UNIVERSIDAD DE EL SALVADOR
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES
SEMINARIO DE GRADUACIÓN EN CIENCIAS JURÍDICAS AÑO 2006.
PLAN DE ESTUDIO 1993

"EL HABEAS DATA COMO MECANISMO DE PROTECCIÓN DE DERECHOS RELACIONADOS CON LA AUTODETERMINACION INFORMATIVA ANTE EL TRATAMIENTO AUTOMATIZADO DE DATOS PERSONALES"

TRABAJO DE GRADUACIÓN PARA OPTAR AL TITULO DE

LICENCIATURA EN CIENCIAS JURIDICAS

PRESENTAN:

MARÍA ELENA HERNANDEZ LEON
ROSA ARLENY TAMAYO LARÍN

DIRECTOR DE SEMINARIO:

DOCTOR JOSE RODOLFO CASTRO ORELLANA

CIUDAD UNIVERSITARIA, SAN SALVADOR, NOVIEMBRE 2006.

UNIVERSIDAD DE EL SALVADOR

RECTORA
DOCTORA MARÍA ISABEL RODRÍGUEZ

VICE-RECTOR ACADEMICO
ING. JOAQUIN ORLANDO MACHUCA GOMEZ

VICE-RECTORA ADMINISTRATIVA
SRA. CARMEN ELIZABETH RODRIGUEZ DE RIVAS

SECRETARIA GENERAL
LICDA. ALICIA MARGARITA RIVAS DE RECINOS

FISCAL GENERAL:
LIC. PEDRO ROSALIO ESCOBAR DASTANEDA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

DECANA
LICDA. MORENA ELIZABETH NOCHEZ DE ALDANA

VICE-DECANO
LIC. OSCAR MAURICIO DUARTE GRANADOS

SECRETARIO
LIC. FRANCISCO ALBERTO GRANADOS HERNANDEZ

COORDINADORA DE LA UNIDAD DE SEMINARIO DE GRADUACION
LICDA. BERTA ALICIA HERNANDEZ AGUILA

DIRECTOR DE SEMINARIO
DOCTOR JOSE RODOLFO CASTRO ORELLANA

A partir de 20 de noviembre 2006.

DEDICATORIA

A DIOS TODO PODEROSO: *Por ser el pilar de mi vida, por su infinito amor y misericordia; y por darme la fuerza y la sabiduría para salir adelante en mis estudios y permitirme coronar una carrera, ya que nunca me ha abandonado en mi diario vivir.*

A MIS HERMANOS: *Víctor y Sandra, por su constante apoyo incondicional, y porque han estado pendientes de mi en todos los momentos de mi vida.*

A MI ASESOR: *Doctor José Rodolfo Castro Orellana, porque con su sabiduría y experiencia, ha sido un valioso guía en el camino recorrido para la realización de este trabajo.*

A MI AMIGA Y COMPAÑERA DE TESIS: *Arleny, me voy satisfecha de haber compartido este trabajo contigo y, sobre todo, por la amistad que siempre me has brindado y por compartir tantas experiencias juntas; te quiero mucho.*

Por todo, muchas gracias …

María Elena Hernández León.

A DIOS TODO PODEROSO: *Por ser mi fundamento y fortaleza, por no dejarme sola en los momentos más difíciles y permitirme culminar mi carrera.*

A MIS PADRES: *por su apoyo incondicional y su confianza.*

A MIS HERMANOS: *por estar a mi lado en cada momento de mi vida.*

A MI ASESOR: *Doctor José Rodolfo Castro Orellana, porque con su experiencia y paciencia ha sido un valioso guía en el camino recorrido.*

A MI AMIGA Y COMPAÑERA DE TESIS: *María Elena, por tu apoyo incondicional y tu amistad sincera, gracias por haber recorrido conmigo este largo camino, siempre tendrás un lugar especial en mi vida.*

Por todo, muchas gracias ...

