unidad ViI

RÉGIMEN LEGAL DE LAS BASES DE DATOS.

[700. INTRODUCCION. 1](#_Toc517078732)

[701. Clasificación 2](#_Toc517078733)

[702. Privacidad. Hábeas Data. 2](#_Toc517078734)

[703. Principios reguladores del tratamiento de datos personales 3](#_Toc517078735)

[704. PRINCIPIO DEL CONSENTIMIENTO. 4](#_Toc517078736)

[705. Datos Sensibles 5](#_Toc517078737)

[706. Derechos Relacionados a los Datos Contenidos en Bases de Datos 6](#_Toc517078738)

[707. DERECHO DE ACCESO 6](#_Toc517078739)

[708. DERECHOS DE RECTIFICACION, ACTUALIZACION O SUPRESIÓN. 6](#_Toc517078740)

[709. DERECHO A LA SEGURIDAD EN LA CONSERVACION 7](#_Toc517078741)

[710. CESION DE DATOS O TRANSFERENCIA DE DATOS. 7](#_Toc517078742)

[711. RESPONSABILIDAD DE LOS OPERADORES DE BASES DE DATOS 7](#_Toc517078743)



## INTRODUCCION.

Siempre ha existido en la sociedad acumulación de información, siempre han existido ficheros de distintos tipos y de distintas características; lo que la informática evidentemente ha aportado son elementos específicamente diferenciales que hacen a la estructuración y al manejo de la información.

Este aporte se plasma en tres grandes ámbitos:

1. **Concentración de la información**: lo nuevo que aporta el instrumental informático al manejo de la información es la posibilidad de concentrar en grandes bancos de datos enormes volúmenes de información de distinto tipo.
2. **Recuperación de la información**: la posibilidad de recuperar rápida y eficientemente la información es el segundo aporte esencial de la informática los bancos de datos.
3. **Transferencia y entrecruzamiento de la información**: este aspecto implica la posibilidad del envío, transferencia o transporte de la información, entrecruzamiento de la información contenida en un banco de datos, entre bancos de datos o entre sistemas ubicados inclusive en jurisdicciones nacionales diferentes.

Este impacto de la informática sobre las bases de datos, importa la aparición de nuevos problemas con consecuencias jurídicas a los que el derecho debe dar respuestas. La determinación del régimen jurídico de las bases de datos está íntimamente ligada a la compresión de dichos problemas que requieren y deben tener soluciones específicas desde el ámbito jurídico.

## Clasificación

Existen varios criterios para clasificar a las bases de datos. Entre los más comunes se pueden mencionar los siguientes tipos:

***Públicos o privados***: La característica distintiva es la determinación de de quién depende la gestión de un banco de datos específico. Los bancos de datos públicos, son aquéllos dependen de algún organismo de la administración pública de los estados (nacionales, provinciales o municipales). El resto son privados.

***Textuales o referenciales***: Esta clasificación de los bancos de datos es en función de las características esenciales de diseño, de estructuración. Está relacionada con la forma en que la información contenida en un banco de datos determinado esté cargada, que puede ser en texto completo, o en forma referencial, es decir, que esté incluida una referencia al contenido esencial del documento o de la información.

***Locales o generales***: Las bases de datos pueden ser de carácter local, orientadas con información que responda al interés específico de un ámbito geográfico determinado o de carácter general.

## Privacidad. Hábeas Data.

El tema de la privacidad relacionada a las bases de datos ha preocupado a los hombres desde hace bastante tiempo, más allá que la primera referencia jurídica dista a fines del siglo XIX, que han tratado de encontrar una adecuada protección a su vida privada y a ciertos aspectos que no solo tienen que ver con el individuo sino también con su entorno familiar, frente a la intromisión arbitraria de otras personas.

El derecho a la Privacidad, es el derecho que tiene toda persona a que se la deje sola, se la deje alejarse en aquellos aspectos de su vida en la que con­sidera sólo reservados a su conocimiento. Pero la irrupción de las tecnologías y las comunica­ciones alteraron profundamente el sentido y la orientación de la protección vida que poco a poco el Derecho Positivo había ido estructurando en relación a la privada

Desde el punto de vista normativo, este derecho empezó a ser regulado desde la década del ‘70. Suecia, Francia, Alemania fueron algunos de los países pioneros en estos temas.

El impacto de las modernas tecnologías no solo se ha producido sobre el clásico derecho a la intimidad, el derecho a la privacidad, sino también sobre otros derechos personalísimos como son el derecho al honor, el derecho a la imagen, el derecho a la identidad dinámica y además, tiene potencialidad de afectar también los derechos de determinados sujetos colectivos como pueden ser la colectividad, una nacionalidad de determinado género o los afectados por algún tipo de enfermedad.

