Artículo	Observación
ARTÍCULO 1° — Objeto y finalidad. La presente ley tiene por objeto proteger los datos personales y garantizar los derechos de sus titulares, de conformidad con lo establecido en el artículo 43, tercer párrafo, de la Constitución Nacional y en los tratados de derechos humanos en los que la República Argentina sea parte, promoviendo el uso responsable de la información en entornos digitales, la innovación tecnológica y el desarrollo económico.	¿Puede una ley que protege un Dcho Humano colocar al mismo nivel la promoción de una actividad económica? La norma no distingue entre el fin principal (proteger un derecho fundamental) y objetivos de política pública (innovación y desarrollo económico). Desde la técnica legislativa, mezclar ambos planos en la cláusula de finalidad puede generar tensiones interpretativas cuando esos objetivos entren en conflicto. Al introducir fines económicos y tecnológicos en el mismo plano interpretativo que la defensa de Derechos Fundamentales se puede desplazar el centro de gravedad de la ley hacia un modelo de ponderación permanente entre los dos elementos lo que, en definitiva, menoscaba la previsibildiad y seguridad jurídica.
ARTÍCULO 2° — Definiciones. A los fines de la presente ley se entiende por: [...] - Tratamiento avanzado de datos: tratamiento de datos a gran escala, que incluya de manera principal el tratamiento de datos sensibles o emplee sistemas de inteligencia artificial o mecanismos de decisión automatizada que afecten de manera sustancial los derechos, intereses o expectativas legítimas del titular de los datos. - Tratamiento intermedio de datos: tratamientos de datos personales de alcance relevante o recurrente en el marco de su actividad, incluyendo de manera accesoria o incidental el tratamiento de datos sensibles. - Tratamiento básico de datos: tratamientos de datos personales de alcance limitado, no sistemáticos o de baja complejidad, sin involucrar habitualmente datos sensibles ni procesos de decisión automatizada que afecte de manera sustancial los derechos, intereses o expectativas legítimas del titular de los datos. [...]	Las categorías prácticamente sólo aparecen nuevamente en el régimen de medidas de seguridad. Esto puede producir un problema de sistematicidad y aplicación por parte de magistrados. Si el legislador considera relevante distinguir tres clases de tratamientos, esa clasificación debería proyectarse, por ejemplo, sobre otros conceptos de la ley como la evaluación de impacto, designación, sandbox, carga documental. ¿Tratamiento de datos a gran escala?, ¿Como se determinaría la graduación de la escala? ¿Qué sería un tratamiento incidental de datos sensibles? Existe el riesgo de que la categoría abarque la posible inferencia de este tipo de datos?

Artículo	Observación
ARTÍCULO 3° — Excepciones a su ámbito de aplicación material. Queda exceptuado de los alcances de la presente ley el tratamiento de datos que efectúe una persona humana para su uso exclusivamente privado o de su grupo familiar y los datos anonimizados en los términos del artículo 2°. La aplicación de la presente ley en ningún caso podrá afectar el secreto de las fuentes de información periodísticas. Tampoco podrá afectar al tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión.	Inquietud:¿Esto incluiría cosas como, por ejemplo, los datos empleados para hacer targeting por canales de stream? Entiendo el caso pueda resultar un tanto específico, sin embargo la ampliación de sentidos del término "medio de comunicación" sucedido en los últimos años obliga a tomar cierto recaudo. Posiblemente esclarecer un poco más el signifificado/alcance de "en ejercicio de la libertad de expresión".
ARTÍCULO 4° — Ámbito de aplicación territorial. Las disposiciones de la presente ley serán de aplicación al tratamiento de datos personales cuando: [...]	El artículo toma una estructura similar al art 3 GDPR pero sin establecer un paralelo a la garantía establecida por el Art. 27 del mismo cuerpo normativo que obliga a los responsables o encargados no establecidos en la Unión a designar un representante en la Unión Europea.
ARTÍCULO 4° — Ámbito de aplicación territorial. Las disposiciones de la presente ley serán de aplicación al tratamiento de datos personales cuando: [....] c) El tratamiento de datos de titulares que residan en la República Argentina sea realizado por un responsable o encargado del tratamiento que no se encuentre establecido en el territorio nacional cuando las actividades de dicho tratamiento se encuentren específicamente dirigidas a la oferta de bienes o servicios a dichos titulares de los datos en la República Argentina, o cuando el responsable o el encargado realice el seguimiento sistemático de sus actos, comportamientos o intereses dentro del territorio argentino.	Qué sería "específicamente dirigidas"? .Se reproduce casi literalmente la regla de extraterritorialidad prevista en el artículo 3.2 del GDPR, pero omite incorporar los criterios interpretativos que el propio modelo europeo ha desarrollado para determinar cuándo una actividad se encuentra efectivamente dirigida a un determinado mercado (Cd. Directrices 3/2018 del European Data Protection Board). Esto traslada íntegramente esa construcción a la futura jurisprudencia argentina, reduciendo la previsibilidad de la norma y aumentando la incertidumbre para responsables, titulares y autoridades de control.
