PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

Fundamentos Para el Tratamiento de Datos Personales

Fundamentos Para el Tratamiento de Datos Personales

El responsable o el encargado del tratamiento de datos deben identificar el fundamento legal que autoriza dicho tratamiento.

Las bases jurídicas para el tratamiento de datos personales deben ser limitadas y estar claramente expresadas en la legislación (es decir, no deben ser fundamentos vagos o amplios, ni una lista abierta de posibles fundamentos de procesamiento). Sin embargo, suele suceder con demasiada frecuencia que las leyes contemplan muchas bases jurídicas.

Entre las bases que pueden aparecer en la legislación se incluyen las siguientes:

- consentimiento del interesado
- garantía de la necesidad del tratamiento para la ejecución de un contrato con el interesado, o para adoptar medidas para celebrar un contrato
- para el cumplimiento de una obligación legal
- para proteger los intereses vitales de un interesado o alguna otra persona;
- para el desempeño de una tarea llevada a cabo en interés público o en el ejercicio de una autoridad oficial, conferida al responsable del tratamiento
- para los fines de intereses legítimos perseguidos por el responsable del tratamiento o terceros, excepto cuando los intereses, los derechos y las libertades del interesado prevalezcan sobre dichos intereses.

A continuación, describimos algunas de estas bases.

Consentimiento

El consentimiento es un principio fundamental de la protección de datos porque permite que el interesado controle cuándo sus datos personales serán sometidos a un tratamiento: se relaciona con el ejercicio de derechos fundamentales de autonomía y autodeterminación.

El consentimiento debe otorgarse de voluntad libre, ser específico, informado y carecer de ambigüedades. Puede ser una declaración por escrito, incluidos medios electrónicos. Debe ser explícito y requerir un proceso activo de la persona, en

lugar de un proceso pasivo de exclusión: como tal, requiere una acción positiva afirmativa. La entidad que trata los datos debe poder demostrar que ha solicitado y recibido el consentimiento.

El consentimiento no es el único fundamento legal para el tratamiento. De hecho, en muchas situaciones de desequilibrio de poder entre la persona y el encargado del tratamiento (por ej. entre un empleado y un empleador), el consentimiento no puede otorgarse de voluntad libre y, por lo tanto, otro fundamento legal debe justificar el tratamiento de los datos personales (por ej. la celebración de un contrato).

Explícito, de voluntad libre y sin ambigüedades

La definición de consentimiento debe reflejar la elección libre e informada de una persona. Por ejemplo, el RGPD incluye la siguiente definición:

> **“el ‘consentimiento’ del interesado hace referencia a toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.”**

Exenciones para Instituciones Públicas

En algunas jurisdicciones, no se requiere notificación ni consentimiento cuando el tratamiento está a cargo de una institución pública durante el ejercicio de sus funciones legales. Este es el caso de Colombia que, en el artículo 10 (a) de la Ley 1581 de 2012, regula el tratamiento y la gestión de la información personal.

Es fundamental que dicho tratamiento esté sometido a medidas adecuadas y específicas para proteger los derechos y las libertadas de las personas.

Consentimiento implícito

Es posible que algunos textos incluyan el concepto de consentimiento implícito. Este fue el caso en el proyecto de ley propuesto para la enmienda de la legislación de protección de datos en Argentina.

Privacy International no cree que el consentimiento "implícito" cumpla con los estándares de un consentimiento específico, de voluntad libre, informado y sin ambigüedades.

El Grupo de trabajo del artículo 29 (el grupo de autoridades europeas de protección de datos) ha estudiado la temática del consentimiento, y en particular el consentimiento implícito, y concluyó que este último "no era apto según el estándar de consentimiento establecido por el RGPD".[1]

Se debe prestar particular atención a dicha disposición para garantizar que exista una guía y condiciones claras sobre los contextos en los que el consentimiento implícito sería suficiente.

Revocación del consentimiento

Los interesados deben tener el derecho a revocar su consentimiento en cualquier momento. Antes de recoger datos, el responsable del tratamiento debe tener la obligación de informar al interesado (en un momento anterior a obtener el consentimiento) de su derecho a revocar el consentimiento. Esta disposición debe además establecer que cualquier revocación de consentimiento dará lugar a la eliminación de los datos personales. El proceso de revocación debe ser un proceso tan sencillo como su otorgamiento. El responsable del tratamiento debe realizar una acción positiva para confirmar a la persona que su solicitud ha sido procesada, su consentimiento revocado y sus datos eliminados.