Rosa Arleny Tamayo Larín

INDICE

Contenido — No. de Página

INTRODUCCION

El presente trabajo de investigación ha sido elaborado con el objeto de analizar las implicaciones que el fenómeno de la informática ha producido o puede producir en el campo jurídico. No obstante las ventajas que ofrece la informática jurídica, produce al mismo tiempo riesgos generados por la desactualización, proliferación y tráfico de los bancos de datos, lo cual puede producir graves violaciones a los derechos fundamentales, por contener dichos bancos o registros, datos denominados sensibles; es decir, relativos a la Intimidad o privacidad. Ello ha llevado a que la mayoría de países europeos y algunos latinoamericanos regulen su protección a través de leyes secundarias o de la Ley fundamental; algunos países latinoamericanos, como Brasil, han considerado que no es suficiente el reconocimiento del derecho en sí ni la protección a través del Amparo, sino que han creado la figura del Hábeas Data como una garantía constitucional.

Los países tendrán más posibilidades de desarrollo humano, en la medida en que se fortalezcan los sistemas de defensa y protección de los derechos fundamentales de los ciudadanos; en tal sentido, la presente investigación pretende contribuir al esfuerzo por alcanzar niveles más elevados de desarrollo humano para los salvadoreños.

En ningún caso este trabajo pretende deslegitimar el uso de la información personal por parte de entidades privadas o públicas, sino prevenir el abuso y la lesión a la persona. No puede dudarse de los grandes beneficios para la persona, derivado de un manejo electrónico de sus datos. Lo fundamental, es darse cuenta de que la Autodeterminación Informativa o Libertad Informática no persigue bloquear el libre flujo de los datos, sino reconocer que frente al poder que la tecnología pone en manos de los recolectores y clasificadores, el individuo debe estar dotado también de la poderosa arma que consiste en que la Ley reconozca su derecho a participar en ese proceso para asegurar que los datos recopilados sean veraces, que no sean más de los que se requiera obtener para fines lícitos y que, en ningún momento puedan ser empleados de forma que se invada el espacio de privacidad que toda persona debe tener garantizado para su realización como tal.

La normativa sobre Autodeterminación Informativa o Libertad Informática y sus prácticas permitiría ordenar y sistematizar el cúmulo de informaciones aisladas que, como tales, no tienen valor significativo, con lo cual mejoraría la protección del Estado y la Seguridad Pública, y evitaría que la falta de orden y controles sean aprovechados por personas o agrupaciones criminales, terroristas o Estados enemigos.

Ahora bien, la regulación adecuada del derecho a la Autodeterminación Informativa o Libertad Informativa no elimina la posibilidad de disponer o hacer negocios con datos ajenos, sino que establece un marco de negociación más ordenada y responsable. Por tanto, el objetivo de esta investigación es proporcionar bases teóricas e ideas sobre la forma de regular, de manera concreta el derecho a la Autodeterminación Informativa o Libertad Informática. En ese sentido, se proponen reglas para la constitución, organización y sistematización de archivos públicos o privados y la transferencia nacional o internacional de datos personales. Si se pretende que la política de inserción en el mundo globalizado sea coherente, es necesario definir un marco normativo que brinde seguridad en el manejo de la información personal en El Salvador.

Una regulación normativa, en materia de protección de datos personales en El Salvador, sería una muestra inequívoca del deseo de

proteger a sus habitantes en todos los ámbitos frente a la posible trasgresión de derechos y, sin duda, una muestra para la comunidad internacional de que el país, respecto a las nuevas tecnologías de la información, posee una clara orientación y regulación dirigida a la transparencia, el manejo público y la responsabilidad para con la ciudadanía.

En su conjunto, la investigación se compone de seis capítulos, los cuales se detallan a continuación:

En el Capítulo I denominado “Antecedentes Históricos sobre Protección de Datos Personales”, en el cual se desarrolla la forma en que la protección de datos personales ha evolucionado a través de la historia, en las legislaciones de los países tanto europeos como latinoamericanos, y por supuesto en nuestro país.