ARTÍCULO 5° — Principio de licitud. El tratamiento de datos personales es lícito si se cumple, al menos, una de las siguientes condiciones: [...] c) El tratamiento se realiza en ejercicio de funciones propias de los poderes del Estado, con fines de defensa nacional, seguridad pública o represión del delito y en virtud de una obligación o disposición legal; [...]	Ponre atención al reciente fallo Torres Abad de la CSJN (Fallos: 349:407) Posiblemente se esté reproduciendo la lógica del actual art. 5.2.b de la 25326 recientemente considerado inconstitucional por la CSJN. Tensión con el principio de legalidad.

Artículo	Observación
ARTÍCULO 5° — Principio de licitud. El tratamiento de datos personales es lícito si se cumple, al menos, una de las siguientes condiciones: [...] g) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan otros derechos y libertades fundamentales del titular. Constituyen intereses legítimos: la prevención del fraude y abusos, la seguridad física y lógica, la protección de redes y sistemas, la gestión administrativa interna, la auditoría, el cumplimiento normativo, la defensa en juicio, el cobro de deudas, el tratamiento de datos dentro del mismo grupo económico, la debida diligencia en operaciones societarias, el desarrollo o la mejora razonable de productos y servicios, la analítica interna y la atención de reclamos, y el entrenamiento de sistemas de inteligencia artificial conforme al artículo 17 (Entrenamiento de sistemas de inteligencia artificial); [...]	Si bien el proyecto delimita legislativamente qué intereses pueden considerarse legítimos, omite desarrollar los criterios que deben regir la ponderación entre esos intereses y los derechos fundamentales del titular. El resultado es un régimen que enumera ampliamente las hipótesis habilitantes, pero regula escasamente las condiciones para evitar que éstas prevalezcan indebidamente sobre el derecho a la protección de datos personales. Se incorpora expresamente el entrenamiento de sistemas de inteligencia artificial como interés legítimo. Esa es una decisión de política legislativa relevante, porque convierte en una habilitación legal expresa una actividad que en el derecho comparado continúa siendo objeto de intenso debate respecto de su compatibilidad con los principios de finalidad, minimización y transparencia.
ARTÍCULO 5° — Principio de licitud. El tratamiento de datos personales es lícito si se cumple, al menos, una de las siguientes condiciones: [...] h) Los datos se han obtenido de bases de acceso público irrestricto y resultan necesarios para los fines del tratamiento; [...]	El inciso presenta un posible problema lógico y sistemático. En primer lugar, la categoría "base de datos de acceso público irrestricto" no aparece suficientemente delimitada. ¿Comprende únicamente registros públicos creados por ley? ¿Incluye también sitios web, blogs o perfiles públicos en redes sociales? La amplitud de la definición impide conocer con certeza el alcance de esta nueva base de licitud. En segundo término, la norma parece asumir que la publicidad de un dato basta para habilitar su tratamiento posterior. Sin embargo, la accesibilidad de un dato no modifica su naturaleza jurídica. Un dato personal continúa siendo un dato personal aunque sea públicamente accesible y, del mismo modo, un dato sensible no pierde tal carácter por haber sido voluntariamente publicado por su titular. La consecuencia práctica de esta redacción puede resultar particularmente problemática. Si una red social pudiera ser considerada una base de datos de acceso público irrestricto, ¿resultaría lícito recopilar mediante técnicas de scraping los integrantes de un grupo público de pacientes afectados por una determinada patología para elaborar una base de potenciales consumidores de productos farmacéuticos? La respuesta afirmativa importaría admitir que la mera publicidad del dato desplaza el régimen reforzado de protección previsto para los datos sensibles, conclusión que parece difícilmente conciliable con los principios que informan el derecho a la protección de datos personales.

Artículo	Observación
ARTÍCULO 8° — Principio de exactitud. Los datos personales deberán ser exactos y, cuando sea necesario según los fines del tratamiento, completos y actualizados. El responsable del tratamiento deberá adoptar medidas razonables para su rectificación, actualización, supresión o bloqueo cuando resulten inexactos, incompletos o no necesarios en relación con dichos fines.	Se recepta el principio de exactitud y constituye, en términos generales, una mejora respecto del régimen vigente. Presenta una pequeña inconsistencia sistemática. La disposición regula conjuntamente la rectificación, actualización, supresión y bloqueo de datos como consecuencias derivadas de un mismo principio. Sin embargo, mientras la rectificación y la actualización constituyen mecanismos destinados a garantizar la exactitud de la información, la supresión de datos por haber dejado de ser necesarios responde("no necesarios en relación con dichos fines."), al principio de limitación de la conservación o de minimización de datos (art 7 del proyecto) y no al principio de exactitud.
