61468

PROGRAMA:

"PROGRAMA DE FORTALECIMIENTO Y FORMULACIÓN DE SISTEMAS CLAVES PARA EL SOSTENIMIENTO SOCIAL Y ECONÓMICO DE LA PROVINCIA DE SAN LUIS: ESTRATEGIAS LUEGO DE LA CRISIS MACROECONÓMICA 2001/2002"

MODULO:

"HABEAS DATA. INTERCAMBIO DE INFORMACIÓN ENTRE ENTES OFICIALES"

INFORME FINAL

"Habeas data. Intercambio de información entre entes oficiales"

-San Luis Conectado-

Integrantes del grupo:

Experto: Santagata Chada, Juan Pablo

Colaboradores: Giunta, Valeria Valentina

Denechuk, Gabriel Alejandro

Alfonso, Marcelo Ignacio

2003-2004

DESARROLLO

1. INTRODUCCIÓN.
2. OBJETIVO.
3. CUERPO

3.1. ACTIVIDAD Nº 1: Establecer las condiciones de utilización de la información contenida en los Registros Públicos.

3.1.1. Relevamiento de los distintos Registros de la Provincia.

3.1.2. Doctrina, Legislación y Jurisprudencia.

3.1.2.1. Antecedentes.

3.1.2.2. Derechos tutelados y Habeas data.

3.1.2.3. Derechos comparados: Nacionales e Internacionales.

3.1.2.4. Jurisprudencia. Casos más importantes. Breve reseña.

3.1.2.5. La acción de Habeas data.

3.1.3. Definición y Clasificación de datos.

3.1.4. Condiciones de tratamiento de datos.

3.1.5. Acuerdos, Auditorias y Control Interno.

3.2. ACTIVIDAD Nº 2: Instrumentar los Mecanismos y Procesos de consulta de la información, en especial la relacionada con la producción y generación de empleo.

3.2.1. Derecho a la Información.

3.2.1.1. Derecho a la Autodeterminación Informativa.

3.2.1.2. Libertad de información y Derecho a la Privacidad.

1. INTRODUCCIÓN.

Una sociedad altamente informatizada, en la que prácticamente cada acto que realizamos queda registrado en alguna base de datos, en la que la implementación de cámaras de vigilancia se está transformando en algo cotidiano, puede dar nacimiento, cuando menos, a una sociedad de cristal, en la que todas las conductas serán observadas y registradas. En una sociedad de tales características, cada acto que realicemos dejará una huella indeleble en nuestra ser, siendo imposible evitar la estigmatización y su consiguiente encasillamiento. Se dará una suerte de "panóptico", tal como fue pensado por Foulcault, que no cesará de vigilar, condicionando nuestras formas de vida.

En este orden de ideas, deviene imprescindible brindar una adecuada protección al derecho a la privacidad, sin dejar nunca de lado la búsqueda del justo equilibrio entre el derecho a la privacidad y el derecho a la información, ya que éste también resulta esencial para respetar los derechos de los ciudadanos.

Respecto a la protección de los datos personales que constituye un criterio de legitimación política de los sistemas democráticos tecnológicamente desarrollados; su reconocimiento supone una condición del funcionamiento del propio sistema democrático, es decir, se trata de una garantía básica para cualquier comunidad de ciudadanos libres e iguales.

En un orden social y en un orden jurídico en el que el ciudadano ya no pudiera saber quién, qué y cuándo y con qué motivo se sabe algo sobre él no sólo menoscabaría las oportunidades del desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental del funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos.

La preocupación actual es el manejo de la tecnología, esto permite un tratamiento extraordinario y eficiente de grandes volúmenes de información, la utilización discrecional de la información pone en peligro derechos y libertad fundamentales como el derecho a la privacidad entre otros. El ser humano necesita de la

información veraz y oportuna, en otros términos, debe tener libertad de recibir y difundir informaciones y opiniones "auténticas" para desarrollar todo su potencial pero requiere de un campo de intimidad, de un ámbito donde puede ser él y nada más.

En cuanto al derecho a la información consideramos que una forma precisa y concreta de terminar con la cruel crisis de representatividad y su ilegitimidad correlativa, es permitirle al ciudadano común, conocer las actuaciones y los actos de los funcionarios. Cuando pueda acceder con absoluta libertad a los trámites, sin rigorismos jurídicos u obstáculos formales - que en la práctica lo impiden- el control será verdadero y el sujeto controlador, tendrá confianza renovada en el controlado.

La única manera de controlar la eficiencia del obrar estatal, reside en la posibilidad de tener acceso y conocimiento de los actos de gobierno. Esto deriva directamente de la forma republicana de gobierno. Por el contrario el "secreto" es propio de la actitud autoritaria y autocrática que significa negar – a cualquier costo– ese control democrático a que tiene, como derecho primario, la sociedad organizada. Así lo ha determinado la propia Corte Suprema al decir: " Si bien la declaración de inconstitucionalidad es un acto de suma gravedad institucional, las leyes son susceptibles de cuestionamiento cuando resultan irrazonables, cuando los medios que arbitran no se adecuan a los fines cuya realización procuran o cuando consagran una manifiesta inseguridad...", "...el principio de razonabilidad debe cuidar especialmente que las normas legales contemplen coherencia con las reglas constitucionales". Fallos: 307.862.

Ante la realidad brevemente descripta creemos que el desafío clave de la sociedad contemporánea "del conocimiento" es crear condiciones sostenibles de progreso económico en un contexto de mercados globales sin sacrificar la solidaridad de base, la cohesión de la sociedad y las instituciones constitucionales que garantizan la libertad.

La meta es desarrollar una dinámica que subordine recursos y capacidades de los sectores público y privado en función de la resolución de problemas y oportunidades relacionados tanto con la competitividad de las estructuras administrativas y

productivas, como con la sensación de pérdida o vulnerabilidad de la población, que no es sólo económica sino también relativa a cuestiones tan esenciales como el empleo, la seguridad, la calidad de vida y el futuro en general.

En este sentido, el papel del Estado resulta indispensable para establecer un marco estratégico cuyo eje principal sea movilizar y articular recursos humanos, científicos y tecnológicos, buscando su utilización y asociación con finalidades social y económicamente relevantes.

Entre otras reformas, el Estado tiene pendiente la construcción de un nuevo modelo de política social, que acompañe al modelo económico. Su objetivo sería lograr una nueva institucionalidad pública, donde lo social sea constitutivo del Estado, lo que le da sentido, y cuyo objetivo central sea la equidad, la inclusión e integración social, la igualdad de oportunidades, y la superación de la pobreza y la vulnerabilidad social. La nueva institucionalidad pública remite al crecimiento de poder de la política social, a la que pone en un pie de igualdad con la política económica para poder conducir y generar las condiciones del fortalecimiento de los sectores más frágiles de la sociedad, facilitar la expresión de sus demandas y producir los mecanismos para la inclusión social y una distribución más equitativa de la riqueza.

2. OBJETIVO.

OBJETIVO GENERAL: Determinar las condiciones de tratamiento de la información que posee el Estado provincial, en relación a los ciudadanos e intra-Poderes a fin de garantizar los actos de gobierno asegurando la disponibilidad de la información; lo que permitirá progresar en el cumplimiento de las metas de equidad, inclusión e integración social.

OBJETIVOS ESPECIFICOS

- Delimitar el cúmulo de derechos y obligaciones del ciudadano y del Estado en la consulta y administración de la información.
- Elaborar la reglamentación necesaria que permita el intercambio de información entre el Estado y los sectores sociales y productivos a fin de un aprovechamiento eficiente de los recursos, dentro del marco de seguridad jurídica.

3. CUERPO.

3.1. ACTIVIDAD N° 1: Establecer las condiciones de utilización de la información contenida en los Registros Públicos.

3.1.1. Relevamiento de los distintos Registros de la Provincia.

Nuestra legislación nacional en su Art. 21 establece la obligación para todo registro o banco de datos de inscribirse en el registro que a tal efecto habilite el organismo de control.

En este contexto y de acuerdo al inciso 2 del mencionado artículo, el registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos encada archivo;

d) Forma de recolección y actualización de datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

Consideramos que el cumplimiento de lo previsto en la norma otorgará una gran dosis de transparencia en el funcionamiento interno del registro, como así también lo dotará de eficiencia; todo ello en beneficio de la seguridad jurídica.

Tomando como punto de partida lo establecido en la ley y a los fines de conocer la realidad de nuestros registros públicos, realizamos el relevamiento de los mismos de acuerdo al siguiente cuestionario:

1. Qué tipo de información manejan.
2. Cómo ingresa y cómo se modifica.
3. Quién introduce información y quién puede consultarla.
4. Cuál es el procedimiento de consulta.
5. Nivel de informatización.

A continuación enumeramos los registros públicos que fueron relevados, expresando entre paréntesis la dependencia funcional.

I. Registro de Antecedentes Personales (P.E.).
II. Registro de Deudores Morosos Alimentarios (P.E.).
III. Dirección Provincial de Ingresos Públicos (P.E.).
IV. Catastro (P.E.).
V. Registro Nacional de las Personas (P.E.N.).
VI. Registro de la Dirección de Obra Social de Empleados Públicos –DOSEP- (P.E.).
VII. Registro de Juicios Universales (P.J.)
VIII. Registro Público de Comercio (P.J.)
IX. Registro Único de postulantes para Adopción (P.J.)

Anexamos también el resultado de dichos relevamientos a los efectos de una mayor compresión de lo desarrollado a lo largo de este informe.

"Anteced. Personales.doc" "Deudores Alimentarios.doc" Catastro.doc ReNaPer.doc "Dir. Pvcial de IIPP.doc"


DOSEP.doc


"Reg. Juicios Universales.doc"


"Reg.Pco. de Comercio.doc"


"Reg. Unico Adoptantes.doc"

3.1.2. Doctrina, Legislación y Jurisprudencia.

3.1.2.1. Antecedentes.

Así como la libertad personal tuvo su antecedente básico en el mundo moderno en el hábeas corpus act. en 1679, que hundía sus raíces en el instituto romano del *interdictum de homine libero exhibendis* y en la Carta Magna de 1215 de Juan Sin Tierra, el hábeas data constituye hoy el reconocimiento del derecho de las personas de disponer de sus datos personales, al igual que de su propio cuerpo y de su libertad ambulatoria.

Los archivos existen desde tiempos inmemoriales; el cambio creado se produjo con la aparición de la tecnología, que hizo desaparecer el límite antes fijado por el espacio y el tiempo.

De esta manera, allí donde ya existía un archivo, un registro, una copia de datos o un respaldo documental, con la aparición de la informática surge una abundancia informativa que hace necesaria la clasificación, la comparación, la sistematización y la recuperación de la misma, convirtiendo la simple reunión informativa en un grandioso archivo de perfiles, de preferencia, de gustos, estructuras económicas, etcétera.

Este cambio, evidentemente, provocó la dispersión de los datos y la pérdida de control sobre ellos.

La antigua privacidad de los archivos, habitualmente conservados en registro manuales escritos, rápidamente se transformó en unos pocos **bites** almacenados en la memoria de una computadora que, desde el funcionamiento de las redes virtuales cómo Internet, facilitan la trasmisión; consecuentemente los datos antes reservados y ciertamente confidenciales pasaron a ser públicos y disponibles para cualquiera.

Las primeras manifestaciones contrarias a esta suerte de invasión en los dominios de lo secreto de los archivos llegaron de la tarea legislativa. Suecia, con el acta de 1973*, y los Estados Unidos a través de la Privacy Act* de 1974 reaccionaron estableciendo reglas y principios para la creación de los archivos y esencialmente, para dar alguna seguridad con el tratamiento de los datos y el derecho la intimidad.

De esta manera la creación de los archivos ha debido respetar ciertas reglas y principios, pero al mismo tiempo reconocer derechos al individuo afectado por el registro, y también al titular de la base de datos. Se establecieron procesos y procedimientos para el almacenamiento, la conservación, la seguridad interna del archivo y las fases para el tratamiento (circulación y venta de la información).

El desarrollo normativo, no obstante, ha debido equilibrar la importancia que tiene la acumulación informativa a los fines de la organización política con la protección del hombre en su derecho a la privacidad, que constituye, por estos tiempos un avance moderno de la libertad de intimidad.

La reforma constitucional de 1994 y los nuevos derechos y garantías.

La reforma incorporó, a partir del artículo 36 y hasta el 43 inclusive, algunos de los llamados "Derecho Humanos de la Tercera Generación".

Pero hay que decir aquí también que la ley 24.309 no mencionaba para nada los habeas data ni la protección de datos personales. Lo más probable es que los legisladores que declararon la necesidad de la Reforma no hayan pensado siquiera en el instituto que acá nos ocupa.

A ello se debe, seguramente, que el habeas data aparezca introducido entre el amparo y el habeas corpus, como una subespecie de la acción de amparo.

La Comisión nº 14 dictaminó a favor de un texto más limitado que el que se aprobó finalmente ("Asimismo toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y que consten en registros públicos o privados y del fin de éstos; y en su caso, para exigir la supresión rectificación o actualización de

aquéllas"). La redacción que el párrafo tuvo finalmente se corresponde en todo con el dictamen de la Comisión de Redacción nº 9.

El miembro informante del despacho de mayoría de Comisión de Nuevos Derechos y Garantías, Rodolfo A. Díaz, expresó al respecto que rehace referencia (con el habeas data) a un ámbito de derechos personales del mundo contemporáneo, en el cual el procesamiento de la información, la acumulación y la circulación han generado amenazas reales a la libertad y a otros derechos personales de los argentinos. "Todos nosotros hemos vivido períodos oscuros de la historia nacional. Pero gracias a Dios, individual y colectivamente, hemos logrado sobrevivir y superarlos. Esta Convención es la expresión histórica, no solamente de nuestra capacidad de supervivencia en esos periodos oscuros de la historia Argentina, sino también de nuestra capacidad de superarlos. Estoy convencido de que estamos abriendo un a puerta al futuro que deja atrás el período sombrío. No hay ningún convencional sentado en esta sala que no sepa a qué me estoy refiriendo cuando digo que existe el riesgo en la acumulación y manipulación (de datos) sobre las personas que puede producir un daño actual y real".

El convencional Ricardo R. Biazzi manifestó: "... La historia Argentina reciente nos muestra claramente la necesidad de consagrar una norma constitucional que defienda a los ciudadanos frente a todo tipo de arbitrariedad o en materia de registros ideológicos, políticos, sindicales, personales o familiares que puedan afectar el derecho a la dignidad y a la propia imagen de las personas en nuestro país".

El convencional Cáceres, luego de relatar una experiencia personal referente a información errónea respecto a las actividades políticas volcadas en expedientes del servicio de inteligencia, a los que tuvo acceso a partir del advenimiento de la democracia en el año 1983, expresó:"Quienes venimos de una militancia larga y sabemos las vidas que ha costado una mala información e incluso a veces la intención de hacer llegar una mala información, valoramos un instrumento como el habeas data..."

Por encima de las diferencias y discusiones terminológicas que acarrea la expresión hábeas data, lo cierto es que el instituto al que se refiere ha sido incorporado a la legislación argentina por obra de la Reforma de 1994 y desde entonces tiene operatividad, aun cuando no estaba reglamentado por ley nacional, es decir que se consideraba directamente articulable por ente la justicia competente.

Antecedentes Nacionales Del Nuevo Art. 43 De La Constitución.

a) El artículo 19 de la Constitución Nacional sus propios antecedentes

Presente en la redacción originaria de la Constitución de 1853, en la Primera Parte, Capitulo Primero, sobre Declaraciones Derechos y Garantías, se encuentra el artículo 19 de nuestra Ley Fundamental.

b) En el artículo 33 de la Constitución Nacional, el constituyente introdujo el tema de los *derechos no enumerados* también llamados *derechos implícitos*, disponiendo que "las declaraciones, derecho y garantías que enumera la Constitución no serán entendidos como negación de otros derechos y garantías no enumerados, pero que nacen del principio de la soberanía del pueblo y de la forma republicana de gobierno"

Esto quiere decir que la enumeración de constitucional no taxativa y la ausencia de expresa mención de un derecho o garantía en el texto fundamental no significa negación de estos, lo que por otra parte pueden hallarse recogidos en tratados, concordatos, acuerdos o declaraciones internacionales a los que la Nación haya adherido o haya ratificado como en las leyes que se dictaran con motivo de aquellos , etc. También pueden ser derechos reconocidos jurisprudencialmente o hallarse integrados de algún modo al ordenamiento jurídico.

c) El Art. 1071 bis del Código Civil. Hasta la inclusión del hábeas data en el actual artículo 43, párrafo 3º, de la Constitución Nacional, todas las acciones referidas a aquél podrían basarse, prácticamente, en el Art.. 33 de la Constitución y en el Art. 1071 bis del Código Civil. A su vez, el Art.19 de la Constitución Nacional es fundamento de la ley 21.173, en virtud de la cual se introdujo el Art. 1071 bis al Código Civil, el que dispone: "El que arbitrariamente se entrometiere en la vida ajena, publicando retrato, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez ,

de acuerdo con las circunstancias; además, podrá este, a pedido del agraviado ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación".

Este articulo realiza una enumeración que no es taxativa y, naturalmente, mantiene intacta su vigencia a pesar del reconocimiento constitucional del habeas data

d) Los Art. 109,110 y 114 del Código Penal.

El Código penal, en su articulo 109, reprime "la calumnia o falsa imputación de un delito que dé lugar a la acción pública...", y en le articulo 110 hace lo propio con la injuria ("El que deshonre o desacredite a otro...")

A su turno, el articulo 114 establece: "Cuando la injuria o la calumnia se hubiera propagado por medio de la prensa en la capital y territorio nacionales, sus autores quedarán sometidos a las sanciones del presente Código y el juez o tribunal ordenará, si lo pidiere el ofendido, que los editores inserten en los respectivos impresos o periódicos, a costa del culpable, la sentencia o satisfacción"

La publicación a que alude el artículo 114 presupone la existencia de un culpable de las calumnias e injurias y un fallo condenatorio.

e) Ley de Propiedad Intelectual, N° 11.723, dispone en su articulo 31: "el retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma, y muerta ésta el cónyuge e hijos o descendientes directos de estos, o en su defecto del padre o de la madre. Faltando el cónyuge, los hijos el padre o la madre o los descendientes directos de los hijos, la publicación es libre. La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios. Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés publico o que se hubiere desarrollado en publico".

Por su parte, el articulo 32 dispone:"El derecho de publicar las cartas pertenece al autor. Después de la muerte del autor es necesario el consentimiento de las personas mencionadas en el articulo que antecede y en el orden ahí indicado".

f) La Ley Nacional del Síndrome de Inmunodeficiencia Adquirida –SIDA- N° 23798, sancionada el 16 de agosto de 1990 y promulgada de hecho el septiembre del mismo año, establece en su articulo 2: "Las disposiciones de la presente ley y de las normas complementarias que se establezcan, se interpretaran teniendo presente que en ningún caso pueda: a) afectar la dignidad de la persona; b) producir cualquier efecto de marginación, estigmatización, degradación o humillación; c) exceder el marco de las excepciones legales taxativas al secreto medico que siempre se interpretaran en forma restrictiva; d) incursionar en el ámbito de la privacidad de cualquier habitante de la Nación Argentina; e)individualizar a las personas a través de fichas, registro o almacenamiento de datos, los cuales, a tales efectos deberán llevarse en forma codificada"

g) La ley 24.766, llamada de confidencialidad, dispone en su articulo 1: "Las personas físicas o las personas jurídicas podrán impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada sin su consentimiento de manera contraria a los usos comerciales honestos..."

Si bien esta ley se encuentra destinada en primer termino a los productos medicinales, viene a marcar un hito en materia de confidencialidad, ya que surge de ella la posibilidad reimpedir que la información sin su consentimiento, amparando a las personas contra los "usos comerciales deshonestos".

h) La Ley 25.065, de tarjeta de crédito en su articulo 53, dispone: "*Prohibición de informar*". Las entidades emisoras de tarjetas de crédito bancarias o crediticias tienen prohibido informar a las «bases de datos de antecedentes financieros personales»sobre los titulares y beneficiarios de extensión de tarjetas de crédito u opcionales cuando el titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciación, sin el perjuicio de la obligación de informar lo que correspondiere al Banco Central de la Republica Argentina. Las entidades informantes serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opcionales de tarjetas de crédito por las consecuencias de la información provista".