El Capítulo II que se denomina “Elementos doctrinarios del Derecho a la Intimidad”, se desarrolla los aspectos relevantes acerca del derecho a la Intimidad, como son concepto, características, sus límites, titulares, la cuestión de si las personas jurídicas tienen o no derecho a la Intimidad, así como los avances tecnológicos de la informática y su incidencia en los derechos fundamentales.

El Capítulo III se denomina: “El Derecho a la Autodeterminación Informativa y la Protección de Datos Personales, en el cual se establece el perfil de un nuevo derecho: el derecho fundamental a la autodeterminación informativa, así como la privacidad sobre los datos personales, donde se contempla lo que se entiende por datos personales, la naturaleza jurídica, el fundamento y autonomía, el bien jurídico tutelado y los mecanismos de protección de los mismos.

En el Capítulo IV denominado: “El Hábeas Data: Caracterización y Naturaleza Jurídica. Registros de Datos Personales y la Transferencia Internacional de Datos”, en el cual se desarrolla los aspectos doctrinarios relativos a la figura del Hábeas Data, como el concepto, naturaleza jurídica, características, el procedimiento del mismo, tomando como referencia la legislación brasileña; planteándose así mismo, la necesidad de incorporar dicha figura en el ordenamiento jurídico salvadoreño. De igual manera, se ha planteado la importancia de conocer la realidad de los registros en nuestro país, estableciendo, el tratamiento que en los mismos se les da a los datos personales, y de las entidades que de alguna manera se relacionan con el almacenamiento de ellos, finalizando con la Transferencia Internacional de Datos.

El Capítulo V se denomina “Análisis de los Resultados de la Investigación”, en el cual se plantea la metodología utilizada para obtener

respuestas a través de las técnicas de investigación documental y de campo, así como el respectivo análisis e interpretación de los resultados de la investigación de campo y la comprobación o no de las hipótesis planteadas.

El Capítulo VI denominado “Conclusiones y Recomendaciones” representa la síntesis de los resultados de los obtenidos en el proceso de investigación. En este capítulo se vierten las apreciaciones y consideraciones personales de las elaboradoras de la presente investigación, y además señala en qué medida fueron comprobadas las hipótesis planteadas en torno al problema de investigación.

Todo esfuerzo investigativo encuentra cierta dificultad, lo cual constituye un obstáculo para el cumplimiento pleno de las metas trazadas; lo cual representa el compromiso de buscar con mayor esfuerzo su superación. En ese sentido, el problema objeto de investigación ha sido concebido bajo el estudio de una diversidad de documentos; sin embargo, la adquisición de los más representativos textos salvadoreños que sobre el tema su pudo obtener y el acceso a la abundante doctrina de vanguardia, no sólo es limitada en términos económicos, sino relativamente inexistentes, ya que en nuestro país por no contar con regulación jurídica acerca del Hábeas Data y el Tratamiento Automatizado de Datos Personales, únicamente se cuenta con

el texto “La Protección de Datos Personales en El Salvador”[1]. No obstante ello, se cuenta con textos que desarrollan el tema y la regulación al respecto en otros países, tanto europeos como latinoamericanos, que fueron de gran utilidad para llevar a cabo la presente investigación, rescatando de ello lo aplicable a nuestro país; ya que, países como el nuestro, han tomado como referencia estudios realizados por autores europeos y latinoamericanos de renombre, por ser dichos estudios aplicables a nuestra realidad.