ARTÍCULO 9° — Principio de seguridad, confidencialidad y responsabilidad proactiva. El responsable del tratamiento y, en su caso, el encargado deberán adoptar y mantener medidas apropiadas para garantizar la seguridad y confidencialidad de los datos personales, protegiéndolos contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, así como para detectar, prevenir y mitigar incidentes de seguridad, conforme a lo establecido en el artículo 30 (Medidas de seguridad según categoría de responsable o encargado). Deberán, asimismo, ser capaces de demostrar la adopción de medidas apropiadas para garantizar el cumplimiento de lo dispuesto en la presente ley ante la autoridad de control.	La obligación de adoptar "medidas apropiadas" vuelve a introducir un concepto jurídico indeterminado cuyo contenido queda librado, en gran medida, a la apreciación del responsable del tratamiento y de la autoridad de control. resultaría conveniente precisar, al menos de manera enunciativa, que la adecuación de dichas medidas debe evaluarse considerando factores tales como la naturaleza de los datos tratados, el volumen del tratamiento, los riesgos para los derechos de los titulares, el estado de la técnica y los costos de implementación para otorgar mayor rpevisibilidad y reducir imprevisibilidad.
ARTÍCULO 11 — Consentimiento. El consentimiento será una de las bases de licitud para el tratamiento de datos personales, y será considerado válido cuando cumpla las siguientes condiciones: a) Libre: otorgado sin coacción ni condicionamientos indebidos; b) Específico: referido a uno o más fines determinados o categorías claramente identificables; c) Informado: basado en información comprensible, accesible y proporcional al uso previsto; d) Inequívoco: manifestado mediante una acción afirmativa clara; y e) Verificable: el responsable debe poder demostrar razonablemente que lo obtuvo. [...]	Se incorpora un régimen de consentimiento que, en su primer párrafo, adopta el estándar de la acción afirmativa clara, pero inmediatamente lo relativiza mediante la admisión del consentimiento tácito para la mayoría de los tratamientos. La coexistencia de ambos modelos - en los términos consagrados- puede dar lugar a tensiones interpretativas y disminuir la seguridad jurídica respecto del estándar de consentimiento efectivamente exigido por la ley.

Artículo	Observación
ARTÍCULO 11 — Consentimiento. El consentimiento será una de las bases de licitud para el tratamiento de datos personales, y será considerado válido cuando cumpla las siguientes condiciones: [...] Salvo en el tratamiento de datos sensibles y de datos personales de niños, niñas y adolescentes, podrá admitirse el consentimiento tácito siempre que surja de manera manifiesta del contexto de la relación entre el titular y el responsable del tratamiento; que el responsable haya informado la finalidad del tratamiento previamente de manera clara, inequívoca y de fácil comprensión al titular y que este último no se haya opuesto. Corresponderá exclusivamente al responsable del tratamiento la carga de probar la configuración de todos los requisitos exigidos para la validez del consentimiento tácito.	En ninguna parte del proyecto se define la idea de esta relación. Sus efectos pueden ser de peso. Comprendería la relación laboral? de consumo? contractual en sentido amplio? El párrafo califica como "consentimiento tácito" un supuesto en el que el responsable informa previamente la finalidad del tratamiento y el titular simplemente no formula oposición. Sin embargo, desde el punto de vista conceptual, la ausencia de oposición no constituye necesariamente una manifestación tácita de voluntad, sino un mecanismo de aceptación por inacción (opt-out). La diferencia no es meramente terminológica. Mientras el "consentimiento tácito" supone que la voluntad puede inferirse de una conducta concluyente del titular, el régimen previsto por el proyecto parece hacer descansar la licitud del tratamiento en el silencio o la falta de oposición del interesado. Esto puede estar en oposición a lo normado por el artículo 263 CCCN. Por otro lado, esta solución tensiona con el propio inciso d), que exige como regla general que el consentimiento sea manifestado mediante una acción afirmativa clara.
ARTÍCULO 12 — Revocación del consentimiento. El titular podrá revocar su consentimiento en cualquier momento. Esta revocación no afectará la licitud del tratamiento basada en el consentimiento previo a su retiro. El retiro deberá poder realizarse por medios simples, gratuitos y equivalentes a los utilizados para otorgarlo.	La aplicación plantea interrogantes cuando la base de licitud invocada es el consentimiento tácito previsto en el artículo 11. En tales supuestos, la licitud del tratamiento previo dependerá de acreditar que el consentimiento tácito se configuró válidamente, cuestión que el propio proyecto construye sobre la ausencia de oposición del titular y el contexto de la relación.
