¿Cotizar un “depa” te cuesta tus datos? Límites legales del uso de tu información personal

Aunque el usuario entrega su información de forma voluntaria al cotizar servicios o inmuebles, las empresas deben respetar principios como finalidad y proporcionalidad, bajo riesgo de sanción.

- Personas ya no darán datos de tarjetas para compras online, ¿qué se usará ahora?

¿Traerás un celular del extranjero en 2026? OSIPTEL advierte que podría bloquearse en 48 horas si no cumple este requisito | Foto: Freepik

Únete a nuestro canal

Newsletter Legal

Gerardo Rosales Diaz

17/04/2026 18H23

Cotizar un departamento, solicitar información sobre un servicio o incluso participar en una promoción digital se ha convertido en una práctica cotidiana.

En ese proceso, los usuarios suelen completar formularios donde consignan datos personales como nombre, número de teléfono, correo electrónico o incluso ingresos aproximados.

Aunque esta entrega se realiza de manera voluntaria, surgen preguntas clave: ¿hasta dónde pueden usar esa información las empresas? ¿Existe un límite legal? ¿Qué ocurre si luego la utilizan para otros fines?

- **LEA TAMBIÉN:** ¿Tus datos están seguros? Denuncias por uso indebido se multiplican por 20 en casi 10 años

CONSENTIMIENTO: REQUISITO INDISPENSABLE, PERO NO ILIMITADO

El tratamiento de datos personales se encuentra regulado por la Ley N.º 29733 y su reglamento, que establecen que toda recopilación debe contar con el consentimiento del titular.

Bruno Mejía, líder de Competencia y Mercados de EY Law, advierte que este consentimiento no es un *“cheque en blanco”*. *“No basta con que el usuario entregue sus datos. Su uso debe corresponder estrictamente al propósito para el cual fueron recabados”*, explica.

En la misma línea, Fabricio Sánchez Concha, socio de Benites, Vargas & Ugaz, precisa que el consentimiento debe cumplir condiciones estrictas: ser libre, previo, expreso, inequívoco e informado.

Esto implica que el usuario debe conocer quién tratará sus datos, con qué finalidad, por cuánto tiempo y si serán compartidos.

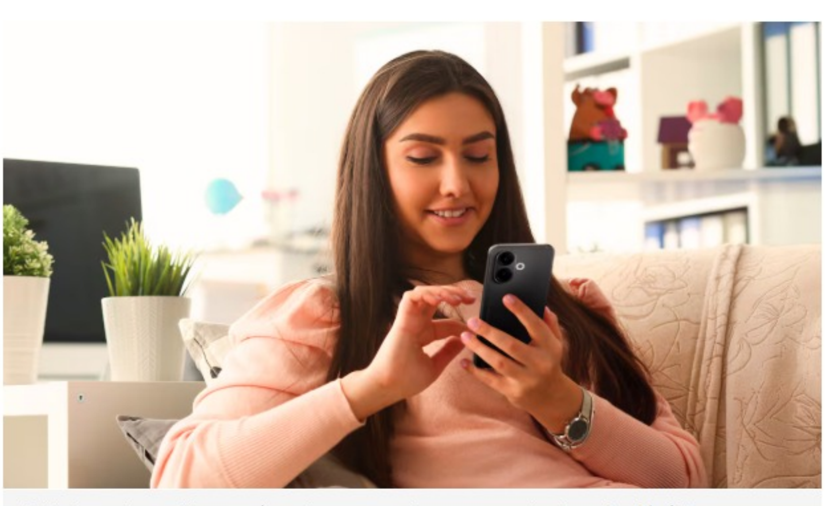
FINALIDAD: EL LÍMITE CENTRAL DEL USO DE DATOS

El principio de finalidad es el eje central de la regulación. Este establece que los datos solo pueden utilizarse para el propósito específico para el cual fueron recopilados.

Esto tiene una implicancia directa: **si un usuario llena un formulario para recibir una cotización, la empresa solo puede usar esos datos para enviar esa información o hacer seguimiento relacionado a esa solicitud.**

Sánchez Concha enfatiza que cualquier uso adicional —como incluir al usuario en campañas de marketing— requiere un consentimiento independiente. Mejía coincide en que extender el uso de los datos más allá de lo informado inicialmente constituye una vulneración directa de la normativa.

En la práctica, este principio busca evitar que las bases de datos se conviertan en activos comerciales reutilizables sin control.



Cuidado con lo que llenas: así pueden usar tus datos tras una simple cotización | Foto: Referencial

- **LEA TAMBIÉN:** Indecopi: presidente de entidad renuncia por “motivos personales”

PUBLICIDAD Y PRÁCTICAS INDEBIDAS

El uso de datos personales para fines publicitarios es uno de los puntos más sensibles. Aquí es donde muchas empresas incurren en errores.

El problema no es enviar publicidad en sí, sino hacerlo sin consentimiento válido. Sánchez Concha señala que prácticas como asumir que el usuario *“acepta”* por llenar el formulario, utilizar casillas pre-marcadas o incluir autorizaciones genéricas no cumplen con la ley.

Por su parte, Mejía advierte sobre el llamado *“consentimiento en bloque”*, que ocurre cuando una sola casilla autoriza múltiples usos (cotización + publicidad + cesión a terceros). Esta práctica impide que el consentimiento sea realmente libre y específico, por lo que puede ser sancionada.

En términos simples: recibir llamadas o correos después de una cotización no siempre es legal.

TRANSFERENCIA DE DATOS: CONDICIONADA A TRANSPARENCIA

Otro punto crítico es la transferencia de datos a terceros, como bancos, aseguradoras o aliados comerciales.

