Luego de más de VEINTE (20) años el ESTADO NACIONAL requiere actualizar su normativa en pos del fortalecimiento de las capacidades estatales de regulación y gestión de políticas públicas con el objetivo de dar respuesta a los nuevos desafíos que imponen las transformaciones tecnológicas y el desarrollo de la economía digital y, a su vez, armonizar con los estándares regionales e internacionales, desde un enfoque de Derechos Humanos y desde una mirada situada y soberana.

TRES (3) pilares: i) el derecho humano a la protección de los datos personales y la autodeterminación informativa, ii) la innovación tecnológica –basada en principios éticos– que promueva un desarrollo económico inclusivo y iii) la construcción de confianza a través de reglas de juego claras.

Capítulo 1 las Disposiciones Generales, donde se incluye el objeto de la ley (artículo 1º) y una serie de definiciones (artículo 2°) que amplían el universo conceptual de la vigente Ley N° 25.326 y su modificatoria. En los artículos 3° y 4° se establecen el ámbito de aplicación material y territorial, respectivamente. Aquí es importante resaltar la incorporación del principio de extraterritorialidad que establece que la normativa se aplicará en distintos supuestos, aun cuando los Responsables de tratamiento de datos no se encuentren en territorio nacional.

En el Capítulo 2 del Proyecto de Ley que se impulsa se instituyen los principios que se deben respetar para el adecuado tratamiento de los datos personales (artículos 6º a 12 y 20). Se enumeran el principio de licitud, lealtad y transparencia y los principios de finalidad; de minimización de datos; el de exactitud; de preeminencia; de responsabilidad proactiva y demostrada y el de seguridad de los datos personales.

El Capítulo 3 del Proyecto de Ley refiere a las transferencias internacionales y en sus artículos 23, 24, 25 y 26 establece TRES (3) mecanismos con distinto nivel de jerarquía para realizar el flujo transfronterizo de datos personales con confianza. Se refiere a transferencias basadas en: una decisión de adecuación; mecanismos que permitan ofrecer las garantías adecuadas o excepciones, que deben darse bajo ciertas condiciones y no pueden utilizarse de manera periódica o habitual.

El Capítulo 4 de la propuesta cuya sanción se propicia incluye los derechos de los titulares de los datos .El proyecto, además, incorpora el derecho a limitación y el derecho sobre las decisiones automatizadas y la elaboración de perfiles.

El Capítulo 5 prevé las obligaciones del Responsable y Encargado de tratamiento, allí se establecen las medidas para el cumplimiento de la responsabilidad proactiva y se incorporan la figura del Delegado de Protección de Datos (Artículo 44), la evaluación de impacto relativa a la protección de datos (Artículo 41) y los mecanismos de regulación vinculantes (Artículo 48).

Asimismo, la iniciativa incorpora, en el artículo 46, la figura del Representante para aquellos Responsables y Encargados que no estén establecidos en la REPÚBLICA ARGENTINA

Los Capítulos 7 y 8 : Autoridad de Aplicación y procedimientos y sanciones a implementar en caso de constatar el incumplimiento de la ley. **LEY DE PROTECCIÓN DE LOS DATOS PERSONAL**

**CAPÍTULO 1**

# DISPOSICIONES GENERALES

ARTÍCULO 1°.- El derecho a la protección de datos personales tiene rango constitucional

ARTÍCULO 2 Anonimización: La aplicación de medidas dirigidas a impedir la identificación o reidentificación, ya sea por el Responsable de tratamiento, Encargado de tratamiento o un Tercero, de una persona humana, sin esfuerzos o plazos desproporcionados o inviables, teniendo en cuenta factores como los costos y el tiempo necesario para la identificación o reidentificación de la persona a la luz de la tecnología disponible en el momento del tratamiento. Es mas laxo que antes (habla de esfuerzo para identificar)

Autodeterminación informativa: El derecho de la persona a decidir o autorizar la recolección, uso de sus datos personales, así como de conocer, actualizar, o suprimirlos, o controlar lo que se hace con su información.

Datos biométricos: Aquellos datos obtenidos relativos a las características físicas o conductuales de una persona humana, que permitan o confirmen su identificación única, tales como imágenes faciales o datos dactiloscópicos, entre otros.

Datos genéticos: Aquellos datos relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud.

