PROGRAMAS DE CONTACT TRACING: RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA

1. INTRODUCCIÓN

- **Régimen de Protección de Datos Personales.**

La protección de datos personales está prevista en el art. 43 de la Constitución Nacional y se encuentra regulada principalmente en la Ley de Protección de Datos Personales N° 25.326 (en adelante, "LPDP"), su Decreto Reglamentario 1558/2001 y toda normativa que ha ido dictando la autoridad de control - hoy la Agencia de Acceso a la Información Pública ("AAIP") -. Este régimen tiene por objeto proteger los datos personales de sus titulares y regular los derechos de habeas data construccionalmente reconocidos.

- **Definición de datos personales y datos de salud/sensibles. (en principio está prohibida la recolección de datos sensibles).**

La LPDP prevé definiciones específicas. Así, comienza definiendo "dato personal" como "*información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"* y "dato sensible" como aquel que revela origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Esta última categoría de datos -que comprende los datos de salud se encuentran especialmente regulados por la LPDP, consagrándoles una protección agravada en base al potencial perjuicio que su tratamiento ilegitimo o inadecuado puede ocasionarle a la persona.

En relación al concepto de tratamiento de datos, la LPDP pretende comprender bajo su definición todas las operaciones que se realicen con los datos personales, así define tratamiento como "*Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones,*

consultas, interconexiones o transferencias".

- **Toda información referida a la ubicación de una persona y/o sus desplazamientos constituye un dato personal.**

Los datos de ubicación de una persona se encuentran alcanzados por la definición de datos personales prevista en la norma. Por ejemplo, este tipo de información pueden recolectarse de: la red o servicio utilizado por el teléfono; sistema de posicionamiento global ("GPS"); torres de celda (operadores móviles); redes wifi; y Bluetooth.

En relación con este punto la AAIP se ha expido en cuanto a que la LPDP no será aplicable siempre que los datos de ubicación se encuentren disociados. En tal caso, podrían los responsables realizar tratamiento que implique monitoreo de datos disociados.

- **Datos personales respecto del contacto con terceras personas**

La información declarada por un titular de datos acerca de las personas con las que esta tuvo contacto son datos personales en los términos de la LPDP, pero no quedarán comprendidos bajo el concepto de datos de ubicación ni de datos de salud o sensibles en la medida que no se proporcionen datos comprendidos bajo esa categoría.

2. CONTACT TRACING o TRACKING

Existe una sutil diferencia entre **contact tracing y contact tracking***,* siendo el primer supuesto el que refiere a la reconstrucción de los puntos de contacto y el segundo al seguimiento constante de la persona. En términos de privacidad el primero sería el menos invasivo y respetuoso de los derechos individuales.

La tecnología que refiere al tracking implica conocer la ubicación de las personas en forma constante mientras que el **tracing** puede conseguirse por medios analógicos como puede ser la declaración de contactos por las personas que sería menos invasivo que el primer supuesto.

Para el caso de utilización de tecnologías que impliquen geolocalización, la AAIP emitió

una guía especifica que se encuentra disponible en su sitio oficial y que pretende brindar lineamientos para la utilización de esta tecnología que potencialmente podría afectar el derecho a la privacidad de las personas[1][1].

Entendemos que las iniciativas locales pretenderían aplicar procesos y herramientas de contact tracing que no tratarían de forma automatizada, por ejemplo, datos de GPS.

3. CONSENTIMIENTO

En principio **la base legal para el tratamiento legítimo de los datos personales es el consentimiento** expreso e informado en los términos de la LPDP. La norma requiere que el titular sea previamente informado acerca de las finalidades, cesionarios, sus derechos entre otros puntos desarrollados en el apartado correspondiente al derecho de información de este documento. El consentimiento -en principio- es lo que circunscribe las aplicaciones y lo que se podrá realizar con el dato recolectado y cabe mencionar que **puede ser revocado** por el titular del dato a quien se le deberá informar acerca del procedimiento para ejercer tal derecho.

En el supuesto en el que se traten o recolecten **datos de salud** (comprendidos bajo la categoría de datos sensibles), se deberá tener en cuenta que en principio, la LPDP prohíbe su recolección y tratamiento (art. 7 LPDP) y establece que nadie puede ser obligado a proveer datos sensibles (art. 7.1. LPDP). Asimismo, la Ley de Salud Pública N.o 26.529 también requiere el consentimiento del titular (art. 4). Además, l**a LPDP establece que los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley** (art. 7.2. LPDP).

