PROTECCIÓN DE DATOS PERSONALES

El Cimiento Constitucional de la Privacidad: El Derecho a la Intimidad y la Acción de Hábeas Data

El marco jurídico de la protección de datos en la República Argentina encuentra su raíz y su máxima jerarquía en la Constitución Nacional, la cual establece las bases éticas y operativas sobre las que debe edificarse cualquier sistema de información. El artículo 19 de la Constitución Nacional consagra el principio de reserva, determinando que "*las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios y exentas de la autoridad de los magistrados*". Este principio, en conjunción con el artículo 18 que tutela la inviolabilidad del domicilio, de los papeles privados y de la correspondencia epistolar, conforma la esfera tradicional del derecho a la intimidad, la cual hoy se extiende analógicamente a las nuevas técnicas de comunicación electrónica y al entorno digital. Como profesionales es fundamental comprender que el diseño de cualquier software, base de datos o entorno inteligente de captura de datos debe respetar este límite constitucional de no intromisión en la vida privada.

La reforma constitucional del año 1994 dio un paso definitivo al incorporar la Acción de Amparo especial o de **hábeas data** en el tercer párrafo del artículo 43. Esta garantía constitucional faculta a toda persona a interponer una acción judicial para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o en los privados destinados a proveer informes. Asimismo, en caso de falsedad, inexactitud o discriminación, permite exigir judicialmente la supresión, rectificación, confidencialidad o actualización de aquellos. Para un ingeniero de software, esto significa que el sistema debe estar estructurado de tal manera que las operaciones de consulta, modificación y eliminación por parte del titular del dato no solo sean técnicamente viables, sino jurídicamente fluidas y seguras.

Ley 25.326, Convenio 108+ y ley de Acceso a la Información Pública

Para reglamentar esta garantía constitucional, el Congreso de la Nación sancionó en el año 2000 la **Ley 25.326 de Protección de Datos Personales**. Esta ley, pionera en Sudamérica, tomó como modelo regulatorio la Directiva 95/46/CE del Parlamento Europeo y la Ley Orgánica de España de 1999, buscando unificar las condiciones de operación de todas las bases de datos públicas y privadas destinadas a dar informes. A nivel internacional, este andamiaje se fortalece con la adhesión de la Argentina al **Convenio 108+** (Convenio para la protección de

las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa), cuya versión actualizada fue refrendada en el país mediante la Ley 27.699 en el año 2022. Este convenio internacional obliga a aplicar las salvaguardas tanto en el sector público como en el privado, regulando el flujo transfronterizo de datos hacia países que no cuenten con niveles adecuados de protección.

En paralelo a la protección de la esfera privada, coexiste el derecho de acceso a la información pública, regulado por la **Ley 27.275 (y en Mendoza por Ley 9070 – Ministerio Público Fiscal Mendoza)**. Esta norma se funda en el principio de presunción de publicidad, según el cual toda la información en poder del Estado se presume pública, salvo excepciones taxativas, y debe ser accesible en formatos electrónicos abiertos que faciliten su procesamiento automático y su reutilización.

El punto de convergencia y control de este trinomio normativo es la **Agencia de Acceso a la Información Pública (AAIP)**, creada como un ente autárquico con autonomía funcional, encargado de velar tanto por la transparencia del Estado como por la fiscalización de la protección integral de los datos personales. Para un profesional de la tecnología, la coexistencia de estas leyes exige el dominio del concepto de **disociación de datos**, técnica mediante la cual se debe ocultar o separar la información personal de un documento público antes de su divulgación para evitar la vulneración de la privacidad.