Datos personales: Información referida a personas humanas determinadas o determinables. Se entiende por “determinable” la persona que puede ser identificada directa o indirectamente por uno o varios elementos característicos de su identidad física, fisiológica, genética, biométrica, psíquica, económica, cultural, social o de otra índole.

Datos personales sensibles: Aquellos que se refieren a la esfera íntima de la persona Titular de los datos, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, orientación sexual, identidad de género, o datos genéticos o biométricos cuando puedan revelar datos adicionales cuyo uso pueda resultar potencialmente discriminatorio para la persona Titular de los datos y que estén dirigidos a identificar de manera unívoca a una persona humana.

Delegado de Protección de Datos: Persona humana o jurídica encargada de informar, instruir y asesorar al Responsable o al Encargado de tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar y supervisar el cumplimiento normativo, y de cooperar con la Autoridad de Aplicación y servir como punto de contacto entre esta y el Responsable o Encargado de tratamiento de datos.

Elaboración de perfiles: Toda forma de tratamiento automatizado o parcialmente automatizado de datos personales consistente en utilizar estos para evaluar determinados aspectos de una persona humana; en particular, para analizar o predecir cuestiones relativas al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, etnia, género o movimientos de dicha persona.

Elaborar ciertos perfiles (aspectos de una persona humana) en base a la información recopilada de datos personales, para analizar o predecir cuestiones relativas a los datos de dicha persona

Encargado de tratamiento: Persona humana o jurídica, pública o privada, que trate datos personales por cuenta del Responsable de tratamiento.

Entidades crediticias: Las entidades que provean información de situación crediticia al BANCO CENTRAL DE

LA REPÚBLICA ARGENTINA. Tienen mas peso que en la ley anterior

Grupo económico: Constituyen un conjunto de empresas que pueden presentarse formal y aparentemente independientes, pero sin embargo se encuentran entrelazadas al punto de formar un todo complejo pero compacto que responde a un mismo interés.

Incidente de seguridad de datos personales: Ocurrencia de uno o varios eventos en cualquier fase del tratamiento que atenten contra la confidencialidad, la integridad o la disponibilidad de los datos personales.

Representante de Responsable o Encargado de tratamiento: Persona que ejerce la representación en el territorio nacional de Responsables o Encargados de tratamiento que no se encuentran establecidos en la REPÚBLICA ARGENTINA.

Responsable de tratamiento de datos personales: Persona humana que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales. Es a quien le son otorgados los datos.

Seudonimización: La aplicación de medidas dirigidas a impedir que los datos personales puedan atribuirse a una persona humana sin utilizar información adicional. Admite la dificultad de anonimizar

Tercero: bajo la autoridad directa del Responsable o del Encargado de tratamiento.

Transferencia internacional: Los datos se almacenan fuera del pais

ARTÍCULO 3°.- Ámbito de Aplicación material de la Ley. Aplica a todo, incluso si se seudoanonimizaron los datos

Guarda el derecho a mantener el secreto de las fuentes periodisticas

Queda exceptuado si es para uso privado o grupo familiar

Tampoco aplica si los datos son anónimos o la persona no puede ser identificada

ARTÍCULO 4°.- Ámbito de Aplicación territorial.

1. El Responsable o Encargado de tratamiento se encuentra establecido en el territorio de la REPÚBLICA

ARGENTINA, aun si el tratamiento de datos tuviese lugar fuera de dicho territorio;

1. No se encuentra establecido en el territorio de la REPÚBLICA ARGENTINA, pero se da alguno de los siguientes supuestos:
2. Realiza tratamiento de datos en el territorio de la REPÚBLICA ARGENTINA mediante cualquier medio o procedimiento, físico o electrónico, actual o futuro, que le permite recolectar, usar, almacenar, indexar o tratar información de personas que se encuentren en dicho territorio;
3. Efectúa actividades de tratamiento relacionadas con: la oferta de bienes o servicios a personas que se encuentren en el territorio de la REPÚBLICA ARGENTINA; o el perfilamiento, seguimiento o control de los actos, comportamientos o intereses de dichas personas;
4. Se encuentra establecido en un lugar en el que se aplica la legislación de la REPÚBLICA ARGENTINA en virtud del derecho internacional o de disposiciones de carácter contractual.

ARTÍCULO 5°.- Principio de neutralidad tecnológica. se aplica a cualquier tratamiento de datos personales, con independencia de las técnicas, procesos o tecnologías -actuales o futuras- que se utilicen para dicho efecto.