No obstante ello, **la LPDP habilita tratar datos de sensibles con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares (art. 7.2 LPDP) y a los profesionales de la salud, los establecimientos sanitarios y autoridades de salud a los efectos del tratamiento de los pacientes y siempre que se respete el secreto profesional.** Así, por ejemplo, un hospital está autorizado a recolectar datos de un paciente de coronavirus sin su consentimiento expreso a los efectos de su tratamiento clínico, pero deberá requerir su autorización en caso de que

[1] La Guía para el Tratamiento de los Datos Personales en el Uso de Herramientas de Geolocalización se encuentra disponible en el siguiente enlace: https://www.argentina.gob.ar/sites/default/files/guia_geolocalizacion_0.pdf

pretenda divulgar el nombre de tal paciente o utilizar los datos para una finalidad distinta a la del tratamiento clínico.

Sin perjuicio de la regla del requerimiento del consentimiento para el tratamiento legítimo, la LPDP prevé las siguientes excepciones al mismo:

- Los datos se obtengan de fuentes de acceso público irrestricto;

- Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal. Este sería el supuesto de los Hospitales Públicos y los distintos Ministerios de Salud que se encuentran facultados a recolectar datos de pacientes a los que asisten -sean casos confirmados o potenciales casos de infectados-;

- Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

Resulta pertinente destacar que estas excepciones al consentimiento también valdrán para los supuestos de cesión de datos (la que en principio debe ser consentida por el titular). Así, por ejemplo, en el caso de datos de salud recolectados por el Ministerio de Salud de la Nación se entiende que este podría cederlos sin requerir el consentimiento de su titular a Ministerios de Salud Provinciales en base a la competencia de estos y siempre que tal cesión se corresponda con los criterios de necesidad y finalidad[2].

Por último, y siguiendo este marco normativo, el Gobierno Nacional emitió la Decisión Administrativa 431/2020 que habilita el intercambio de información entre sus dependencias[3] y legitima así por ejemplo el intercambio de información entre la Dirección Nacional de Migraciones y el Ministerio Salud acerca de quienes hayan ingresado al país y provengan de países o territorios considerados endémicos a los efectos de monitorear un potencial caso o asegurar el cumplimiento de la cuarentena obligatoria.

---

[2] A esta conclusión ha llegado también la AAIP que expone su criterio en la Guía para el tratamiento de los datos personales ante el Coronavirus Covid-19 disponible en su sitio web oficial: https://www.argentina.gob.ar/sites/default/files/guia_coronavirus_0.pdf .

[3] A través de la Decisión Administrativa 431/2020, se ha habilitado la cesión de los datos e información entre dependencias de la Administración Pública con el único fin de realizar acciones útiles para la protección de la salud pública, durante la vigencia de la emergencia en materia sanitaria por coronavirus COVID-19. del cedente y del cesionario, y en principio con el previo consentimiento del titular de los datos, al que se le deberá informar sobre la finalidad de la cesión e identificar al cesionario

4. DISOCIACIÓN

La disociación consiste en una operación que permite que la información obtenida no pueda asociarse a persona determinada o determinable. Este procedimiento implica más que sólo borrar nombre y apellido. La disociación debe ser definitiva e irreversible, es decir que no pueda conseguirse identificar a la persona titular de estos datos a los que se les aplico un mecanismo de disociación.

En virtud del artículo 7.2. y 11.3. de la LPDP, este proceso de disociación debiera aplicarse siempre que se pretenda ceder datos de pacientes con fines estadísticos o científicos.

La AAIP aprobó criterios orientadores de aplicación de la LPDP a través de la Resolución 4/2019 y explicitó que no será considerada persona determinable en los términos de la LPDP – y en consecuencia quedará fuera del ámbito de aplicación de la LPDP - cuando el procedimiento que deba aplicarse para lograr su identificación requiera la aplicación de medidas o plazos desproporcionados o inviables.

5. CESIÓN

La cesión de datos personales se encuentra regulada específicamente bajo la LPDP que entiende este concepto en un sentido amplio, abarcando así la revelación -aún de forma temporal- o envío de datos a una persona distinta del titular de los datos personales.

En relación con este punto, la LPDP establece que los datos personales sólo podrían ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo

Sin perjuicio de lo anterior, la LPDP distingue el supuesto en el que los datos son transferidos a un tercero a los efectos de la prestación de un servicio de procesamiento (transferencias de tipo C2P o “Controller to Processor”) y regula en particular los requerimientos que deben cumplirse en este caso. Un típico ejemplo de procesamiento de datos por parte de un tercero se da cuando un responsable de tratamiento delega en un tercero el alojamiento de dichos datos o cuando se solicita al tercero que recolecte la información (como el caso de los censistas). Ante estos supuestos, la norma establece la obligación de celebrar un contrato por escrito con dicho tercero, en el cual se incluyan

ciertas cláusulas específicas.