Finalidad, Objetivos y el Derecho a la Autodeterminación Informativa

La Ley de Protección de Datos Personales tiene como finalidad última garantizar el honor y la intimidad de las personas, así como también asegurar el efectivo control de las personas sobre el uso de sus propios datos. Doctrinaria y jurisprudencialmente, este control se traduce en el derecho a la **autodeterminación informativa**, conceptualizado como la facultad que tiene todo individuo de decidir cuándo, cómo y qué información sobre su propia persona es objeto de tratamiento o procesamiento automatizado. Este concepto va mucho más allá del tradicional derecho pasivo a ser dejado en paz; es una prerrogativa activa que confiere al titular un protagonismo central para intervenir en el proceso de circulación de sus datos, verificando su veracidad, destino y confidencialidad.

En la práctica profesional, el respeto a la autodeterminación informativa se traduce en una competencia de diseño ético y técnico de los sistemas de información. El desarrollador no debe ver al usuario como una fuente inagotable de datos listos para ser capturados sin control, sino como el soberano de su identidad digital. Cada base de datos, cada interfaz de registro de usuarios y cada flujo de telemetría debe concebirse respetando este señorío del individuo sobre su propia información, garantizando que el tratamiento de datos no erosione su libertad individual ni derive en clasificaciones o perfiles invisibles que atenten contra su dignidad.

La Clasificación de los Datos

La correcta arquitectura de una base de datos requiere una rigurosa clasificación de la información según su naturaleza legal, pues de ello dependen las medidas de seguridad y los niveles de acceso que se deben implementar. La ley define como **dato personal** a toda información de cualquier tipo referida a personas físicas o de existencia ideal (personas jurídicas) que estén determinadas o que resulten determinables. Por ejemplo, una dirección de protocolo de Internet (IP) o una dirección de correo electrónico se consideran técnicamente datos personales si permiten individualizar al usuario que opera detrás de la máquina.

Por otro lado, la normativa define de manera taxativa los **datos sensibles**, que son aquellos datos personales que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, así como la información referente a la salud o a la vida sexual. La formación de archivos o registros que almacenen información que directa o indirectamente revele datos sensibles está estrictamente prohibida, con la única excepción de los registros de miembros que lleven organizaciones religiosas, políticas o sindicales para su propio funcionamiento, o cuando medien razones de interés general autorizadas por ley. A estas categorías se añaden de forma especial los **datos genéticos y biométricos**, los cuales permiten la identificación unívoca del individuo a través de rasgos físicos o conductuales, y los datos sobre **antecedentes penales** o contravencionales, que únicamente pueden ser objeto de tratamiento por parte de las autoridades públicas competentes en el marco de sus leyes respectivas. El ingeniero en ciencias de la computación debe saber que la inclusión de campos que contengan datos sensibles en el diseño de un formulario o base de datos es de carácter restrictivo y requiere el cifrado obligatorio y medidas críticas de control de acceso.

La siguiente tabla esquematiza la clasificación legal de los datos según la Disposición y su nivel de criticidad asociado:

Categoría de Dato	Definición Legal	Ejemplos Prácticos	Nivel de Seguridad
Datos Personales Generales	Información referida a personas físicas o de existencia ideal (jurídicas) determinadas o determinables.	Nombre, DNI, CUIT, IP de red, correo electrónico, domicilio.	Básico (Control de accesos generales y copias)
Datos Sensibles	Revelan origen racial/étnico, opiniones políticas, convicciones religiosas, afiliación sindical, salud o vida sexual.	Filiación política, credo religioso, diagnósticos médicos, historial de salud.	Crítico (Cifrado fuerte, prohibición general de archivo)
Datos Especiales y Biométricos	Rasgos físicos/conductuales únicos o relativos a antecedentes judiciales.	Huellas dactilares, reconocimiento facial, ADN, antecedentes penales.	Crítico (Cifrado, consentimiento explícito, alto resguardo)

El Archivo y el Tratamiento de Datos

Para el diseño de sistemas legamente conformes, es indispensable manejar con precisión la terminología operativa de la ley. Se entiende por **archivo, registro, base o banco de datos** al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, ya sea electrónico o no, independientemente de la modalidad de su formación, almacenamiento, organización o acceso. Esta definición es tecnológicamente neutra, lo que significa que abarca desde un archivo de texto plano o una hoja de cálculo local hasta sofisticadas arquitecturas distribuidas de bases de datos relacionales, no relacionales o almacenamiento estructurado en la nube.