**CAPÍTULO 2**

# TRATAMIENTO DE DATOS PERSONALES

ARTÍCULO 6º.- Principio de licitud, lealtad y transparencia. Los datos personales deben ser tratados de manera lícita, leal y transparente. Lícito si se realiza conforme a lo establecido en la Ley. Leal si el Responsable de tratamiento no trata los datos por medios engañosos o fraudulentos. Es transparente si la información vinculada al tratamiento de los datos es fácilmente accesible y utiliza un lenguaje sencillo y claro.

ARTÍCULO 7º.- Principio de finalidad. La recoleccion debe tener un fin determinado

ARTÍCULO 8º- Principio de minimización de datos. Los datos personales deben ser tratados de manera que sean adecuados y limitados a lo necesario en relación con los fines para los que fueron recolectados. A solicitud de la Autoridad de Aplicación, los Responsables de tratamiento deberán proveer una justificación de la necesidad de tratar los datos en cada caso.

ARTÍCULO 9º.- Principio de exactitud. Los datos personales objeto de tratamiento deben ser exactos, completos, comprobables y actualizados. Si fuera necesario actualizarlos, se deben adoptar todas las medidas razonables para que no se altere su veracidad.

ARTÍCULO 10.- Principio de preeminencia. Ante dudas, el titular de los datos tiene la razon

ARTÍCULO 11.- Plazo de conservación. No se pueden tener eternamente, salvo algunos casos con fines estadisticos.

ARTÍCULO 12.- Principio de responsabilidad proactiva y demostrada. El Responsable y el Encargado de tratamiento de los datos personales tomar las medidas necesarias con el fin de garantizar un tratamiento adecuado de los datos, y el cumplimiento de la ley.

ARTÍCULO 13.- Bases legales para el tratamiento de datos. Mas de una opción para admitir el tratamiento de datos personales, una de ellas es que el titular presente conformidad para el tratamiento (detallándose el fin de este)

ARTÍCULO 14.- Consentimiento. Si el tratamiento de datos es por consentimiento, se requiere que este sea previo (consentimiento antes), expreso (titular afirma su voluntad), especifico (si tiene varios fines, titular da consentimiento para cada uno), informado (titular cuenta con la info de como se los van a utilizar a sus datos) e inequivoco (debe aclararse claramente la autorización del Titular) para las finalidades determinadas mediante una declaración o una acción afirmativa

ARTÍCULO 15.- Revocación del consentimiento. Se puede revocar el consentimiento en cualquier momento, sin obligación de fundamentar, y el procedimiento debe ser gratuito y sencillo

ARTÍCULO 16.- Información a la persona Titular de los datos. El titular debe recibir los datos que se detallan en este articulo. Entre ellos, los datos del responsable, el plazo que se mantendrán los datos, si va a haber o no decisiones automatizadas de por medio.

1. Datos del Responsable de tratamiento; en su caso, del Delegado de Protección de Datos y, en el supuesto de los Responsables o Encargados de tratamiento no establecidos en la REPÚBLICA ARGENTINA, los de su Representante en el territorio nacional;
2. Con que datos personales se van a tratar
3. Que fines tienen los datos
4. Los derechos de la persona Titular de los datos y como ejercerlos
5. Aquella información sobre las transferencias internacionales de datos, con inclusión de países de destino, identidad y datos de contacto del destinatario.;
6. El plazo durante el cual se conservarán los datos personales o, si esto no es posible, los criterios utilizados para determinar este plazo;
7. La existencia o no de decisiones automatizadas o semiautomatizadas, incluida la elaboración de perfiles;
8. El derecho a presentar una denuncia del incumplimiento de la ley

ARTÍCULO 17.- Tratamiento de datos sensibles. Se debe implementar la responsabilidad reforzada que implica mayores niveles de seguridad, restricciones de acceso, uso.

Se prohíbe el tratamiento de datos sensibles que conlleve perjuicio o discriminación hacia la persona Titular de datos personales. No se pueden usar datos sensibles en casos que conlleve a perjuicio o discriminacion

ARTÍCULO 18.- Tratamiento de datos del sector público. Deben explicitar muy bien el tratamiento

Además, el Sector Público debe implementar planes de protección de datos personales y de formación y capacitación en la materia para su personal (manejan BD de datos personales)

En el caso de niñas, niños y adolescentes menores de DIECISÉIS (16) años, pueden dar consentimiento, pero necesitan siempre consentimiento del adulto responsable.