3.1.2.2. Derechos tutelados y Habeas Data.

Al referirnos a los derechos tutelados por el Habeas Data es necesario establecer la dicotomía existente entre derecho a la intimidad (vida privada) versus poder informático, aunque en realidad el contrincante es el titular de la base de datos que lo acopió y procesó con una posible finalidad de lucro al suministrarlos luego a terceros. Se ha dicho con razón que el aspecto más innovador de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud y este valor económico mueve el uso y el abuso (Romeo Casabona, C.M., Poder informático y seguridad jurídica, Fundesco, 1987).

1)- El derecho a la intimidad: Toda persona tiene un rincón de los secretos donde no permite el acceso a los demás, nadie debe ni tiene el derecho de husmear en él, es inviolable, porque es privada. El derecho a la intimidad, a la privacidad, es un derecho natural, personalísimo, inalienable del ser humano.

En el devenir de la historia la vida íntima y reservada de las personas ha ido creciendo a medida que se ha ido limitando el ansia expansionista del poder público. Como consecuencia de la confrontación de la idea de libertad frente al omnipresente poder público, surge el derecho a la intimidad como un conjunto de poderes y facultades para garantizar la exclusión del Estado en el ámbito más secreto del individuo.

Desde ese punto de vista y teniendo en cuenta la diversidad de medios modernos susceptibles de atentar al derecho a la intimidad, la Comisión CALCUTT, lo define como "el derecho del individuo a que se proteja la intromisión, ya sea mediante medios físicos directos o mediante la publicación de una información, en su vida personal o en sus asuntos personales o en la vida o asuntos personales de su familia".

Los conflictos que se suscitan en torno al derecho a la intimidad provienen, por lo general, del ejercicio del derecho a la información, entendido como abarcador de las libertades de investigar, de expresión, de recibir y difundir información y de opinión.

Son las injurias, el engaño y el atentado al honor de la persona, las afectaciones a la intimidad producida por la información "abusiva".

Debemos tener en cuenta que archivos o bases de datos referentes a las personas han existido siempre como por ejemplo: los asientos en el Registro Civil y Capacidad de las Personas, los libros parroquiales (constancias de bautismos, casamientos, etc.), ficheros escolares, médicos, los de antecedentes penales, etc., pero no eran de tan fácil acceso como ocurre hoy en día con la aparición de la informática y los ordenadores electrónicos. Esta situación ha hecho aumentar en gran magnitud la amenaza potencial del derecho a la intimidad.

No resultaba suficiente para contener las arremetidas del novedoso poder informático. Se requería un afinamiento y extensión de su conceptualización para darle respuesta. Fue surgiendo así el nuevo derecho a la protección de datos, o derecho a la autodeterminación informativa, también llamado por algunos libertad informativa, categorizado como un derecho humano de tercera generación (Ekmekdjian, Miguel Ángel, Tratado de derecho constitucional, Depalma, 1993).

El derecho a la intimidad va siendo complementado con el derecho a la dignidad, al honor, a la imagen del individuo respecto de sus semejantes, en definitiva el derecho a controlar los propios datos personales que otros tienen registrados y el uso que hagan de los mismos.

La intimidad no es simplemente una ausencia de información acerca de nosotros en la mente de los demás; con mayor precisión es el control que nosotros tenemos acerca de la información que nos atañe (Lloveras de Resk, María Emilia, La intrusión a la intimidad a través de la informática, en J. A. 1989-II-917).

Tampoco es del caso negar absolutamente la registración de datos, sería absurdo descartar la utilidad de semejante herramienta brindada por la tecnología. El quid radica en darle cauce. Uno de ellos es el consentimiento, lo que presupone el previo conocimiento del titular del dato. Otro es la finalidad del banco de datos.

Antecedentes Normativos

El primer antecedente normativo lo encontramos en la ley de marcas, Nº. 3975, en su artículo 4, prohibía el uso del nombre o el retrato de una persona a favor de un tercero, a menos que ella misma, o sus herederos, dieran el consentimiento. Prohibía no sólo la difusión sino también el registro como si fuera una marca o diseño del comercio, la industria o la agricultura. Evidentemente esta ley ya tendía a la protección de la imagen en sí misma, independientemente de que hubiera o no desmedro a la personalidad.

La ley 11.723 de propiedad intelectual, sancionada el 28 de septiembre de 1933, al referir sobre la imagen le otorga protección legal en el Art. 31 el cual dispone "El retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma, y muerta ésta, de su cónyuge e hijos o descendientes directos de éstos, o en su defecto del padre o de la madre....

La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios..."

Dando un salto cronológico, a efecto de completar la mención de antecedentes, diremos que la ley de marcas, número 22.362, en su artículo 3 enumera los casos en que no está permitida la registración, y en el inciso "h" menciona "El nombre, seudónimo o retrato de una persona, sin su consentimiento o el de sus herederos, hasta el cuarto grado inclusive".

La ley habla de retrato fotográfico, pero debe entenderse analógicamente que están comprendidas toda la forma de reproducción de la imagen: pintura, retrato a lápiz, escultura, en cine o video, relieve, etc. Por supuesto que debe incluirse también la caricatura, la representación teatral, la de un sketch en televisión, etc.

2)- Derecho de autodeterminación informativa: La primera mención que se formuló respecto de la llamada "autodeterminación informativa" proviene de la entonces República Federal Alemana y ha suscitado desde su aparición un gran debate sobre su naturaleza.

En sus comienzos la protección de datos personales aparecía como necesaria sólo en cuanto a la protección de los datos sensibles (religión, procedencia étnica, ideas

políticas, participación sindical, situación financiera, tendencias sexuales, etc.), pero la posibilidad de "cruzamiento de datos" por medio de las computadoras desvirtuó esta categoría frente a la creciente necesidad de que la tutela alcance a toda clase de información.

En su voto en el célebre caso "Urteaga", el ministro de la C.S.J.N. Petrachi reseñó el proceso que puede reconocerse en la evolución de la jurisprudencia del Tribunal Constitucional Alemán, que había sostenido la "teoría de las esferas", según la cual se establecía una mayor o menor protección diferenciada de acuerdo con el mayor o menor grado de afectación de la intimidad. Esta tutela restrictiva fue abandonada a favor de una tutela considerablemente más amplia, expresaba en la célebre "sentencia del censo", a la que se le atribuye la configuración del concepto de "autodeterminación informativa" o "libertad informática" que actualmente se reconoce como el fundamento de hábeas data en las legislaciones que contemplan derechos análogos.

El punto central de la argumentación fue la consagración de la "autodeterminación informativa". Según este concepto es el ciudadano quien debe decidir sobre la cesión y el uso de sus datos personales. Este derecho, se dijo que puede ser restringido por medio de una ley, por razones de utilidad social, pero respetando el principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad.

De lo expuesto se puede inferir que el derecho a la autodeterminación informativa esta íntimamente relacionado con el control de las informaciones que nos afectan, toda vez que no importa si un dato personal pertenece o no a la esfera privada de una persona (protegida por la intimidad como no interferencia), sino que lo importante son las posibilidades de relacionarlo informáticamente con otros datos y la finalidad de ese proceso. Esto significa que no es el conocimiento de determinados datos personales lo que pone en peligro la libertad de las personas, sino el uso que se haga de la información resultantes de interrelacionarlos y del perfil que se obtenga. Lo que esta en juego es la propia identidad de las personas.

3)- El derecho a la identidad y privacidad: Surge que el habeas data protege un "complejo de derechos personalísimos", que incluyen la privacidad y la identidad, relacionados a su vez con la imagen y con los conceptos de verdad e igualdad.

Compartimos la tesis que sostiene que el hábeas data ampara la identidad pero aclarando que ello no implica descartar que el hábeas data proteja también el derecho a la privacidad. Sucede que cuando los datos divulgados son sensibles, se afecta también este derecho, y de ahí que el mismo sea también objeto de tutela por esta acción.

En síntesis, el hábeas data no sólo protege entonces el derecho a la privacidad sino también el derecho a la identidad a través de los valores "verdad" e "igualdad". Todo dependerá de la situación que se intenta amparar por el hábeas data.

4)- Derecho a la información: El derecho a la información que se instala entre las garantías del habeas data no piensa en el carácter individual sino en el alcance general que tiene toda persona para solicitar información sobre la existencia de bancos de datos, sus finalidades y la identidad de sus responsables. La ley nacional lo contempla en el Art. 13.

El derecho a la información se presenta como una garantía de la publicidad de los actos que lleven a cabo los archivos.

La finalidad del derecho a la información no consiste únicamente en saber quienes son los titulares ni cuantos bancos de datos existen; la garantía proyecta un control directo sobre el tratamiento que se efectúa sobre la información que a la persona le atribuyen.

En síntesis, el derecho a la información es una garantía general para la publicidad de los actos de tratamiento de datos personales que efectúen los archivos.

5)- Derecho de Acceso: Es el derecho de entrada a los bancos de datos y la garantía principal que tiene la persona para conocer que información existe sobre ella. El derecho de solicitar y obtener información de un archivo o registro, para saber si el mismo contiene o no información personal que a alguien concierne,

constituye el fundamento esencial del habeas data. A el se refiere el Art. 14 inc. 1 de la ley nacional.

Resuelto el problema del acceso, el individuo puede resolver conductas posteriores. En este sentido, validará la información contenida; podrá ratificar la autorización prestada si ella se hubiese requerido; tendrá la facultad de exigir la actualización o rectificación de los datos; planteará la supresión del dato sensible, y en cada caso queda de manifiesto el poder de control de la persona sobre los archivos de datos personales.

Es importante destacar que el derecho de acceso no le corresponde únicamente al particular afectado por la información almacenada en un banco de datos sino a toda persona que acredite un interés legítimo para actuar.

6)- Derecho a controlar el archivo y los datos personales: La base del derecho a la protección de los datos personales está en el libre consentimiento que pueda dar quien sea requerido a esos efectos, y el control que a posteriori se pueda ejercer.

Esta vigilancia apunta hacia dos objetos precisos: controlar al archivo autorizado para que cumpla la finalidad oportunamente expuesta al requerir la autorización, y verificar la actualidad de los datos para que no se ofrezca información obsoleta, equívoca o inexacta.

Este derecho contemplado en el Art. 16 inc. 1 de la ley nacional, comprende cuatro prerrogativas íntimamente vinculadas:

- el derecho a la rectificación;
- el derecho a la actualización;
- el derecho a la confidencialidad y
- el derecho al silencio y al olvido mediante la cancelación del dato.

7) Los derechos humanos de tercera generación: Cuando se habla de derechos humanos de tercera generación se alude al orden cronológico de aparición de algunos derechos individuales e incluso reconocidos en forma genérica a la población, como el derecho a la mejor calidad de vida, la defensa del ecosistema, los

derechos de los consumidores, el derecho de los pueblos al desarrollo y al progreso, el derecho a la autodeterminación informativa, etc.

Conforme lo refieren Ekmekdjian, Miguel Angel y Pizzolo(h), Calogero, citando a Pérez Luño, estos derechos y libertades de la "tercera generación" se presentan como una respuesta al fenómeno de la "contaminación de la libertades" (liberties pollution), concepto con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías.

Llegamos así, detalla Gaibrois, a la década del '80 a partir de la cual se habla de nuevas reivindicaciones de los derechos humanos, que se refiere a temas propios tales como la llamada calidad de vida, la paz misma o, el caso que nos ocupa, la "libertad informática", enunciado este último que quizá condense postulados cibernéticos.

Válganos la trascripción efectuada para acceder a las consideraciones que el autor establece respeto de las características de los nuevos derechos informáticos. A saber: a) una nueva fundamentación (pues si la libertad y la igualdad fueran valores guía en la primera y en la segunda etapa, los derechos de la tercera tiene como principal valor la solidaridad); b) nuevos instrumentos de tutela (aquí es donde se hizo necesario implementar el hábeas data en el terreno de la informática, así como el hábeas corpus lo fue en la tradición de las libertades y el amparo en los demás derechos), y c) nuevas formas de titularidad (otorgándose a los ciudadanos en general legitimación activa en diversos casos para defenderse de las agresiones a bienes colectivos o intereses difusos).

Sobre este último punto, Bergel dice: "la flexibilidad en la legitimación procesal activa exige también, por las peculiaridades que entraña la defensa de esos derechos, una ampliación de la legitimación pasiva que permita superar determinadas trabas formales que anteriormente habían dejado en la impunidad conductas atentatorias o lesivas para los derechos fundamentales".

De todo ello surge que a los derechos de tercera generación, le corresponden también garantías de tercera generación, existiendo una línea que va desde el antiguo hábeas corpus inglés al amparo y desde allí al hábeas data.

La reforma constitucional de 1994 incorpora a sus rasgos garantistas este modo de protección de los derechos de las personas en la medida en que pudieran verse afectadas su honor o su honra, o pudiera ser perturbada su intimidad; derechos todos garantizados por el Art. 19 de la Constitución Nacional, o servir como un instrumento de discriminación, prohibido por lo que dispone la ley 23.592 y los tratados y convenciones internacionales incorporados por el articulo 75, inciso 22 de la Constitución Nacional.

3.1.2.3. Derecho Comparado.

En nuestro país, el hábeas data se encuentre legislado no sólo en la Constitución Nacional sino también en el Derecho Público Provincial.

La ley 4444 de la provincia de Jujuy explica que el derecho de acceso libre a las fuentes de información pública "puede ejercerlo toda persona físico o jurídica, radicada en la provincia, sin que sea necesario indicar las razones que lo motivan, y establece el proceso de acceso a la información que se concreta mediante una solicitud y contestación por escrito, por la autoridad pública, de los datos requeridos".

Algunas **constituciones provinciales** contemplan el hábeas data en forma implícita al regular los efectos del derecho a la intimidad: Constitución de Córdoba (Art. 50), de Tierra del Fuego (Art. 45), de Buenos Aires (Art. 20.3), de Catamarca (Art. 11), de Formosa (Art. 10), de San Juan (Art. 26 y 27), y de San Luis (Art. 21), entre otras.

Resumiendo y siguiendo a Puccinelli que, en el caso argentino, el tema relativo a los datos personales y al acceso a la información pública ha tenido regulaciones diversas : mientras algunas de las provincia consideraron en sus Constituciones solo un aspecto de la protección de aquellos datos ocupándose de los antecedentes policiales y penales (La Rioja, Salta y San Juan), o de establecer el derecho de acceso a las fuentes de información (Catamarca y Formosa, además de Río Negro y San Luis que por otra parte también regularon el habeas data), otras fueron mas

allá, consagrando el habeas data como acción especifica de garantía (Ciudad autónoma de Buenos Aires, provincia de Buenos Aires, Córdoba Chaco, Chubut, La Rioja, Jujuy, Río negro, San Luis, Sanjuán y Tierra del Fuego), aunque con diseños bien diversos. Además de la regulación constitucional, o en lugar de ella, algunas provincias asumieron el tema en la legislación subconstitucional (v.gr. Tucumán y Jujuy).

En el Art. 75 inc. 22 se le da jerarquía constitucional a los tratados internacionales que también reconocen y protegen el derecho a la intimidad.

"Corresponde al Congreso:

Aprobar o desechar tratados concluidos con las demás naciones y con las organizaciones internacionales y los concordatos con la Santa Sede. Los tratados y concordatos tienen jerarquía superior a las leyes.

La Declaración Americana de los Derechos y Deberes del Hombre; la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; la Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial; en las condiciones de su vigencia, tienen jerarquía constitucional, no derogan artículo alguno de la primera parte de esta Constitución y deben entenderse complementarios de los derechos y garantías por ella reconocidos. Sólo podrán ser denunciados, en su caso, por el Poder Ejecutivo Nacional, previa aprobación de las dos terceras partes de la totalidad de los miembros de cada Cámara.

Los demás tratados y convenciones sobre derechos humanos, luego de ser aprobados por el Congreso, requerirán el voto de las dos terceras partes de la totalidad de los miembros de cada Cámara para gozar de la jerarquía constitucional".

Sintéticamente nos referiremos a dos tratados internacionales que son ley vigente en nuestro país; **la Declaración Universal de los Derechos Humanos** de 1948, se expresa que la libertad de opinión y expresión "incluye en no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión". Este

derecho a recibir información es reproducido en la Convención Internacional de Derechos Civiles y Políticos del año 1966 y en el Pacto de San José de Costa Rica.

Asimismo, en el **Pacto de San José de Costa Rica** de 1969, existen referencias concretas no sólo al derecho a la privacidad sino también al derecho de todo individuo a conocer las informaciones que se refieran a su persona, mediante los recursos legales pertinentes. En sus artículos 11 y 12 sienta el principio de la prohibición de injerencias arbitrarias o abusivas en la vida privada, la familia, el domicilio y la correspondencia, así como la defensa contra los ataques a la honra o a la reputación. A su vez, en su artículo 25 inciso segundo, el Pacto refiere a los instrumentos de protección de ese derecho mediante la creación de un recurso judicial y consagra el compromiso de los Estados Partes: a) a garantizar que la autoridad competente prevista por el sistema legal del Estado decidirá sobre los derechos de toda persona que interponga tal recurso; b) a desarrollar las posibilidades del recurso judicial; c) a garantizar el cumplimiento, por las autoridades competentes de toda decisión en que se haya estimado procedente el recurso".

En la Comunidad Europea la **Directiva 95/46**, el art. 8 se refiere al Tratamiento de categorías especiales de datos, en el apartado 1 dice: "los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad."

Creemos oportuno hacer una sucinta referencia a **la LORTAD (Ley Orgánica de Tratamiento Automatizado de Datos)** de España, la cual agrupa en dos grandes apartados los principios fundamentales para la protección de datos.

El primero de ellos es el grupo de derechos que corresponden al sujeto de datos que son los siguientes: a)- consentimiento, b)- derecho de información, c)- derecho de acceso, d)- derecho de rectificación, e)- derecho a la veracidad de los datos, f)- derecho de indemnización de los perjuicios.

El segundo grupo es el conjunto de principios relacionados con el propio fichero que contiene los datos personales y que son: a)- principio de legalidad en la captación de los datos, b)- principio de unicidad, c)- principio de adecuación, d)- principio de caducidad, e)- principio de seguridad.

3.1.2.4. Jurisprudencia. Casos más importantes. Breve reseña.

Desde la Reforma constitucional del año 1994 hasta la sanción de la ley 25326 en octubre del 2000, existió un vacío legal que fue suplido por las decisiones jurisprudenciales.

A continuación detallamos algunos de estos fallos:

En la causa "Urteaga", cinco magistrados (Nazareno, Moliné O'Connor, Boggiano, Vázquez y Petrachi) se pronunciaron a favor de la acción de hábeas data como proceso constitucional que tutela el derecho a la verdad. En tanto, los restantes jueces consideraron que la acción de amparo es la vía idónea de protección de dicho derecho. Cuatro jueces que señalaron el hábeas data como remedio tutelar del derecho a la verdad, innovan con relación a la legitimación procesal para iniciar esta acción. La promoción de la acción de hábeas data no está limitada a la persona directamente afectada sino que -en determinados supuestos- se extiende también a sus familiares directos.

En la causa Ganora, y otro s/ Habeas Data, del 16/09/1999, la C.S.J.N. dispuso "el habeas data constituye la accion que garantiza el derecho que toda persona tiene a decidir por sí misma en qué medida compartirá con los demas sus sentimientos, pensamientos y los hechos de su vida personal". Mas adelante el mismo fallo dice "la protección legal que establece el habeas data se dirige a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga; este derecho forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad."

En la causa Estado Nacional (DGI) c/ Colegio Público de Abogados de Capital Federal, del 13/02/1996, el Superior Tribunal ha admitido en torno a la libertad informática que "en la era de las computadoras el derecho a la intimidad ya no puede reducirse a excluir a terceros de la zona de reserva, sino que se traduce en la facultad del sujeto de controlar la información personal que de él figuran en los registros, archivos o bancos de datos."

A nivel internacional el antecedente jurisprudencial por excelencia es la sentencia sobre la ley del censo de 1982, dictada el 15/12/19983 por el Tribunal Constitucional Federal Alemán, donde se perfila el derecho a la autodeterminación informativa, diciendo que "la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por si mismo cuándo, y dentro de qué límites procede revelar situaciones referentes a la propia vida."

3.1.2.5 La acción de Habeas data.

La herramienta procesal destinada a proteger los datos personales es el Habeas Data, el cual se fundamenta en los carriles constitucionales expresos del Art. 43 y en los implícitos del Art. 18, como reglas para un debido proceso.