ARTÍCULO 13 — Régimen de datos seudononimizados. El tratamiento de datos personales seudonimizados será lícito, sin necesidad de cumplir con alguna de las condiciones del artículo 5°, cuando el tratamiento se realice con fines de: [...]	ADVERTENCIA: Ojo!. Esta solución resulta discutible desde la técnica legislativa. La propia definición contenida en el artículo 2 restablece que la seudonimización no elimina el carácter personal del dato, sino que únicamente reduce la posibilidad de identificar a su titular mediante la aplicación de medidas técnicas u organizativas adicionales. Mientras que la anonimización hace desaparecer el dato personal, la seudonimización mantiene su naturaleza jurídica como dato personal. Si ello es así, no resulta evidente por qué la sola aplicación de una medida de seguridad como la seudonomización podría dispensar al responsable de acreditar una base de licitud para su tratamiento.

Artículo	Observación
ARTÍCULO 14 — Tratamiento de datos sensibles. Los datos sensibles únicamente pueden ser objeto de tratamiento cuando: [...] e) El tratamiento se refiera a datos manifiestamente hechos públicos por su titular; [...]	Se reitera comentario realizado al artículo 5 respecto a que la publicidad no altera el carácter sensible del dato. La utilización de una red social, la participación en un foro o la integración de un grupo abierto en línea no necesariamente implican la voluntad de habilitar cualquier tratamiento ulterior de esos datos
ARTÍCULO 14 — Tratamiento de datos sensibles. Los datos sensibles únicamente pueden ser objeto de tratamiento cuando: [...] j) El tratamiento se realice con fines históricos, estadísticos o de investigación científica; y, en estos dos últimos casos, siempre que se adopten medidas de seudonimización, sujetas a las condiciones del artículo 13 (Régimen de datos seudonimizados);	Veáse comentario a Art 13.
ARTÍCULO 17 — Entrenamiento de sistemas de inteligencia artificial. El tratamiento de datos personales para entrenamiento, desarrollo y evaluación de sistemas de inteligencia artificial será válido como interés legítimo conforme al artículo 5 (Principio de licitud), inciso f), cuando: a) No incluyan datos sensibles, salvo consentimiento expreso; b) El responsable implemente medidas de seguridad proporcionales al impacto y conforme a estándares internacionales; y c) El titular cuente con un mecanismo claro, gratuito y accesible para ejercer su derecho de oposición en sistemas de inteligencia artificial. La oposición ejercida producirá efectos a partir del siguiente ciclo de entrenamiento o actualización del modelo, debiendo el responsable documentar y ser capaz de acreditar ante la autoridad de control, en la medida que ello le sea requerido, la efectiva exclusión de los datos objetados.	La solución desplaza el análisis desde la ponderación caso por caso hacia una habilitación legal de alcance general, ampliando significativamente el ámbito de aplicación del interés legítimo previsto en el artículo 5. En este sentido, podría considerarse la incorporación de salvaguardas adicionales que refuercen la protección de los titulares, tales como la exigencia de P.I.A.s específicas para estos tratamientos, criterios más precisos para la ponderación de intereses

Artículo	Observación
ARTÍCULO 19 — Transferencia internacional. Toda transferencia internacional de datos personales es lícita si, a reserva de las demás disposiciones de la presente, el país u organismo internacional receptor ha sido declarado con un nivel de protección adecuado por la autoridad de control. A falta de una decisión de adecuación, la transferencia internacional de datos personales también será lícita si: [...] f) El responsable elija infraestructura tecnológica ubicada fuera de la República Argentina, siempre que el proveedor garantice medidas técnicas de seguridad adecuadas;	Las medidas técnicas de seguridad constituyen un elemento distinto del nivel de protección jurídica ofrecido por el país de destino. La licitud de una transferencia internacional no depende exclusivamente de la seguridad informática del proveedor, sino también del marco normativo aplicable a los datos una vez transferidos, de las facultades de acceso de las autoridades públicas extranjeras y de la existencia de mecanismos efectivos de tutela para los titulares
ARTÍCULO 23 — Supresión de datos en sistemas de inteligencia artificial ya entrenados. Cuando el titular solicite la supresión de datos personales utilizados en entrenamientos previos de sistemas de inteligencia artificial, el responsable deberá evaluar en primer término si dicha supresión es técnicamente viable sin comprometer la integridad fundamental del modelo, entendida como su estabilidad, rendimiento o funcionalidad esencial. Si la supresión no resultara técnicamente viable, el responsable deberá documentar la imposibilidad mediante un informe técnico con carácter de declaración jurada, realizada bajo condiciones de confidencialidad frente a terceros, pero accesible para la autoridad de control y para el propio titular. En tales casos, el responsable aplicará medidas alternativas que permitan mitigar el impacto del tratamiento previo, incluyendo: el bloqueo inmediato del uso futuro de esos datos; su exclusión en nuevos ciclos de entrenamiento, ajuste o versiones posteriores del modelo; y la anonimización del registro cuando ello sea técnicamente posible. Todo el procedimiento deberá desarrollarse de conformidad con el principio de transparencia establecido en el artículo 10 (Principio de transparencia).	No se establece ompensación ecónomica de algún tipo al titular de los datos por el uso de los mismos.