Se prohíbe realizar el tratamiento de datos personales de niños, niñas y adolescentes en los juegos, aplicaciones, desarrollos e innovaciones tecnológicas, u otras actividades afines que involucren información personal, más allá de lo estrictamente necesario para la realización de la actividad.

ARTÍCULO 20.- Principio de seguridad de los datos personales. Medidas de seguridad (y tecnológicas) que deben tomarse en el caso de los datos personales. El Responsable y el Encargado de tratamiento de datos personales deben garantizar la seguridad y confidencialidad de los datos personales.

Para ello deben adoptar un sistema de administración de riesgos y tomar en cuenta las categorías y volumen de los datos personales, la probabilidad de riesgos, el estado de la técnica.

El Responsable y el Encargado de tratamiento deben adoptar las medidas de seguridad considerado los siguientes factores:

1. El carácter sensible de los datos personales tratados;
2. El desarrollo tecnológico;
3. Las posibles consecuencias de un incidente de seguridad para las personas Titulares de los datos;

ARTÍCULO 21.- Notificación de incidentes de seguridad. En caso de incidente de seguridad, el responsable tiene 72hs para dar aviso (en un lenguaje claro y sencillo)

ARTÍCULO 22.- Deber de confidencialidad. El Responsable, el Encargado y las demás personas que intervengan en cualquier fase del tratamiento tienen deber de confidencialidad de los datos accedidos.

**CAPÍTULO 3**

# TRANSFERENCIAS INTERNACIONALES

ARTÍCULO 23.- Principio general de las transferencias internacionales. El receptor debe ser seguro, y el emisor es el “responsable”.

ARTÍCULO 26 – Excepciones a la transferencia internacional. Las transferencia pueden realizarse por excepciones si se cumple alguna de estas:

1. Que el Titular da consentimiento;
2. Que sea necesaria para la ejecución de un contrato entre la persona Titular de los datos y el Responsable de tratamiento
3. Que la transferencia sea necesaria:
4. Por razones de interés público;

**CAPÍTULO 4**

# DERECHOS DE LOS TITULARES DE LOS DATOS

ARTÍCULO 27.- Derecho de acceso. La persona Titular de los datos, previa acreditación de su identidad, tiene derecho a saber si se están tratando sus datos personales, y solicitar información sobre ellos.

Mas específicamente, tiene derecho a:

1. Razones del tratamiento y bases legales que las legitiman.
2. Los datos personales que se traten;
3. Los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales;
4. La relativa a las transferencias internacionales de datos que se hayan efectuado o se prevea efectuar, con inclusión de países de destino y base legal que justifica la transferencia; Se incluye el tema de transferencias internacionales
5. El plazo previsto de conservación de los datos personales o, de no ser ello posible, los criterios utilizados para determinar este plazo;
6. La existencia del derecho a la rectificación o la supresión de datos personales, así como a oponerse a dicho tratamiento;
7. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, en tales casos, información significativa sobre la lógica aplicada, siempre que ello no afecte derechos intelectuales del Responsable de tratamiento.

ARTÍCULO 28.- Derecho de rectificación. La persona Titular de los datos tiene el derecho a obtener del Responsable de tratamiento la rectificación de sus datos personales cuando estos resulten ser inexactos, falsos, erróneos, incompletos o desactualizados. Tienen 5 días para que el responsable se rectifique

ARTÍCULO 29.- Derecho de oposición. El titular puede oponerse al tratamiento

La persona Titular de los datos también puede oponerse al tratamiento de sus datos personales si tuvieran por objeto la publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles. Cuando la persona Titular de los datos se oponga al tratamiento para esos propósitos, sus datos personales deben dejar de ser tratados. Perfil o publicidad pueden ser denegados por el titular.

ARTÍCULO 30.- Derecho de supresión. La persona Titular de los datos tiene derecho a solicitar la supresión de sus datos personales al Responsable de tratamiento.

ARTÍCULO 31.- Decisiones automatizadas y elaboración de perfiles. El titular puede solicitar revisiones por PERSONAS HUMANAS. Se entiende por decisiones parcialmente automatizadas o semiautomatizadas a aquellas en las que no hay intervención humana significativa.