Podemos definir el Habeas Data como "un derecho puesto en cabeza de cualquier persona a efecto de que por la vía más expedita prevista por la misma Constitución pueda tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y en caso de falsedad o discriminación, exigir la supresión, rectificación o actualización de aquellos, con la única limitación de que no podrá afectarse el secreto de las fuentes de información periodística".

El habeas data ha sido concebido principalmente para tutelar a los derechos de los particulares frente a quienes colectan, tratan o distribuyen datos (ya sean particulares o del estado) y pretende brindar una herramienta efectiva tanto a quienes colectan información ante la negativa injustificada de acceso a las fuentes de información pública, como a la sociedad, que también cuenta con el derecho a

informarse a través de quienes luego de recabada la información la proyectarán hacia ella.

La acción prevista en el Art. 43, párrafo 3° de la Constitución Nacional permite dividir el habeas data en dos etapas: la primera, relativa al acceso a la información, otorgando la posibilidad de que toda persona tome conocimiento de los datos a ellas referidos que conste en registros o bancos de datos públicos o privados y de su finalidad; y la segunda, una vez que comprobada la falsedad o discriminación, otorga el derecho para exigir su supresión, rectificación, confidencialidad o actualización.

El Art. 43 permite en una primer etapa el ejercicio de la acción por la persona afectada tendiente a "tomar conocimiento de las datos a ella referidos y de su finalidad". Es decir que el acción ante puede conocer no sólo que datos extienden sobre su persona el registro, sino también con qué objetivo de ellos están en el registro.

La toma de conocimiento implica el ejercicio del "derecho de acceso información". Este derecho de acceso tiene por finalidad permitiría al individuo el control sobre la información que le concierne que es en esencia uno de los objetivo principal del hábeas data.

Una vez que se han tomado conocimiento del dato y de su finalidad, se deberá probar que sí existe falsedad o que se genera un trato discriminatorio para poder hacer a los otros derechos, es decir a la segunda etapa del proceso de hábeas data.

Este desarrollo normativo, busca el equilibrio entre el derecho de información y el derecho a la intimidad. Entre la información que necesita la sociedad y el derecho del individuo a la protección de su ámbito privado y de sus datos personales.

Tal equilibrio debe existir para que haya equidad y justicia. Contribuye a ese equilibrio la posibilidad de todas las personas a saber de la existencia de archivos, manuales o informáticos, que contengan datos individuales, así como la finalidad de los mismos y el contenido del información que se registra en un archivo de datos. Además, el derecho de modificar aquellos datos personales que por incorrecto, parciales o desactualizados ocasionen o puedan ocasionar perjuicios. El hábeas

data es precisamente la acción judicial por la cual se puede llegar a esta rectificación.

El objeto de la acción de habeas data es tomar conocimiento de los datos referidos al amparista y de su finalidad, y a exigir su supresión, rectificación, confidencialidad o actualización.

También permite conocer la finalidad o la razón por la cual constan tales datos en los registros en que se encuentran y el destino para el que se los prevee utilizar.

La interpretación de la norma, así como la reglamentación legal a dictarse, debe realizarse teniendo en cuenta el bien jurídico protegido que es el derecho a la intimidad, a lo que hay que agregar el derecho de identidad, según el cual toda persona tiene derecho a ser identificada por medio de las reales circunstancias de su personalidad. Estos derecho pueden verse lesionado no sólo cuando el destino de los bancos de datos sea el de proveer informes, si no en cualquier caso, por la simple existencia de datos erróneos en cualquier registro.

El Habeas data al posibilitar la corrección de informaciones erróneas o su eliminación, protege en la persona su derecho a la imagen o perfil personal. Porque uno de los objetivos de la acción es evitar la propagación de la información incorrecta lo que afecta en ultima instancia, la identidad de una persona.

En definitiva, se trata de proteger la correspondencia de datos de una persona una realidad (exactitud) y la privacidad o el más íntimo ámbito personal frente al asombroso desarrollo de la informática.

El hábeas data responde a la necesidad de garantizar explícitamente libertad de intimidad de la persona, principalmente frente al avance de la informática, a partir de la explosión tecnológica. Se trata de proteger al ser humano frente a la libertad informática.

Respecto de la legitimación pasiva de esta acción, la misma podrá plantearse contra autoridades públicas o particulares que dirijan bases de datos o registros que suministren informes.

Un interrogante significativo que se platea es si la autoridad pública puede alegar razones de seguridad del Estado, o similares, para suministrar información.

En principio y como el texto constitucional no contempla excepciones, la respuesta es que siempre debe suministrarse la información requerida. Sin embargo hay constitucionalistas (Ekmekdjian) que admiten excepciones pero con carácter sumamente restrictivo.

Respecto a la legitimación activa del habeas data, al no hacer distinción los textos normativos, entendemos que se posibilita su ejercicio tanto a personas individuales como colectivas, pues donde la ley no distingue el intérprete tampoco debe hacerlo.

En referencia de estas últimas cabe formular una aclaración: tratando de una persona jurídica no será el derecho a la intimidad el que esté afectado, pues éste último no es posible predicarlo de aquella.

3.1.3. Definición y Clasificación de datos.

La clasificación de los datos a los efectos de la protección brindada por el Hábeas Data puede encontrarse en la misma ley o bien en la doctrina vigente.

De acuerdo a ley 25.326 de Protección de Datos Personales, Art. 2 los datos se clasifican en:

- **Datos Personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- **Datos sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- **Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

En la doctrina existen numerosos criterios de clasificación de datos, pero nos parece mas adecuado y completo el expuesto por Osvaldo A. Gozaíni que transcribimos a continuación:

Según la identificación del Titular del Dato, se clasifican en:

- **Dato Nominativo**: es el dato de persona física o jurídica conocida e identificada. Según Uicich estos datos pueden subclasificarse en Dato Directo, cuando el titular se identifica sin necesidad de proceso alguno y Dato Indirecto, cuando el titular se identifica pero no directamente sino mediante el agrupamiento de datos.
- **Dato Innominativo o Anónimo:** es el dato de uso estadístico o científico que no identifica a persona alguna sino a sus actividades.

Según la Confidencialidad de la Información, se clasifican en:

- **Dato que no afecta la Sensibilidad de la Persona**: es el dato rutinario que se obtiene de fuentes fácilmente accesibles y que no hiere los sentimientos más íntimos de la persona.
- **Dato que no afecta la Sensibilidad de la Persona o Dato Sensible:** es el dato de contenido privado que socava la intimidad de la persona y que puede registrarse e informarse sólo con autorización expresa del titular o cuando lo disponga una ley por razones de interés general. Estos son los datos referidos a ideologías, creencias, origen racial y étnico, salud, vida sexual y condenas penales.

Según la Complejidad para obtener el Dato, se clasifican en:

- **Dato Público**: información que se encuentra disponible para cualquiera por encontrarse en registros o lugares de acceso público. No tienen restricción para su conocimiento y difusión.
- **Dato Privado y Confidencial:** el dato Privado es el que la persona reserva en su intimidad, el Dato Confidencial es aquel que por su alta sensibilidad no se puede divulgar ni transmitir a terceros (secreto profesional, datos militares, etc).

Ahora bien, teniendo en cuenta el bien jurídico tutelado por el Habeas Data y los relevamientos efectuados, podemos agrupar los datos existentes hoy en los distintos Registros Públicos de la Provincia, tanto de manera informática como física, de acuerdo al siguiente detalle:

Datos Personales (no sensibles):

- Nombre y Apellido o Razón Social si se trata de una persona de existencia ideal
- Repartición, si se trata de un ente estatal
- Tipo y Número de Documento o CUIT
- Sexo
- Domicilio Actual y Anteriores
- Motivo por el que figura como deudor alimentario
- Estado Civil
- Fecha de Nacimiento / Defunción / Casamiento

Datos sensibles:

- Datos Morfológicos
- Fichas Dactilares
- Fotografías
- Datos de Familiares Directos
- Historial de Antecedentes Personales
- Lugares donde ha trabajado
- Resultado de Examen técnico-psicológico y socioecómico

Para la realización y análisis de lo expuesto en este documento, hemos tomado como única clasificación la que distingue los Datos Sensible de los Datos No Sensibles, ya que es la que contempla distinto tratamiento en el texto normativo vigente.

3.1.4. Condiciones de Tratamiento de los Datos.

A los efectos de la realización de este trabajo, cuando hablamos de tratamiento de datos estamos haciendo referencia a la definición que de este concepto enuncia la Ley 25.326 en su Art. 2: "son las 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 su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias."

Velásquez Bautista sostiene que si se observa y analiza la evolución que han sufrido estos procedimientos a lo largo del tiempo y en los distintos países del mundo, se evidencia que como consecuencia del avance de la tecnología se ha pasado de un tratamiento manual de datos a uno mecánico , y de éste al automático o automatizado.

Sin perjuicio de esta evolución que ha sido consecuencia directa e inmediata de la transformación tecnológica de los últimos tiempos, la protección legal conferida a las personas respecto a sus datos personales debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual ; ya que el alcance de la protección no debe depender de las técnicas utilizadas sino tener como fin el bien jurídico tutelado.

No debemos olvidar que al legislar sobre este tema, se tiene como objetivo garantizar a cualquier persona física o jurídica el respeto de sus derechos fundamentales, concretamente su derecho a la autodeterminación informativa con relación a su vida privada y demás derechos personalísimos; así mismo la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los

datos correspondientes a su persona o bienes. De hecho, este es el fin primordial establecido en el Anteproyecto de Convención Americana sobre Autodeterminación Informativa y en numerosos textos normativos a nivel nacional e internacional.

Así, los archivos y bancos de datos están sujetos a cumplir determinadas obligaciones en su actividad, tanto en la etapa de búsqueda, localización y almacenamiento del dato (almacenamiento propiamente dicho) como en la etapa de clasificación, procesamiento y seguridad del dato (tratamiento de los datos).

En la etapa de **almacenamiento de datos personales**, es preciso que el archivo o banco de datos obtenga los mismos con el consentimiento del titular. El consentimiento es el punto de partida para la legalidad de los archivos; ya que de acuerdo a las normas vigentes no existe autorización implícita: Ley 25.326 Art. 5 inc. 1 "El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito o por otro medio que permita se le equipare, de acuerdo a las circunstancias."

En la etapa de **tratamiento de datos**, es cuando se producen las invasiones mas reiteradas a la intimidad y en la que la privacidad de las personas sufre por la ausencia de controles efectivos y específicos. Por este motivo el archivo debe regirse por el principio de "Calidad de los Datos"; principio que está contemplado normativamente en el Art. 4 de nuestra ley y que establece una serie de requisitos que deben cumplirse en la administración de la información y que resumimos a continuación:

- debe ser adecuada para el objetivo que el archivo persigue
- debe ser pertinente y no excesiva con la finalidad del registro
- debe ser proporcional en el almacenamiento de datos (se deben guardar sólo los datos necesarios)
- deben usarse los datos para el fin perseguido y no para un fin distinto
- la información debe ser exacta (actual) y actualizada periódicamente

- está prohibida la búsqueda y almacenamiento de datos por medios fraudulentos, desleales o ilícitos

Es en este contexto que los archivos y banco de datos quedan obligados a cumplir también con el principio de "Seguridad de los Datos", que incluye requisitos de seguridad técnica y física para sí y para garantizar a las personas concernidas sobre la confidencialidad y secreto de la información aportada; Ley 25.326 Art. 9: "Inc.1- El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Inc. 2- Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad".

En este deber de resguardar la seguridad de sus archivos que debe cumplir el banco de datos para evitar accesos no autorizados o la penetración a la red por personas distintas a las que están autorizadas para hacerlo, deben contemplarse dos aspectos igualmente importantes: el cuidado que se debe tener con las personas que tratan la información y custodian la seguridad del archivo por un lado; y la protección de los datos en particular por otro.

Así, los archivos o bancos de datos tratan de garantizar la seguridad y de generar confianza en las personas sobre su confidencialidad, utilizando distintos métodos que están orientados a asegurar el sistema informático, a controlar a las personas que trabajan en el archivo y a impedir el ingreso de terceros a las bases de datos. Estos métodos contemplan los aspectos de Seguridad Técnica, Seguridad Lógica y Seguridad organizada por Vía Reglamentaria; que hacen en definitiva a un único y completo concepto de Seguridad.

La **Seguridad Técnica** supone la integración de elementos externos al equipamiento (hardware y software) para que controlen y aseguren los riesgos normales y anormales del mismo. Se refiere básicamente a las instalaciones donde funciona el archivo o banco de datos, censores infrarrojos, circuito de cámaras de control, contraseñas, seguros de riesgo, sistemas de alarmas, etc.

La **Seguridad Lógica** se vincula con la intromisión que pueda sufrir una base de datos y las acciones que puedan implementarse para evitar este hecho. Son medidas organizacionales que deben definirse e implementarse frente a la debilidad de los sistemas para evitar o contrarrestar las interferencias en la información (control de usuarios, control de acceso, etc.).

La **Seguridad establecida por Vía Reglamentaria** recae sobre el responsable del archivo y surge como consecuencia de la imposibilidad de generar por vía normativa consignas sobre medios y acciones técnicas y lógicas que resuelvan la seguridad de los archivos o bancos de datos. Se ha sugerido entonces el establecimiento de niveles para identificar dónde debe ponerse el foco y establecerse límites de acuerdo al grado de riesgo existente.

- **Nivel Básico:** El archivo o banco de datos debe contar con un manual de instrucciones de conocimiento y aceptación obligatorios para todas las personas que trabajan en su ámbito, y sobre todo de aquellos que tienen la tarea de incorporar y procesar datos . Este manual debe complementarse con controles de acceso y procedimientos de identificación y autenticación para dichos accesos (identificación del usuario).
- **Nivel Medio:** En este nivel se toma en consideración el tipo de archivo creado. Se trata de registros sobre infracciones administrativas, penales, situación patrimonial, etc. donde además de cumplirse con las medidas del nivel básico, el archivo o banco de datos debe tener un responsable de la seguridad encargado del control directo y auditoría permanente del sistema. En algunos casos, se incorpora como recaudo adicional operar en lugares cerrados donde el acceso sea restringido.

- **Nivel Alto:** es el nivel destinado para el tratamiento de datos sensibles. Las medidas de seguridad se extreman para impedir el acceso a ellos y la responsabilidad por su violación es superior. El establecimiento de prevenciones y controles debe ser permanentes y las infracciones penadas y multadas.

3.1.4.1. La Situación en Nuestros Registros Públicos Provinciales

De acuerdo a los relevamientos efectuados sobre los distintos Registros Públicos existentes en la Provincia y tomando como punto de partida lo establecido por leyes, doctrina y jurisprudencia en lo relativo al Habeas Data, se evidencia que los Datos que constan en los mismos son en general datos no sensibles y en la mayoría de los casos se trata de datos que de acuerdo a lo establecido en la Ley Nacional 25.326 Art. 5 inc 2, no requieren el consentimiento del titular de los mismos para ser almacenados o divulgados.

En cuanto a las condiciones de almacenamiento y tratamiento de los datos, hemos mencionado precedentemente que como consecuencia del avance de la tecnología se ha pasado de un tratamiento manual de datos a uno mecánico , y de éste al automático o automatizado. Sin embargo, esta realidad no es la que se verifica en la actualidad en nuestros Registros Públicos provinciales.

Tal vez como consecuencia de la falta de una ley provincial que reglamente la parte operativa de lo establecido por la Ley 25.326, no hay uniformidad en cuanto a la manera y condiciones de administrar dichos datos, sino que depende del Registro en cuestión.

Existen Registros Públicos que cuentan con cierto grado de informatización en la información que administran, aunque no con tecnología de avanzada ni de manera excluyente, ya que conviven de manera paralela el sistema informático con la administración física y manual de la información; con el riesgo de inconsistencias, imposibilidad de efectuar controles y burocratización que esta doble administración

conlleva. En cambio, otros Registros Públicos, realizan una administración exclusivamente física y manual de los datos.

Tampoco hay conocimiento y concientización por parte de los administrativos que trabajan en los Registros de la garantía protegida por la institución del Habeas Data, de las disposiciones legales al respecto ni de los resguardos que deben contemplarse a fin de disminuir los riesgos potenciales; a excepción de los Registros de Antecedentes Personales y de Adoptantes, donde se custodia y resguarda de manera adecuada la información allí contenida.

Creemos que sería óptima una actualización y reingeniería en el funcionamiento de los Registros Públicos; no sólo con el fin de garantizar el cumplimiento de los requisitos y obligaciones legales vigentes sino también para optimizar su funcionamiento. Con este objetivo desarrollamos a continuación la opción que hemos considerado más conveniente:

De manera general, consideramos que la mejor opción para realizar la administración y actualización de datos en los Registros Públicos es partir de una Base Única de Información a través de herramientas informáticas que, a través de una eficiente y eficaz administración de permisos y controles derivada de un exhaustivo análisis de casos y delimitación de responsabilidades, permita a cada Registro en particular acceder a modo de consulta y actualización exclusivamente a la información que le es propia.

Esta alternativa tiene un sinnúmero de ventajas tanto operativas como de seguridad jurídica, las cuales se resumen a continuación:

- Permite consolidar toda la información existente en un único lugar y en un medio electrónico, generando datos confiables al evitar la coexistencia de bases paralelas con información errónea e inconsistente que existe en la actualidad como también optimizar la administración de recursos (herramientas informáticas, personal administrativo, soporte técnico, etc.) que están implícitos en el estado actual de los Registros de la Provincia.

- Al contar con toda la información en un único lugar al que puede accederse desde las distintas reparticiones de acuerdo a los permisos otorgados y con registro de las consultas y modificaciones realizadas; se cuenta con una herramienta que permite fiscalizar y auditar el accionar de los empleados de la Administración Pública para, de esta manera, salvaguardar los Derechos personalísimos a la Intimidad y a la Identidad resguardados por la Constitución Nacional y al mismo tiempo asegurar y garantizar la no-comercialización o el uso indebido de dicha información o la sanción a quien haya incurrido en este hecho, si corresponde; situaciones éstas contempladas en los arts. 9,10, 31 y 32 de la Ley Nacional 25.326.
- Se disminuyen y mejoran los tiempos de respuesta de la administración pública al ciudadano optimizando de esta manera los tiempos administrativos internos y externos y permitiendo la reasignación de tareas dentro de cada Registro; ya que la consulta de la documentación física existente solo se realizaría en casos excepcionales

De manera particular, consideramos que los Registros Públicos además de observar en su actividad los deberes ya descriptos de consentimiento, legalidad, calidad y seguridad de los datos deben cumplimentar también el Deber de Confidencialidad, contemplado en el Art. 10 de la ley 25.326: "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 su relación con el titular del archivo de datos".

Adicionalmente, los procedimientos de recolección, almacenamiento, información, modificación y supresión de los datos variarán según se trate de Datos Personales (no sensibles) o de Datos Sensibles.

En el caso de los **Datos No Sensibles,** su tratamiento está contemplado en la Ley 25.326 Art. 5 inc.2 a, b y c y de acuerdo a lo establecido en dicho artículo, no se necesita el consentimiento del titular de los mismos. Este tipo de datos puede ser recolectado e informado al ciudadano sin restricciones. Sin embargo, esta relativa flexibilidad que se evidencia en el tratamiento de los datos no sensibles no se refleja

en lo relativo a la actualización o supresión de los mismos; ya que de acuerdo al Art. 16 inc.5 de la Ley 25.326 no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

Los **Datos Sensibles** en cambio son informaciones que afectan la esfera máxima de intimidad y privacidad personal y por ello merecen un tratamiento particular. Su tratamiento está contemplado en la Ley 25.326 Art. 7 y de acuerdo al mismo estos datos sólo pueden ser recogidos, tratados y transmitidos con consentimiento expreso del titular, salvo que prime el interés general o lo disponga una ley.

Cabe aclarar que la mayor protección legal y rigidez que se establece para el tratamiento de los datos sensibles no responde al dato en sí mismo sino al uso discriminatorio que puede hacerse de él.

Tanto si se trata de datos sensibles como de datos no sensibles, no podemos pasar por alto que los datos personales son informaciones que deben resguardarse de filtraciones no queridas y es por este motivo que debe ponerse especial precaución en la información que se incorpora y se brinda desde el archivo y particularmente a las transferencias que de estos datos se hagan vía e-mail; ya que ello requiere resguardos y condiciones de seguridad específicos que en caso de no cumplirse permiten la dispersión ilimitada del dato, con las consiguientes responsabilidades y sanciones administrativas y penales que se generan. Sobre este aspecto, expondremos y desarrollaremos más detalle en la Actividad N° 2 del presente Proyecto al referirnos a los mecanismos y procesos de consulta de la información.