Por su parte, el **tratamiento de datos** se define como el conjunto de 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. En términos de ingeniería de software, cada una de las operaciones del ciclo de vida del dato —desde el momento en que se captura mediante una interfaz (recolección), se procesa en el backend (modificación y relacionamiento), se resguarda en un disco (conservación) y se elimina de los servidores (destrucción)— constituye un acto de tratamiento de datos regulado por la ley. Por lo tanto, el desarrollador es el responsable de programar estas funciones de modo que el sistema mantenga la trazabilidad y la seguridad en cada una de estas etapas de tratamiento.

Los Sujetos de la Relación de Datos y la Arquitectura de Computación en la Nube

La ley individualiza a tres sujetos esenciales en toda relación de datos: el responsable, el titular y el usuario de datos. El ***responsable del archivo o banco de datos*** es la persona física o jurídica, pública o privada, que es la titular del archivo y que tiene el poder de decisión sobre la finalidad del tratamiento. El ***titular de los datos*** es la persona física o de existencia ideal cuyos datos son objeto de tratamiento. Por último, ***el usuario de datos*** es toda persona, pública o privada, que realiza el tratamiento a su arbitrio, ya sea en bases de datos propias o mediante conexión con las mismas. A estos roles, el Convenio 108+ añade la figura del ***encargado del tratamiento***, que es aquella persona física o jurídica, autoridad pública o servicio que da tratamiento a los datos personales en nombre y por cuenta del responsable del tratamiento.

Esta delimitación de roles adquiere una importancia crítica al momento de estructurar soluciones de **cloud computing** o computación en la nube. Cuando una empresa migra sus servicios a un proveedor de infraestructura en la nube, el proveedor actúa técnicamente como un encargado del tratamiento, mientras que la empresa contratante sigue siendo la responsable de la base de datos. Esto exige la firma de un contrato detallado de prestación de servicios de tratamiento de datos, el cual debe establecer taxativamente que el proveedor de la nube solo procesará la información siguiendo las instrucciones y órdenes de la empresa contratante, prohibiéndole utilizar los datos para fines propios o cederlos a terceros, incluso para fines de

mera conservación. Asimismo, el contrato debe garantizar que la infraestructura del proveedor cumpla con los niveles de seguridad y confidencialidad exigidos por la legislación del país de origen de los datos, previendo mecanismos para la total supresión o reintegro de la información una vez finalizada la relación contractual. Si los servidores de la nube están ubicados en el extranjero, se configura una **transferencia internacional de datos**, la cual requiere el previo consentimiento expreso del titular o la existencia de un marco contractual adecuado aprobado por la autoridad de control local.

Principios Rectores

La formación y operación de cualquier archivo de datos es lícita únicamente si se encuentra debidamente inscrita ante el organismo de control y si respeta estrictamente los principios rectores que establece la ley. Como futuros profesionales, deben memorizar y aplicar estos principios en cada desarrollo técnico que realicen. El ***principio de pertinencia y no exceso*** determina que los datos recogidos deben ser ciertos, adecuados y no excesivos en relación al ámbito y la finalidad específica para la que se obtuvieron. Por ejemplo, si una aplicación de análisis crediticio requiere evaluar la solvencia económica de un cliente, es ilícito y excesivo que el sistema le exija datos sobre su filiación política, orientación sexual o creencias religiosas.