La transferencia de datos internacionales se encuentra estrictamente regulada por la LDPD. En tal sentido, se establece que la trasferencia a países que no proporcionen niveles de protección adecuados se encuentra en principio prohibida. No obstante lo antedicho, la normativa establece que la transferencia a países con niveles inferiores de protección de datos podrá realizarse si se da alguno de los siguientes supuestos: (i) el titular del dato consiente expresamente dicha transferencia; (ii) los niveles adecuados de protección emanan de cláusulas contractuales; o (iii) de sistemas de autorregulación.

6. PRINCIPIO DE CALIDAD DEL DATO O MINIMIZACIÓN

La LPDP prevé una serie de principios para el tratamiento legítimo de datos personales, uno de ellos es el **principio de calidad de los datos o de minimización**. Este ordena a que los responsables solo recolecten y traten aquellos datos personales estrictamente necesarios para la finalidad que se pretende y durante el plazo que esta finalidad así lo justifique. En términos prácticos esto se traduce en lo siguiente:

- Los **datos personales que se recojan deben ser ciertos, adecuados, pertinentes y no excesivos** en relación con la finalidad. Por ejemplo, en el caso de procesos de *Contact tracing* implementadas a los efectos de prevenir y contener los contagios de COVID-19, no debería recolectarse aquellos datos que invadan la privacidad de los titulares y no sean necesarios a tal fin en un sentido estricto.

- La **recolección de datos no puede hacerse por medios desleales, fraudulentos o de forma contraria a la LDPD**. Es decir, que la información del tratamiento debe ser clara y transparente para el titular.

- Los datos personales recolectados **no podrán aplicarse a un fin distinto del que motivó su recolección**. Por ejemplo, los datos recolectados en el marco de programas que pretendan mitigar los efectos de la pandemia no podrán utilizarse con fines distintos a estos.

- Los **datos deben ser exactos y actualizarse en el caso de que sea aplicable**. En el supuesto en el que se detectara datos erróneos o inexactos deberán suprimirse.

- Los datos deben ser almacenados y procesados de forma tal que se **garanticen los derechos de acceso, rectificación y supresión de los titulares.**

- Los datos deberán ser **conservados mientras sean útiles para la finalidad que originó su recolección y deberán suprimirse cuando esta devenga abstracta**. En el caso de programas implementados para mitigar efectos de la pandemia por COVID-19, los datos recolectados en su consecuencia deberán eliminarse cuando esta pandemia haya pasado.

7. DERECHO DE LOS TITULARES

DERECHO A SER INFORMADO

La LPDP establece obligaciones de información estrictas para los responsables. El titular del dato debe tener a su alcance la información en relación con las finalidades, procesos y flujos de datos a la que será sometida sus datos recolectados. Resumidamente, se deberá informar y contestar los siguientes interrogantes al momento de tratar los datos -incluyendo la recolección-:

- ¿**Para qué** fines se recolecta la información?

- ¿**Quiénes** podrían acceder a la información a quienes se les compartirá o cederá la información?

- ¿Es **obligatorio proveer los datos personales**? ¿**qué consecuencias** tendría no proporcionarlos o proporcionar datos inexactos?

- Además, se debe informar acerca del **registro de la base de datos y de los derechos de acceso, rectificación y supresión de los datos**.

DERECHO DE ACCESO

El titular de los datos, previa acreditación de su identidad tiene **derecho a solicitar y obtener información de sus datos personales**. Por su parte el responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido

intimado fehacientemente.

DERECHO A REQUERIR LA RECTIFICACIÓN, ACTUALIZACIÓN Y SUPRESIÓN DE LOS DATOS PERSONALES

El titular podrá pedir la **rectificación, supresión o actualización de los datos personales** y el responsable deberá cumplir con ello -en caso de ser procedente- en el plazo máximo de cinco días hábiles de recibido. Es dable destacar que existirán supuestos en las que el responsable podría válidamente oponerse a tales requerimientos, por ejemplo, la supresión no procederá cuando pudiese causar perjuicios a derechos o intereses legítimos como puede ser el caso que una norma requiera la conservación de la información.

DEBER DE SECRETO /CONFIDENCIALIDAD

La LPDP prescribe que tanto el responsable del tratamiento como todas las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al guardar secreto profesional respecto de estos. Esta obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

En virtud de esta obligación, se entiende que **todas las personas involucradas en el procesamiento o tratamiento de datos personales deberán estar sujetas a regímenes de confidencialidad.**

Sin perjuicio de lo anterior, la misma LPDP seguidamente establece que el deber de guardar confidencialidad cederá en caso de orden judicial o cuando mediaran razones de seguridad pública, defensa nacional o salud pública.