3.1.5. Acuerdos, Auditorias y Control Interno.

La ley nacional proyecta la creación de un órgano de control estatal que tendrá como misión controlar a empresas y organismos públicos que venden datos; órgano que en la realidad no ha sido creado ocasionando la falta de control y de definición de principios rectores en este aspecto.

La necesidad de principios deontológicos establecidos en un código tipo es inevitable en el uso por otros de datos personales.

Por ello surge este anhelo de contar con normas éticas que guíen las conductas de los usuarios y titulares de archivos.

De ello se ocupa el Art. 30 de la ley nacional, que dice:

"1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

En particular, se ha continuado la consigna emitida en Europa por la directiva 95/46 CE. La Asociación Española de Comercio Electrónico ha presentado el primer código ético de protección de datos pionero en Europa.

El código se basa en cuatro normas voluntarias como son el derecho de oposición del usuario al almacenamiento y utilización de su información, la protección de menores mediante la limitación y clarificación del uso de los datos que éstos aportan, la posibilidad de rechazar el uso de correo electrónico para actividades comerciales y el sometimiento de las empresas a un comité de control del cumplimiento que realizará auditorias periódicas al azar.

A continuación presentamos un modelo tipo de convenio que permita la realización de auditorias de manera permanente en los registros públicos provinciales. Creemos que es fundamental la conformación de una Comisión Auditora, la cual debería estar integrada por un representante de cada uno de los tres Poderes del Estado Provincial, por el Defensor del Pueblo y por representantes de las ONGs que tengan por misión la protección de los derechos humanos y el resguardo de las garantías personales.

También presentamos un modelo de manual de responsabilidades, normas y conductas de uso interno en consonancia a lo previsto en el mencionado art. 30 de la ley nacional. Creemos conveniente incluir en este documento una constancia de toma de conocimiento y aceptación por parte del personal del Registro.

Convenio entre los Registros y la Comisión Auditora para la Auditoría del Sistema y/o Procedimiento en el Tratamiento de Datos Registrados.

Entre el Registro..... dependiente del Poder ..... representado en este acto por .....con domicilio legal en .....por una parte y la Comisión Auditora representada en este acto por.....en adelante la Comisión, por otra parte, convienen en celebrar el presente acuerdo que ordenará y regirá las relaciones jurídicas, a partir de la fecha de suscripción del presente instrumento que se generen entre las partes como consecuencia del cumplimiento por parte del Registro de las funciones y obligaciones establecidas en la Ley Nacional N° 25.326 y conforme a las siguientes cláusulas.

PRIMERA: La Comisión efectuará a pedido del Registro y/o de las ONGs que estén comprometidas con el respeto a los Derechos Humanos, en la forma y condiciones que se determinen más adelante, la Auditoría del Sistema y/o Procedimiento en el Tratamiento de Datos Registrados.

La vigencia del presente convenio será de un período de veinticuatro (24) meses a partir de la firma del mismo, salvo que una de las partes lo denuncie, debiendo notificar fehacientemente a la contraparte en término no menor de 30 días hábiles. En forma anual las partes efectuarán los reajustes del convenio que estimen pertinentes.

El plan detallado, la metodología de selección de la muestra y su alcance pormenorizado se encuentran desarrollados en el ANEXO I que integra el presente convenio.

SEGUNDA: Con referencia a las tareas enunciadas en la cláusula primera, las partes de común acuerdo establecen que se presentarán informes de auditoría del Sistema y/o Procedimiento en el Tratamiento de Datos Registrados según se estipula en el Anexo I.

TERCERA: El Registro se compromete a facilitar las tareas a realizar por parte de La Comisión y establecidas en la cláusula primera del presente acuerdo. A tal efecto facilitará al personal de La Comisión el acceso a sus dependencias, la información y documentación que se solicite, aportando los recursos humanos y materiales que resulten necesarios. La información y demás datos que lleguen a conocimiento del personal de La Comisión afectado al cumplimiento de estas tareas tendrán carácter estrictamente confidencial.

CUARTA: Las partes acuerdan que los papeles de trabajo u otros antecedentes, que se confeccionen como consecuencia de los trabajos de Auditoría estarán a disposición de El Registro, quien tendrá derecho a solicitar las copias que estime necesarias. De igual forma La Comisión dará respuesta a toda consulta que le solicite El Registro en razón de las tareas que realice.

QUINTA: Para todos los efectos del presente, en lo sucesivo La Comisión será representada por el Presidente. En el caso de El Registro por su responsable o director.

En prueba de conformidad, las partes enunciadas en el encabezamiento suscriben el presente convenio en San Luis a los ..... días del mes ..... de 2003, en tres (3) ejemplares de un mismo tenor y a un solo efecto.

ANEXO I

ASUNTO: Auditoría continua del Sistema y/o Procedimiento en el Tratamiento de Datos Registrados para el período 2 de enero de 2004 y por el transcurso de veinticuatro (24) meses (enero de 2006).

1. Alcance:

La auditoría incluirá la planificación de las tareas, la evaluación selectiva de la estructura de sistemas de control interno del Sistema y/o Procedimiento en el Tratamiento de Datos Registrados; la obtención de evidencia objetiva y suficiente que posibilite a los auditores la emisión de los informes mensuales sobre el trabajo realizado que incluirá la descripción y cuantificación del mismo y las recomendaciones.

2. Objetivo:

Revisar los controles e identificar problemas en del Sistema y/o Procedimiento en el Tratamiento de Datos Registrados y emitir informes de manera sistemática y permanente para que se realicen las correcciones necesarias.

3. Procedimientos:

Cada Registro se auditará trimestralmente y a los fines de cumplir con el cronograma La Comisión auditará como máximo 4 Registros por mes.

El tamaño de la muestra en cada Registro dependerá de la cantidad de información que procesa, partiendo de un mínimo del 10 % (diez por ciento) hasta un máximo del 30% (treinta por ciento).

Se prevén las siguientes entregas iniciales: (I) programación del trabajo de campo durante el primer mes; (II) un primer informe antes de finalizar la segunda semana de marzo de 2004. El resto de la programación podrá ser realizada mensualmente según la experiencia que se vaya acumulando o ajustes que se realicen durante el período de ejecución del trabajo a la metodología o a los procedimientos aplicables (de común acuerdo entre las partes firmantes del Convenio).

4. Recursos humanos a afectar

Respecto de los recursos humanos a ser afectados se ha previsto un equipo de 5 personas para todo el período del convenio por un total de 14400 horas hombre.

5. Presupuesto de auditoría

Costo total de la auditoría.

a)Honorarios

Manual de Responsabilidades, Normas y Conductas.

A – Objeto

El objeto de la presente norma es definir y establecer los procedimientos, obligaciones y conductas que debe conocer y cumplir el personal del archivo o banco de datos en el desempeño de sus funciones, como también definir los controles y delimitar las responsabilidades que correspondan; en especial en lo relativo al aseguramiento de la confidencialidad y la seguridad jurídica en el almacenamiento y tratamiento de datos personales.

B – Ámbito de Aplicación

La presente norma es aplicable a todos los sectores y tareas comprendidas dentro del archivo o banco de datos, especialmente a los sectores y personas que cumplen tareas de:

- Búsqueda y recolección de datos

- Almacenamiento de los mismos

- Clasificación y procesamiento de datos

- Actualización de la información

- Seguridad de los datos y de las instalaciones del Registro o banco de datos

- Interconexión, adquisición o cruzamiento de la información con otras bases de datos

- Información, transmisión y cesión de datos

C – Recursos Protegidos

Se protege todo recurso contenido en el archivo o banco de datos, sea que el mismo exista de manera física o informatizada.

A los efectos de esta norma se entiende por recurso tanto a las instalaciones del Registro o banco de datos (archivos, ficheros, documentación en general, computadoras, sistemas informáticos, sistemas de seguridad, etc.) como a los datos personales contenidos en él, especialmente los datos sensibles.

D – Seguridad de los Archivos

El Titular o Responsable del archivo o banco de datos tiene la obligación de establecer todas las medidas que sean necesarias y pertinentes a fin de mantener la confidencialidad e integridad de los datos personales frente a actos exteriores que puedan ponerlos en peligro.

Para ello debe definir claramente los procedimientos y medidas de seguridad que deben aplicarse a todos los ámbitos del Registro o banco de datos y que tengan como fin proteger los datos personales y las propias instalaciones del Registros contra riesgos de pérdida parcial o total, destrucción, modificación y acceso inadecuado.

En caso de detectarse deficiencias en estos sistemas o procedimientos, el personal que identifique la misma debe informar inmediatamente al Titular o Responsable del archivo, o a quien corresponda de acuerdo a la estructura organizacional, a fin de que se supla el inconveniente y se definan las acciones correctivas y preventivas que correspondan.

E – Funciones y Obligaciones del Personal

El personal tiene a su disposición y se compromete a tomar conocimiento de lo establecido en la Ley 25.326 respecto a la protección de datos personales y a actuar en el desempeño de sus funciones de acuerdo a lo dispuesto por dicha ley.

Así mismo, y en consonancia con la reglamentación vigente, se compromete a cumplir con las siguientes normas internas:

1- Realizar todas las acciones pertinentes y necesarias a fin de proteger la seguridad y confidencialidad de todo recurso contenido en el archivo o banco de datos, sea que el mismo exista de manera física o informatizada.

2- Actuar con diligencia y responsabilidad, de manera de asegurar que los datos que se incorporen al archivo o banco de datos hayan sido obtenidos con el consentimiento expreso del titular y que no sean excesivos o no pertinentes con los fines del archivo.

3- Actuar con buena fe y honestidad, a los fines de garantizar la actualidad y verdad de la información contenida en el archivo o banco de datos.

4- Asegurar el derecho de acceso del titular de los datos al Registro o banco de datos, como también dar a conocer al mismo los motivos por los que los datos se registraron.

5- No utilizar la información contenida en el Registro o banco de datos para un destino distinto a aquel fin con el que fue creado el Registro ni tampoco para beneficio propio.

6- Queda prohibida la manipulación, el uso indebido y la comercialización de la información para fines o actividades no contempladas en el archivo o banco de datos.

7- Cumplir y respetar los procedimientos y medidas de seguridad internas que defina el Titular o Responsable del archivo o banco de datos para el desempeño de sus funciones y el resguardo de la información en él contenida.

8- Colaborar con los controles y auditorias tanto internas como externas que acuerden, definan y autoricen los Responsables del archivo o banco de datos.

F – Control y Auditoría

El Titular o Responsable del Registro tiene libertad para establecer y definir, dentro de los límites normativos vigentes, los controles y auditorías que estime necesarios para garantizar el cumplimiento de lo establecido en la ley 25.326 y las disposiciones internas vigentes en el archivo o banco de datos.

Los controles y auditorías podrán ser realizados por personal del Registro destinado exclusivamente a tareas de control o bien por personal externo como consecuencia de convenios de auditoría o contratación de consultoras especializadas en dicha tarea.

Para efectuar los controles, se analizará tanto la documentación existente de manera física como toda operación registrada en los sistemas informáticos o de seguridad con los que cuente el archivo o banco de datos.

G – Prevenciones y Sanciones

En caso de detectarse desvíos o irregularidades, se procederá a analizar la causa de los mismos a fin de detectar si el personal ha actuado como consecuencia de un error involuntario, deficiencias en los sistemas y procedimientos vigentes o si ha existido mala fe o negligencia en el desempeño de sus funciones.

En el primer y segundo caso, se procederá a implementar las acciones correctivas y preventivas que correspondan (capacitación, modificaciones en los sistemas de seguridad, validaciones en los sistemas informáticos, actualización del manual interno de normas y conductas, etc).

En el tercer caso, se analizará con el sector de RRHH la sanción administrativa a imponer de acuerdo a la gravedad del acto y por mal desempeño de sus funciones. Ello sin perjuicio de la responsabilidad por daños y de las sanciones penales que de acuerdo a la ley correspondan por la infracción cometida.

Toma de Conocimiento y Aceptación del Manual Responsabilidades, Normas y Conductas

En la ciudad de ....., a los ..... días del mes de ..... del año ....., declaro tomar conocimiento y aceptar para el desempeño de mis funciones lo establecido en el Manual de Responsabilidades, Normas y Conductas.

.....

Firma del Empleado

.....

Aclaración

.....

Número de Legajo

3.2. ACTIVIDAD Nº 2: Instrumentar los Mecanismos y Procesos de consulta de la información, en especial la relacionada con la producción y generación de empleo.

3.2.1. Derecho a la Información.

Concepto de información: en un sentido corriente o genérico, "información" es sinónimo de noticia o de mensaje. Esta expresión vincula el contenido de una cosa significada a un individuo receptor. "Informare", significa, en latín, "poner la forma". El mensaje es lo que permite construir una forma para el receptor mediante el ensamblaje de los signos que se le ofrecen. El Diccionario de la Lengua de la Real Academia Española define al término "informar", en su tercera acepción, como: "Dar forma sustancial a una cosa".

Antecedentes: en derecho comparado a partir de la década del 50 nos muestra a países como los Estados Unidos que por el instituto del " Freedon of information Act" se reconoce el derecho a la vista con las características apuntadas. En igual sentido Francia e Italia fueron dictando las normas que determinan el derecho a saber, como perteneciente a una tercera generación de derechos humanos, después de los civiles y políticos y de los económicos y sociales.

En Suecia el derecho a la vista tiene rango constitucional, como así también en España, porque se ha tomado conciencia de la necesidad de fomentar a la información como un derecho político de la colectividad, que no necesita justificar su razón, sino que por el contrario, debe en su caso acreditarse una necesidad legal y fundada de reserva para limitarlo. Se ha desplazado de esta forma el "onus probandi".

Asimismo, existen antecedentes argentinos del derecho público provincial, como ser el de la provincia de Chubut que en 1992 dictó su ley 3764 en esta materia y el más reciente de la Ciudad Autónoma de Buenos Aires con el dictado de la ley 104 en el año 1998.

Desarrollo: Vinculado al proceso constitucional de hábeas data aparece este derecho a la información que representa varias cosas importantes.

La solicitud de información se justifica en el principio republicano de publicidad de los actos de gobierno y, por esta razón, la sola condición de ser ciudadano habilita a requerir información sin importar los motivos del requerimiento.

Si la transparencia es una de las estrategias más eficaces de control del gobierno por parte de la ciudadanía, no puede ser el mismo gobierno el que decida si brinda la información evaluando en cada caso si existen buenas razones para que un ciudadano requiera información. Por este motivo, la información debe poder ser requerida por cualquier ciudadano y no sólo por aquellos que la administración considere poseen la legitimación para ello.

En torno a los fundamentos que le ofrece a la garantía constitucional creada es evidente que el derecho , desde esta perspectiva, permite al individuo exigir al banco de datos la información que tenga sobre su persona.

Sin embargo, debemos recordar que en el conjunto de posibilidades que encuadra el derecho a la información aparecen la libertad de expresión, la libertad de prensa y de imprenta, la libertad de opinión y otras que , confrontadas con la potencialidades que ofrece el hábeas data, pueden ocasionar algunas reservas.

Ahora bien, el derecho a la información resume en los hechos tres actividades: a)- la libertad de investigar; b)- la libertad de difundir, y c)-la libertad de recibir información y opiniones, cada una de ellas tiene el correlato de la responsabilidad, razón por la cual existe otro derecho personal a no recibir información distorsionada, y su reflejo en el derecho a no ser objeto de una información falsa o abusiva. Lo que se conoce como *"El derecho a la información veraz"*. Veracidad de la información supone mantener actualizado el archivo y conservar la información oportunamente tomada de acuerdo con las reales circunstancias en que sucedieron (situación real del afectado).

3.2.1. Derecho a la Autodeterminación Informativa.

La persona que presta su autorización para tomar información que le concierne tiene el derecho a exigir que esos datos se mantengan actualizados, y a ratificar el consentimiento cuando ellos puedan transferirse a terceros. También puede revocar la autorización conferida, pero esta decisión no tiene efectos retroactivos.

La autorización o consentimiento consiste en un acto expreso del titular de los datos por el cual está de acuerdo en ser incorporado a un banco de información personal. Antes de prestarlo debe ser informado sobre la finalidad que el archivo persigue y destino que tendrán sus datos.

Esta es la base o pilar del llamado derecho a la "autodeterminación informativa", que pretende encolumnar el tratamiento de los datos a partir de la decisión libre y voluntaria de las personas.

Siendo el consentimiento, el punto de partida para la legalidad de los archivos, el art. 5 de la Ley Nacional de Protección de Datos Personales Nº 25.326 indica: "*1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.*

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6º de la presente ley."

La norma articula el consentimiento con la información: no existe autorización implícita, y en caso de duda, pensamos que debe estarse por la ausencia de consentimiento. Cuando se autorice el uso de datos personales, se debe saber para qué finalidades. Por tanto, apenas prestada la autorización, el interesado adquiere un derecho de control sobre el registro y tiene disponibles las acciones pertinentes, sea para acceder al archivo o para fiscalizar la exactitud, o rectificar, cancelar o exigir la supresión.

3.2.1.2 Libertad de Información y Derecho a la Privacidad.

La libertad de información trasciende el quid que, en su tiempo, produjo la libertad de expresión. Mientras ésta pretende resolver el problema de la intervención de los poderes públicos en materia de censura o prohibición previas, la libertad informativa tiene que afrontar una dimensión muy diferente a la de otrora, si se tiene en cuenta el alcance inusitado de los medios de comunicación y la mentada globalidad que ella alcanza.

Mientras en origen la libertad de manifestarse (expresar ideas y reunirse sin obstáculos ni impedimentos de orden legal) era un expreso reconocimiento a una sociedad libre, actualmente la libertad admitida no se puede interpretar sin límites.

Comienza así el conflicto entre preferencias. ¿Qué es más importante, proteger la libertad de información o la libertad de intimidad? ¿ Acaso es posible establecer jerarquías?

Para encontrar las respuestas es preciso hurgar en la vida privada para saber –o reconocer- aquello que es intangible y que, aún invocando libertades fundamentales, no puede socavarse por la dignidad que exige la persona humana.

En este sentido, la intimidad individual y familiar, la honra, la propia imagen, la reputación, son valores que la prensa no puede comprometer amparada por la libertad de expresión y opinión. Éste es un punto sin discusión; la intimidad exige un plano de vida privada y familiar que permite la realización de la persona sin interferencia ni intromisiones. Es por ello que existen datos que por su sensibilidad con la persona no se pueden registrar ni divulgar sin el previo consentimiento del particular.

Por otra parte, en el derecho a la información la necesidad de expresar la verdad y conocer la verdad son aspectos esenciales para ella y un límite preciso para su justificación. Informar lo que no es cierto transforma la difusión en una calumnia.

En cambio, uno puede expresar ideas o pensamientos a través de la presa sin involucrar a terceros, ejerciendo un legítimo derecho que no refiere a la información. Por eso, la libertad de expresión es más amplia que la libertad de información.

Terminando con el desarrollo del presente tema, entre la libertad de expresión y el derecho a la intimidad existe un conflicto que sólo se puede resolver con prudencia y adecuación a los tiempos y a las personas.

Sin embargo, existen algunas reglas que no pueden olvidarse:

a) Sólo la defensa del interés público justifica las intromisiones o indagaciones sobre la vida privada de una persona sin su previo consentimiento.

b) En el tratamiento informativo de los asuntos en que medien elementos de dolor o afición en las personas afectadas, el periodista evitará la intromisión gratuita y las especulaciones innecesarias sobre sus sentimientos y circunstancias.

c) Las restricciones sobre invasiones en la intimidad deberán observarse con especial cuidado cuando se trate de personas ingresadas en centros hospitalarios o en instituciones similares.

d) El periodista deberá evitar nombrar en sus informaciones a los familiares y amigos de personas acusadas o condenadas por un delito, salvo que su mención resulte necesaria para que la información sea completa y equitativa.

e) Se evitará nombrar a las víctimas de un delito, así como la publicación de material que pueda contribuir a su identificación, actuando con especial diligencia cuando se trate de delitos contra la libertad sexual.

f) Los criterios indicados en los dos principios anteriores se aplicarán con extremo rigor cuando la información pueda afectar a menores de edad. En particular, el periodista deberá abstenerse de entrevistar, fotografiar o grabar a los menores de edad sobre temas relacionados con actividades delictivas o enmarcables en el ámbito de la privacidad.

g) El periodista deberá evitar la publicación de datos (sobre la raza, color, religión, origen social, o sexo de una persona, o cualquier enfermedad o minusvalía física o mental que padezca), salvo que guarden relación directa con la información publicada.