El ***principio de finalidad*** establece que los datos objeto de tratamiento no pueden ser utilizados para propósitos distintos o incompatibles con aquellos que motivaron su obtención original. Si un usuario entrega su correo electrónico para recibir un aviso de compra, la empresa no puede desviar ese dato para enviarle publicidad no solicitada o vender su contacto a terceras compañías sin su consentimiento inequívoco. El ***principio de exactitud*** obliga a mantener la información actualizada y a suprimir o sustituir de oficio los datos inexactos o incompletos. La ***limitación en el tiempo*** exige que los datos sean destruidos o anonimizados mediante técnicas de disociación cuando hayan dejado de ser necesarios o pertinentes para los fines de su recolección. Finalmente, el ***principio de consentimiento*** estatuye que el tratamiento de datos es ilícito sin el consentimiento libre, expreso e informado del titular, el cual debe constar por escrito o por un medio técnico equiparable que garantice la autoría e integridad de la declaración. Este consentimiento es siempre revocable, sin efectos retroactivos.

Principio Rector	Descripción del Deber	Implicación para Informática / Sistemas
Pertinencia	Los datos deben ser ciertos, adecuados y no excesivos en relación con el fin de su recolección.	Evitar solicitar datos no relacionados con el servicio (ej. religión del usuario en apps comerciales).
Finalidad	La información no puede ser utilizada para fines distintos o incompatibles con los que motivaron su obtención.	No desviar correos de facturación para publicidad no solicitada sin consentimiento expreso del usuario.
Exactitud	Los datos deben ser exactos, actualizados y completarse o suprimirse de oficio si están desactualizados.	Proveer paneles de autogestión de perfil y rectificación ágil (plazo de 5 días hábiles por ley).
Limitación en el Tiempo	Los datos deben ser destruidos o anonimizados cuando dejan de ser necesarios para el fin original.	Programar triggers o tareas programadas de borrado definitivo o procesos de disociación de datos.
Consentimiento	El tratamiento de datos es ilícito sin el consentimiento libre, expreso e informado del titular.	Diseñar pantallas de registro con términos claros; el consentimiento debe ser inequívoco y revocable.

Las Excepciones al Consentimiento Previo y su Rigurosa Interpretación

Si bien el consentimiento del titular es la regla general que legitima el tratamiento de los datos, la ley prevé excepciones puntuales y de interpretación restrictiva en las cuales no es necesario contar con dicha autorización. Es vital que un desarrollador de software o diseñador de procesos conozca estas excepciones para no implementar bloqueos innecesarios en los flujos de información legítimos, pero cuidando siempre de no exceder los límites legales. El consentimiento no es requerido cuando los datos se obtengan de fuentes de acceso público irrestricto, o cuando se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal expresa.

Asimismo, se exceptúan del consentimiento previo aquellos listados cuyos datos personales se limiten de forma estricta a nombre y apellido, documento nacional de identidad (DNI), identificación tributaria o previsional (CUIT/CUIL), ocupación, fecha de nacimiento y domicilio.

También es lícito el tratamiento cuando los datos deriven de una relación contractual, científica o profesional del titular, siempre y cuando sean estrictamente necesarios para el desarrollo y fiel cumplimiento de dicha relación. La última excepción relevante está vinculada a las operaciones que realicen las entidades financieras y a las informaciones comerciales o de calificación crediticia que de ellas deriven, de acuerdo con las normativas bancarias aplicables, lo que permite el funcionamiento de sistemas automatizados de scoring y consulta crediticia sin necesidad de consentimiento para la mera cesión ligada al giro comercial. Fuera de estos

supuestos expresos, cualquier tratamiento de datos sin consentimiento constituye una infracción grave pasible de sanciones administrativas y penales.

Derechos de los Titulares

El diseño de la experiencia de usuario en sistemas informáticos debe contemplar la habilitación sencilla y directa de los derechos que la ley confiere a los titulares de los datos. En primer lugar, el ***derecho de información*** exige que, al momento de recabar los datos, se informe previamente al usuario de manera clara sobre la finalidad del tratamiento, la existencia de la base de datos, la identidad del responsable, el carácter obligatorio o facultativo de sus respuestas y la posibilidad de ejercer sus derechos de acceso, rectificación y supresión.

