ECIJA OTERO
Av. Apoquindo 3669, Piso 13,
Las Condes, Santiago - Chile
Tel: +562 2361 8900
www.ecija.com

COVID-19 vs. Teletrabajo – Trabajo a distancia. ¿Estamos tomando las medidas para prevenir ciberataques? ¿Estamos cumpliendo con los estándares de privacidad y protección de datos personales?

COVID-19 y Transformación Digital

Ante la declaración oficial de la OMS, del COVID-19 como una pandemia, el 11 de marzo recién pasado y, las medidas de urgencia decretadas, tales como prohibición de aglomeración de grupos de más de 50 personas, cierres de comercios, cuarentena decretadas en ciertas comunas; llevaron obligadamente a la transformación digital a pasos agigantados; de esta forma, muchas empresas, pymes, organizaciones y empleadores (tanto en el mundo como en Chile) se vieron en la necesidad de organizar que sus empleados, trabajen en forma remota desde su hogares, para así bajar los riesgos de contagios mientras los empleados se trasladaban desde un lugar a otro, y/o trabajaban en oficinas o espacios poblados de personas. No obstante, junto a esta llamada transformación digital, ha estado presente la discusión sobre la seguridad en el trabajo a distancia o en el teletrabajo. Visualicemos cuales serían algunos de los nuevos escenarios que estamos enfrentando ante esta transformación digital y que medidas podemos tomar al respecto.

Seguridad

Las empresas, pymes, compañías u organizaciones parecieran haber olvidado tener en cuenta los mayores riesgos que implica el trabajo a distancia o el teletrabajo, para la seguridad de sus redes, sistemas y datos y, no han tomado las medidas de seguridad o los protocolos recomendados o necesarios al respecto.

En temas de seguridad, hemos visto que existen mayores riesgos de exposición de datos confidenciales. Así, hemos recopilado información de distintos medios de acceso público, que un área de preocupación es que los empleados, como una manera para facilitar el trabajo, lo hacen a través de dispositivos personales o fuera del entorno seguro de la organización; o bien, se envían correos electrónicos - a cuentas personales - con archivos adjuntos que contienen datos confidenciales de la empresa u organización, o cargan esos datos en cuentas personales en almacenamiento en la nube.

Uso de herramientas tecnológicas

Junto a la puerta que se ha abierto a problemas de seguridad mencionados en el párrafo anterior, se ha sumado la falta de equipos o hardware proporcionado por el empleador, lo cual ha contribuido al aumento de riesgos exponenciales, por el uso que genera la utilización creciente de los dispositivos personales (no seguros) por parte de los empleados, particularmente si esos dispositivos pueden conectarse a la red o sistemas de la organización de forma remota.

En este punto cabría tener presente la Ley 21.220 que comenzó a regir el 01 de abril recién pasado y, regula el trabajo a distancia y el teletrabajo y que nos hace preguntarnos: ¿Puede el trabajador proveer los equipos para el teletrabajo o trabajo a distancia? La ley señala que los equipos, las herramientas y los materiales para el trabajo, incluidos los elementos de protección personal, deberán ser proporcionados por el empleador. Asimismo, cabe agregar, que el trabajador no podrá ser obligado a utilizar elementos de su propiedad. Igualmente, los costos de operación, funcionamiento, mantenimiento y reparación de equipos serán siempre de cargo del empleador.

Privacidad. Tratamiento de Datos Personales

Por otra parte, debemos tener presente, el tema de la privacidad y el tratamiento de datos. Recordemos que nuestra ley de datos personales 19.628 tiene plena vigencia en esta modalidad de trabajo y los datos que se envían fuera de la red de una empresa u organización no solo generan exposición a mayores brechas de seguridad, sino también podrían crear obligaciones en materia de normativas de privacidad y leyes de protección de datos personales, debiendo notificar a los clientes de la empresa, a los reguladores, a los trabajadores, etc.

El procesamiento de datos personales en registros o bancos de datos por entidades públicas o privadas está sujeto a las disposiciones de la Ley N ° 19.628 (en adelante, la "Ley de Privacidad", o "LDP") y el Artículo 19 N ° 4 de la Constitución Chilena, excepto si se realiza en ejercicio de la libertad de opinión y de presentación de informes, que se rige por la ley a que se refiere el artículo 19 No. 12 de la Constitución chilena.

Cualquier persona puede procesar datos personales, siempre que se realice de manera coherente con la LDP y para los fines permitidos por la ley. En cualquier caso, dicho proceso debe respetar el ejercicio pleno de los derechos fundamentales de los titulares de dichos datos y las normas de la LDP.

La LDP establece que cualquier persona puede procesar datos personales y es necesario cumplir con las disposiciones contenidas en ésta. Así, se requiere para el procesamiento de datos, cumplir con aquellas relacionadas con la autorización o el consentimiento del interesado, el principio de finalidad (los datos personales se utilizarán solo para los fines para los que se han recopilado, y esos fines deben estar permitidos por la ley chilena) y notificar sobre la posible comunicación pública de los datos.