ARTÍCULO 32.- Derecho a la portabilidad de datos personales. El titular puede solicitar el traspaso de datos(copia). Si se tratan datos personales mediante medios electrónicos o automatizados, la persona Titular de los datos tiene derecho a obtener una copia de los datos personales que hubiere proporcionado al Responsable de tratamiento

ARTÍCULO 33.- Derecho de limitación. El titular puede limitar el tratamiento de los datos

ARTÍCULO 34.- Ejercicio de los derechos. Los responsables tienen 10 dias para responder.

Hay seis meses para reiterar pedidos o reclamos. En caso de hacerlo antes el responsable puede cobrar (monto razonable)

**CAPÍTULO 5**

# OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTO

ARTÍCULO 36.- Deberes del Responsable de tratamiento.

1. Implementar medidas apropiadas, útiles, oportunas, pertinentes y eficaces para garantizar y poder demostrar el adecuado cumplimiento de la presente Ley y las normas reglamentarias
2. Garantizar a la persona Titular de los datos, el pleno y efectivo ejercicio del derecho de protección de datos, especialmente conocer, actualizar, rectificar, suprimir sus datos personales u oponerse al tratamiento de estos;
3. Cumplir con el deber de informar a la persona Titular de los datos sobre la finalidad de la recolección y sus derechos;
4. Tratar los datos personales bajo condiciones de seguridad apropiadas
5. Implementar medidas para garantizar que los datos personales sean veraces, actualizados, completos, exactos y comprobables;;
6. Tramitar las solicitudes presentadas por la persona Titular de los datos, y responderlas de manera completa y oportuna;
7. Verificar que los Encargados de tratamiento, o quienes estos subcontraten, ofrezcan garantías suficientes para realizar el tratamiento de datos personales conforme a los requisitos de la presente Ley y garanticen la protección de los derechos de la persona Titular de los datos; dicha verificación debe realizarse con anterioridad a la contratación.
8. En caso de que corresponda, designar un Delegado de Protección de Datos. Tiene que tener una persona designada a la protección de datos. Sino, se debe establecer una persona o área que asuma la función de protección de datos personales y de trámite a las solicitudes de las personas Titulares de los datos.

ARTÍCULO 37.- Deberes del Encargado de tratamiento.

1. La prestación de servicios de tratamiento de datos por cuenta de terceros entre un Responsable y un Encargado de tratamiento debe quedar formalizada mediante un contrato por escrito.
2. El Encargado de tratamiento debe limitarse a llevar a cabo solo aquellos tratamientos de datos encomendados por el Responsable de tratamiento;
3. Los datos personales objeto de tratamiento deben aplicarse o utilizarse con el fin que figure en el contrato, y no deben ser cedidos a otras personas.
4. Una vez cumplida la prestación contractual, los datos personales tratados deben ser devueltos al Responsable de tratamiento o destruidos, estos solo pueden conservarse 2 años
5. En caso de que corresponda, debe designarse un Delegado de Protección de Datos, al igual que en caso de el Responsable de el tratamiento de los datos. En caso de no corresponder la designación de un Delegado de Protección de Datos, debe establecerse una persona o área que asuma la función de protección de datos personales y trámite de las solicitudes de las personas Titulares de los datos.

ARTÍCULO 38.- Política de tratamiento de datos personales. Los Responsables y los Encargados de tratamiento deben desarrollar sus políticas para el tratamiento de los datos personales en un lenguaje claro y sencillo

Si se cambia la política de tratamiento, deben pedir nuevamente la autorización al titular.

ARTÍCULO 40. - Protección de datos desde el diseño y por defecto. El Responsable de tratamiento debe, desde el diseño y antes del tratamiento, prever y aplicar medidas tecnológicas y organizativas apropiadas para cumplir los principios y garantizar los derechos de las personas Titulares de los datos.

El Responsable de tratamiento debe aplicar las medidas tecnológicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento.

ARTÍCULO 41.- Evaluación de impacto relativa a la protección de datos personales. Si el Responsable de tratamiento va a realizar algún tipo de tratamiento de datos que pueda presentar un alto riesgo de afectación a los derechos de las personas Titulares, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto relativa a la protección de los datos personales.

Esta evaluación es obligatoria en los siguientes casos:

1. Evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado y semiautomatizado, como la elaboración de perfiles.
2. Tratamiento de datos sensibles a gran escala.