Ambos especialistas coinciden en que esta práctica solo es válida si el usuario ha sido informado previamente y ha dado su consentimiento específico. Esto implica que la empresa debe indicar claramente quién recibirá los datos y para qué.

Por ejemplo, una inmobiliaria no puede compartir datos con una entidad financiera para ofrecer créditos hipotecarios si el usuario no autorizó expresamente esa finalidad.

Este punto es clave porque muchas veces el usuario desconoce que su información puede circular más allá de la empresa con la que tuvo el primer contacto.

- **LEA TAMBIÉN:** Boom de contrataciones: solo la mitad de empresas está lista para gestionar talento con datos

PROPORCIONALIDAD: NO TODO DATO ES NECESARIO

La ley también exige que los datos solicitados sean adecuados y necesarios para la finalidad del servicio.

En una etapa inicial de cotización, lo razonable es pedir datos de contacto. Sin embargo, solicitar información como DNI, dirección exacta, estado civil o ingresos puede resultar excesivo si no hay una justificación clara.

Sánchez Concha advierte que recolectar datos desproporcionados puede constituir una infracción, mientras que Mejía señala que el nivel de información debe aumentar progresivamente conforme avance la relación comercial, no desde el primer contacto.

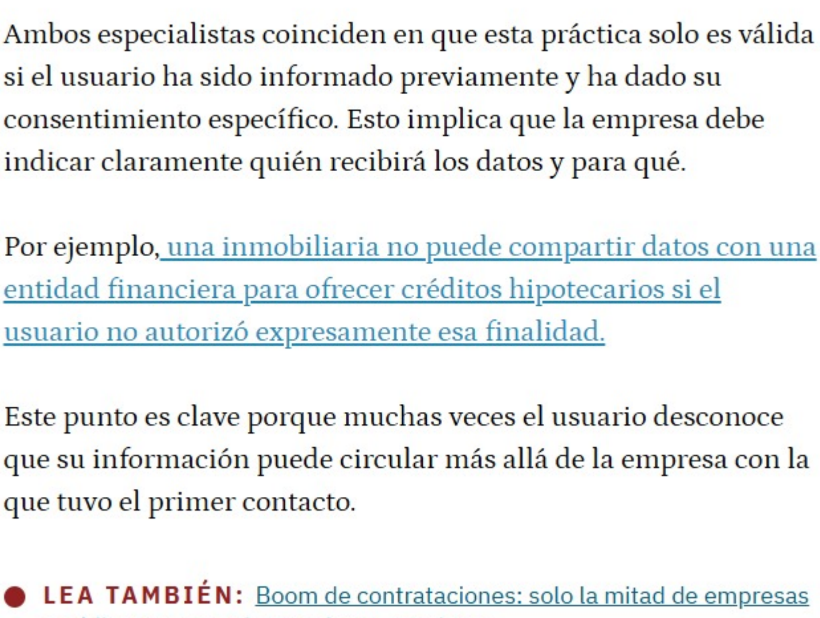
Este principio busca evitar la sobreexposición innecesaria de información personal.

PLAZO DE CONSERVACIÓN: NO INDEFINIDO

Un aspecto menos visible, pero relevante, es el tiempo durante el cual las empresas conservan los datos.

Mejía explica que la normativa no fija un plazo específico general, pero sí exige que este sea determinado, razonable y comunicado al usuario. En otras palabras, las empresas no pueden almacenar información indefinidamente.

En la práctica, esto significa que si una empresa informó que conservaría los datos por un periodo determinado —por ejemplo, dos años— no debería seguir utilizándolos pasado ese plazo.



Consentimiento y límites en el uso de datos personales | (Foto referencial: Freepik)

- **LEA TAMBIÉN:** Reportan caída global de Facebook: servicio está suspendido en cuentas personales y negocios

SANCIONES: DEL ÁMBITO ADMINISTRATIVO AL PENAL

El incumplimiento de estas reglas puede generar consecuencias importantes.

Sánchez Concha explica que las sanciones administrativas pueden alcanzar hasta 100 UIT, dependiendo de si la infracción es leve, grave o muy grave. Esto incluye casos como solicitar datos innecesarios o tratar información sin consentimiento.

Por su parte, Mejía advierte que **el marco legal ha evolucionado hacia un enfoque más severo, incorporando incluso sanciones penales para casos como la comercialización o posesión indebida de bases de datos personales.**

Esto eleva significativamente el riesgo para las empresas que no cumplen la normativa.

DERECHOS DEL USUARIO: CONTROL SOBRE SU INFORMACIÓN

Finalmente, los usuarios no están desprotegidos. La normativa reconoce los derechos ARCO: acceso, rectificación, cancelación y oposición.

Esto permite al usuario saber qué datos tiene una empresa, corregirlos, eliminarlos o impedir su uso para determinados fines. Además, puede revocar su consentimiento en cualquier momento.

Si la empresa no responde o incumple, el usuario puede acudir a la Autoridad Nacional de Protección de Datos Personales o incluso a la vía judicial para reclamar una indemnización.

- **LEA TAMBIÉN:** Clientes de 4 bancos grandes ganarán poder al compartir datos, ¿quiénes se beneficiarán más?

SOBRE EL AUTOR

Gerardo Rosales Diaz

Abogado especialista encargado de Enfoque Legal en Diario Gestión - Actualmente, ocupa la posición de analista legal en el área de Economía en el Diario Gestión.

ÚLTIMAS NOTICIAS

EE.UU. abre portal para reembolso de aranceles aduaneros

Elecciones 2026: Lo que está en juego en Perú

Presupuesto “dormido”: 1,442 distritos no han usado ni la cuarta parte de...

Jorge Nieto: “La ONPE ha roto la legitimidad del proceso electoral”

Omar Mariluz: “Fuera Piero Corvetto”