El ***derecho de acceso*** faculta al titular a solicitar y obtener información completa y gratuita sobre sus datos incluidos en cualquier registro público o privado destinado a proveer informes, debiendo el responsable evacuar el pedido en un plazo máximo e improrrogable de diez días corridos. Técnicamente, la información debe ser suministrada de forma clara, exenta de codificaciones, en un lenguaje accesible para el conocimiento medio de la población y cubriendo la totalidad del registro concerniente al titular, sin revelar datos de terceros. Por su parte, el ***derecho de rectificación, actualización o supresión*** obliga al responsable del sistema a realizar los cambios requeridos en un plazo máximo de cinco días hábiles de recibido el reclamo o advertido el error. Finalmente, el Convenio 108+ introduce el ***derecho de toda persona a no estar sujeta a una decisión automatizada*** que la afecte significativamente (como un scoring de crédito o una selección de personal algorítmica) sin que se consideren sus opiniones, así como el derecho a conocer el razonamiento y la lógica subyacente que utiliza el sistema de inteligencia artificial o algoritmo para procesar su perfil personal.

Obligaciones de los Responsables de Bases de Datos y Niveles de Seguridad

El cumplimiento normativo impone a las organizaciones y a sus equipos de tecnología dos obligaciones operativas fundamentales: el *deber de confidencialidad* y el *deber de seguridad*. El ***deber de confidencialidad o secreto profesional*** obliga a todas las personas que intervengan en cualquier fase del tratamiento de datos a guardar reserva sobre los mismos, una obligación que subsiste de manera vitalicia aun después de finalizada la relación laboral o contractual con la empresa o con el titular del dato. El obligado solo puede ser relevado de este deber mediante una orden judicial fundada o por razones excepcionales de seguridad o salud pública.

En lo que respecta al ***deber de seguridad***, el responsable debe adoptar las medidas técnicas y organizativas necesarias para garantizar la integridad, confidencialidad y disponibilidad de los datos personales, evitando su adulteración, pérdida, fuga, consulta o tratamiento no autorizado.

En Argentina, la Disposición 11/2006 de la autoridad de control estructuró estas exigencias en tres niveles de seguridad: *básico, medio y crítico*, conforme a la sensibilidad de los datos

tratados. El ***nivel básico*** aplica a datos identificatorios generales; el ***nivel medio*** se exige cuando se tratan datos patrimoniales, financieros o de solvencia; y el ***nivel crítico*** es de cumplimiento obligatorio cuando se procesan datos sensibles, biométricos o antecedentes penales. Para cada nivel, el responsable debe diseñar e implementar controles específicos, tales como registros de auditoría (logs) de acceso a los servidores, cifrado de datos en reposo y en tránsito, planes de contingencia para la continuidad de las operaciones y la redacción obligatoria del Documento de Seguridad de Datos Personales, que detalla de forma exhaustiva las medidas implementadas. Queda terminantemente prohibido registrar información personal en bases de datos que no reúnan estas condiciones de seguridad.

Nivel de Seguridad	Datos de Aplicación	Medidas Técnicas Requeridas
Básico	Datos identificatorios generales (nombre, DNI, dirección, correo, teléfono).	Identificación y autenticación única de usuarios, control de accesos autorizados, copias de seguridad semanales, almacenamiento seguro.
Medio	Datos patrimoniales, de solvencia crediticia y transacciones financieras.	Nivel Básico + Registro obligatorio de accesos (logs), controles de acceso físico a servidores, auditorías de seguridad periódicas.
Crítico	Datos sensibles, biométricos, genéticos o antecedentes penales.	Nivel Medio + Cifrado obligatorio de datos en reposo y en tránsito, logs detallados de cada transacción (lectura/escritura), plan de contingencia formal, redacción obligatoria del Documento de Seguridad.

