individuos no se prepararon adecuadamente, o aún no están listos para afrontar las consecuencias de dicha implementación.

En México, la implementación del teletrabajo se vio materializada en enero del 2021 con una reforma a la Ley Federal del Trabajo (la "Reforma"). Esta Reforma reconoce el desempeño de actividades remuneradas en lugares distintos al establecimiento del patrón, por lo que no se requiere la presencia física en el centro de trabajo. Entre otras, las nuevas obligaciones derivadas de dicha reforma, requiere que las empresas, **implementen mecanismos que ayuden con la preservación de la seguridad de la información y datos utilizados por las personas trabajadoras; asumir los costos derivados del trabajo, incluyendo telecomunicaciones y electricidad; y respetar el derecho a la desconexión de las personas al término de la jornada laboral**. Por su parte, dentro de las obligaciones de los empleados, encontramos que estos deben **cumplir con las políticas de protección de datos, así como las restricciones sobre el uso y almacenamiento de los mismos**. Aunque cumplir con estas obligaciones pudiera parecer sencillo, en la práctica se dejan muchos cabos sueltos de ambas partes, generando así riesgos, particularmente respecto de la protección de la información y los datos personales.

Sin los cuidados correctos, la implementación de esta modalidad del trabajo puede tener impactos negativos tanto para las empresas, como para los trabajadores. Así, desde una perspectiva de protección de la información y de los datos personales, ya que el trabajador se encuentra fuera del respaldo e infraestructura de las oficinas, el cuidado de la información es determinante, ya que al contar con una menor seguridad los riesgos respecto de la pérdida de la misma aumentan. Basta ver el incremento en ciberataques en los últimos años para comprender que existe un riesgo latente al no contar con la infraestructura adecuada. Sin embargo, en algunos casos el trabajar fuera de la infraestructura de las oficinas ha llevado a algunas empresas a implementar invasivos modelos de monitoreo de sus empleados. En algunos casos con miras a confirmar los periodos de trabajo, y en otros para remediar la falta de seguridad de la información. Si bien pudiera parecer que incrementar la vigilancia ayuda a disminuir riesgos, en

algunos puede llegar a incrementarlos, ya que, al existir una mayor supervisión de parte de las empresas, se pueden tratar datos personales de manera indebida, ya sea por un exceso de tratamiento o por transferencias de datos indebidas.

Queda entonces claro, que el incremento en estos riesgos sugiere que existen problemas que se deben resolver. Para poder determinar cuáles son las medidas de seguridad adecuadas, es necesario antes comprender la naturaleza de los riesgos a los que pudieran estar expuestos los datos personales. Los riesgos difícilmente se podrán erradicar por completo, pero sí se pueden minimizar a través de la mejora continua. De esta manera, primero se tienen que identificar las posibles amenazas y su naturaleza, para que entonces se puedan proponer las medidas de seguridad que son adecuadas para minimizar cada uno de los riesgos identificados.

Atendiendo a la naturaleza general de la materia protegida, identificamos dos tipos distintos: (i) la información y datos en general; y (ii) los datos personales. Al identificar cada uno de estos para determinar las medidas de seguridad para garantizar la protección de la primera, estarán dictadas por la propiedad industrial tratándose de secretos industriales, y por el derecho civil o mercantil, en la medida que existan contratos de confidencialidad, aunque también puede estar protegida por otras ramas jurídicas dependiendo de la naturaleza de los datos como el secreto profesional o el secreto bancario, entro otros. Por su parte, la protección de los datos personales se regula por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("LFPDPPP") (o en su caso por la Ley General de Datos Personales en Posesión de Sujetos Obligados, aunque el alcance de este análisis se limita a la protección de datos personales en posesión de particulares.

Para abordar adecuadamente la protección de datos personales, debemos partir del principio que, independientemente del contrato individual o colectivo de trabajo, el contrato de teletrabajo o el aviso de privacidad, en todo tratamiento de datos personales siempre debe existir una expectativa razonable de privacidad. Este principio es determinante para poder entender los alcances del teletrabajo en México, ya que el derecho de supervisión previsto por la Ley Federal del Trabajo tras la Reforma es muy amplio.

Respecto de los riesgos en la protección de datos personales, identificamos una dualidad según su origen. Por una parte, la protección de los datos personales frente a ataques de terceros; y por otro, la protección de los datos personales por el impacto en la implementación de nuevas tecnologías. En el primero el riesgo es externo, sobre todo por los ciberataques que van en aumento; y en el segundo, normalmente, es un riesgo que se crea por actos u omisiones internas, es decir que en su gran mayoría el responsable de los datos está en control de la situación. Atendiendo en particular a la Reforma, podemos identificar como ésta considera tanto riesgos externos como internos.