Esto se relaciona directamente con lo que se entiende por datos de carácter personal.

Son todas aquellas informaciones susceptibles de ser atribuidas a una persona y que tienen aptitud para identificar a esa persona. En tal sentido podemos distinguir aquellos datos referidos a personas pero que han sido sometidos a un proceso de disociación, es decir que se les han extraído, eliminado o bloqueado aquellos aspectos de la información que permitirían identificar a uno o más sujetos.

Cuando se habla de datos de carácter personal se está refiriendo a un conjunto de informaciones acerca de una realidad específica, que es en principio un ser humano, pero que en lo que respecta a la protección de la ley se ha extendido incluso a personas de existencia ideal y que permite identificarlo a partir precisamente de la información y los datos que están allí contenidos.

Sobre el tratamiento que este tipo de información puede tener es que se ha tratado de establecer principios reguladores, principios que ponen límites y establecen pautas sobre cómo debe ser el tratamiento de este tipo particular de información, que a partir de la aplicación de las tecnologías informáticas y las telecomunicaciones, adquieren una dimensión y una potencialidad riesgosa que era desconocida anteriormente.

## Principios reguladores del tratamiento de datos personales

### Licitud

Nadie puede, en principio, recolectar datos, acopiar información, que no tenga un propósito socialmente válido. Este principio apunta a que nadie pueda tener datos de un sujeto si no es para aplicarlos a un fin socialmente válido y lícito es decir, permitido por el ordenamiento jurídico. Este primer principio es el que invalida nulifica, excluye del ordenamiento jurídico a cualquier base de datos que no responda a estos criterios y a estos parámetros.

Para tener en claro este principio se deben precisar cuáles son los aspectos de la vida de una persona que deben ser preservados de manera tal que, quien violente esta reserva o esta valla, esté incurriendo en una actitud ilícita o esté efectuando una recolección de datos con un fin socialmente inválido.

Un aspecto fundamental está en el Art. 18 de la Constitución Nacional que protege los papeles y la correspondencia privada, para tener una idea de cómo desde antaño se ha entendido que existe una zona de reserva, un aspecto de la personalidad que toda persona tiene derecho a excluir a los demás de su conocimiento. Sin ninguna duda las modernas tecnologías y en particular por ejemplo el correo electrónico o la navegación a través de Internet han complicado este panorama. También se encuentra un ejemplo en la Ley de Derechos de Autor o de Propiedad Intelectual, la Ley 11.723 (tengamos en cuenta que es del año 1933) que veda aún hoy el uso de la fotografía de una persona sin su autorización, salvo cuando es para fines de divulgación científica o educativa y esto por supuesto respetando determinados contextos.

Cuando hablamos de datos no nos estamos limitando sólo a la información contenida en un formato texto, sino que también estamos incluyendo las imágenes, a la voz y a otras capturas de este comportamiento declaraciones de voluntad en cualquier lenguaje que sea reproducible frente a terceros.

### Finalidad

Este principio implica que los datos deben ser recogidos con una finalidad explícita y no ser tratados posteriormente con una finalidad distinta o de una manera incompatible con el propósito con el que fueron requeridos originariamente, salvo cuando se trata de darle a esos datos un tratamiento histórico, estadístico o científico y siempre y cuando los Estados ofrezcan las garantías oportunas para ello.

### Pertinencia

Nadie tiene derecho a requerir información que no sea pertinente, es decir, que no vaya a cumplir alguna finalidad directamente vinculada al propósito que se ha declarado al requerir esta información.

### Exactitud

El dato que no debe ser ni equívoco ni ambiguo. Es decir, en el dato personal el rigor en su selección, en su tratamiento y en su difusión es mucho mayor que cuando uno puede manejar algún otro tipo de información. Un dato inexacto, por desactualizado o por incompleto, puede convertirse en un dato tremendamente perjudicial, aún cuando en la parcialidad que exprese el dato sea cierto, sea verídico

### Datos no excesivos

Los datos, por otro lado, deben ser conservados en forma identificable sólo durante el período que sea indispensable para que pueda identificarse el sujeto.

### Confidencialidad

La regla en materia de datos de carácter personal debiera ser la confidencialidad, no la publicidad. Esto no porque no sea posible que determinados datos de carácter personal tengan carácter público. De hecho un conjunto de circunstancias que rodean a las personas, -nombre, profesión, en algunos casos domicilio o teléfono o eventualmente la dirección de correo electrónico- en muchos casos se desprende de la manera en que han sido proporcionados, que no hay una pretensión de que sean reservados, todo lo contrario, están expuestos a propósito para que sean conocidos, para permitir la comunicación con los titulares de esos datos, su ubicación, su hallazgo, etc. Pero esto debiera ser siempre el resultado de una operación previa voluntaria.