En virtud que el objeto de la investigación desarrollada implicó examinar actividades estatales y de entes particulares encargados del registro y almacenamiento de datos personales, y debido a la actitud burocrática, característica de dichas instituciones, ello se convirtió en un impedimento para la adquisición pronta y oportuna de la información necesaria para la verificación y enriquecimiento de la investigación. En ese sentido, no se pudo aplicar el instrumento de la Entrevista no estructurada dirigida a Magistrados de la Sala de lo Constitucional de la Corte Suprema de Justicia, así mismo no se pudo aplicar el instrumento de la Encuesta dirigida a los Colaboradores Judiciales de la Referida Sala; ello con la justificación que la institución no puede adelantar criterio al respecto. A todo eso se suma la falta de conocimiento acerca del Hábeas Data, haciendo menos factible obtener la opinión pública derivada de posibles entrevistas que sobre la misma se pretendió efectuar.

[1] Ayala Muñoz, José María y otros: “La Protección de Datos Personales en El Salvador”.

No obstante esas limitaciones, nuestro estudio ha logrado cumplir en forma adecuada los objetivos propuestos al inicio; otros interesados en el tema podrán superar las dificultades aquí señaladas y ocuparse de aspectos específicos del problema.

CAPITULO I

1. ANTECEDENTES HISTORICOS SOBRE PROTECCION DE DATOS PERSONALES.

Desde los albores de la humanidad, la información constituyó no sólo un bien precioso, sino también el principal factor de civilización; la humanidad comenzó lentamente a tejer redes de información por medio de las cuales compartió los primeros y más rudimentarios progresos; con el tiempo y la disposición de ciertos adelantos técnicos como la imprenta, la información no sólo comenzó a circular más rápidamente y a acelerar el progreso, sino que también pasó a constituirse en un valor primario para convertirse en un elemento indispensable; de ahí nace la necesidad de proteger los datos suministrados por las personas, cuyos antecedentes pueden encontrarse en dos momentos, que a continuación se mencionan: por un lado tenemos el *antes del periodo tecnológico* y por el otro *el periodo tecnológico*. Esta

división atiende a la necesidad que surge de brindar protección a dichas informaciones, por el peligro que sufren, debido a los medios por los cuales pueden ser transgredidos[2].

1.1 PERIODO PRE TECNOLOGICO.

En cuanto al Periodo Pre – Tecnológico: durante el año de 1361, se encontraban leyes para la protección de la privacidad de las personas; por ejemplo, la Justicia del Acta de Paz Inglesa, en la que se contemplaba el arresto para los fisgones, y para quienes en secreto escuchaban las conversaciones de otros; en el año de 1766, el Parlamento Sueco decreta el Acta de Acceso a los Registros Públicos, a fin de que el gobierno tuviese información usada sólo para fines legítimos.

Asimismo, en el año de *1792 la Declaración de los Derechos del Hombre y del Ciudadano dispuso que la Propiedad Privada era inviolable y sagrada; en virtud de lo cual, en Francia se prohíbe la publicación de hechos privados, y en 1858 se aplican severas multas por estas contravenciones*[3].

[2] Alfaro Escoto, D. A. y otros. Ob. Cit. Pág. 1
[3] Alfaro Escoto, D. A. y otros. Ibídem. Pág. 2

De esta manera, se han citado algunas de varias leyes que surgieron en el Período Pre Tecnológico.

1.2 PERIODO TECNOLOGICO.

En lo que respecta al Período Tecnológico, los más recientes y contundentes avances propios del siglo veinte, como las nuevas formas de comunicación telegráfica, telefónica, radiofónica, televisiva y telemática, conformaron la denominada Tecnología de la Información. Es de todos conocido lo que ha significado el avance de la informática en el almacenamiento y transmisión de datos personales.

