



Únicamente para fines específicos:

Los datos privados solo pueden ser tratados con autorización del titular o si la ley lo faculta

Evite entregar esa información que es sensible, aunque sea común que las empresas o instituciones se la soliciten.

Con tantas estafas que se reportan en redes sociales y entre amigos y conocidos, cada vez causa más recelo y desconfianza entregar los datos personales a empresas, instituciones o personas desconocidas.

Y casos hay muchos. Jair Goffman, gerente general de una empresa, con motivo de la comida anual de Fiestas Patrias, concurrió con su personal al Restaurante Parrilladas Valerio, de Quilicura. Al momento de solicitar la factura, el garzón le solicitó el e-RUT y la cédula de identidad para verificar los datos. Los facilitó, pero se percató de que le estaban tomando una foto al último documento. Reclamó y le dijeron que esa era la instrucción que tenían.

Solicitó que eliminaran la foto de inmediato, “pero todos sabemos que igual queda el registro”, manifestó a Línea Directa. Y añadió que el encargado le precisó que solo pedían el RUT de la compañía, y que no se quedaban con imágenes de la cédula. No obstante, la preocupación lo llevó a bloquear el documento y requerir uno nuevo.

En el restaurante —junto con lamentar lo ocurrido— nos señalaron que el local cumple estrictamente las exigencias del SII para la emisión de boletas y facturas y que para tal efecto solicitan el e-RUT y la cédula del representante. Aseguran que no conservan copia ni imagen alguna de las cédulas de identidad de sus clientes.

“No existe dentro de nuestros procedimientos autorizados ni habituales la toma de fotografías de cédulas de identidad de clientes ni la retención de tales imágenes. Si en esta ocasión se capturó una, se trató de una acción aislada no autorizada por la administración”, indicaron. Y enfatizaron en que fue debidamente eliminada en el acto y que ya instruyeron medidas correctivas para que no vuelva a ocurrir.

Uso indebido de datos

Stephanie Astudillo, abogada y académica coordinadora de la Clínica Jurídica de UDLA, sede Viña del Mar, nos aclaró que la actual Ley N° 19.628 sobre Protección de la Vida Privada establece que los datos perso-

Sepa qué medidas vienen a futuro para resguardar aún más este derecho que le otorga la ley, que protege los antecedentes personales.

NUEVA LEY
La normativa que entrará en vigencia en diciembre de 2026, amplía estos resguardos al regular principios como la minimización de datos, crear una agencia de protección de datos y establecer sanciones administrativas severas. Con ello, la defensa de la intimidad deja de depender solo de acciones judiciales y pasa a contar con un resguardo institucional más robusto.



Educación ciudadana

La académica de la UDLA considera que, para fortalecer la protección, es esencial fomentar la educación ciudadana respecto al valor y cuidado de los datos personales, así como promover prácticas empresariales responsables en su tratamiento. También se requieren ajustes normativos frente a desafíos que imponen nuevas tecnologías, como la IA y el big data, cuyo uso puede implicar riesgos de perfilamiento y vigilancia. La protección de datos no es solo un reto legal, sino también cultural y tecnológico, afirma.

den constituir un uso indebido de datos, especialmente porque el número de serie del documento es requerido para trámites relevantes, lo que aumenta el riesgo de fraudes.

La nueva Ley 21.719 —que entrará en vigencia en diciembre de 2026 y que regula la protección y el tratamiento de los datos personales— refuerza este criterio al consagrar el principio de proporcionalidad y exigir que el tratamiento de datos se realice solo para fines específicos y lícitos. “En consecuencia, solo se justifica en trámites legales, bancarios o de seguridad, pero no en situaciones cotidianas”, aclara Astudillo.

Añade que, actualmente, es posible entregar datos básicos como nombre, dirección, profesión o RUT cuando resultan necesarios para cumplir un contrato, emitir una boleta o prestar un servicio. También se considera válido proporcionar información de contacto para fines comerciales, siempre que se respete el derecho a oponerse, afirma.

Lo que no corresponde es solicitar datos sensibles, como los relacionados con salud, religión o ideología, salvo que exista una autorización legal expresa. La Ley 21.719 moderniza esta regulación y establece que solo se pueden recolectar datos pertinentes, adecuados y no excesivos, siempre informando al titular la finalidad de su uso. De esta forma, su entrega debe limitarse al mínimo es-

trictamente necesario según el contexto.

Sin embargo, comenta que debe tenerse en cuenta que en Chile existen plataformas como el “Rutificador”, que con el simple nombre o número de RUT permiten conocer el domicilio de una persona, lo que demuestra lo delicado de compartir estos datos.

La profesional recalca que la Ley N° 19.628 protege la intimidad reconociendo derechos como el acceso, rectificación, cancelación y oposición al tratamiento de datos personales. Además, impone a quienes manejan información el deber de secreto y la prohibición de usar los datos para fines distintos de los informados.

En caso de infracción, la persona puede recurrir a tribunales para obtener amparo e incluso reclamar indemnización. Astudillo advierte que la responsabilidad de resguardar los datos también recae en los usuarios. Dice que nunca se debe permitir que se fotografíen tarjetas de crédito por ambos lados, ya que ello puede facilitar fraudes o estafas.

La nueva ley amplía estos resguardos al regular principios como la minimización de datos, crear una agencia de protección de datos y establecer sanciones administrativas severas. Con ello, la defensa de la intimidad deja de depender solo de acciones judiciales y pasa a contar con un resguardo institucional más robusto, recalca.

Resguardo de empresas

La profesional también se refiere al tema a nivel de empresas y organismos públicos. Afirma que mientras siga vigente la Ley 19.628, estos deben cumplir con obligaciones como solicitar consentimiento informado, abstenerse de recolectar datos sensibles, salvo excepciones, y atender solicitudes de acceso, rectificación o eliminación.

Sin embargo, deben prepararse para el cambio que trae la nueva que exige una transformación más profunda.

Entre las medidas necesarias se encuentran la implementación de políticas internas de protección de datos, la capacitación permanente del personal, el reforzamiento de protocolos de seguridad y la creación de canales efectivos para que las personas puedan ejercer sus derechos. “Ya no bastará con guardar la información, sino que, será indispensable demostrar que se gestiona y protege activamente, bajo estándares modernos de privacidad y seguridad”, enfatiza.