ARTÍCULO 42.- Contenido de la evaluación de impacto.

1. Una descripción de las operaciones de tratamiento de datos previstas y de los fines del tratamiento.
2. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad;
3. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales.

ARTÍCULO 43.- Informe previo. El responsable lo tiene que realizar a la autoridad de aplicación sobre la evaluación de impacto(si es de alto riesgo).

El informe debe incluir:

1. Las obligaciones respectivas del Responsable y Encargado de tratamiento
2. Los fines y medios del tratamiento;
3. Las medidas para minimizar los riesgos identificados y proteger los derechos de las personas Titulares de los datos;
4. En su caso, los datos de contacto del Delegado de Protección de Datos;
5. La evaluación de impacto relativa a la protección de datos;

ARTÍCULO 44.- Delegado de Protección de Datos. Caracteristicas. Es designado por el Responsable y Encargado de tratamiento en estos casos:

1. Cuando se trate de una autoridad u organismo público;
2. Cuando las actividades del Responsable o Encargado de tratamiento de datos personales requieran un control permanente y sistematizado.

Si los Responsables y Encargados de tratamiento no se encuentran obligados a la designación de un Delegado de Protección de Datos, de acuerdo a lo previsto en este artículo, pueden designar uno de manera voluntaria.

La designación como Delegado de Protección de Datos debe recaer en una persona que reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

El rol de Delegado de Protección de Datos puede ser desempeñado por un empleado del Responsable o Encargado de tratamiento.

El Responsable o Encargado de tratamiento está obligado a respaldar al Delegado de Protección de Datos en el desempeño de sus funciones, y a facilitarle los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados.

El Delegado de Protección de Datos debe ejercer sus funciones de manera autónoma y libre de interferencias, sin recibir instrucciones, y solo debe responder ante el más alto nivel jerárquico de la organización.

No puede ser destituido ni sancionado por desempeñar sus funciones.

ARTÍCULO 45.- Funciones del Delegado de Protección de Datos.

1. Informar y asesorar a los Responsables y Encargados de tratamiento de las obligaciones a su cargo;
2. Promover y participar en el diseño y aplicación de una política de tratamiento de datos personales;
3. Supervisar el cumplimiento de la presente Ley y de la política de protección de datos;
4. Asignar responsabilidades, concientizar, formar al personal y realizar las auditorías correspondientes;
5. Ofrecer el asesoramiento que se le solicite para hacer una evaluación de impacto relativa a la protección de datos, cuando entrañe un alto riesgo de afectación para los derechos de las personas Titulares de los datos, y supervisar luego su aplicación;
6. Actuar como referente ante la Autoridad de Aplicación para cualquier consulta sobre el tratamiento de datos efectuado por el Responsable o Encargado de tratamiento.

ARTÍCULO 46.- Representantes de Responsables y Encargados de tratamiento. Cuando el Responsable o el Encargado de tratamiento no se encuentren establecidos en la REPÚBLICA ARGENTINA, tienen que designar uno en el territorio nacional

Excepto cuando:

1. El tratamiento sea ocasional;
2. Se trate de organismos públicos extranjeros.

El Representante debe actuar en nombre del Responsable o del Encargado de tratamiento, y responderá los pedidos y solicitudes de la Autoridad de Aplicación y de las personas Titulares de los datos. También puede ser objeto de un procedimiento sancionatorio ante el incumplimiento por parte del Responsable o del Encargado de tratamiento.

ARTÍCULO 47.- Registro. Créase el REGISTRO NACIONAL PARA LA PROTECCIÓN DE LOS DATOS PERSONALES. Deberán inscribirse obligatoriamente en el mismo:

1. Los Responsables y Encargados de tratamiento que deban tener un Delegado de Protección de Datos.
2. Los Responsables y Encargados de tratamiento de datos que deban contar con un Representante en la REPÚBLICA ARGENTINA.

**CAPÍTULO 6**

# PROTECCIÓN DE DATOS DE INFORMACIÓN CREDITICIA

ARTÍCULO 49.- Protección de datos de información crediticia del sector financiero y no financiero. Solo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al credito

Prohibe tratamiento de datos de parientes . No admite utilizar datos de servicios públicos (esenciales)

ARTÍCULO 50.- Plazo de conservación de la información crediticia. 5 años

ARTÍCULO 51.- Deber de comunicación. Deben comunicar como es la formula para puntuar de acuerdo al comportamiento crediticio.