Por su parte el responsable y las personas que intervengan en cual­quier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada la relación con el titular del archivo de da­tos.

Según la ley cualquier obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Este principio lleva a otro de los principios fundamentales en esta materia que es el del consentimiento.

## PRINCIPIO DEL CONSENTIMIENTO.

Los datos de carácter personal sólo pueden ser almacenados y difundidos por terceros cuando ha mediado un consentimiento, que en algunos casos deberá ser expreso, libre e informado tal como señalan la mayoría de las legislaciones.

La ley 25.306 que es la que regula la protección de los datos personales, establece que no es necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obliga­ción legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesa­rios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes.

En todos los demás casos el titular debe prestar su consentimiento libre, expreso e informado, que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo con las circunstancias. Si esta condición no se cumple el tratamiento de esos datos será ilícito.

El consentimiento sólo es válido cuando se le ha notificado previamente a la persona cuál es la finalidad de esa recolección, de esa operación de juntar información sobre esa persona y además se le ha advertido para qué se va aplicar, para qué se va a utilizar esa información y cuáles son las consecuencias de negarse a brindar esta información y además deben señalar cuáles son los posibles receptores de esa información.

El consentimiento puede considerarse implícito (o no ser necesario como dice la ley) cuando la información resulta necesaria para la ejecución de un contrato en el cual el interesado es parte, o para la aplicación de alguna medida precontractual adoptada precisamente a petición del interesado, o cuando se trata del cumplimiento de una obligación a la que esté sujeta el responsable de los datos, o en una expresión que la ley argentina ha recogido un poco ambiguamente, cuando sea necesario para proteger el interés vital del interesado.

Se excluye esa obligación del consentimiento de interesados cuando los datos se obtengan de fuentes de acceso público irrestricto.

Otra de las excepciones es que se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

Tampoco es necesario el consentimiento cuando se trate de listados cuyos datos se limiten a nombre, documento de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio

Existe una categoría de datos que requieren un tratamiento especial y que se ha identificado en el mundo entero como *datos sensibles*.

## Datos Sensibles

En general se entienden incluidos en esta categoría de datos sensibles, a los datos referidos a condiciones políticas, ideológicas, religiosas, cuestiones raciales y algunos aspectos vinculados con la salud o con la conducta sexual. Esta enumeración ha sido reproducida en nuestra ley.

Pareciera que no todos estos datos tienen la misma importancia como datos sensibles. Tienen quizás una connotación y un riesgo mucho mayor los datos referidos a la salud. En esta materia la horizontalización de los negocios y las actividades lucrativas vinculadas a la salud, que no sólo están concentradas en las empresas prestadoras de servicios de salud o de medicina prepaga o de seguros de salud, sino que tienen impacto en la mayoría de la actividad aseguradora, no sólo de los seguros de riesgos de trabajo, las administradoras de fondos de jubilaciones y pensiones, los seguros de vida, los seguros de retiro, sino también las políticas de empleo en el acceso al empleo, es donde más hay que trabajar y precisar los conceptos.

Para tener una idea por ejemplo nuestro país tiene una ley, la Ley N° 23.798 de lucha contra el SIDA que establece criterios muy rigurosos y precisos de confidencialidad en el tratamiento de los resultados y de la detección de una persona que conviva con HIV o que esté enferma de SIDA, e incluso además de establecerlo la ley, el decreto reglamentario que rige en la Argentina es muy preciso sobre cómo deben conservarse los datos y a quienes son los únicos sujetos que se está autorizado a transmitirle esta información que debe ser en un contexto de información adecuada a nivel cultural del receptor, que apunten fundamentalmente a su tranquilidad y a su contención psicológica y a formar parte de su tratamiento y en modo alguno pueden convertirse por impericia o incluso por dolo en un elemento de marginación o discriminación.

## Derechos Relacionados a los Datos Contenidos en Bases de Datos

La ley establece una serie de derechos que tienen los titulares de los datos respecto de esos datos obrantes en bases de datos

## DERECHO DE ACCESO

Implica el conocimiento cierto de los datos personales que sobre uno tengan terceros. De este se desprenden los derechos de rectificación, actualización, supresión o confidencialidad.

Este derecho puede instrumentarse por vías administrativas o me­diante una acción judicial.