9. DEBER DE SEGURIDAD

La LPDP prohíbe almacenar datos en bases de datos que no garanticen niveles de seguridad e integridad (art.9 LPDP) y en la misma línea obliga a los responsables a adoptar medidas técnicas y organizativas que garanticen la confidencialidad y seguridad

de los datos personales de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado. Asimismo, estas medidas deberán permitir detectar desviaciones intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

La AAIP ha emitido a través de la Resolución 47/2018 medida de seguridad recomendadas para el cumplimiento de esta obligación. Los lineamientos previstos en esta Resolución contienen recomendaciones para el tratamiento de datos personales en medios informatizados y analógico, reforzando medidas en caso de tratamientos de datos sensibles.

10. EVALUACIÓN DE IMPACTO

Las evaluaciones de impacto a la privacidad no resultan obligatorias bajo la actual redacción de la LPDP. No obstante ello, la AAIP ha incluido este tipo de procedimientos previos como deseables y fuertemente recomendables de implementar antes de lanzar aplicaciones o procesos que impliquen tratamientos de datos personales[4]. Lo anterior, toda vez que se entiende que una evaluación de impacto ayuda a identificar y mitigar riesgos asociados a la privacidad, al mismo tiempo que colabora en el diseño de procedimientos, sistemas o proyectos respetuosos de los derechos de los titulares de datos y de la normativa aplicable. Además, la evaluación de impacto y atender a la privacidad desde el diseño ahorraría costosas revisiones o readecuaciones ex - post.

La AAIP ha emitido junto con la Autoridad de Control de la República de Uruguay una Guía de Impacto en el Tratamiento de Datos Personales disponible al público que sirve a los efectos de diseñar e implementar este proceso de evaluación en miras de procurar el cumplimiento de la LPDP[4].

11. SANCIONES

El incumplimiento al régimen de protección de datos personales puede derivar en sanciones administrativas, penales y/o a demandas por daños civiles.

[4] Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones aprobada por la Disposición 18/2015 y la Guía para el tratamiento de los datos personales en el uso de herramientas de geolocalización disponible en:
https://www.argentina.gob.ar/sites/default/files/guia_geolocalizacion_0.pdf

• SANCIONES ADMINISTRATIVAS: Apercibimiento, suspensión, clausura o cancelación de la base de datos; y Multas desde $1.000 a $100.000, dependiendo de la naturaleza de la infracción, las que pueden acumularse hasta $ 5.000.000 (pesos cinco millones).

• SANCIONES PENALES: La LPDP introdujo los delitos regulados bajo el art. 117 y 157 bis del Código Penal. Este tipo penal refiere a la acción de insertar o ceder datos falsos; al acceso ilegítimo, de cualquier forma, a un banco de datos personales; y a la revelación a otro de información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar.

• CONSECUENCIAS CIVILES: En el supuesto en el que el incumplimiento al régimen de protección de datos personales ocasione daños a los titulares de los datos. Además, la LPDP reglamenta la acción judicial de protección de los datos personales o habeas data a fin de ejercer los derechos reconocido en este régimen.

12. CHECK LIST

En conclusión, previo a implementar programas que impliquen recolección y tratamiento de datos personales, deberán analizarse los siguientes aspectos:

Evaluación de Impacto a la Protección de Datos Personales	A fin de garantizar desde el diseño la implementación de programas y proyectos respetuosos de los derechos a la privacidad y a la normativa vigente.
Si se involucran aplicaciones o software	Tener en cuenta para su desarrollo los lineamientos previstos por la Disposición 18/2015
Consentimiento	El tratamiento se debe basar en el consentimiento o en su defecto en una de las excepciones a este previstas por la LPDP. Debe darse por escrito y en los términos de la LPDP
Registrar las bases de datos personales	El registro de la base de datos ante la Agencia de Acceso a la Información Pública es declarativo y requisito para el tratamiento legítimo.
Calidad de Datos	Ciertos, adecuados, pertinentes, exactos y no excesivos

(principio de minimización)	No pueden ser utilizados para finalidades distintas o incompatibles Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes
Confidencialidad	El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de estos.
Cesión	En principio, sólo con consentimiento del titular y para el cumplimiento de los fines del interés legítimo del cedente y del cesionario. La cesión para prestación de servicios (ej.: alojamiento de datos) y la transferencia internacional está especialmente regulada. En principio, estará prohibida la transferencia a países que no garanticen legislación adecuada
Seguridad	Medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales. Resolución 47/2018 de la Agencia de Acceso a la Información Pública

Tener en cuenta que este documento no es exhaustivo y que tiene como objeto solamente informar acerca de los principios generales que rigen la materia en Argentina