Artículo	Observación
ARTÍCULO 24 — Derecho de oposición. El titular de los datos puede oponerse al tratamiento de sus datos, o a una finalidad específica de éste.	El artículo reconoce el derecho de oposición, pero no regula sus efectos ni establece los criterios que deben seguirse una vez ejercido. No se precisa, en particular, si la oposición obliga al responsable a cesar el tratamiento, bajo qué circunstancias podría continuar realizándolo ni cómo debe resolverse la eventual colisión entre los motivos invocados por el titular y la base de licitud utilizada por el responsable. La ausencia de estas reglas resulta especialmente relevante en aquellos tratamientos fundados en el interés legítimo, respecto de los cuales el derecho de oposición constituye una de las principales garantías del titular. La formulación excesivamente escueta puede trasladar a la reglamentación, a la autoridad de control o a los tribunales la determinación del contenido efectivo de un derecho reconocido por la propia ley.
ARTÍCULO 25 — Derecho a revisión en decisiones automatizadas y elaboración de perfiles. El titular tendrá derecho a solicitar la revisión de decisiones basadas exclusivamente en tratamientos automatizados, incluida la elaboración de perfiles, que afecten de manera sustancial los derechos, intereses o expectativas legítimas del titular de los datos. Ante una solicitud del titular, el responsable deberá adoptar medidas proporcionales al tipo de tratamiento, el contexto y los efectos sobre el titular. La respuesta podrá consistir en una revisión con intervención humana, en la provisión de información general sobre los principales factores considerados, o en cualquier otra medida adecuada a las circunstancias. En ningún caso esta obligación implicará la divulgación de algoritmos, modelos, ponderaciones ni información técnica o comercialmente sensible. Este derecho no será aplicable cuando la decisión resulte necesaria para la ejecución de una relación contractual, esté autorizada por normativa aplicable, o no produzca efectos jurídicos ni impactos significativos sobre el titular. Tampoco será aplicable cuando su ejercicio implique una afectación desproporcionada al funcionamiento del servicio o a intereses legítimos del responsable.	La regulación propuesta debilita significativamente el contenido del derecho que pretende reconocer. Si el titular tiene derecho a solicitar la revisión de una decisión automatizada, la respuesta del responsable debería garantizar una revisión efectiva y, cuando corresponda, una intervención humana significativa. Sin embargo, el artículo permite satisfacer la solicitud mediante la mera provisión de “información general sobre los principales factores considerados” o a través de “cualquier otra medida adecuada a las circunstancias”. De este modo, el ejercicio de un derecho a revisión podría concluir sin que la decisión cuestionada sea efectivamente revisada. Asimismo, resulta excesiva la disposición según la cual el ejercicio de este derecho no podrá implicar “en ningún caso” la divulgación de algoritmos, modelos, ponderaciones o información técnica o comercialmente sensible. La protección de secretos comerciales puede justificar salvaguardas específicas, pero no debería operar como una prohibición absoluta que impida proporcionar la información necesaria para comprender e impugnar una decisión. Esta cuestión adquiere particular relevancia cuando sistemas automatizados son utilizados por organismos públicos para adoptar decisiones capaces de determinar o afectar derechos. La norma debería contemplar, al menos, mecanismos que permitan el acceso a la información pertinente por parte del titular, la autoridad de control y los órganos judiciales, cuando ello resulte necesario, bajo condiciones adecuadas de confidencialidad

Artículo	Observación
	Las excepciones previstas resultan excesivamente amplias. En particular, las referencias genéricas a decisiones autorizadas por “normativa aplicable” y a una eventual afectación desproporcionada de los “intereses legítimos del responsable” introducen conceptos abiertos que pueden terminar vaciando de contenido el derecho reconocido. Se recomienda establecer con mayor precisión los supuestos excepcionales y exigir, aun en tales casos, garantías equivalentes que permitan al titular comprender, cuestionar y obtener una revisión efectiva de las decisiones que produzcan efectos significativos sobre sus derechos o intereses.