* Las consideraciones expuestas corresponden al Código Deontológico de la Federación de Asociaciones de Prensa de España.

3.2.2. – Condiciones Técnicas.

La protección de las personas debe aplicarse tanto al tratamiento de automáticos de datos como a su tratamiento manual.

Los archivos manuales constituyen una parte de la historia del mundo. La Comunidad Económica Europea a través de la Directiva sobre Tratamiento de datos señala, en cuanto respecta al tratamiento manual, que solo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas. En particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada miembro; que las carpetas y conjuntos de carpetas, así como sus portadas, que estén estructuradas conforme a criterios específicos, no están comprendidas en ningún caso en el ámbito de aplicación de la presente directiva.

La informática, modifico sustancialmente el espacio y el tiempo para conservar la información. Se pueden crear, agregar, modificar y consultar un volumen muy grande de datos ya sean personales o no; en los que se deben proteger los datos utilizando medidas de seguridad. Por ello el alcance de la protección no debe depender de las técnicas utilizadas, pues de lo contrario daría lugar a riesgos graves de elusión.

Archivos penales

Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en marco de las leyes y reglamentaciones respectivas. Los archivos de las condenas que se dictaron de manera pública, son los mas protegidos y menos accesibles.

La persona que transmite la información penal debiera reservar en la difusión sólo el dato consistente en la situación procesal, y nada más. Es imprescindible resguardar la reserva y confidencialidad de otros datos que surgen del relevamiento jurídico efectuado en las etapas sumariales donde necesariamente se investigan aspectos de la personalidad que no son parte de la información a comunicar.

Por ello, en 1997 la Comisión de Bélgica afirmaba que "la posibilidad de usar bases de datos centralizadas o integradas para buscar los antecedentes penales de una persona crea riesgos para la protección de datos que son totalmente desproporcionados respecto a los medios tradicionales de acceso o publicación de los casos judiciales. La evolución tecnológica debe ir acompañada de una mayor discreción respecto a la revelación de la identidad de las partes que se encuentran en los archivos de los casos judiciales".

Otro punto a tener muy en cuenta es la transmisión del dato penal requerido por otro juez interviniente, pues si lo que se pretende es mantener la confidencialidad, no debiera en caso alguno solicitarse por el juez civil o penal o de cualquier otra jurisdicción más datos de los que son absolutamente necesarios. También es preciso garantizar la reserva del trámite, de modo tal que en el mismo intervengan solamente aquellos que pueden ver la información. Inclusive, para las partes el alcance del secreto debiera extenderse impidiendo la extracción de copias del expediente donde figure la información sensible.

Archivos Fiscales

Los bancos de datos en materia fiscal se forman esencialmente con las declaraciones juradas que efectúan los contribuyentes amparados por el secreto y confidencialidad del sistema.

El secreto fiscal esta dispuesto en el artículo 101 de la ley 11.683, para toda documentación que se exponga, incluyendo los papeles privados de los que el Fisco toma conocimiento.

La seguridad de la base de datos (que pasa a ser eminentemente informática) se resuelve por un conjunto de mecanismos compuesto por reglas de filtrado en los

ruteadores, listas de control de accesos, firewall (paredes de fuego) y mecanismos de encriptar por equipo (hardward) las claves de seguridad e identificación personal de los usuarios y los algoritmos de encriptación. La comunicación que se establezca entre el contribuyente y el servidor estará encriptada en tiempo real. Las claves de seguridad e identificación personal se resguardan en un equipo con estrictas medidas de seguridad física y lógica. Ante cualquier violación, mecanismos de seguridad lógicos deberán impedir la recuperación de los datos allí almacenado.

Registro electoral y las fichas de los partidos políticos

El padrón electoral es una típica base de datos con información elemental para autorizar la emisión del voto en los sufragios de elección de representantes y autoridades. Estos datos son de público conocimiento en tiempos preelectorales, mientras que se mantiene en reserva en otros tiempos.

El carácter de este archivo impide considerar al hábeas data como vía procesal idónea para acceder y solicitar algunas de las pretensiones establecidas en el artículo 43, toda vez que las correcciones que se debieran hacer por actualizaciones o rectificación deben tramitar ante la justicia electoral.

Es diferente la situación de los padrones de afiliados a partidos políticos. Una ficha de afiliación partidaria suele requerir datos históricos de la persona, quizás el más importante; estos datos deben pretejerse ya que la persona no pretende hacer manifestaciones a terceros a cerca de su afiliación a un partido político.

3.2.2.1. Medidas de Seguridad.

Seguridad técnica

La seguridad técnica, evidentemente, cambia y se transforma constantemente, al punto que no es posible sentar reglas sobre tal o cual mecanismo para certificar el cumplimiento de la regla.

No obstante existen algunas guías: "las protecciones han de ser físicas y lógicas (entre estas ultimas están los paquetes de control de accesos) y existir una separación de entornos y una segregación de funciones, además de una

clasificación de la información; y deben existir los medios para garantizar su eficiencia: asignación de responsables de los ficheros, administración de la seguridad, auditoria informática interna y posible contratación de la externa."

En materia informática la seguridad técnica supone la integración de elementos externos al equipamiento (hardware y software) para que los controlen y aseguren de riesgos normales y anormales. Básicamente se refiere a instalaciones donde funciona el archivo, censores infrarrojos, blindajes, cámaras de televisión, contraseñas, seguros de riesgo, etcétera.

Seguridad lógica

Se vincula con la intromisión que pueda sufrir una base de datos, sea desde otras terminales (locales o remotas), y las acciones que se pueden intentar para evitarlo.

En definitiva son medidas organizacionales que deben adoptarse frente a la debilidad de los sistemas para contrarrestar las interferencias en la información.

Como en el caso anterior son múltiples las posibilidades de protección, las medidas más frecuentes tienen en común los pasos que orienta el llamado "libro naranja" del Departamento de Defensa de los Estados Unidos de América, del que se toman diez procesos:

a) Control de acceso: permite que solo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.

b) Medios de almacenamiento: se debe chequear la integridad de los datos antes de almacenarlos para ver que no se destruye alguna información existente.

c) Control de memoria: verificar que no se accedan a posiciones de la memoria en donde no esta permitido, ya que puede haber información que no se deba acceder.

d) Control de usuario: se decide que permisos posee cada usuario y que es lo que puede hacer.

e) Control de acceso especifico: existen algunos usuarios que tienen permisos específicos, como por ejemplo el administrador tiene acceso total a todo.

f) Control de comunicación: se deben especificar claramente que datos son los que se pueden comunicar a los interesados en obtener información del sistema en cuestión.

g) Control de transferencias: se debe proteger cuando se deben transferir de un organismo a otro. Una de las formas que se utilizan para esta función puede ser la utilización de Internet; con lo que se deben extremar las medidas de seguridad para proteger la privacidad de los datos. Se deben utilizar mecanismos que posean los tres componentes siguientes:

   - Una información secreta, como claves y contraseñas, conocida por las entidades participantes.
   - Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
   - Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quien envía qué a quién y cuándo.

h) Control de organización: se refiere a los mecanismos de control y auditorias que el organismo debe realizar para verificar que se esta cumpliendo la protección y resguardo de los datos.

Un mecanismo lógico de protección es el "encriptado" que asegura un sistema de filtración al que solo pueden llegar quienes tienen permitida la entrada (lo cual se consigue a través de la firma digital o de claves de identificación).

Criptografía simétrica

La criptografía simétrica o de llave secreta: consiste en una clave compartida por dos entidades, una transmisora y otra receptora, que sólo es conocida por ellas. Se dice que el sistema es simétrico porque requiere de un proceso de especificación de la clave.

Existen varios métodos Criptografía simétrica, entre ellos encontramos:

- Sustitución: Es el sistema más básico. La clave consiste en una tabla de equivalencias de caracteres.
- Permutación: consiste en alterar el orden de las letras siguiendo una regla determinada. Normalmente se utiliza una tabla de tamaño determinado en la que se inserta el texto original que es transformado mediante la sustitución de las columnas por las filas.
- Esteganografia: es un caso especial de confusión intercalada. Consiste simplemente en camuflar el texto intercalándolo dentro de otro mensaje. Podemos elaborar un mensaje de contenido irrelevante pero de forma que siguiendo cierta pauta de eliminación podamos reconstruir el texto original.
- Mixtos: consiste en alguna combinación de los anteriores.

Criptografía Asimétrica

La criptografía asimétrica o de llave pública o asimétricas: en la cual se usan dos claves (sistema binario), una pública que, como su nombre lo indica, es de público conocimiento, y otra privada, la cual no es revelada ni transmitida a persona diferente a la cual la misma pertenece. En este sistema asimétricos la clave pública se usa para cifrar el mensaje y la privada para descifrarlo. Este tipo de criptografía es el utilizado en firma digital.

Gestión del sistema de seguridad

Los sistemas de seguridad requieren de un sistema de gestion, el cual debe comprender dos campos bien amplios e importante:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que solo pueda ser accedida por aquellas entidades autorizadas.

- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

Protección de datos en Internet

Actualmente las entidades que posean informaciones personales, utilizan Internet como una herramienta para brindarle información al usuario, ya sea para brindarle un servicio de E-mail, presentación de declaraciones juradas, solicitud de información, el intercambio de datos entre entidades, entre otras. Por ello se deben prever unas estrictas medidas de seguridad y proveer la defensa de la privacidad ante la agresión de terceros.

El usuario de Internet podrá reclamar un código de conducta, donde sus derechos respeten, al menos las siguientes consignas:

- Ser informado de la identidad y la ubicación de las organizaciones que ofrecen comercio electrónico y validar estos datos
- Recibir la formación adecuada sobre sus derechos en el ciberespacio.
- Con sus datos personales el individuo podrá:
  - Disfrutar de la oportunidad y la habitualidad individual para navegar y efectuar las operaciones comerciales en el anonimato.
  - Ser informado desde el comienzo sobre la finalidad y las posteriores utilizaciones y divulgaciones de los datos personales recopilados por los usuarios de éstos.
  - Exigir que la información personal recogida sea exacta y se almacene en condiciones de seguridad.
  - Tener derecho de acceso y de corregir los datos inexactos.
  - Optar por la exclusión voluntaria (Opt out).
  - Solicitar que los datos almacenados de niños se sometan a la autorización y control de los padres.

Seguridad organizada por vía reglamentaria

El convenio 108 del CE ha resuelto que se tomen medidas de seguridad adecuadas para la protección de datos personales con el fin de evitar inconvenientes derivados de la destrucción, perdida accidental o provocada, así como para eliminaren el mayor grado de certeza posible la intromisión de archivos y la difusión no autorizada.

En la exposición de Motivos se confírmale sentido de las medidas al exponerlas en relación con las funciones que se deben asegurar: a)la vulnerabilidad de los datos (por eso los datos sensibles exigen medidas de prevención más estrictas); b) la necesidad de que el acceso sea restringido; c)que el archivo o la recolección de los datos tenga en cuenta el tiempo que permanecerá disponible el dato; d) los riesgos propios de cada archivo; e) la finalidad prevista

En países donde el tema esta en ciernes existe un vacío legislativo evidente que puede permitir interferir las bases de datos sin que la acción tenga prevista una consecuencia punible. Por eso buena parte de las leyes que se proyectan se basan en crear organismos centralizados para resolver la complejidad del problema y orientar con medidas las acciones a concretar.

La imposibilidad de generar por vía normativa una consigna sobre medios y acciones técnicas y lógicas que resuelvan la seguridad de los archivos con datos personales ha sugerido el establecimiento de niveles para identificar donde ha de asentarse la mayor preocupación.

En tal sentido se establecen escalas de riesgo:

1. Nivel básico: orienta a que el responsable del archivo tenga un manual de instrucciones de conocimientos obligatorio para todas las personas que actúan bajo su dependencia y, sobre todo, de aquellos que tienen la tarea de incorporar datos y procesarlos a los fines que el registro ha previsto. Este documento debe contener, como mínimo, el ámbito de aplicación y los recursos protegidos; las medidas, normas procedimientos y estándares aplicados; las funcionalidades y obligaciones del personal; la estructura de los

archivos o bancos de datos con la descripción de los sistemas de información que los tratan; los procedimientos de notificación, gestión y respuesta ante las eventuales incidencias; procedimientos previstos para la actualización permanente del manual, entre otras. En este nivel es obligatorio que exista una relación de personas que tengan derecho al acceso, y establecer procedimientos de identificación y autenticación para dicho acceso. Es en otros términos, el método de identificación del usuario.

2. Nivel medio: en este nivel la actividad de simple colección de datos agrega el aditamento del tipo de archivo creado y, por ello, la mayor intensidad en los sistemas de seguridad. Hablamos de registros sobre infracciones administrativas, penales, crédito, situación patrimonial, servicios financieros, etcétera, en los cuales, además de cumplir las medidas señaladas anteriormente para el nivel básico, deben tener un responsable de seguridad, encargado de control directo y auditoria permanente del sistema. La identificación del usuario es más exigente agregándose a la autenticación el recaudo de operar en lugares cerrados donde el acceso sea restringido.
3. Nivel alto: es el nivel destinado para el tratamiento de datos sensibles. La directiva 94/95 CE, en el articulo 8(tratamiento de categorías especiales de datos) dice: "Los estados miembros prohibirán el tratamiento de datos personales que releven el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad". Las medidas se extreman, así como las responsabilidades por su violación son superiores. El establecimiento de prevenciones ha de ser permanente y las infracciones penadas y multadas. El segundo problema es la protección directa sobre los datos personales que se han colectado para el archivo.

El nivel de seguridad difiere en los de fácil acceso respecto a los denominados sensibles.

En unos (por el caso, nombre y apellido, domicilio, teléfonos, identificación, estado civil) la simplicidad del acceso y la multiplicación de lugares de búsqueda impiden sentar reglas demasiadas estrictas.

En otros datos mas privados y personales(o personalísimos, como la ideología, enfermedades, hábitos sexuales, etc) se reserva un tratamiento más severo requiriendo un alto nivel de seguridad para impedir el acceso a ellos.

Obligaciones del archivo

Una de las cuestiones a esclarecer de inmediato consiste en saber quien debe responder por el cumplimiento de los principios establecidos y asumir las consecuencias derivadas.

Algunos autores dicen que hay que averiguar si la responsabilidad por incumplimientos debe recaer exclusivamente sobre el titular del archivo, o si debe ser compartida entre las personas involucradas en la recogida, procesamiento o transmisión de datos personales.

En todo caso la situación tiene que establecer la diferencia entre:

a) Administrador del archivo: es el verdadero responsable porque tiene el control y el poder de decisión. También se denomina *usuario,* cuando la persona – publica o privada- realiza a su arbitrario el tratamiento de datos o a través de conexión con los mismos.

b) Persona encargada del tratamiento: es la persona física o jurídica, autoridad publica, servicio o cualquier otro organismo que, solo o juntamente con otros, trata datos personales por cuenta del responsable del tratamiento. En otros términos, es el operador de las bases, quien esta obligado por el código de confidencialidad que debe tener el lugar donde trabaja.

c) Característica del servicio: obedece a la característica pública o privada del banco de datos. Los archivos públicos se rigen por responsabilidades propias, los privados están sujetos a la ley que autoriza su funcionamiento y al órgano de fiscalización respectivo.

d) Interconexión de los datos: generalmente es realizado por terceras personas contratadas para ello.

El articulo 10 (deber de confidencialidad) establece que:

> *"1. Es 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 su relación con el titular del archivo de datos"*
>
> *"2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad publica, la defensa nacional o a la salud publica"*

Esta situación merece ser considerada en la doble dimensión que supone. Por un lado el deber del archivo, registro o banco de datos para dar estricto cumplimiento con los principios y deberes a que se encuentra obligado, y por otro las sanciones civiles (resarcitorias) y penales (represiones) que la violación determine.

En adelante, quien se considere dañado por la información personal almacenada, deberá probar el perjuicio y la gravedad de los daños para obtener una indemnización.

3.2.3. El Proceso de Comunicación.

Concepto de comunicación: el Diccionario de la Lengua de la Real Academia Española, en relación a lo que aquí nos interesa, define a la "comunicación" como "*trato, correspondencia entre dos o más persona*"; "*transmisión de señales mediante un código común al emisor y al receptor*". Por su parte el vocablo "comunicar" indica "*hace a otro partícipe de lo que uno tiene*", "*descubrir, manifestar o hacer saber a alguien alguna cosa*"; "*conversar, tratar con alguien de palabra o por escrito*".

Los autores Ricci Bitti y Bruna definen a la comunicación como "*el proceso que consiste en transmitir y hacer circular informaciones; o sea un conjunto de datos, todos o en parte desconocidos por el receptor antes del acto de la comunicación*".

La principal finalidad de la comunicación es convertirse en un estímulo de conocimiento.

En síntesis, la idea de comunicación hace referencia a un complejo proceso que se establece entre las personas y que implica transmisión y aprehensión de una información determinada.

La raíz etimológica del vocablo confirma lo antes dicho, comunicación provienen del término latino "communico – are". Ambos tienen la misma raíz: *"communis"* (común), que hace inequívoca referencia la concepto de algo compartido, de comunidad, de participación, de comunión. La comunicación es, precisamente, eso: un acercamiento entre personas.

Elementos de la comunicación

a) Los sujetos: son el emisor y el receptor. Se trata de dos roles bien diferenciados, independientemente de quiénes sean el o los sujetos que asumen cada función. Por un lado un experto, un entendido, alguien que conoced todas y cada una de las circunstancias que rodean a la materia de que se trata; por el otro, integrará esta relación aquel que busca al primero que busca precisamente por carecer de los conocimientos que este tiene y para la satisfacción de alguna necesidad (la provisión de una cosa o la prestación de algún servicio). El primero es el "profesional del contrato" y el segundo el "profano". En conclusión, es el conocimiento sobre un objeto determinado que el otro polo de la relación no posee, lo que confiere al "profesional" el carácter de tal.

b) El mensaje: es la información que se transmite en el acto comunicacional. Es el "contenido conceptual" que también se denomina "información" en sentido amplio. Podemos distinguir, a grandes rasgos, dos componentes del mensaje: por una parte aquellos contenidos conceptuales que ya se encuentran incorporados en el receptor (a veces denominados "redundantes"), y por otro lado los nuevos contenidos que constituyen lo que, en sentido estricto, se

denomina "información", que "no es otra cosa que la medida de originalidad de un mensaje".

c) El código: es el "lenguaje" (verbal o gestual) en el que el contenido conceptual (mensaje) es traducido a fin de poder ser transmitido al receptor de la información. En otras palabras, es el "sistema de referencia con base en el cual se produce el mensaje". El código impacta en la raíz de la información; la determina y hace posible su transmisión. Existen multiplicidad de códigos. Cualquiera de ellos puede ser usado para transmitir la misma información. La adecuada elección del código se produce a partir de una valoración de las circunstancias relativas a lo demás elementos de la comunicación y al contexto que la rodea. Sólo así el éxito del acto comunicativo podrá estar asegurado.

d) El canal: el tema del canal ha provocado grandes desencuentros en la doctrina científica. Puede definirse como "ese medio físico-ambiental que hace posible la transmisión de una información o de un mensaje". En sentido coincidente se ha dicho que "...es todo soporte material que vehicula un mensaje desde un emisor a un receptor a través del espacio y del tiempo". En consecuencia, el concepto de canal debe entenderse de la siguiente manera: *es todo soporte material de la información.*

e) El contexto: cada proceso de comunicación; integrado por un conjunto de actos comunicativos se realiza en una situación de terminada. Muchas son las circunstancias de personas, tiempo, espacio, tecnología y lugar que la rodean. El contexto condiciona inevitablemente a la comunicación. Es el "entorno físico o de situación -político, histórico, cultural o de cualquier otra índole- en el cual se considera un hecho". El contexto no es un elemento "estructural" de la comunicación. Más bien constituye un elemento "externo" que inevitablemente está presente, aunque "desde fuera" del acto comunicativo. Es, por decirlo de alguna manera, el "medio" en el cual la información se gesta y se transmite entre los sujetos. El contexto puede presentar diversas formas. Entre otras, edad, sexo, salud, religión, raza, nivel educativo, nivel

socioeconómico, profesional y cultural del emisor y del receptor. También los adelantos técnicos con los que cuenten estos sujetos, a la hora incluso de poder seleccionar un canal, tienen una influencia decisiva. En lo estrictamente "externo", las circunstancias políticas, sociales, históricas, culturales y económicas del medio en el cual se desarrolla el acto comunicativo constituyen su escenario, y son determinantes.