Hoy en día, en las sociedades modernas, una persona compra un electrodoméstico, abre una cuenta corriente en un banco, paga sus impuestos, va a un hospital o es atendido por un médico, para lo cual llena formularios en los que debe anotar datos personales; así mismo, en la gestión de relaciones sociales, jurídicas y económicas se da la exigencia del intercambio y flujo de datos personales, gestión realizada con el auxilio de las nuevas tecnologías, con la informática[4]; además el auge de las comunicaciones ha producido modificaciones de los sistemas de comunicación y flujo de datos. Sin embargo, y gracias a los avances de la

[4] Ayala Muñoz, José María y otros. Ob. Cit. Pág. 20

informática y las telecomunicaciones, personas inescrupulosas pueden hacer uso de los datos de carácter personal *para ofrecer, en calidad de intermediarios, servicios de información que pueden ser perjudiciales para las personas en sus relaciones sociales*[5]. Esto genera incertidumbre jurídica para las personas y graves violaciones a los derechos fundamentales, específicamente, al derecho a la Autodeterminación Informativa o Libertad Informática, como manifestación del Derecho a la Intimidad.

Esta situación ha llevado a que algunos países europeos y latinoamericanos regulen su protección a través de leyes secundarias o de la Ley fundamental. Así por ejemplo, *países como Brasil han considerado que no basta el reconocimiento del derecho en sí, ni la protección a través del Amparo, sino que han incorporado a su legislación la figura del Hábeas Data como garantía constitucional.*[6]

En la sociedad tecnológica, también hacen su aparición nuevas formas de derechos humanos, desconocidas por las sociedades anteriores; ese es el caso del derecho a la información que ha tomado formas diversas, de acuerdo con la articulación práctica de la vida social de nuestro tiempo, lo cual motiva en cierta forma a que, *en Europa Occidental, así como en los Estados Unidos de Norteamérica y países de América Latina, se reconozca*

[5] Ayala Muñoz, José María y otros. Ibídem. Pág. 21
[6] Alvarado Bonilla, Karla María y otros: "Hábeas Data como Garantía de Protección de la Persona frente al Tratamiento de sus Datos Personales". Pág. 1

el Derecho a la Protección de los datos personales y a la Autodeterminación sobre el destino de los mismos, aunque se establecen en las legislaciones un tratamiento diferente de acuerdo al país en que se aplique[7]; en ese sentido, puede hablarse de dos formas en cuanto a la técnica jurídica de protección de datos personales; una de ellas es a través de la legalidad, y otra con la incorporación de un mecanismo procesal o garantía en el ámbito constitucional.

Debido a la importancia que siempre ha tenido la información, y que tal interés se destaca especialmente en este siglo, por la vertiginosa proliferación y la incidencia que sobre los derechos humanos están produciendo las nuevas tecnologías, en lo que respecta al presente estudio, se han iniciado dos frentes de batalla: uno, ocupado de los avances informáticos sobre los derechos personales (cuya meta se centraba especialmente en la limitación de la actividad de los operadores de las bases y bancos de datos en el tratamiento de datos personales), y otro, preocupado por la eliminación de límites abusivos al derecho a informarse y permitir el libre acceso y tratamiento de datos vacantes. Ambos confluyeron a la hora del dictado de las normas sobre tratamiento de datos personales, e incluso en algunas versiones del Hábeas Data.

[7] Alvarado Bonilla, Karla María y otros. Ibídem. Pág. 3

En el primero de los casos, aunque se destacó que la problemática de los daños a las personas cuyos datos se encuentran registrados en archivos no es, ciertamente, un fenómeno atribuible exclusivamente a la "era informática"[8], y que la labor normativa constitucional se inició tempranamente con la sanción de la Constitución de Weimar de 1919, cabe coincidir con ESTADELLA YUSTE en que "*el derecho a la «protección de datos» pertenece a la contexto de la era informática, y ciertamente resulta atrevido afirmar que esta compleja disciplina legal estuviera ya implícita en las referencias generales al derecho a la Intimidad inserta en cuerpos normativos de ámbito nacional e internacional de la era pre informática*"[9], pese a que la existencia de los rudimentarios sistemas de registro propios de la etapa anterior al advenimiento de las computadoras ya auguraba los riesgos que un fichero con datos incompletos, falsos o utilizados para un propósito diferente para el cual se habían recogido podía tener en la persona afectada.