ARTÍCULO 26 — Derecho a la portabilidad de los datos personales. El titular tendrá derecho a recibir sus datos personales en un formato estructurado y de uso común, y a que sean transmitidos a otro responsable, siempre que se realice exclusivamente por medios automatizados y que no afecte a derechos de terceros, salvo que su ejercicio imponga una carga financiera o técnica excesiva o irrazonable sobre el responsable o encargado del tratamiento. Este derecho será aplicable a los datos proporcionados directamente por el titular. No incluirá los parámetros internos de modelos, ponderaciones algorítmicas ni información técnica protegida por secreto comercial.	La regulación incorpora excepciones excesivamente abiertas al ejercicio del derecho. En particular, permitir su denegación cuando imponga una carga financiera o técnica “excesiva o irrazonable” deja en manos del responsable una valoración que puede vaciar de contenido la portabilidad, sin establecer criterios objetivos para determinar cuándo se configura dicha carga. Asimismo, debería precisarse el alcance de la expresión “datos proporcionados directamente por el titular”, a fin de evitar interpretaciones excesivamente restrictivas respecto de información generada a partir de su utilización de un servicio. La regulación debería procurar que la portabilidad constituya una herramienta efectiva de interoperabilidad y movilidad del titular entre prestadores.
ARTÍCULO 28 — Abuso de derecho. El responsable del tratamiento podrá negarse a dar curso a una solicitud o, en su defecto, cobrar un canon razonable basado en los costos administrativos, cuando:	La disposición utiliza la categoría de “abuso de derecho” para habilitar restricciones al ejercicio de derechos fundamentales y, en determinados casos, el cobro de un canon. La fórmula requiere criterios especialmente estrictos. Resulta particularmente problemática la posibilidad de rechazar una solicitud cuando su cumplimiento “revele necesariamente información comercial confidencial o secretos industriales”. La existencia de información protegida puede justificar mecanismos de confidencialidad, acceso restringido o disociación, pero no debería operar automáticamente como causa de denegación de un derecho reconocido por la ley. El problema reproduce la tensión advertida en el artículo 25: el secreto comercial aparece configurado como un límite absoluto, en vez de como un interés que debe ser armonizado con los derechos del titular.

Artículo	Observación
ARTÍCULO 29 — Excepciones al ejercicio de los derechos. En el caso de bases de datos públicas, los responsables del tratamiento podrán, mediante decisión fundada, denegar los derechos enumerados en este Título en los siguientes supuestos: a) Cuando sea necesario para la protección de la defensa de la Nación, del orden y la seguridad públicos, o para la protección de los derechos e intereses de terceros; o b) Cuando el ejercicio de los derechos pudiera obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del ambiente, la investigación de delitos penales o la verificación de infracciones administrativas. En cualquier caso, el responsable del tratamiento debe brindar acceso a los datos en cuestión cuando el titular demuestre que son necesarios para ejercer su derecho de defensa.	Las excepciones aplicables a bases de datos públicas se encuentran formuladas en términos demasiado amplios. Expresiones como “protección de los derechos e intereses de terceros” o la eventual obstaculización de actuaciones administrativas pueden abarcar una cantidad muy significativa de tratamientos estatales. La norma debería exigir que toda restricción sea necesaria, proporcional, temporal y vinculada concretamente con la finalidad que justifica la excepción, garantizando además mecanismos efectivos de revisión.
ARTÍCULO 30 — Medidas de seguridad según categoría de tratamiento. Las medidas adoptadas para garantizar la seguridad y confidencialidad de los datos personales deberán ser proporcionales a la naturaleza, finalidad y contexto del tratamiento y de conformidad con la categoría en la que se encuentre encuadrado según las definiciones del artículo 2 (Definiciones). [...]	La categorización entre tratamientos básicos, intermedios y avanzados puede resultar útil para aplicar obligaciones proporcionales. Sin embargo, el proyecto convierte justamente algunas de las principales garantías frente a tratamientos de alto riesgo en obligaciones meramente eventuales. Para los tratamientos avanzados dispone la realización de evaluaciones de impacto únicamente “cuando corresponda”. No establece qué supuestos obligan a realizarlas, quién determina su procedencia, cuáles deben ser sus contenidos mínimos ni si deben efectuarse antes del inicio del tratamiento. Tratándose de operaciones a gran escala, datos sensibles, inteligencia artificial o decisiones automatizadas con efectos sustanciales, la evaluación de impacto debería constituir una obligación previa y claramente reglada, no una posibilidad sujeta a determinación posterior del responsable.

Artículo	Observación
ARTÍCULO 32 — Subcontratación. El encargado puede suscribir un contrato para subcontratar servicios que impliquen el tratamiento de datos cuando exista una autorización general o específica del responsable del tratamiento. En estos casos, el subcontratado asume el carácter de encargado en los términos y condiciones previstos en esta ley.	En materia de subcontratación, admitir una autorización "general" del responsable sin prever mecanismos de información sobre la incorporación o sustitución de subencargados puede reducir significativamente el control sobre la cadena efectiva de tratamiento. Se recomienda establecer una obligación de trazabilidad que permita al responsable —y cuando corresponda al titular— conocer qué actores intervienen en el tratamiento y bajo qué condiciones.