En consecuencia, de conformidad con la LDP, a menos que la ley lo permita expresamente, la recopilación de datos debe cumplir tanto con el consentimiento como con la regla de notificación y el requisito de la limitación de propósito, entre otros requisitos. Sin embargo, una excepción al consentimiento del titular de datos es aquellos recopiladas o que estén disponibles en fuentes de libro acceso al público, En el caso del requisito de autorización, el interesado debe estar debidamente informado sobre el propósito del almacenamiento y la posibilidad de comunicación a terceros. La autorización debe ser por escrito. La autorización puede ser revocada, pero sin efecto retroactivo, que también debe ser por escrito. Los datos personales deben usarse solo para los fines para los que se han recopilado, a menos que provengan de fuentes públicas o se hayan recopilado de ellas. En cualquier caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos

La LDP actualmente no incluye una disposición específica con respecto a las restricciones a las transferencias internacionales de datos de información personal. Sin embargo, la transferencia de datos personales fuera de la jurisdicción de Chile puede considerarse como un tratamiento de datos y requerirá autorización y se le aplicarán otras restricciones establecidas por la LDP.

El incumplimiento de esas disposiciones, tales como: la falta de consentimiento del interesado puede exponerlo a riesgos como multas entre aproximadamente USD $ 75 a USD $ 760. Además, debido a que las multas se determinan en un procedimiento sumario ante el tribunal, los riesgos de disputas legales y demandas son altos. Además, la LDP establece que los daños no monetarios y monetarios que resulten del procesamiento incorrecto de los datos personales serán compensados.

Como hemos mencionado, actualmente se está discutiendo un proyecto de ley destinado a reemplazar la LDP en el Congreso Nacional, que establece derechos, obligaciones, para adecuarse a estándares semejantes e incluso más estrictos que la GDPR. De esta forma, además de los derechos ARCO, se incluye la creación de una entidad independiente, con plena autoridad para regular, fiscalizar el tratamiento de datos personales, con facultades de imponer multas, etc.

Datos Sensibles

En términos generales, en Chile y en el derecho comparado, la normativa de protección de datos recoge la prohibición general de tratamiento de los datos de salud –clasificados como datos sensibles, salvo que exista consentimiento expreso de interesado o que dicho tratamiento pueda ampararse en alguna de las excepciones recogidas en las leyes

respectivas. De esta manera, los gobiernos se han amparado en excepciones del interés público o los intereses vitales de los interesados o de la sociedad, para evitar una propagación incontrolada del virus, haciendo hincapié en el hecho de que únicamente se deben recabar aquellos datos que sean necesarios para la lucha contra la epidemia o que hayan sido solicitados por las autoridades competentes con este fin y, respetando en la medida de lo posible la privacidad de los interesados.

En este mismo camino, de conformidad a nuestra ley de protección de datos personales, que regula el tratamiento de las bases de datos, el estado de salud de una persona (la enfermedad de una persona) es un dato personal sensible y, además, según el Código Sanitario, el contenido de la ficha clínica es reservada, salvo para el uso de la autoridad sanitaria para ejercer sus facultades, los tribunales y el Ministerio Público.

Phishing – Malware

Mucho se ha publicado que el COVID-19 ha generado nuevas oportunidades para los ciberatacantes , lo cual es una realidad concreta, ya que aprovechan y lo han hecho, para utilizar el temor de la pandemia, enviando correos electrónicos de phishing que dicen contener actualizaciones a las políticas de la empresa asociadas con COVID-19, requiriendo a los empleados que estos validen sus datos o credenciales y/o pidiéndole que instalen software adicional para permitir la conectividad remota; todo lo cual permitiría a los ciberdelincuentes oportunidades para infiltrarse en las redes y sistemas de la compañía. Lo mismo ha sucedido con páginas relacionadas con informaciones no oficiales relacionadas con el COVID-19.

Por otra parte, no debemos olvidar el aspecto positivo que esto ha generado en cuanto al desarrollo de nuevos servicios online o la mejora de ellos, tales como el soporte remoto (extendiendo la capacidad de autoservicios en la web, como los chatbots, la capacitación, etc.).

CSIRT

Por otra parte, ha crecido enormemente con alto riesgo de fraude, el phishing de páginas de bancos o de correos, que la autoridad chilena a través del Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, ("CSIRT"), ha publicado en sus reportes e indicado las medidas ha tomar al respecto.

En el Reporte No. 40 el CSIRT Informa con alto riesgo de fraude: … la activación de tres portales fraudulentos asociados a un IP que suplantan el sitio web oficial de Banco Estado, Banco de Chile, Banco BCI, el que podría servir para robar credenciales de usuarios de esa entidad. Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida. Asimismo, ha aumentado enormemente la suplantación de identidad.