En el segundo de los casos, es a partir de las disposiciones de la Constitución Española de 1978,[10] en especial de la conjugación entre el artículo 105, literal *b* (el cual manda a la Ley regular el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte

[8] Basta recordar al repecto –por sólo recurrir a nuestra historia reciente- las nefastas consecuencias que sobre vastos sectores de las sociedades han producido ciertos regímenes totalitarios y autoritarios, cuyas prácticas genocidas fueron diseñadas a partir de los archivos (entonces no informatizados) de los denominados "organismos de inteligencia".
[9] Estadella Yuste. Olga: "La protección de la Intimidad frente a la transmisión internacional de datos personales", citada por Puccinelli, Oscar. Ob. Cit. Pág. 83.
[10] Puccinelli, Oscar. Ibídem. Pág. 83.

la seguridad y defensa del Estado, la averiguación de los delitos y la Intimidad de las personas), y el artículo 20, numeral 1, literal *d* (que establece el derecho fundamental a comunicar y recibir libremente información veraz por cualquier medio), que se comienzan a desplegar en el Derecho Constitucional Indoiberomericano normas que tienden a reconocer estos derechos y a veces también tutelados mediante vías específicas (como es el caso de la Constitución peruana de 1993).

1.2.1 Protección de Datos en Europa y Estados Unidos de Norte América.

A principios del siglo XX, en pleno proceso de despegue del constitucionalismo social, se gestó en Alemania la simiente de lo que posteriormente sería, luego de mutaciones evolutivas, el derecho a la Protección de Datos Nominativos. En efecto, según explica SPOTA, el derecho a controlar la información personal nace, y en el plano constitucional, en 1919, cuando la Constitución de Weimar otorgó a los funcionarios públicos, entre otros derechos, el de examinar su expediente personal[11].

A excepción de este aislado precedente, sólo cuando los ordenadores mostraron un notable incremento en los riesgos provenientes del tratamiento

[11] Spota, Alberto A., disertación pronunciada en las Segundas Jornadas Nacionales sobre Temas Constitucionales Relevantes: "El amparo después de la reforma constitucional", Rosario, Argentina, 1/9/95, citado por Puccinelli, Oscar. Ibídem. Pág. 84.

de datos personales -esto es a partir de la década de los años setenta- comenzó el proceso de desarrollo normativo del derecho a la protección de datos. Así, los países tecnológicamente más avanzados (especialmente, los europeos) fueron elaborando paulatinamente la legislación específica sobre el tema, apuntando a establecer reglas concretas para enfrentar la nueva problemática.

Tal proceso no fue nada pacífico, pues surgieron dos pretensiones jurídicas contrapuestas, cuyo punto fundamental de disenso se centró en si cabía o no conceder facultades de intervención sobre los datos personales a favor de las personas concernidas. De tal forma, que frente a quienes propusieron un derecho a la protección de datos (con base en el derecho a la Intimidad), se alzaron voces que pretendían mantener el *staus quo*, es decir, no someter la problemática a regulación alguna, posición que no prosperó.

Desde aquél derecho *to be left alone* (estar solo) de COOLEY por WARREN y BRANDEIS[12] allá por 1890 en su ya tradicional opúsculo *The right to privacy* (el derecho a la Privacidad) publicado en el *Harvard Law Review* (Boletín de Derecho de Harvard), hasta la fecha, el concepto de *privacy* ha ampliado notablemente su contenido, no sólo en el derecho norteamericano, sino también en la totalidad de los países occidentales, y

[12] WARREN y BRANDEIS, citados por Puccinelli, Oscar. Ibádem. Pág.84

ciertos contenidos atribuidos a este por determinados ordenamientos, tienen, en otros, autonomía respecto de la Intimidad, o bien son absorbidos por otros derechos.