La Reforma considera que las empresas deben implementar mecanismos que ayuden con la preservación de la seguridad de la información y datos utilizados por los trabajadores; y por la

otra, la obligación de los trabajadores de cumplir con las políticas de protección de datos, así como las restricciones sobre su uso y almacenamiento de los mismos. Estas obligaciones tienen la intención de prevenir que terceros tengan acceso a la información y datos personales utilizados por la empresa. Alineado con lo anterior, la LFPDPPP incluye una obligación legal para los responsables del tratamiento de datos personales, de establecer y mantener la seguridad de los datos personales, por lo que deben contar con análisis de riesgos de datos personales que consistan en identificar peligros, y estimar los riesgos a los datos personales. Este concepto es amplio y puede incluir desde ayudar a los trabajadores a adecuar sus redes y módems en casa, hasta el llevar a cabo seminarios internos para levantar el nivel de conocimiento de los trabajadores en esta área y respecto de los riesgos como el *phishing*.

Con la intención de ayudar a los responsables a disminuir estos riesgos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ("INAI") publicó las *"Recomendaciones para reconocer las principales amenazas a los datos personales a partir de la valoración respecto al riesgo";* estas recomendaciones proponen la creación de protocolos de gestión de riesgos para buscar mantener el riesgo por debajo del objetivo fijado. Los posibles mecanismos de seguridad para disminuir riesgos incluyen el implementar respaldos de la información, el cifrado de la información, medidas de acceso restringido a la información y datos personales, acciones de revisión y mantenimiento continuo, entre otras. Por lo tanto, mantener la seguridad no es solo un tema conveniencia, de discusión de riesgos o de prevención de pérdida de activos de la empresa, sino que es un tema necesario para cumplir con las obligaciones legales establecidas en la Ley Federal del Trabajo y en la LFPDPPP. Atendiendo a la modernidad, cabe señalar que cuando la empresa, como responsable del tratamiento, pretenda contratar servicios de cómputo en la nube para llevar a cabo dicha supervisión, mediante la adhesión a los términos y condiciones del proveedor, es necesario que dichos proveedores cumplan con los criterios mínimos impuestos por la LFPDPPP y su Reglamento.

De manera similar, la Reforma establece que las empresas pueden implementar mecanismos, sistemas operativos y cualquier tecnología utilizada para supervisar el teletrabajo. Sin embargo, dicha supervisión no puede ser absoluta y debe estar limitada. Al respecto, tanto la Ley Federal del Trabajo, como la LFPDPPP, están alineadas, ya que prevén que la supervisión y el tratamiento de datos personales deben ser proporcionales a su objetivo, garantizando el derecho a la intimidad de las personas. Esta limitación debe ser aplicable también a las demás obligaciones consideradas en la Ley Federal del Trabajo, como asumir los costos derivados del trabajo, incluyendo telecomunicaciones y electricidad; y respetar el derecho a la desconexión de las personas al término de la jornada laboral, ya que en el cumplimiento de éstas se podrían llegar a tratar datos personales como los incluidos en los recibos de pago de servicios de internet o de electricidad, ya sea los propios del trabajador o de un tercero, si es que el recibo está a nombre de otra persona, o la obtención de datos personales de terceros por el uso de cámaras o micrófonos.

Desde una perspectiva de privacidad, previo a la implementación de controles de supervisión como el uso de cámaras o micrófonos, las empresas deberían instrumentar un procedimiento interno que les permita atender el riesgo que dicha implementación de nuevas tecnologías supone para la protección de datos personales, así como para mitigarlos. Muchas veces el sentido de urgencia por la situación en la que nos encontramos parece superar la obligación legal que tienen todos los responsables del tratamiento de datos personales, de adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad. Al respecto el INAI publicó la *"Guía para la elaboración de evaluaciones de impacto a la privacidad"*, con el objetivo de que los responsables puedan obtener beneficios de la implementación de evaluación de impacto a la privacidad, o de alcanzar resultados en el marco de su esquema de protección e inclusive dentro de sus sistemas de gestión. Es recomendable que estas evaluaciones no se lleven a cabo de manera aislada como un simpe reporte, sino que deben ser consideradas desde la planeación del proyecto mismo, e inclusive, pueden mantenerse después de su implementación, en el entendido de que nuevos riesgos podrían surgir conforme el proyecto avance o se modifique.

De manera similar a la obligación de establecer y mantener la seguridad de los datos personales, la LFPDPPP establece una invitación para que las empresas instrumenten procedimientos para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías. Instrumentar estos procedimientos no solo ayuda a las empresas a cumplir con su obligación de adoptar medidas para garantizar el debido tratamiento de los datos, sino también permiten implementar un enfoque de privacidad por diseño, en concordancia con las mejores prácticas internacionales.

Es por lo anterior que, si bien la Reforma trae grandes beneficios para proteger de una manera más clara nuevas modalidades de trabajo, también es claro que la implementación de la misma no se puede dar, sin considerar el impacto pueda tener para la información y datos personales, ya que hacerlo podría no solo suponer un mayor riesgo para las empresas, sino también el incumplimiento de preceptos legales.