El hecho de contar con el consentimiento no debe anular la obligación que tienen los responsables del tratamiento de cumplir con los principios de protección de datos, incluidos el de transparencia, lealtad, limitación de finalidad y minimización de datos. Incluso si se cuenta con el consentimiento, los responsables del tratamiento deben considerar cuidadosamente (por ejemplo, mediante una evaluación de impacto de la protección de los datos) cualquier perjuicio a los derechos de las personas como resultado del tratamiento, y tomar las medidas necesarias para mitigarlos.

Interés Público

Otro fundamento legal que suele reconocerse en la legislación de protección de datos es la necesidad del tratamiento de los datos personales si el responsable lo emprende en interés público.

Una consideración fundamental aquí es que es posible que la legislación de protección de datos no defina qué constituye el "interés público" y, en cambio, delegue esa determinación a quienes traten los datos o a la autoridad a cargo de la protección de los datos. La ausencia de una definición y la falta de claridad en torno a lo que constituye el "interés público", así como su interpretación frecuentemente amplia, generan la inquietud de que este fundamento actúe como un vacío jurídico. El fundamento de interés público debe estar definido claramente para evitar abusos. Por ejemplo, debe ser posible enumerar los fundamentos específicos en interés público (por ej. la administración de justicia) y garantizar que dicha lista sea clara y exhaustiva.

Si existirá una condición que permitirá el tratamiento de datos en situaciones de emergencia, dicha condición debe considerarse y definirse con sumo cuidado y detalle. Todas las bases jurídicas para el tratamiento de datos deben someterse a otras salvaguardas para proteger los derechos y los intereses del interesado, incluyendo la lealtad, la transparencia y una evaluación del impacto de la protección de datos, que claramente tome en cuenta cualquier perjuicio o efecto adverso para las personas.

Por lo tanto, entre las recomendaciones para la autoridad de protección de datos se podrían incluir las siguientes:

- Realizar un mapa de la legislación con disposiciones de "interés público" para clarificar qué se incluiría
- Solicitar que la autoridad de control independiente elabore una guía adicional y realice una prueba del fundamento legal de "interés público"
- Solicitar que las autoridades públicas expliquen claramente qué consideran que constituye el interés público
- Si se aplicará para permitir el tratamiento de datos personales sensibles, la autoridad de control independiente debe definir con antelación el umbral más elevado de "interés público" que debe cumplirse antes de que los datos personales sensibles puedan ser tratados sin consentimiento o algún otro fundamento legal.

Interés legítimo

Con frecuencia, los marcos de protección establecerán que, si el responsable del tratamiento de datos puede demostrar un interés legítimo, entonces dicho interés constituye un fundamento legal para dicho tratamiento. Dado el amplio alcance del término "interés legítimo", es fundamental que se especifique esta condición. Por ejemplo, el responsable del tratamiento debe también demostrar que: el tratamiento es necesario y proporcional para el interés legítimo perseguido y que no invalida los derechos del interesado.

Esta condición puede interpretarse ampliamente y da lugar a abusos. De ser posible, se debe evitar su inclusión en la legislación.

Si se incluye esta disposición y no existen dudas, en el ejercicio de equilibrios, de que existe un perjuicio para la persona, entonces la presunción será que el tratamiento no debe continuarse. Asimismo, es imperativo que los responsables del tratamiento notifiquen claramente a las personas sobre el interés legítimo específico en el que se están basando (es decir, no pueden sencillamente basarse en un interés legítimo genérico o vago), y que realicen una evaluación del perjuicio a las personas caso por caso, incluido un mecanismo de inclusión.

No todas las bases jurídicas están disponibles para todos los responsables del tratamiento. Por ejemplo, la capacidad de recurrir a una justificación de interés legítimo ha sido restringida para las autoridades públicas en el RGPD. Esto significa que las autoridades públicas no pueden basarse en esta justificación cuando el tratamiento se realiza durante el desempeño de sus funciones. Por el contrario, las autoridades deberán identificar el interés público y la función estatutaria o la tarea pública relevante.

Tratamiento de Datos Personales Sensibles

En el caso del tratamiento de datos personales sensibles, se deben cumplir condiciones adicionales. Las situaciones en las que el tratamiento de datos personales sensibles está permitido deben ser limitadas. Si se recurre al consentimiento para justificar el tratamiento de datos personales sensibles, es extremadamente importante que sea explícito y que cumpla con todos los requisitos antes mencionados (es decir, que sea informado, de voluntad libre y específico).

Para fortalecer el principio de limitación de finalidad (estipulado en otra sección de la legislación), la disposición sobre los datos personales sensibles debe reafirmar que dichos datos no pueden recibir un tratamiento adicional para otros fines, o por parte de terceros que no estén identificados en la legislación.