Si hay un cambio de situación crediticia, tienen un plazo de 10 días hábiles en comunicarlo

**CAPÍTULO 7**

# AUTORIDAD DE APLICACIÓN

ARTÍCULO 53.- Autoridad de Aplicación. La Autoridad de Aplicación de la presente Ley es la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE LOS DATOS PERSONALES.

ARTÍCULO 54.- Facultades de la Autoridad de Aplicación.

1. Ejercer la supervisión de las actividades efectuadas por el Responsable y Encargado de tratamiento de datos personales.
2. Tramitar los requerimientos y denuncias interpuestos en relación con el tratamiento de datos
3. Solicitar información a los Responsables o Encargados de tratamiento, Delegados de Protección de Datos y Representantes, los que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos que se les requieran.
4. Dictar órdenes, comunicaciones, y otros actos administrativos para garantizar el debido tratamiento de los datos personales y los derechos de las personas Titulares de los datos, y aplicar las sanciones por violación de esta Ley y de las Reglamentaciones;
5. Constituirse en querellante en las acciones penales que se promovieren por violaciones a la presente Ley;
6. Interponer acciones colectivas de habeas data conforme a lo establecido en esta Ley;
7. Aprobar las cláusulas contractuales modelo para la transferencia internacional de datos;
8. Promover, organizar y desarrollar programas tendientes a la protección de datos personales de niños, niñas y adolescentes en internet, juegos electrónicos y otras plataformas digitales;
9. Divulgar los derechos de las personas Titulares de los datos en relación con el tratamiento de datos personales, e implementar campañas pedagógicas para capacitar a los ciudadanos, Responsables y Encargados de tratamiento acerca del ejercicio y garantía del derecho fundamental a la protección de datos;

**CAPÍTULO 8**

# PROCEDIMIENTOS Y SANCIONES

ARTÍCULO 56.- Trámite de protección de los datos personales. La denuncia es gratuita (a través de la Autoridad de Aplicación)

ARTÍCULO 58.- Notificaciones. Son válidas las notificaciones realizadas por medios electrónicos conforme la normativa que dicte la Autoridad de Aplicación, teniendo en consideración el principio de neutralidad tecnológica.

ARTÍCULO 61.- Sanciones. La Autoridad de Aplicación puede aplicar a los Responsables y Encargados de tratamiento, y a sus representantes, las siguientes sanciones:

1. Apercibimientos;
2. Multas;
3. Suspensión de las actividades relacionadas con el tratamiento de datos personales;
4. Cierre temporal de las operaciones;
5. Cierre definitivo de las operaciones.

ARTÍCULO 62.- Determinación de la unidad móvil. Se usa una unidad móvil de multa

ARTÍCULO 63.- Multas. Ahora, la multa es importante (a nivel monetario) ya que prevee ponerlo en función de la facturación

ARTÍCULO 65.- Graduación de penas. Las sanciones deben ser graduadas, según las peculiaridades del caso específico, con atención a los siguientes criterios:

1. La naturaleza y dimensión del daño o peligro a los intereses jurídicos tutelados por la presente Ley;
2. El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción. La reincidencia en la comisión de la infracción;
3. La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Autoridad de Aplicación;
4. El incumplimiento de los requerimientos u órdenes impartidas por la Autoridad de Aplicación;
5. El reconocimiento o aceptación expresa que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar;
6. La condición económica del infractor;
7. La adopción demostrada de medidas correctivas y mecanismos y procedimientos internos tendientes al tratamiento seguro y adecuado de los datos y capaces de minimizar el daño;
8. La adopción de mecanismos de regulación vinculantes;
9. La proporcionalidad entre la gravedad de la falta y de la sanción;
10. La designación voluntaria de un Delegado de Protección de Datos;
11. La notificación oportuna de incidentes de seguridad;

ARTÍCULO 75.- Las normas de la presente Ley son de orden público y de aplicación en todo el territorio nacional

LEY VIGENTE: hay condenas penales

ARTICULO 32. — (Sanciones penales).

1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:

* "1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.
* 2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas

información falsa contenida en un archivo de datos personales.

* 3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
* 4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

2. Incorpórase como artículo 157 bis del Código Penal el siguiente: "Será reprimido con la pena de prisión de un mes a dos años el que:

* 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
* 2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".