El día 13 de abril, CSIRT ha identificado una campaña de phishing a través de un correo electrónico que supuestamente proviene del servicio de correos electrónicos Zimbra. "*El mensaje informa a quien recibe el correo, que la cuenta ha excedido el límite de cuota establecida por el administrador, y es posible que no pueda enviar o recibir correos hasta que vuelva a validar la cuenta. El atacante pone a disposición un enlace para realizar la validación. Si la víctima accede al enlace, ésta es dirigida a un sitio falso que imita el correo*

corporativo de Zimbra, donde se le solicita el nombre de usuario y contraseña, tras lo cual se expone al robo de credenciales".

Se recomienda consultar el Protocolo de Seguridad Para Trabajo a Distancia emitido por el Equipo de Respuesta de Incidentes de Seguridad Informática del Ministerio de Interior (CSIRT) https://www.csirt.gob.cl/media/2020/03/Protocolo-de-seguridad.pdf

Decisiones Apuradas y sus Consecuencias

Otro punto de vulnerabilidad que los expertos han indicado es que la presión por reforzar la capacidad para soportar el trabajo remoto (en la infraestructura de IT) lleva a decisiones de implementación rápidas que aumentan las probabilidades de intrusiones no deseadas y, eso abre una nueva ventana de riesgos a través de los sistemas y redes operados por proveedores de servicios externos que respaldan las aplicaciones y los flujos de datos necesarios para facilitar una fuerza de trabajo remota efectiva.

Resulta esencial proteger los datos confidenciales de la organización cuando los empleados trabajan desde su hogar; como el proteger la red y los sistemas de la empresa u organización. Asimismo, es fundamental, proteger y cumplir con la normativa referida a los datos personales no solo de propiedad de la empresa sino también de sus trabajadores y de sus clientes, en cualquier escenario, especialmente cuando los empleados están trabajando desde sus hogares (teletrabajo o trabajo a distancia).

Medidas. Trabajo conjunto de empresas, pymes y, empleadores, junto al liderazgo de abogados especialistas en estas materias

Es aquí donde los abogados especialistas en materias de privacidad, ciberseguridad y, TMT, pueden entrar a desempeñar un rol de liderazgo, de guía, en el compliance, para trabajar en conjunto con los equipos de IT, RRHH, de las empresas, pymes, u organizaciones o empleadores, en aquellos esfuerzos que deben hacer para adaptarse a estos nuevos paradigmas.

Los desafíos ante esta transformación digital, en cuanto a la forma y lugar de trabajo, que llegaron para quedarse, nos enfrenta ante nuevos escenarios en materias de regulación en privacidad y ciberseguridad, que son transversales para todas las entidades, sean estas de carácter público o privado, con o sin fines de lucro; que no han sido abordados y que están afectando ámbitos tan cotidianos como la forma que se administra la información de los trabajadores.

Estamos en un periodo de constantes cambios y de incertidumbre no solo en cuando a las normas laborales, si no también en la normativa de delitos informáticos, cuyo proyecto de ley está pronto a ver la luz.

El proyecto de ley de delitos informáticos cambia los paradigmas, es así como incorpora en la Ley 20.393 sobre Responsabilidad Penal de las Personas Jurídicas, los delitos de perturbación informática, acceso ilícito, interceptación ilícita, daño informático, falsificación informática, fraude informático y abuso de dispositivos; incluyendo de esta manera, dentro del compliance temas de ciberseguridad y privacidad. Recordemos, que los cambios vienen desde que entrara en vigor la protección constitucional en el 19 No. 4 de la C.P.R. la protección al tratamiento y protección a los datos personales, la que se efectuará en la forma y condiciones que determine la ley;

Asimismo, es importante tener presente que las empresas u organizaciones deben prepararse con antelación a todos los cambios normativos que hemos mencionados, donde incentivamos a asesorarse para crear políticas de auto-regulación que serán consideradas por la autoridad, modificando y adaptando sus políticas internas, sus contratos con proveedores, sus reglamentos, etc., en materias de privacidad, tratamientos de datos personales y de ciberseguridad.

Es por eso, que reiteramos que los abogados especialistas en materias de privacidad, ciberseguridad y tecnología hoy cumplen un rol fundamental, que trabajando en conjunto con las empresas, pymes, u organizaciones, tienen la capacidad de colaborar y guiar en la evaluación de las riesgos, brechas de seguridad, compliance, auto-regulación, y políticas de privacidad y ciberseguridad y resultados, que significarán una inversión al corto y largo plazo y una real contribución en mitigar dichos riesgos, amenazas e incumplimientos, que hemos tratado de resumir aquí .

"*Never leave that till tomorrow which you can do today*" (Benjamin Franklin) and "*Leave nothing for tomorrow which can be done today*" (Abraham Lincoln).

Macarena López
Head TMT, Privacidad, Cyber & IP