ARTÍCULO 34 — Mecanismos de autorregulación vinculantes. Los responsables y encargados podrán elaborar, adoptar y utilizar mecanismos de autorregulación vinculantes destinados a contribuir a la correcta aplicación de la presente ley, tales como códigos de conducta, reglas de buenas prácticas, normas corporativas vinculantes, sellos, marcas, certificaciones internacionales y otros mecanismos equivalentes, nacionales o internacionales [...] La falta de homologación previa no obstará a la validez y eficacia de dichos mecanismos como prueba del cumplimiento del principio de seguridad, confidencialidad y responsabilidad proactiva, ni a su consideración como factor de mitigación en procedimientos sancionatorios. [...]	La disposición corre el riesgo de otorgar efectos jurídicos relevantes a estándares elaborados unilateralmente por los propios regulados. Si tales mecanismos serán considerados evidencia privilegiada de cumplimiento o circunstancia atenuante, deberían existir requisitos mínimos de transparencia, independencia, verificación y control público.
ARTÍCULO 35 — Bases de datos públicas. La creación, modificación sustancial o supresión de bases de datos pertenecientes a autoridades u organismos públicos solo podrá efectuarse por norma de alcance general, publicada en el Boletín Oficial. [...] La creación o modificación sustancial de la base de datos deberá ser comunicada a la autoridad de control, en la forma y plazo que establezca la reglamentación. La norma que disponga la supresión de una base de datos deberá establecer el destino de la información contenida en ella o las medidas que se adopten para su destrucción, anonimización o archivo, según corresponda.	Las limitaciones a los derechos de acceso, información, rectificación, supresión u oposición en materia de seguridad e inteligencia deberían encontrarse determinadas por la propia ley con suficiente precisión. No parece adecuado que el alcance concreto de esos derechos pueda ser reducido posteriormente mediante reglamentación administrativa. La norma debería definir los supuestos, condiciones, duración y mecanismos de revisión de las restricciones, asegurando especialmente su carácter excepcional, necesario y proporcional.

Artículo	Observación
ARTÍCULO 40 — Facultades de la autoridad de control. La autoridad de control tendrá las siguientes funciones y atribuciones: [...]	El régimen de facultades debe analizarse conjuntamente con el artículo 43. La autoridad recibe facultades de auditoría e inspección, pero luego se le prohíbe de manera absoluta acceder a código fuente, algoritmos o propiedad intelectual. Esta limitación puede tornar materialmente imposible una fiscalización efectiva de determinados sistemas automatizados. La confidencialidad puede y debe protegerse mediante salvaguardas específicas, pero no parece razonable impedir por ley que el organismo especializado pueda acceder, cuando sea indispensable para una investigación, justamente a los elementos técnicos necesarios para determinar si el tratamiento cumple la normativa.
ARTÍCULO 43 — Verificación de oficio o por denuncia de un tercero. La autoridad de control verificará el cumplimiento de la ley de oficio o por denuncia de un tercero. A tal fin, la autoridad podrá: a) Requerir informes y acceso a la documentación pertinente; y b) Realizar inspecciones o auditorías técnicas sobre los sistemas de tratamiento, bajo el principio de confidencialidad. En ningún caso esta facultad podrá implicar la divulgación, entrega o acceso a código fuente, algoritmos, secretos comerciales o propiedad intelectual de los inspeccionados.	ADVERTENCIA: La prohibición absoluta de que las facultades de auditoría impliquen “acceso a código fuente, algoritmos, secretos comerciales o propiedad intelectual” compromete seriamente la capacidad de fiscalización de la autoridad. No todos los procedimientos exigirán acceso a estos elementos, pero en determinados sistemas —particularmente decisiones automatizadas o herramientas de inteligencia artificial— pueden constituir evidencia indispensable para determinar cómo se produjo el tratamiento cuestionado. La solución adecuada no parece ser prohibir el acceso, sino establecer mecanismos rigurosos de confidencialidad, reserva y utilización limitada de esa información.
ARTÍCULO 45 — Recomendación. Detectada una infracción que no revista gravedad o dolo manifiesto, la autoridad de control emitirá, antes de sancionar, una recomendación de cumplimiento. En ella se detallarán las medidas correctivas que el responsable debe adoptar en un plazo determinado. Si el responsable cumple satisfactoriamente con la recomendación, la autoridad podrá dar por finalizado el proceso con un apercibimiento.	Debería revisarse la utilización del concepto de “dolo manifiesto” como criterio para determinar cuándo corresponde una recomendación previa a la sanción. La responsabilidad administrativa en materia de protección de datos no debería depender necesariamente de categorías subjetivas propias de otros regímenes de responsabilidad.