3.2.4. Procedimiento de Consulta.

El derecho a la vista o consulta de la información y las actuaciones administrativas constituye a partir de la reforma constitucional de 1994 una categoría de los derechos fundamentales o derechos humanos constitucionales por aplicación de los principios y derechos a la tutela judicial efectiva y a la información establecidos en los distintos pactos incorporados con raigambre constitucional por aplicación del derecho de integración.

Estos derechos forman parte del nuevo bien común internacional, que se refleja en los instrumentos supranacionales ya señalados, que tornan operativo lo dispuesto en el artículo 14 de la Constitución Nacional sobre el derecho a peticionar. En tal sentido así lo expresa la Declaración Americana de los Derechos y deberes del Hombre en su artículo XXIV cuando establece: "toda persona tiene derecho a peticionar peticiones respetuosas a cualquier autoridad competente, ya sea por motivo de interés general, ya por interés particular, y el de obtener pronta resolución". -

Como consecuencia de este nuevo bien común internacional, vemos entonces en el derecho nacional e internacional disposiciones tendientes a asegurar la garantía contemplada por el Derecho a la Información. Por ejemplo, **la Asamblea del Concejo de Europa** en el año 1979 por la recomendación N° 854 invitó a sus estados miembros, a introducir un sistema de libertad de información que permita reconocer el derecho subjetivo de acceso a los documentos de la administración pública. **En el derecho argentino**, existen antecedentes del derecho público

provincial, como ser el de la provincia de Chubut que en 1992 dictó su ley 3764 en esta materia y el más reciente de la Ciudad Autónoma de Buenos Aires con el dictado de la ley 104 en el año 1998.

Este proceso legal avanza día a día reflejándose en la promulgación de nuevas leyes y reglamentaciones que tienen como fin normar y regular el aspecto operativo del Derecho a la Información, de manera de encontrar un justo equilibrio entre los derechos de los particulares y las obligaciones del Estado, salvaguardando los aspectos de seguridad mínimos que esta nueva institución debe respetar y proteger.

En la actualidad, no es posible considerar constitucional ninguna limitación al derecho de acceso a la información y su toma de conocimiento. Por lo tanto, toda disposición o actitud que niega ese derecho a cualquier persona física o jurídica, no sólo es inconstitucional sino que genera responsabilidades por incumplimiento de los mandatos relacionados.

Como consecuencia de ello es que pesa sobre el Estado y sus funcionarios la obligación de definir un Procedimiento de Consulta de Información que:

- asegure y garantice el derecho de acceso a la misma por todos los ciudadanos
- cumpla con los controles y límites establecidos legalmente para salvaguardar la intimidad del titular de los datos y al mismo tiempo los intereses de la Nación, cuando corresponda
- establezca sanciones en caso de incumplimiento a lo dispuesto por las normas vigentes.

En consonancia, la **ley nacional N° 1556 del Empleado Público** establece en sus artículos N° 40 y 43 las obligaciones de los empleados de la administración pública frente a los demás agentes de la Administración Pública y el público administrado; y sus correlativas sanciones ante los eventuales incumplimientos; y la **ley de Derecho a la Información de la Provincia de Santa Fé** establece en su artículo 7: "Todos los funcionarios públicos y/o agentes responsables de los tres poderes del Estado,

están obligados a facilitar el acceso a la libre información. Caso contrario su conducta será considerada arbitraria, siendo directamente responsable por falta grave en ejercicio de sus funciones y sujeto pasible de las sanciones que se establezcan reglamentariamente"

3.2.4.1. Organización de la Información.

Como consecuencia directa de los derechos que la Constitución Nacional reconoce a los usuarios y consumidores de bienes y servicios en su artículo 42, en especial el mencionado Derecho a la Información, que comprende en sí mismo el derecho a una información adecuada, veraz y en condiciones de trato equitativo y digno; se hace necesario analizar y definir las condiciones óptimas de organización de la información existente en poder del Estado y del Sector Privado y la administración de la misma.

Pues, es deber del titular del Registro no sólo asegurar el acceso a la información por quienes estén legitimados o autorizados para hacerlo sino también mantener la confidencialidad y secreto de la información que almacena, debiendo cederla únicamente en los supuestos expresamente autorizados. Por ello, toda base de datos debe ser segura y secreta, debiendo protegerse la información y evitando por los medios que fueran necesarios toda invasión o penetración ilegítima.

Tanto la organización de la información como las medidas de seguridad a implementarse y el acceso por parte del ciudadano deben contemplar las diferentes herramientas de archivado, modificación y consulta de acuerdo al medio de almacenamiento utilizado, a saber: información contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, discos ópticos, microfilmes, películas, o en cualquier formato y que haya sido creada u obtenida por el órgano requerido que se encuentre en su posesión y bajo su control.

Si bien es cierto que la existencia de Registros (públicos y privados) no es nueva sino que se evidencia desde siempre; el avance tecnológico de las últimas décadas implica la administración de un volumen mayor de información como también la

posibilidad de acceso y transmisión de la misma por medios más rápidos y menos evidentes que, de no contarse con una administración segura en los aspectos lógicos y técnicos, es difícil sino imposible poder controlar. En este aspecto, se hace necesario que todo archivo o institución que administre información relativa a las personas tenga en cuenta que en su día a día debe contemplar dos reglas esenciales:

- la protección de los derechos de las personas
- las obligaciones del archivo

En este sentido, la ley sobre el Derecho al Libre Acceso a la Información Ambiental de la ciudad de Buenos Aires establece en su artículo 5 "Las entidades públicas y privadas comprendidas en el artículo 2 tienen las siguientes obligaciones

a) Prever una adecuada organización y sistematización de la información que se genere en las áreas a su cargo, de conformidad con el procedimiento que establezca la reglamentación de la presente ley;

b) Facilitar el acceso directo y personal a la información que se les requiera por esta ley y que se encuentre en la órbita de su competencia y/o tramitación, sin perjuicio de adoptar las medidas necesarias para evitar el entorpecimiento del normal desarrollo y funcionamiento de sus actividades..."

En paralelo, en el sector privado se han definido y establecido códigos éticos o de conducta en cumplimiento de lo requerido a este tipo de archivos por la ley nacional 25.326.

Consideramos que tanto en el sector público como privado y ya sea mediante códigos éticos o de conducta o bien a través de la normativa dictada o a dictarse en cada provincia; en lo referente a la organización de la información y su administración, deben contemplarse los siguientes aspectos:

- Definición precisa del objeto de los servicios a prestar, dirigidos en el caso de Empresas de Información Comercial a procurar la transparencia de la información comercial, crediticia y patrimonial, mediante la provisión de información destinada a prevenir el fraude y fomentar el crédito, facilitando la concertación de negocios en general.
- Obligación de garantizar al Titular del Dato su derecho a conocer la información que sobre su persona conste en los Bancos de Datos, detallando incluso quienes tuvieron acceso a su información. A tal fin, deberá verificarse adecuadamente la identidad del peticionante
- Compromiso de preservar el buen uso de la información
- Asegurar igualdad de oportunidades y respeto en el trato, procurando asistencia, colaboración y solidaridad.
- Compromiso a trabajar en pos de la erradicación de prácticas reñidas con la ética y/o que violen el marco regulatorio vigente.
- Compromiso de adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y la confidencialidad de los datos almacenados, respetando y haciendo respetar el deber de confidencialidad respecto de la información tratada.
- Compromiso a realizar controles periódicos tendientes a detectar los desvíos que puedan haberse presentado respecto a los puntos detallados.

Se hace imprescindible la coexistencia de la totalidad de los aspectos mencionados precedentemente ya que no alcanza con cumplir sólo con la toma de medidas de seguridad técnica, las cuales han sido desarrolladas con mayor amplitud en el punto 3.2 del presente informe o con una normativa interna o legal; ya que deben complementarse necesariamente ambos aspectos si se quiere garantizar de manera plena el derecho de acceso a la información y el cumplimiento de las obligaciones que pesan sobre quien posee los datos.

Así, por ejemplo, en materia judicial se han definido las **Reglas de Heredia** que establecen las reglas mínimas que deben cumplirse para la difusión de información judicial en Internet, a saber:

Regla 1. La finalidad de la difusión en Internet de las sentencias y resoluciones judiciales será:

a - El conocimiento de la información jurisprudencial y la garantía de igualdad ante la ley

b - Para procurar alcanzar la transparencia de la administración de justicia.

Regla 2. La finalidad de la difusión en Internet de la información procesal será garantizar el inmediato acceso de las partes o quienes tengan un interés legitimo en la causa, a sus movimientos, citaciones o notificaciones.

Regla 4. En cada caso los motores de búsqueda se ajustarán al alcance y finalidades con que se difunde la información judicial.

Regla 5. Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; o víctimas de violencia sexual o doméstica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales.

En este caso se considera conveniente que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o inicializados, salvo que el interesado expresamente lo solicite y ello sea pertinente de acuerdo a la legislación.

Regla 7. En todos los demás casos se buscará un equilibro que garantice ambos derechos. Este equilibrio podrá instrumentarse:

a - en las bases de datos de sentencias, utilizando motores de búsqueda capaces de ignorar nombres y datos personales;

b - en las bases de datos de información procesal, utilizando como criterio de búsqueda e identificación el número único del caso.

Se evitará presentar esta información en forma de listas ordenadas por otro criterio que no sea el número de identificación del proceso o la resolución, o bien por un descriptor temático.

Cabe aclarar que estar reglas son recomendaciones que se limitan a la difusión en Internet o en cualquier otro formato electrónico de sentencias e información procesal y que no alcanzan al acceso de documentos en las oficinas judiciales ni a las ediciones en papel.

Al mismo tiempo, son reglas mínimas que no obstan a que los organismos o entidades involucrados utilicen procedimientos de protección que contemplen una mayor rigurosidad.

3.2.4.2. Definición y Regulación del Procedimiento.

El pleno derecho de acceso a la información debe implicar la posibilidad cierta para que cualquier persona, en función de un interés personal o general, lleve adelante investigaciones efectivas y pueda ejercer las debidas acciones, y el efectivo ejercicio del derecho de defensa social.

Una ley, decreto o procedimiento interno destinado a regular el acceso a la información debe partir de establecer cuestiones básicas que garanticen los derechos y obligaciones que hemos venido desarrollando, a saber:

- **Legitimación activa:** debe reconocerse la posibilidad de ejercicio del derecho de acceso a la información a todo ciudadano.
- **Tipo de Información**: debe definir de manera clara el tipo de información que el sector público y privado tienen obligación de brindar. La regla general debe ser la de acceso a toda la información que las entidades de dichos sectores

almacenen y tengan en su poder; con excepciones expresamente establecidas y que estén definidas de manera taxativa. Al mismo tiempo, estos criterios a aplicar deben ser los mismos cualquiera sea el medio de almacenamiento de la información, sin distinción del uso o no de tecnologías; es decir que alcanza todos los formatos en que la información puede ser administrada.

- **Acceso:** a fin de dar igualdad de trato a todos los ciudadanos y de asegurar el acceso por todos, el principio que debe regir para el acceso es el de gratuidad. El acceso debe ser gratuito en tanto no se requiera la reproducción de la información. Si hubiera costos de reproducción, en principio, éstos deberían ser a cargo del solicitante.
- **Plazos de Respuesta:** en la medida de lo posible, los plazos de respuesta a los requerimientos de información deben ser breves, a los fines de asegurar el cumplimiento del objetivo perseguido por el interesado y de esta manera garantizar el pleno ejercicio de sus derechos.

Consecuentemente, los organismos y entidades destinadas al almacenamiento y transmisión de la información, deben asegurar a los ciudadanos que las perspectivas que ha abierto la tecnología van siendo desarrolladas conforme lo requiere el conjunto de los ciudadanos y en beneficio de ellos, y que los derechos que, también les deben ser reconocidos, son efectivizados y se encuentran suficientemente protegidos.

De ello surge que deben establecerse obligaciones que recaigan de manera directa sobre quienes usan, manipulan, almacenan y transmiten los datos. A manera de ejemplo enumeramos las siguientes:

a - Obligación de asegurar que la información que administran cumple con los requisitos legales establecidos;

b - Obligación de verificar periódicamente la actualización y realidad de los datos;

c - Obligación de velar por que las informaciones sean corregidas o suprimidas según la voluntad del individuo y que se guarden solamente por el período establecido para ello;

d - Obligación de seguridad, en cuanto a que el acceso de terceros no controlados sea adecuado a los contenidos almacenados, transferidos o manipulados;

e - Obligación de controlar que la información sea mostrada exclusivamente a las personas identificadas y nunca a personas cuya identidad no haya podido ser constatada fehacientemente;

f - Obligación de aceptar toda responsabilidad, incluso penal, que se hayan establecido por la publicación de las informaciones que forman parte del registro o base de datos.

Así, el Registro Nacional de la Propiedad Inmueble en el artículo 21 de la ley 17.801 establece que "El registro es público para el que tenga interés legítimo en averiguar el estado jurídico de los bienes, documentos, limitaciones o interdicciones inscriptas..." y el Decreto 2080/80, dispone en su artículo 60 que, a los efectos del artículo 21 de la ley 17.801, "Se presume que tienen interés legítimo, en conocer los asientos registrales, además de sus titulares:

a) Los organismos del Estado Nacional, provincial y de las municipalidades;

b) El Poder Judicial de la Nación y de las provincias;

c) Los que ejerzan las profesiones de abogado, escribano, procurador, ingeniero o agrimensor;

d) Los martilleros públicos, los gestores de asuntos judiciales y administrativos reconocidos como tales ante el Registro, y las personas debidamente autorizadas por los profesionales mencionados en el inciso anterior".

3.2.4.2.1. Limitaciones al Derecho de Acceso a la Información.

Si bien hemos dicho que el principio que debe regir en el tema que estamos desarrollando es el de acceso a TODA la información, existen casos particulares que, por el interés que representan o el bien jurídico que puede verse afectado, deben ser excluidos de este principio y la normativa o reglamentación a dictarse debe garantizar su confidencialidad.

Sin embargo, si se quiere evitar que la excepción se convierta en regla y que ante la menor duda se opte por no brindar la información y de esta manera se lesione el derecho constitucional de acceso a la misma, debe establecerse de manera taxativa cuáles son los casos en que dicha información no debe brindarse. En general, los motivos de estas excepciones se relacionan con cuestiones de seguridad pública, los usos comerciales honestos y la protección de los derechos a la privacidad y a la intimidad de las personas.

Existen en la actualidad diversas leyes que contemplan estas excepciones de manera expresa y taxativa, inclusive la ley nacional 25.623 define las mismas de manera genérica.

Hemos optado por detallar lo establecido en la **ley 24.766 de Confidencialidad sobre Información y Productos que estén Legítimamente bajo control de una Persona y se divulgue indebidamente de manera contraria a los Usos Comerciales Honestos**, por ser una ley específica y detallada al respecto. Así, dejando de lado lo particular del tipo de producto y procedimiento que regula, la ley mencionada establece lo siguiente:

Artículo 1 - Las personas físicas o jurídicas podrán impedir que la información que está legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honesto, mientras dicha información reúna las siguientes condiciones:

a) Sea secreta en el sentido que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y

b) Tenga un valor comercial por ser secreta; y

c) Haya sido objeto de medidas razonables para mantenerla secreta, tomadas por la persona que legítimamente la controla. Se considerará que es contrario a los usos comerciales honestos el incumplimiento de contratos, el abuso de confianza, la instigación a la infracción y adquisición de información no divulgada por terceros que supieran o no, por negligencia grave, que la adquisición implicaba tales practicas.

Artículo 3 - Toda persona que con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a una información que reúna las condiciones enumeradas en el artículo 1 y sobre cuya confidencialidad se los haya prevenido, deberá abstenerse de usarla y de revelarla sin causa justificada o sin consentimiento de la persona que guarda dicha información o de su usuario autorizado

Artículo 9 -... no estará protegida la información que hubiera caído en el dominio público en cualquier país, por la publicación de cualquiera de los datos protegidos, la presentación de todos o partes de los mismos en medios científicos o académicos, o por cualquier otro medio de divulgación.

Artículo 10 - Quedará exceptuado de la protección, la información cuya publicación sea necesaria para proteger al público o cuando se adopten medidas para garantizar la protección de dicha información contra todo uso comercial deshonesto.

Artículo 11 -... El acceso por terceros a la información de manera contraria a los usos comerciales honestos, dará derecho a quien la posea a ejercer las siguientes acciones:

a) Solicitar medidas cautelares destinadas a hacer cesar las conductas ilícitas.

b) Ejercer acciones civiles destinadas a prohibir el uso de la información no divulgada y obtener la reparación económica del perjuicio sufrido.

3.2.4.2.2. Responsabilidades.

De acuerdo a lo establecido en la Ley 25.326, las empresas y organizaciones son responsables de la seguridad y confidencialidad de los datos personales que manejan; ya que pesan sobre ellas el deber del "secreto profesional".

No debemos olvidar que el tratamiento de datos personales involucra a varias personas, de modo tal que podría afirmarse que la responsabilidad se comparte en la medida de la culpa. La distribución del deber puede dividirse entonces en tres categorías de responsabilidades:

a - La Responsabilidad del titular del archivo, que debe cumplir con los deberes y obligaciones que le incumben en su rol y que han sido desarrollados a lo largo del Primer Informe de este trabajo.

b – La Responsabilidad derivada del poder de vigilancia, individualizada en la persona o personas que tienen a su cargo el cumplimiento del deber de seguridad (secreto y confidencialidad de los datos)

c – La Responsabilidad del usuario, que es la persona autorizada por el titular del archivo para la utilización de determinados datos personales.

En la práctica hay que diferenciar los archivos públicos de los privados, ya que rigen principios diferentes en materia de responsabilidad según se trate de uno o de otro.

En el caso de los **Registros Públicos**, la responsabilidad se rige por las normas sustanciales que aplican consecuencias jurídicas a la actividad lícita o ilícita del Estado. No interesa si la conducta del empleado público es la causa generadora de la intromisión, la culpa es del Estado como responsable directo. Ello sin perjuicio de las sanciones administrativas que se establezcan internamente y de la responsabilidad penal que pueda caer sobre el agente de la administración que haya incurrido en la falta.

En el caso de los **Registros Privados**, quien trabaja en bancos de información suscribe un acuerdo de confidencialidad que lo hace responsable por su violación.

Frente al afectado, las leyes de tratamiento de datos pretenden no distribuir la responsabilidad entre operadores y directores del registro, prefiriendo establecer la solidaridad a partir del amplio criterio que tiene el enunciar al "responsable del fichero". Ello, también sin perjuicio de las sanciones administrativas internas que puedan corresponder a quien violó el deber de confidencialidad.

Cabe aclarar, que las sanciones y responsabilidades establecidas tanto normativamente como a nivel de procedimientos internos no sólo contemplan el caso de violación al deber de confidencialidad sino también aquellos casos en que el funcionario, agente o empleado se niega a brindar la información o el acceso a la misma de manera infundada y contrariando lo establecido.

Así, el **Decreto 929/00 de la Provincia de Misiones** establece en su artículo 25 "El funcionario público o agente responsable que en forma arbitraria obstruya el acceso del solicitante a la información requerida, o la suministre en forma incompleta u obstaculice de cualquier modo el cumplimiento del presente decreto, faltará a los deberes impuestos a los empleados públicos por la Ley N° 1.556" y en su artículo 26 "El funcionario público o agente, que faltare a los deberes establecidos en el artículo anterior, será pasible de las sanciones de apercibimiento, o de suspensión de hasta treinta días o cesantía conforme lo establece el artículo 43 de la Ley N° 1.556"

La **Ley nacional 25.326** procede a incorporar al Código Penal el artículo 157 bis, reprimiendo con prisión de un mes a dos años a quien revele datos secretos, elevando al doble el mínimo y el máximo de la pena cuando se trate de funcionario público.

Y la Ley 3794 establece el Deber de facilitar el libre acceso de la información en su artículo 3 "Todo funcionario público de cualquiera de los poderes del Estado Provincial y de las Corporaciones Municipales, deberá facilitar el acceso personal y directo a la documentación y antecedentes que se le requieran y que estén bajo su jurisdicción y/o tramitación, ello sin perjuicio que se arbitren las medidas necesarias para evitar el entorpecimiento al normal desarrollo y funcionamiento de los servicios y actividades que ejecute el Órgano al que se le formule el requerimiento" y la Responsabilidad del funcionario en caso de Incumplimiento en su artículo 6 "Los

funcionarios públicos y/o agentes responsables de los tres poderes del Estado Provincial y de las Corporaciones Municipales, que en forma arbitraria e infundada no facilitaren el acceso del particular a la información solicitada o la suministrare en forma incompleta u obstaculizare el cumplimiento de los objetivos de esta Ley, será considerado como incurso en grave falta de sus deberes y será pasible de las sanciones que por vía reglamentaria se fijen y que serán adoptadas por la jurisdicción en la que revistare el responsable.