También es importante que se proporcione la protección más elevada a los datos que revelan datos personales sensibles mediante la elaboración de perfiles y el

uso de información proxy (los encargados del tratamiento de los datos pueden inferir, derivar y predecir datos personales sensibles sin que estos hayan sido proporcionados explícitamente).

Las condiciones para el tratamiento de datos personales sensibles deben ser limitadas, y se debe prestar especial atención en el caso de que se propongan condiciones como la de "datos personales que el interesado ha hecho manifiestamente públicos" (artículo 9 del RGPD). Este enfoque da lugar a preguntas como: ¿qué significa "hacer públicos"? ¿Cómo puede verificarse que una persona los ha hecho públicos? Además, es importante destacar que si una persona ha hecho públicos los datos, ¿significa eso que los datos pueden ser utilizados por cualquier otra persona para cualquier finalidad?

Esto resulta particularmente relevante a la luz de los desarrollos recientes: el avance del movimiento de datos abiertos y las leyes de transparencia pública significan que existe una cantidad creciente de bases de datos y otros registros (es decir, registros de propiedad, registros fiscales o bases de datos electorales) que conservan datos personales. El hecho de que dichos datos hayan sido hecho públicos (por motivos de interés público, transparencia y responsabilidad) no significa que los datos conservados puedan ser utilizados para fines distintos de los que se definieron al momento de su recogida.

Asimismo, ha sido una inquietud permanente de Privacy International el uso de la Social Media Intelligence (SOCMINT) como técnica aplicada por parte de las fuerzas, los cuerpos de seguridad y otras agencias, que se está replicando en todo el mundo. Se sostiene que, sin estar sujeto a ninguna reglamentación, autorización judicial o control independiente, el uso de estos datos es legal porque no interfiere con el derecho a la privacidad, y que depende únicamente de los así llamados datos "disponibles públicamente". Nosotros rechazamos este argumento. El tratamiento de datos "públicamente disponibles" en las plataformas de redes sociales tiene consecuencias claras y graves para la privacidad de las personas. El hecho de que los datos estén públicamente disponibles no justifica su recogida, conservación, análisis o cualquier otra forma de tratamiento sin regulación ni control.[2]

El tratamiento de datos personales para fines científicos, históricos o estadísticos

En algunas ocasiones, se suele aclarar en los marcos de protección de datos que el tratamiento de datos personales con fines científicos, históricos o estadísticos podría ser un fundamento legal legítimo.

Para evitar abusos e interpretaciones amplias de este fundamento legal:

- Es necesario aclarar qué constituye la finalidad estadística y científica. Se deben incluir más detalles en la legislación, o se deben elaborar orientaciones para definir mejor este concepto.
- Dicho fundamento legal no debe eximir al responsable o el encargado del tratamiento de todas sus obligaciones, y se deberán proporcionar salvaguardas adecuadas para el tratamiento de datos personales para estos fines.
- Una de las salvaguardas podría garantizar que los datos no se usarán para tomar decisiones sobre las personas, y que el tratamiento se prohibirá si fuera motivo de perjuicios.
- El interesado debe seguir teniendo los derechos sobre sus datos, incluido el derecho a ser informado y el derecho a objetar que sus datos se traten para estos fines.

El tratamiento de datos personales y la libertad de expresión y de acceder a la información

El Estado debe tomar las medidas necesarias para reconciliar el derecho a la protección de datos personales con el derecho a la libertad de expresión y de acceder a la información. Esto puede incluir el tratamiento para fines periodísticos y de derechos humanos, y fines académicos, artísticos o de expresión literaria. Al momento de encontrar un equilibrio de estos dos derechos, es posible que existan exenciones y derogaciones de las obligaciones y los derechos de los interesados.

Para fines periodísticos, podría aplicarse una exención en la medida en que sea necesario para 1) proteger el derecho a ejercer el derecho fundamental a la libertad de expresión y opinión para fines periodísticos y 2) para proteger las fuentes. Asimismo, recomendamos que una disposición de este estilo incluya otros ejercicios legítimos del derecho a la libertad de expresión, como es el caso de las investigaciones llevadas a cabo por organizaciones independientes no gubernamentales.

Referencias

1 Grupo de trabajo del artículo 29, Directrices sobre el consentimiento en virtud de la reglamentación 2016/769, adoptada el 28 de noviembre de 2017, según su última revisión y entrada en vigor el 10 de abril de 2018, pp. 30. Disponible en http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

2 Para obtener más información, consulte el documento explicativo de Privacy International, disponible en https://privacyinternational.org/explainer/55/social-media-intelligence

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471