Artículo	Observación
ARTÍCULO 46 — Infracciones. Constituyen infracciones a la presente ley las siguientes conductas: a) Infracciones leves I) Incumplimiento de deberes de información; II) Deficiencias en registros y documentación; o III) Incumplimiento de términos para responder solicitudes. b) Infracciones graves I) Tratamiento sin base legal; II) Violación de principios fundamentales; III) Incumplimiento de derechos del titular; o IV) Deficiencias en medidas de seguridad. c) Infracciones muy graves I) Tratamiento masivo de datos sensibles sin autorización; II) Uso discriminatorio de datos sensibles; III) Violaciones masivas de seguridad; IV) Desobediencia a órdenes de la autoridad; V) Reincidencia en infracciones graves; u VI) Obstaculización de investigaciones de la autoridad de control mediante ocultamiento, destrucción, falsificación o alteración de documentos, o negativa de acceso a instalaciones.	La tipificación presenta categorías excesivamente abiertas para un régimen sancionatorio. Expresiones como “violación de principios fundamentales”, “deficiencias en medidas de seguridad” o “violaciones masivas de seguridad” requieren mayor precisión. La previsibilidad de las conductas sancionables constituye una garantía tanto para los titulares como para los regulados. Se recomienda definir criterios que permitan diferenciar con claridad infracciones leves, graves y muy graves a fines de evitar la inaplicabilidad de la norma en instancia judicial.

Artículo	Observación
ARTÍCULO 50 — Sector público. Las sanciones consistentes en multas económicas previstas en este Título no serán de aplicación al Sector Público Nacional, definido por el artículo 8 de la Ley N° 24.156. En caso de que la autoridad de control advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá las actuaciones a la autoridad jerárquica correspondiente y a los organismos de control interno para el inicio de las investigaciones disciplinarias que correspondan.	El régimen establece una diferencia sustancial entre responsables públicos y privados. Frente a incumplimientos estatales, las multas quedan excluidas y la consecuencia prevista consiste fundamentalmente en remitir las actuaciones a la autoridad jerárquica y a los organismos de control interno. Dado que algunos de los tratamientos con mayor capacidad de afectar derechos fundamentales son realizados precisamente por el Estado, el régimen debería garantizar mecanismos de responsabilidad y consecuencias institucionales suficientemente eficaces. La exclusión de las multas puede ser razonable por la naturaleza del sujeto sancionado, pero debería complementarse con obligaciones correctivas, mecanismos de responsabilidad de los funcionarios intervinientes y medidas específicas de transparencia y rendición de cuentas.
TÍTULO X — SANDBOX REGULATORIO ARTÍCULO 62 — Sandbox regulatorio. La autoridad de control podrá autorizar, mediante resolución fundada, la implementación de entornos regulatorios de prueba para proyectos innovadores que involucren el tratamiento de datos personales, incluyendo aquellos basados en inteligencia artificial, nuevos modelos de negocio o mecanismos alternativos de cumplimiento.	La regulación propuesta otorga a la autoridad de control una potestad especialmente amplia para autorizar “condiciones diferenciadas respecto de las obligaciones establecidas en la presente ley”. La disposición no determina qué obligaciones pueden ser flexibilizadas ni establece un núcleo de garantías inderogables. Una autoridad administrativa podría, de ese modo, autorizar excepciones temporales a obligaciones impuestas directamente por el Poder Legislativo. La ley debería establecer expresamente qué disposiciones resultan indisponibles dentro de un sandbox —principios generales, derechos de los titulares, tratamiento de datos sensibles, seguridad, transparencia y mecanismos de reclamación— y delimitar cuáles obligaciones estrictamente instrumentales podrían flexibilizarse. También deberían contemplarse mecanismos de publicidad de los proyectos autorizados, criterios objetivos de admisión, supervisión periódica, revocación de la autorización y condiciones específicas para el tratamiento de los datos obtenidos durante las pruebas.

Artículo	Observación
ARTÍCULO 66 — Orden público y jurisdicción federal. Las normas de la presente ley contenidas en los Títulos I, II, III, IV, V, VI y XII son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias y a la Ciudad de Buenos Aires a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La competencia federal regirá respecto de: a) Los tratamientos de datos efectuados por las autoridades u organismos públicos pertenecientes a la Administración Pública Nacional; y b) Los tratamientos de datos efectuados por el sector privado, cuando los datos se encuentren accesibles en redes interjurisdiccionales, nacionales o internacionales.	Debe revisarse la amplitud de la competencia federal respecto del sector privado cuando los datos se encuentren “accesibles en redes interjurisdiccionales, nacionales o internacionales”. En el entorno digital contemporáneo, prácticamente cualquier base o servicio conectado a Internet puede quedar alcanzado por esta fórmula, con el resultado potencial de federalizar una porción muy significativa de los litigios sobre protección de datos. La norma debería utilizar un criterio de conexión más preciso que permita determinar cuándo existe verdaderamente un interés federal suficiente para desplazar la competencia local. Es de resaltar que, en el estado actual del arte, una norma amplia que haga prevalecer el privilegio de la competencia federal tiene la potencialidad de menoscabar sustancialmente la jurisdicción ordinaria de las provincias.