3.2.4.2.3. Procedimiento.

OBJETIVO:

El objeto del presente procedimiento es definir y regular los derechos y obligaciones del ciudadano y del Estado en lo referido a la consulta y administración de la información contenida en sus distintos órganos.

ALCANCE:

El presente alcanza a todo archivo público como también a cualquier órgano perteneciente a la administración central, descentralizada, de entes autárquicos, empresas y sociedades del Estado, sociedades anónimas con participación estatal mayoritaria, sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el Estado tenga participación en el capital o en la formación de las decisiones societarias.

DERECHOS Y OBLIGACIONES:

Los usuarios y beneficiarios de servicios del Estado y todo ciudadano en general, deben contar con la posibilidad de tener un efectivo acceso a la información en las condiciones que establecen el presente procedimiento y la normativa vigente.

Toda persona tiene derecho a solicitar y recibir información completa, veraz, adecuada y oportuna de cualquier órgano perteneciente a la administración central y

descentralizada de los poderes del Estado, sin que sea necesario acreditar derechos subjetivos, interés legítimo o las razones que motivan el requerimiento.

Frente a la Administración Pública el ciudadano goza de los siguientes derechos:

- DERECHO a acceder a los archivos y registros públicos con las limitaciones legalmente establecidas.

- DERECHO a conocer el estado de tramitación de las actuaciones administrativas en las que tenga la condición de interesado y a obtener copias de los documentos contenidos en ellas.

- DERECHO a identificar las autoridades y personal que tramitan los procedimientos y a responsabilizarlas cuando legalmente corresponda.

Correlativamente a estos derechos de los ciudadanos, todo funcionario y empleado público de cualquiera de los poderes del Estado tiene la obligación de facilitar el acceso personal y directo a la documentación y antecedentes que se le requiera y que estén bajo su jurisdicción y/o tramitación, ello sin perjuicio de que se arbitren las medidas necesarias para evitar el entorpecimiento del normal desarrollo y funcionamiento de los servicios y actividades que se ejecuten en el ámbito requerido y de las limitaciones que existan establecidas por la normativa vigente en resguardo de los derechos tutelados.

PROCEDIMIENTO:

- La solicitud de información a un organismo comprendido en esta ley deberá ser realizada en forma oral o escrita, con el detalle necesario para identificar la misma con un esfuerzo razonable y con la identificación del requirente, sin estar sujeta a ninguna otra formalidad. No puede exigirse la manifestación del propósito de la requisitoria y debe entregarse al solicitante de la información una constancia del requerimiento.

- El acceso público a la información es gratuito en tanto no se requiera la reproducción de la misma. Los costos de reproducción son a cargo del solicitante. No se podrán imputar otros costos a la solicitud de información que no sean los que surjan de la solicitud de copias de los registros o documentos en los que conste la información requerida

- Se debe permitir al titular de datos personales que figuren en los archivos el acceso a la información contenida en los mismos, en cuyo caso:

a) se debe constatar la identidad del interesado;

b) si la persona pregunta, hay que informarle sobre las fuentes, finalidades y destinos de los datos;

c) las respuestas serán por pantalla, de manera oral o escrita, con envío a domicilio, mensaje electrónico u otra vía (siempre que sea confidencial y segura y cumpla lo establecido en cada repartición u organismo);

- Todo archivo público u órgano estatal alcanzado por el presente procedimiento debe poner a disposición del público para inspección y copiado:

a) La información contenida en documentos escritos, fotografías, grabaciones, soporte magnético o digital, o en cualquier otro formato y que haya sido creada u obtenida por él o que se encuentre en su posesión o bajo su control;

b) Registros de datos que deban ser publicados de acuerdo a la ley;

c) Toda otra información de utilidad para el ejercicio del derecho al acceso a la información.

- La solicitud de información requerida de acuerdo a lo establecido en la normativa vigente y en el presente procedimiento debe ser satisfecha según los siguientes plazos:

a) en un plazo no mayor de 10 (diez) días hábiles, cuando la información se encuentre en poder de la Autoridad de Aplicación.

b) en un plazo no mayor de 30 (treinta) días hábiles, cuando la información se encuentre en poder de terceros.

c) en un plazo no mayor de 10 (diez) días corridos cuando se trate de rectificación de la información

d) en un plazo no mayor de 5 (cinco) días hábiles cuando se trate de correcciones de datos erróneos.

- La administración no tiene la obligación de crear o producir información con la que no cuente o no tenga obligación de contar al momento de efectuarse el pedido.

- En caso que existiere un documento que contenga, en forma parcial, información que no sea de acceso público, de ningún modo la administración podrá negar el acceso al resto de la información de ese documento que no se encuentre contenida entre las excepciones previstas.

Asimismo, deberá indicarse que se ha omitido información por estar contemplada en una de las excepciones y la extensión y ubicación de la información omitida, salvo que esto atente contra el interés protegido por la excepción.

- Si el solicitante tuviera alguna discapacidad, se le deberá proveer la información en un formato alternativo accesible a las capacidades del solicitante.

- Sólo podrá negarse a brindar la información objeto de la solicitud si se verificara que la misma no existe o que está incluida dentro de alguna de las excepciones previstas en el presente procedimiento y en la normativa vigente.

En tal caso, el órgano deberá proporcionar al solicitante un informe fundado del que surja de manera expresa la excepción que consideró aplicable.

- Ante la denegación expresa o tácita por parte del funcionario responsable de facilitar el acceso a la información conforme las disposiciones vigentes, el afectado podrá recurrir en amparo de su derecho vulnerado ante los jueces que correspondan.

EXCEPCIONES:

El principio general del acceso a la información, se podrá limitar sólo en los siguientes casos:

1) Cuando la información y documentación afecte la esfera de la intimidad personal o familiar de las personas, a su honor y a su propia imagen;

2) Cuando se trate de bases de datos de domicilios o teléfonos

3) Cuando la información, antecedentes y documentación fuere declarada secreta o reservada, en forma previa, por resolución fundada en razones de seguridad o de un interés público prevaleciente efectivamente determinado.

4) Cuando pudiere ocasionar un peligro a la vida o la seguridad de una persona;

5) Cuando sea información de terceros que la administración hubiera obtenido en carácter confidencial y la protegida por el secreto bancario.

6) Cuando se trate de información que pudiera poner en peligro el correcto funcionamiento del sistema financiero o bancario;

7) Cuando se trate de información que pudiera revelar la estrategia a adoptarse en la defensa o tramitación de una causa judicial, o de cualquier tipo que resulte protegida por el secreto profesional.

8) Cuando fuere dispuesta por magistrado en resguardo y defensa de los derechos individuales y garantías constitucionales de los ciudadanos.

9) En casos de sumarios administrativos, hasta la etapa de la formulación de los cargos por parte del instructor sumariante.

10) Cuando se dispongan por leyes especiales.

SANCIONES:

- En caso de incumplimiento de las leyes vigentes en materia de confidencialidad, quien incurriera en dicha infracción se hará pasible de la pena que por su responsabilidad corresponda conforme con el Código Penal, y otras normas penales

concordantes para la violación de secretos, sin perjuicio de la responsabilidad penal en que se incurra por la naturaleza del delito.

- Los funcionarios de los organismos comprendidos en el presente procedimiento serán pasibles de las acciones que pudieran corresponder por aplicación del punto precedente mas la pena de exoneración y multa y toda otra sanción administrativa que se encuentre establecida en la normativa interna y legal vigente.

Anexo: Proceso de Consulta

"Proceso de Consulta de Información.ppt"

3.2.4.3. Centros de Acceso Comunitario.

En el presente punto desarrollamos brevemente lo relacionado con los lugares físicos en donde la comunidad tenga real acceso a las nuevas tecnologías informáticas. En la provincia de San Luis se los denomina Centros de Acceso Comunitario, mientras que en general se los conoce como Centros Tecnológicos Comunitarios.

Básicamente los CAC son redes informáticas locales conectadas a Internet con contenidos y desarrollos de Web comunitarias, localizadas en conglomerados humanos de nivel socioeconómico bajo o en localidades de escasa demografía o de desfavorable localización geográfica.

La Misión de los CAC es promover el acceso equitativo, el uso y la apropiación social de las nuevas tecnologías de la información y las comunicaciones (TICs), por considerarlo condición facilitadora de la inclusión social, contribuyendo así al desarrollo socioeconómico y la cohesión de la sociedad en su conjunto.

Esta misión adquiere especial relevancia debido al impacto que prometen las nuevas tecnologías en el progreso económico y social.

Objetivos generales

- Integrar los subprogramas, a fin de ponerlos al servicio de la producción y del trabajo, contribuyendo así a la inclusión laboral y social.
- Relacionar y consolidar, en cada localidad de la provincia, los emprendimientos productivos en actividad, contribuir a generar nuevos y promover la participación de capitales en el financiamiento de tales emprendimientos.
- Brindar acceso a las TICs a los sectores productivos, a través de los CAC, mediante acciones de capacitación y el aprovechamiento de la innovación tecnológica aplicada a la producción.
- Proporcionar soporte técnico a las actividades de difusión, comunicación y capacitación en las áreas de salud y educación.

3.2.5. Relación entre el Estado y el Sector Privado en la generación de empleo.

En este punto mostramos la relación que existe entre las empresas de Recursos Humanos que funcionan en la Provincia con el Estado provincial.

3.2.5.1. Empresas de Colocación de Personas (Recursos Humanos).

Realizamos un relevamiento de las principales empresas cuyo objeto es la colocación de personas en el mercado laboral.

Las empresas entrevistadas fueron las siguientes: Adecco, Man Power y Vademécum.

Cuestionario

1. ¿reciben y/o envían información de y al Estado provincial?
2. ¿cómo y en qué casos?
3. ¿cómo generan y actualizan la base de datos?

4. ¿tienen convenios de colaboración con el Estado provincial?

La respuesta a la preguntas 1, 2 y 4 en las tres empresas fue idéntica por la negativa. En cuanto a la pregunta 3, solamente Adecco contestó, las restantes empresas mantuvieron reserva.

Adecco a través de su página en Internet permite el acceso a la base de datos a los postulantes y a las empresas que requieren personal. El procedimiento técnico, respecto a los postulantes, es a través del llenado de la ficha de inscripción, una vez ingresado se le otorga un código de acceso para poder realizar las modificaciones que considere oportunas y, si lo desea, darse de baja de la base. En relación a las empresas que requieren personal, previo a la firma de un contrato, el procedimiento es similar al anterior, es decir, a través de un código de acceso pueden ver la base de datos, lo que no pueden es realizar modificaciones a la misma.

En relación a las preguntas 1 y 4, las tres empresas coincidieron en la necesidad de trabajar en conjunto con el Estado (nacional, provincial y municipal). En el caso puntual de Adecco, en el primer trimestre del presente año se habían comenzado las negociaciones para lograr un acuerdo de cooperación, dicho acuerdo se relacionaba con el Plan Provincial de Pasantías Laborales. Luego las actuaciones se paralizaron.

3.2.5.2.Convenio.

Presentamos un modelo de convenio entre el Estado Provincial y las Empresas de Colocación de Personas, para permitir la cooperación y la coordinación de tareas, a fin de permitir la inserción de personas en el mercado laboral.

CONVENIO DE COOPERACION ENTRE EL ESTADO PROVINCIAL Y LAS EMPRESAS DE COLOCACIÓN DE PERSONAS.

El Convenio tiene como objetivo que los ciudadanos en edad productiva en situación de desempleo se integren al campo laboral y/o generen emprendimientos productivos.

OBJETIVOS

1. Fomentar y promover lo relacionado con la defensa de los intereses de los ciudadanos en edad productiva que actualmente se encuentren en situación de desempleo o sub empleo, sin discriminación de carácter político, religioso, geográfico o racial.
2. Propulsar el crecimiento fomentando y desarrollando el sistema social como organización y la participación solidaria entre todos los ciudadanos.
3. Peticionar ante las autoridades competentes para que se planifiquen, proyecten y ejecuten las obras y acciones necesarias para el progreso de la comunidad, tales como las referentes a la salud, la educación y especialmente las relacionadas con la generación de empleo.
4. Propiciar y fomentar diversas manifestaciones de carácter social y cultural.

ANEXO

Entre **EL ESTADO PROVINCIAL Y LAS EMPRESAS DE COLOCACIÓN DE PERSONAS** en adelante La EMPRESA, representada en este acto por su ....., con domicilio legal en ..... y **EL ESTADO PROVINCIAL** en adelante EL ESTADO representado en este acto por el Sr. Gobernador de la Provincia, las partes acuerdan celebrar un CONVENIO DE COOPERACION, en consideración a:

Que es importante para la comunidad contar con una fuente de saber especializado con funcionarios, profesionales e investigadores que aporten sus conocimientos para la formación y el perfeccionamiento de la sociedad y para el desarrollo óptimo de programas conjuntos que sean aportados en beneficio de la provincia.

El presente **Convenio de Cooperación** se regirá por las siguientes cláusulas:

PRIMERA: EL ESTADO y La EMPRESA se comprometen a prestarse colaboración mutua en actividades que sean de interés para ambas partes, como:

1. Asistencia técnica y capacitación en actividades productivas actuales.

2. Organización de cursos de formación, seminarios y jornadas de interés para las partes.

3. Realización de trabajos conjuntos en el estudio de las necesidades básicas, como la salud, la educación, especialmente las relacionadas con los mini emprendimientos.

4. Realización de ediciones, publicaciones o producciones conjuntas de interés común para las partes.

5. Otras acciones que se acuerden en **protocolos adicionales** al presente convenio en base a los objetivos arriba señalados.

SEGUNDA: Todas las actividades y proyectos conjuntos que se lleven a cabo deberán ser objeto de un **protocolo adicional** que fijará las características y condiciones de la actividad o proyecto a ejecutarse, el objeto del mismo, plazo de ejecución, responsables de ambas partes, formas de financiamiento, dependencias intervinientes, administración y destino final de los bienes afectados al proyecto, previsión de las consecuencias en caso de incumplimiento y toda otra condición o circunstancia que se estime conveniente.

TERCERA: Los protocolos serán firmados por los representantes de las partes.

CUARTA: Este Convenio regirá a partir de su firma por las partes y tendrá una duración de 2 (dos) años, excepto manifestación en contrario efectuada por alguna de las partes y comunicada a la contraparte en forma fehaciente con 3 (tres) meses de anticipación, debiendo cumplirse hasta su terminación los planes de trabajo acordados previamente.

QUINTA: En caso de controversias las partes se someterán a los Tribunales de la Ciudad de San Luis.

En prueba de conformidad, se firman dos (2) ejemplares de un mismo tenor y a un solo efecto, en la ciudad de San Luis a los ..... días del mes de .....del año .....

3.3. ACTIVIDAD N° 3: "Generación de Convenios Marco de intercambio de datos entre los Poderes del Estado y de éste con ONGs y PYMES".

El diseño de esta actividad consiste en que por vía normativa se elaboren Convenios de administración e intercambio de datos entre los poderes del Estado y de éste con ONGs y PYMES, con la finalidad optimizar el uso de la infraestructura informática, tanto en equipamiento (hard) como en desarrollos de programas (soft).

3.3.1. CONVENIOS MARCO DE INTERCAMBIO DE DATOS.

1)- Acuerdo de Intercambio de datos entre Entes Estatales.

Entre el REGISTRO NACIONAL DE LAS PERSONAS, en adelante REGISTRO CIVIL, representado en este acto por el Sr....., DNI N°.....; y el Organismo / Repartición / Ministerio, etc, representado en este acto por el Sr....., DNI N°....., por la otra parte, en adelante EL ORGANISMO; convienen en firmar el presente acuerdo, el que se regirá por las cláusulas siguientes:

PRIMERA: El presente acuerdo, tiene por objeto coordinar el intercambio y cruzar los datos registrados y a registrarse en las distintas bases de datos existentes a nivel nacional y provincial, y a permitir la interacción entre éstas.

SEGUNDA: Ambas partes se comprometen a brindar sus mejores esfuerzos para colaborar recíprocamente en el cumplimiento de las finalidades plasmadas en el presente acuerdo y a fin de garantizar el libre ejercicio del derecho de acceso a la información en el ámbito nacional y provincial; sin perjuicio de respetar el derecho a la intimidad y honor de las personas; asegurando el derecho consagrado en el artículo 43 de la Constitución Nacional, reglamentado por la Ley de Protección de los Datos Personales, N° 25.236. La normativa citada, y toda aquella derivada que se dicte en el futuro constituirá el marco legal en el que se interpreten todas las

cláusulas del presente acuerdo, y aquellas actas complementarias que se celebren en el futuro.

TERCERA: A fin de cumplir con los objetivos mencionados en la cláusula precedente, EL ORGANISMO y el REGISTRO CIVIL constituirán en el término de TREINTA (30) días, a partir de celebrado el presente, un equipo técnico conformado por agentes de ambos organismos, quienes deberán coordinar un Plan de Actividades. Dicho Plan definirá los alcances, plazos, recursos y resultados esperados de las actividades, que serán puestos a consideración de EL ORGANISMO y el REGISTRO CIVIL, quienes deberán aprobarlo expresamente por acta complementaria. Asimismo, el mencionado equipo técnico deberá proponer los procedimientos y estándares técnicos necesarios para permitir el cruzamiento de información.

CUARTA: EL ORGANISMO se compromete a exigir en todos los trámites que realicen las personas físicas ante dicha EL ORGANISMO, la obligación del uso y registración del DNI / LE / LC.

QUINTA: Asimismo, EL ORGANISMO, se compromete a mantener en sus bases de datos un conjunto de datos que serán definidos en el equipo técnico, consistente en los mínimos indispensables para asegurar las finalidades mencionadas en la cláusula segunda; y estándares técnicos y procedimientos que establezca el REGISTRO CIVIL, con el objeto de permitir el intercambio, cruzamiento, conectividad y disponibilidad de la información en todo el sistema de interacción de datos que origina el presente acuerdo. Las bases de datos deberán ser actualizadas en forma mensual y el ORGANISMO, mensualmente, integrará al REGISTRO CIVIL las nuevas bases de datos que genere en el futuro.

SEXTA: El REGISTRO CIVIL y EL ORGANISMO se comprometen a compartir los resultados producto del intercambio y cruzamiento de la información que surge del presente acuerdo instrumental y de las actividades a desarrollar entre ambas partes.

SEPTIMA: Ambas partes se proveerán mutuamente asistencia técnica en todas las acciones referidas a la ejecución del presente acuerdo y de las actas

complementarias que en su consecuencia se suscriban. Tal asesoramiento incluirá, en particular, aspectos metodológicos de homogeneización de las bases de datos (homologación) y tratamiento de la información y, cuando sea menester, recibirán diagnósticos específicos y la recomendación de acciones concretas.

OCTAVA: Ambas partes se comprometen a estudiar los informes de asesoramiento de la otra parte, produciendo los comentarios y planes de implementación correspondientes, dentro de los TREINTA (30) días de recibidos.

NOVENA: Todos los derechos de propiedad intelectual, de cualquier naturaleza que sea, sobre cualquier informe, trabajo, estudio u obra producida como consecuencia de este acuerdo, pertenecerá exclusivamente a la parte que lo haya generado, y se regirá de acuerdo a los convenios que haya celebrado, en su caso, con sus autores. De tratarse de trabajos compartidos, la propiedad de los derechos será conjunta de ambas partes.

DECIMA: Toda información que el REGISTRO CIVIL remita a EL ORGANISMO, a pedido de ésta, llevará, en todos los casos, un código de acceso, que le será informado al funcionario responsable del organismo o a quién éste autorice expresamente y bajo su responsabilidad. EL ORGANISMO se compromete, en todos los casos en que solicite información, a respetar los límites de su competencia específica y a no utilizar los datos que requiere para fines distintos a aquellos que motivaron su obtención. EL ORGANISMO asume su exclusiva responsabilidad por la utilización de estos datos.