Riesgos en el Entorno Digital, Ciberprivacidad y Soluciones Tecnológicas de Diseño

La era digital y la hiperconectividad han potenciado geométricamente las amenazas a la privacidad, haciendo que la ciberseguridad sea una disciplina inseparable de la protección de datos personales. Entre los principales **riesgos en internet** que comprometen la privacidad, se destaca el seguimiento y perfilado invisible de los usuarios en la web mediante el uso abusivo de **cookies** y tecnologías de rastreo sin transparencia ni control. Asimismo, la proliferación de brechas y fugas de datos masivas expone la información personal de millones de ciudadanos a la ciberdelincuencia, facilitando fraudes de suplantación de identidad digital, ataques de phishing orientados al robo de credenciales financieras y extorsiones mediante el secuestro de información por ransomware. A esto se suma el surgimiento de deepfakes con inteligencia artificial que comprometen la imagen y el honor de las personas, así como las graves amenazas internas en las organizaciones provocadas por negligencias del personal o accesos no autorizados a las bases de datos de producción por parte de los desarrolladores.

Para mitigar estos riesgos de forma efectiva, la mera aplicación de parches o soluciones de seguridad reactivas es insuficiente. La ingeniería informática actual exige la adopción del ***principio de privacidad por diseño y por defecto***, el cual impone que la protección de datos personales sea una variable estructural integrada en todas las fases del ciclo de vida del desarrollo de sistemas. Esto se materializa a través de soluciones tecnológicas robustas como el **cifrado o encriptación** de datos, el cual transforma la información en un formato incomprensible para cualquier intruso no autorizado que logre traspasar las barreras de red. Asimismo, se deben implementar controles de acceso basados en roles y con el principio de mínimo privilegio, garantizando que el personal solo acceda a los datos estrictamente necesarios para su función. Finalmente, la obligatoriedad de implementar la **autenticación en dos fases** (2FA o MFA) se consolida como una de las barreras de seguridad más efectivas de la actualidad para neutralizar el uso de credenciales robadas y proteger el acceso a las cuentas de usuario y servidores de datos.

Vías de Reclamación

Frente a la vulneración de los derechos de protección de datos, o cuando un sistema de información no responde de manera adecuada a las solicitudes de acceso, rectificación o eliminación, el titular de los datos cuenta con dos vías de reclamación paralelas y complementarias: la administrativa y la judicial.

La vía administrativa se sustancia mediante la denuncia del hecho ante la **Agencia de Acceso a la Información Pública** (AAIP). Como autoridad de aplicación, la AAIP tiene amplias facultades de investigación y fiscalización, pudiendo realizar auditorías de oficio, requerir información de sistemas y programas, solicitar órdenes judiciales para acceder a locales de servidores e imponer severas sanciones administrativas que abarcan desde apercibimientos y clausuras temporales hasta multas de alto valor económico aplicables a los responsables que incumplan con la ley.

La vía judicial habilita la interposición directa de la acción constitucional de **hábeas data**, la cual tramita por el procedimiento sumarísimo y urgente de la acción de amparo ante los tribunales correspondientes. Esta vía es idónea para exigir de manera inmediata la exhibición de los datos almacenados, su rectificación o su total supresión cuando se demuestre su falsedad, desactualización o su carácter discriminatorio o prohibido.

Es fundamental que los profesionales de la computación sean plenamente conscientes de que las violaciones graves a este régimen no solo generan responsabilidades civiles resarcitorias por daños y perjuicios, sino que también están tipificadas como **delitos penales** en el Código Penal Argentino. Insertar a sabiendas datos falsos en un archivo de datos personales, o acceder ilegítimamente y sin autorización a un banco de datos violando sistemas de seguridad y confidencialidad (delito de hacking), conlleva severas penas de prisión e inhabilitación especial para el ejercicio profesional. La seguridad de la información y el cumplimiento ético de la ley no son, por tanto, simples recomendaciones técnicas, sino un pilar legal e ineludible de la idoneidad profesional en la era digital.