El art. 14 de la ley argentina específicamente plantea que el titular de los datos, previa acre­ditación de su identidad, tiene derecho de solicitar y obtener información de los datos per­sonales inclui­dos en los bancos de datos públicos o privados destinados a proveer infor­mes.

Por titular de los datos se entiende, en los términos de la ley, que es *toda persona física – en el caso de la ley argentina agrega o de existencia ideal – con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley*.

El res­ponsable, es quien administra, quien es titular de un banco de datos, de una base de datos y el usuario (que puede ser quien ha recibido esta información y la está utilizando, por ejemplo, para decidir si una persona es apta o no para un empleo o para un cargo docente, para un cargo público o para otorgarle un crédito), deben proporcionar la información solicitada dentro de los 10 días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido o se haya evacuado la información o esta se estimara insuficiente, se puede iniciar la acción judicial (acción de hábeas data).

El otro requisito que pone este art. 14 es que el derecho de acceso al que se refiere este artí­culo solo puede ser ejercido en forma gratuita a intervalos no inferiores a 6 meses, salvo que se acredite un interés legítimo al efecto.

La información debe ser sumi­nistrada en forma clara, sin códigos, sin encriptamientos, sin ocultamientos, sin deter­minadas palabras que uno deba tener que interpretar y en su caso acompañada de una explicación, en leguaje accesible al conocimiento medio de la población de los términos que se utilicen. La in­formación no basta transmitirla tal como está registrada en el banco de datos, sino que debe ser adaptada a un lenguaje claro, comprensivo que no genere dificultades para un estándar medio cultural.

Finalmente el método empleado para suministrar la información la ley lo establece en forma muy amplia, puede ser suministrado por escrito, telefónicamente, por medios electrónicos u otros medio idóneo a tal fin.

## DERECHOS DE RECTIFICA­CION, ACTUALIZACION O SUPRESIÓN.

En este sentido la primera referencia debe ser a la Constitu­ción al Art. 43, párrafo 3º que esta­blece que además de este derecho de acceso al que nos hemos referido previamente, toda persona tiene de­recho a la rectificación, actualización o supresión de los datos que sean inexactos o falsos o que sean discriminatorios.

El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo que fija la ley.

## DERECHO A LA SEGURIDAD EN LA CONSERVACION

Es el derecho a que los datos no sólo no sean conocidos o no tengan acceso a ellos quienes no están autorizados o quienes por la naturaleza de los datos no debieran tener acceso a ellos, sino que además los datos sean conservados adecuadamente.

Esto introduce un conjunto de requisitos de naturaleza técnica, que prácticamente todas las legislaciones imponen, y que también lo establece nuestra norma nacional la 25.326 y que serán motivo seguramente de la reglamentación cuáles son las pautas que deberán observar los responsables de ficheros y de bancos de datos para garantizar la seguridad de los datos de carácter personal que acumulen y procesen.

## CESION DE DATOS O TRANSFERENCIA DE DATOS.

Los datos personales objeto de tratamiento como regla general no pueden ser cedidos.

Si lo fueren, tiene que serlo para el cumplimiento de los fines directamente relacionados con el interés legítimo del que cede y del que los recibe.

Cualquier cesión debe contar con el con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión y sobre la identidad de a quién le son cedidos los datos.

El consentimiento del titular para la cesión es revocable en cualquier momento.

Según la ley el consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los mismos supuestos en que no es necesario para la recolección.

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumpli­miento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

En cuanto a la transferencia internacional de los datos, en principio sólo puede hacerse cuando los países u organismos internacionales o supranacionales, proporcionen niveles de protección adecuados.

También puede hacerse en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico.

c) Transferencias bancarias o bursátiles.

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

## RESPONSABILIDAD DE LOS OPERADORES DE BASES DE DATOS

En primer lugar, la ley establece una obligación clara para todo aquel que manipule una base de datos de carácter personal, de adecuar su operatoria a la normativa y por otro lado la ley establece tres niveles diferenciales de responsabilidad.

1. En primer lugar la responsabilidad patrimonial, enormes multas administrativas y por otro lado la responsabilidad por eventuales daños y perjuicios causados a terceros.

2. El segundo nivel de responsabilidad es el que se denomina responsabilidad en cascada, es decir la organización que manipule datos de carácter personal no es responsable sólo por lo que hace con esos datos, sino que también es responsable por la acción del tercero cesionario de esos datos que viole también los principios establecidos en la norma

3. El tercer nivel de responsabilidad es la responsabilidad penal. La ley incluye tres nuevos tipos penales que incriminan a aquel gestor de un banco de datos personal que viole los principios establecidos en la norma.