DECIMOPRIMERA: Los datos que brinde EL ORGANISMO deberán ser ciertos, adecuados, pertinentes y haber sido obtenidos de conformidad con sus competencias específicas y las normas que lo autorizan a obtenerlo, bajo su exclusiva responsabilidad. EL ORGANISMO en su carácter de responsable del archivo de datos debe adoptar las medidas que resulten necesarias para asegurar el respeto a los derechos de los titulares de los datos personales, de conformidad a lo prescripto en el artículo 43 de la Constitución Nacional y la Ley N° 25.236.

DECIMOSEGUNDA: El REGISTRO CIVIL podrá transferir los datos recibidos de EL ORGANISMO, si éste ha comunicado el consentimiento del titular de esos datos o, si bien no ha mediado ese consentimiento cuando:

1) la transferencia o cesión de los datos tiene como causa una obligación legal;
2) los datos provienen de fuentes de acceso público irrestricto;
3) la transferencia se realiza entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias.

DECIMOTERCERA: Las partes se comprometen a no proceder al intercambio y cruzamiento de los datos de las personas, cuando el resultado de tal acción por parte de los firmantes, implique la obtención de información relativa a la orientación religiosa, política, sindical, sexual y/o toda otra, de carácter sensible, que afecte la privacidad del titular del dato, a menos que pudiera realizarse, con fines estadísticos o científicos, sin identificación de sus titulares.

DECIMOCUARTA: Las partes acuerdan otorgar a todos los datos, que en virtud del presente acuerdo se procesen, el carácter de confidenciales, para lo cual toda persona que intervenga en el tratamiento de los mismos está obligada a guardar secreto, del que sólo podrá ser relevado mediante resolución judicial, o cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública. El REGISTRO CIVIL manifiesta que todos sus agentes han firmado un convenio interno de confidencialidad de acuerdo a lo establecido en la presente cláusula. Por su parte EL ORGANISMO se compromete a que todos los agentes que intervengan en el tratamiento de los datos, objeto de este acuerdo, firmen un convenio interno de confidencialidad a los mismos efectos descriptos en el párrafo anterior. El obligado al mantenimiento del secreto no quedará relevado aunque finalice su relación con el titular del archivo de datos.

DECIMOQUINTA: Cada una de las partes será responsable por los actos o hechos de sus dependientes, consultores o agentes, contrarios a la Ley N° 25.236, en los términos de ésta norma.

DECIMOSEXTA: Las partes se obligan a dotar a sus sistemas internos de intercambio de datos, de la protección necesaria para brindar seguridad en cuanto al acceso a la información, su confidencialidad y privacidad, respecto de las personas físicas y jurídicas sobre las que se posea información, de acuerdo a los estándares y normas nacionales e internacionales vigentes al respecto

En prueba de conformidad se firman dos ejemplares de un mismo tenor y a un solo efecto a los ..... días del mes de .....de .....-

2)- Acta acuerdo entre el Gobierno de la Provincia de San Luis y las Organizaciones No Gubernamentales.

En la Ciudad de San Luis, a los ..... días del mes de .....del año ....., se reúnen el Sr. ....., DNI N°....., en su carácter de Representante del Gobierno de la Provincia de San Luis, en adelante EL ESTADO y el Sr. ....., DNI N° ....., en su carácter de Representante de la entidad ....., en adelante el LA INSTITUCIÓN a fin de acordar lo siguiente:

Objetivos

Facilitar la recepción, transmisión, intercambio y registro de información vinculada con el bien social, la generación de empleo y producción y la capacitación dirigida a la ciudadanía en general; en los casos en que sea oportuno la colaboración, intercambio y/o intervención de ambas partes.

Compromisos asumidos por las partes

1 - EL ESTADO determinará los procedimientos básicos a los cuales se ajustará la presentación, recepción, consulta y transmisión de la información vinculada con el presente acuerdo, como así también las pautas para la conservación y almacenamiento de datos y documentación.

2 - Las presentaciones que deben efectuar las instituciones en virtud de lo acordado en el presente se llevarán a cabo con programas aplicativos definidos por EL ESTADO.

3 - Los sistemas para la recepción, validación y transmisión de información a EL ESTADO serán desarrollados por LA INSTITUCIÓN y homologados por EL ESTADO.

4 – LA INSTITUCIÓN y EL ESTADO deberán instrumentar los mecanismos que garanticen la inalterabilidad y seguridad en el acceso de los archivos y de los datos contenidos en los mismos.

5 – LA INSTITUCIÓN deberá comunicar a EL ESTADO el nombre del responsable del cumplimiento de los puntos contenidos en este acuerdo.

6 – EL ESTADO definirá y acordará con LA INSTITUCIÓN los criterios de seguridad informática que se deberán aplicar para la recepción de los datos y para la posterior transmisión de la información resultante.

7 – LA INSTITUCION proveerá interconexión entre su red y la red de EL ESTADO, según las pautas técnicas definidas por éste.

8 - Los recursos que resulte necesario afectar para la ejecución de este convenio serán solventados por las partes, conforme las responsabilidades precedentemente establecidas.

9 - Cada una de las partes (EL ESTADO y LA INSTITUCION) designarán formalmente al funcionario responsable de ejecutar el presente acuerdo (uno por parte) y coordinar las actividades necesarias para su desarrollo, implementación y operación. Entre otras tareas podrán aprobar los cronogramas de trabajo, suscribir acuerdos técnicos de detalle, acordar plazos de cumplimiento de proyectos desarrollados e implementados, recibir y enviar notas entre las partes y suscribir toda otra información oficial que resulte necesaria.

10 - El presente convenio podrá ser rescindido por cualquiera de las partes, con la previa notificación formulada en tal sentido en forma fehaciente a la otra parte, con una antelación mínima de noventa (90) días corridos.

11 - A los efectos del presente acuerdo LA INSTITUCION constituye domicilio en ..... de la ciudad de ..... y EL ESTADO en ..... de la ciudad de ....., donde se darán por válidas todas las notificaciones y comunicaciones que se efectúen entre las partes. En prueba de conformidad se firman dos (2) ejemplares de un mismo tenor y a un solo efecto.

3.3.2. NORMATIVA

Presentamos los Proyectos de normativa, los cuales, según el criterio adoptado, pueden ser elaborados por vía de Decreto o Resolución del Poder Ejecutivo o bien tener el alcance de ley general elaborada por la Legislatura Provincial.

Objetivos y fundamentación que debería cumplir la Ley provincial:

1. Respeto de los Derechos Humanos y los valores trascendentes de las personas.
2. Reafirmar la responsabilidad y competencia del Estado en la determinación de la política de administración de datos contenidos en los bancos de datos provinciales.
3. Garantizar a toda la población el acceso a la información contenida en los bancos de datos.
4. Garantizar a la población económicamente activa y a las personas jurídicas el acceso a la información comercial, crediticia y productiva que administre el Estado a fin de posibilitar la transferencia de resultado obtenidos en las actividades científicas desarrolladas por el Estado.
5. Asegurar a todos los sectores de la comunidad el ejercicio efectivo de su derecho a informarse, capacitarse y perfeccionarse.
6. Desburocratizar la Administración.
7. Asegurar una justa distribución de los servicios de almacenamiento y tratamiento de la información

8. Propender a la integración de la educación, el trabajo y la producción.
9. Destacar el valor estratégico de la información, para el crecimiento económico y el mejoramiento social de la Provincia.
10. Contribuir a conservar y acrecentar el patrimonio informático a fin de desarrollar toda el potencial con proyección económico social.

RESOLUCIÓN N° ..... - 2004

San Luis, ...de.....de 20.....

VISTO:

El Decreto N° ..... mediante el cual el Gobierno de la Provincia establece como política la estrategia de colaboración y participación de las Organizaciones No Gubernamentales en los programas y objetivos definidos por el Estado en lo relativo a la generación de empleo y producción; y

CONSIDERANDO:

Que en función de la asignación de dichos objetivos resulta pertinente establecer un mecanismo uniforme mediante el cual los Ministerios, los Programas, Subprogramas y Organismos Descentralizados dependientes del Estado Provincial celebren los Convenios de Colaboración e Intercambio de Información que el cumplimiento de sus respectivas funciones haga aconsejable.

Que resulta menester lograr un tratamiento ordenado, eficaz y coordinado en la celebración de los mencionados Convenios entre los distintos estamentos del Estado Provincial y terceros, evitando superposiciones, y facilitando el acceso a los mismos por parte de todas las áreas involucradas.

Que en tal marco, resulta conveniente delegar en el área de CONTROL DE GESTION, la atribución de otorgar, cuando así corresponda, la expresa y previa conformidad a la celebración de los referidos Convenios.

Que el Programa Legal y Técnico del Ministerio de la Legalidad ha tomado la intervención que le compete conforme lo establecido en las normas vigentes.

Por ello,

EL GOBERNADOR DE LA PROVINCIA DE SAN LUIS

RESUELVE:

ARTICULO 1° — Establécese que los Ministerios, Programas, Subprogramas y Organismos Descentralizados dependientes del Estado Provincial deberán,

con carácter previo a la firma de todo Convenio de Colaboración e Intercambio de Información, informar el contenido del mismo al organismo respecto del cual dependan, así como al área de CONTROL DE GESTION.

ARTICULO 2° — Delégase en CONTROL DE GESTION la atribución de autorizar, mediante su conformidad expresa, la suscripción de los Convenios Colaboración e Intercambio de Información referidos en el artículo anterior.

ARTICULO 3° — Una vez autorizados y suscriptos los convenios mencionados en el Artículo 1° de la presente Resolución, las respectivas áreas deberán remitir copias auténticas de los mismos al área de CONTROL DE GESTION.

ARTICULO 4° — Las áreas involucradas deberán informar a CONTROL DE GESTION acerca de las Actas Complementarias que eventualmente se suscribieren, y de los compromisos y obligaciones que en virtud de ellas se asumieren.

ARTICULO 5° — Dentro del plazo de DIEZ (10) días hábiles a partir de la fecha de publicación en el Boletín Oficial de la presente resolución, los Ministerios, Programas, Subprogramas y Organismos Descentralizados dependientes del Estado

Provincial deberán informar a CONTROL DE GESTION acerca de los Convenios Marco de Colaboración e Intercambio de Información celebrados que se encuentren vigentes, remitiendo copia de los mismos, estableciendo si han tenido principio de ejecución y, para este último caso, detallando tanto el listado de las personas involucradas, cuanto todo otro dato de interés relacionado con dichos convenios que no surja del respectivo texto de los mismos.

ARTICULO 6° — Comuníquese, publíquese, y oportunamente archívese. —

4.CONCLUSIÓN

De manera conceptual, la interacción comunicacional es eficaz cuando una vez culminado su proceso, el sujeto receptor – acreedor de la información – puede satisfacer su interés de obtener un conocimiento pleno de aquello que le incumbe directamente y que está fuera de su conciencia. Por ello la información debe cumplir con una serie de requisitos. Necesariamente debe ser clara, precisa, exacta, completa, verdadera, comprensible y dirigida.

Hecho el estudio de los bancos de datos del Estado provincial y de las condiciones de acceso a la información allí contenida, se hace indispensable elaborar la normativa provincial necesaria a fin de cumplir con la meta descripta en el inicio del presente desarrollo.

La realidad de los bancos de datos provinciales es merecedora de críticas; la principal es que funcionan como "islas", desarrollando sus tareas de manera independiente, sin intercomunicación entre los distintos organismos que manejan los mismos datos o información vinculada entre sí; generando el no deseado resultado de duplicidad y dicotomía en la información, además de la negativa consecuencia del mal aprovechamiento de los recursos, sean estos físicos o humanos. De más esta aclarar que es prioridad para el Estado provincial encontrar la solución práctica a este problema. Dicha posible solución ya se encuentra desarrollada en ideas y directrices que se dirigen a la creación de un único banco de datos, de donde todas las reparticiones publicas obtengan la información deseada.

Hemos detectado que los mayores inconvenientes y errores se encuentran en los registros de la propiedad inmueble, catastro y en el registro de Personas Jurídicas.

Respecto a los recursos humanos en la Provincia no existe una concientización generalizada acerca de la responsabilidad que acarrean en sí mismas las tareas de recolección, almacenamiento y administración de datos personales y es por ello que debe ponerse énfasis en la necesidad de la existencia de una norma que regule en su parte operativa esta actividad (procedimientos, plazos, condiciones mínimas de seguridad, responsabilidades, excepciones, controles, sanciones, etc.).

En cuanto al respeto de el derecho de libre acceso a la vista de las actuaciones administrativas y acceso a la información se encuentran en plena vigencia, la cual, tiende a plasmar un accionar de la administración pública para evitar actos de corrupción y que sea verdadera garantía para todos los ciudadanos.

La organización deficiente ya señalada de los Registros de Personas Jurídicas, motivó una gran dificultad de obtener información acerca de las ONGs , Sociedades Comerciales, Cooperativas, Fundaciones, etc. que desarrollan su objeto social en la Provincia y que el mismo se relacione directamente con la producción, en cualquiera de sus niveles, y la generación de empleo. Todos los esfuerzos a este respecto lo realiza el Gobierno de la Provincia a través de una Plan Social de Empleo conocido como "Plan de Inclusión Social", del cual nos eximimos de realizar comentarios por exceder las intenciones del presente trabajo.

5. RESUMEN EJECUTIVO.

"Habeas Data. Intercambio de información entre entes oficiales"

OBJETIVO GENERAL: Determinar las condiciones de tratamiento de la información que posee el Estado provincial, en relación a los ciudadanos e intra-Poderes a fin de garantizar los actos de gobierno asegurando la disponibilidad de la información; lo que permitirá progresar en el cumplimiento de las metas de equidad, inclusión e integración social.

ACTIVIDADES.

ACTIVIDAD Nº 1: "Establecer las condiciones de utilización de la información contenida en los Registros Públicos"

La protección de los datos personales constituye un criterio de legitimación política de los sistemas democráticos tecnológicamente desarrollados. Su reconocimiento supone una condición del funcionamiento del propio sistema democrático.

ACTIVIDAD Nº 2: "Instrumentar los Mecanismos y Procesos de consulta de la información, en especial la relacionada con la producción y generación de empleo."

Una forma precisa y concreta de terminar con la cruel crisis de representatividad y su ilegitimidad correlativa, es permitirle al ciudadano común, conocer las actuaciones y los actos de los funcionarios, con absoluta libertad y sin rigorismos.

ACTIVIDAD Nº 3: "Generación de Convenios Marco de intercambio de datos entre los Poderes del Estado y de éste con ONGs y PYMES".

Entre otras reformas, el Estado tiene pendiente la construcción de un nuevo modelo de política social, que acompañe al modelo económico. Su objetivo sería lograr una nueva institucionalidad pública, donde lo social sea constitutivo del Estado, lo que le da sentido, y cuyo objetivo central sea la equidad, la inclusión e integración social.

CONCLUSIÓN.

Respecto a los recursos humanos en la Provincia no existe una concientización generalizada acerca de la responsabilidad que acarrean en sí mismas las tareas de recolección, almacenamiento y administración de datos personales y es por ello que debe ponerse énfasis en la necesidad de la existencia de una norma que regule en su parte operativa esta actividad (procedimientos, plazos, condiciones mínimas de seguridad, responsabilidades, excepciones, controles, sanciones, etc.).

En cuanto a la organización administrativa de los organismos estudiados esta lejos de ser la ideal, a fin de la utilización de las herramientas informáticas, tanto en equipamiento como en sistemas. El mayor inconveniente resulta ser el aislamiento operativo entre los bancos de datos.

6. BIBLIOGRAFÍA.

- Acta Acuerdo entre la Administración Federal de Ingresos Públicos -AFIP- y el Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires

- Anteproyecto de Convención Americana sobre Autodeterminación Informativa.

- Argentina ya tiene su Ley de Habeas Data, en Revista APPEI "El profesional Informático"; www.aecride.edu.ar

- Bergel, Salvador Dario: El hábeas data: instrumento protector de la privacidad, en "Revista de Derecho Privado y Comunitario", n° 7, "Derecho Privado en la reforma constitucional", Ed. Rubinzal-Culzoni, Santa Fe, 1999.

- Cesario: "Habeas Data" Ley 25.326.

- Convenio de Colaboración entre el Ministerio de Trabajo, Empleo y Seguridad Social y el Sistema de Identificación Nacional Tributario y Social en el marco del Programa Jefes de Hogar

- Decreto N° 929/00 de la Provincia de Misiones sobre Creación del Programa "El Estado al Servicio del Ciudadano"

- Derecho a la Información – Proyecto de Ley de la Provincia de Santa Fé; www.consultorweb.com

- Ekmekdjian, Miguel Angel y Pizzolo(h), Calogero: Hábeas data. El derecho a la intimidad frente a la revolución informática. Ed. Depalma, Bs. As.,1998.

- El Derecho a la Información: Código de Etica; CIEC - Cámara de Empresas de Información Comercial

- Gaibrois, Luis Mauricio: El habeas data argentino. La libertad informática es un derecho humano, "Revista de la Asociación de Magistrados y Funcionarios de la Justicia Nacional", año VII, n° 10, junio de 1984, págs. 18 a 26.

- Gil Domínguez, Andrés: La verdad: un derecho emergente, "L.L.", 1999-A-219 a 223.

- Gobernabilidad y Transparencia – Acceso a la Información: Conclusión Final sobre necesidades de ley operativa y roles; www.britishcouncil.org.ar

- Gozaíni, Osvaldo Alfredo: Habeas Data – Protección de Datos Personales.

- Guahnon, Silvia V. y Somer, Marcela P.: Habeas Data Procedimiento Aplicable, Revista de Derecho Procesal.

- Habeas Data (Comisión Dra. Mauro), www.personales.ciudad.com.ar

- Investigación: Demandas Ciudadanas de Información; www.unc.edu.ar

- La Protección de los Datos Personales en los Sistemas Informáticos – La Instrumentación en la Argentina; Maria Eugenia Valesani, Sonia Mariño y David La Red Martinez, Facultad de Cs. Exactas y Naturales y Agrimensura – Universidad Nacional del Nordeste

- Leguisamón, Héctor Eduardo: Procedimiento y Aspectos Procesales del Habeas Data, Revista de Derecho Procesal.

- Ley N° 104 de la Ciudad de Buenos Aires sobre Acceso a la Información

-.Ley N° 3764 de la Provincia de Chubut sobre Libertad de Información – Deberes del Funcionario Público; www.cippec.org/espanol/derechodeacceso

- Ley Nacional N° 24.314 sobre Accesibilidad de Personas con Movilidad Reducida. Modificación Ley N° 22.431

- Ley Nacional N° 24.766 de Confidencialidad sobre Información y Productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los Usos Comerciales Honestos; www.derecho.unc.edu.ar

- Ley sobre el Derecho al Libre Acceso a la Información Ambiental de la ciudad de Buenos Aires; www.saij.jus.gov.ar

-Martella, Lilián P.: Habeas Data: Garantía de una Dimensión Fundamental de la Libertad, www.ceride.gov.ar/servicios/comunica/ponencias.

-Mattelart, Armand : "La mundialización de la comunicación".

-Mattelart, Armand y Mattelart, Michele: "Historia de las teorías de la comunicación".

- Nespral, Bernardo: "Derecho de la Información".

- Ossola, Federico y Vallespinos, Gustavo: "La Obligación de Informar".

- Paladella Salord Carlos - Datos Personales contenidos en Bases de Datos y Registros Electrónicos; Estudios sobre Tecnología y Privacidad.

- Palazzi, Pablo Andrés: El Habeas Data en el Derecho Argentino, Organización Mundial de Derecho e Informática, Revista Internacional de Derecho e Informática.

- Palazzi, Pablo Andrés: Protección de Datos Personales, Privacidad y Habeas Data en América Latina; www.ulpiano.com.

- Pandiella, Juan Carlos: El Bien Jurídico Tutelado por el Habeas Data; www.foroabogadossanjuan.org.ar

- Proyecto de Reglamentación Constitucional del Derecho de Acceso a la Información, Subcomisión de Asuntos Constitucionales

- Régimen Jurídico de los Bancos de Datos – Habeas Data; Paula Mariana Rómulo y Carlos Bedini, Asociación de Abogados de Buenos Aires, www.aaba.com.ar

- Reglas Mínimas para la Difusión de Información Judicial en Internet – Reglas de Heredia; Investigación de International Development Research Centre (IDRC), Canadá

- Requisitos Mínimos para una Ley de Acceso a la Información Pública; Comisión de Asuntos Constitucionales de la Cámara de Diputados de la Nación, www.cippec.org/espanol/derechodeacceso

- Vidas Privadas – Vidas Públicas - ¿Vidas paralelas? ; Sebastián castelli y Nicolás Salvi

INDICE GENERAL