Como bien lo indica ZUÑIGA URBINA, “El Estado de la sociedad post industrial sumido en esta dialéctica de la socialización de lo estatal y estatalización de lo social, hace del derecho a la Intimidad no sólo una libertad negativa, sino también una libertad positiva; puesto que se trata no sólo de tutelar la subjetividad de la injerencia ajena (estatal o privada), sino de preservar la identidad y libertad frente al intenso e invisible poder informático. Así la privacidad o intimidad se convierte en un límite para el Estado, definiendo lo privado a partir de lo público, pero no reduciéndolo a lo estatal, dado que en sociedades organizacionales (R. MAYNTZ) como las actuales el poder informático está imbricado con la burocracia y la tecnocracia y tiene en los grandes grupos económicos y corporaciones su principal amenaza. En consecuencia, la ligazón «*privacy-property right*» propia del individualismo posesivo (MACPHERSON) está obsoleta [...] En la actualidad, el derecho a la intimidad conserva su núcleo original de libertad negativa (BERLIN) o *status libertatis* de «obrar o no obrar, sin ser obligado a ello o sin que se lo impidan otros sujetos» (BOBBIO). El derecho a la intimidad, en concreto su garantía procesal de *hábeas data*, es concreción de una libertad positiva, denominada libertad informática o derecho a la

autodeterminación informativa (PEREZ LUÑO, LUCAS MURILLO, LOSANO)"[13]

Con esta concepción, y tal como lo indica MORALES GODOS[14], el derecho a la intimidad cobra una dimensión mayor, por cuanto debe garantizar contra intrusión no consentida, los aspecto de la vida que uno reserva para sí y la información sobre la misma, y además debe proteger el desarrollo de la interioridad, de su poder ser, es decir, de la libertad. Hay un aspecto privadísimo de contenido negativo, que impide la intrusión en el ámbito privado de la persona; y un aspecto público, de contenido positivo que protege y garantiza la libertad personal.

Y esta proyección, según recuerda ZUÑIGA URBINA[15], podía observarse en el propio planteamiento de BRANDEIS, quien siendo miembro del Tribunal Supremo norteamericano, y en una célebre *dissenting opinio* en el caso "Olmstead vs. United States" (1928), premonitoriamente advirtió: "El gobierno dispone ahora de medios más sutiles y de más largo alcance para invadir la vida privada. Los descubrimientos y las invenciones han hecho posible para el gobierno obtener que se declare ante la Corte lo que se

[13] Zuñiga Urbina, Francisco: "El derecho a la intimidad y sus paradigmas", citado por Puccinelli, Oscar. Ibídem. Pág. 86.
[14] Morales Godos, Juan: "El derecho a la intimidad y el conflicto con el derecho a la información", Ponencias I Congreso Nacional de Derecho Civil y Comercial, noviembre 1993, Lima, Perú, citado por Puccinelli, Oscar. Ibídem. Pág. 87.
[15] Puccinelli, Oscar, citado por Puccinelli. Ibídem. Pág. 87.

murmura en el *toilette* [...] El progreso de la ciencia, que proporciona al gobierno nuevos métodos de espionaje, no se va a detener con el medio de interceptar los teléfonos. Quizás algún día se desarrollen los medios por los cuales se pueda reproducir papeles en los Tribunales sin sacarlos de los cajones secretos, y por los cuales el gobierno pueda exponer a jurado los más íntimos acontecimientos del hogar. Los progresos en la ciencia psíquicas pueden dar medios para explorar las creencias, pensamientos y emociones inexpresadas... ¿Es posible que la Constitución no proporcione protección alguna contra tales invasiones de la seguridad personal?"

La respuesta a la interrogante planteada la dio el tiempo, y particularmente la labor de la doctrina y la jurisprudencia norteamericanas; primero con el establecimiento de límites a la libertad de prensa y de ciertos requisitos conectados con el debido proceso en la obtención de pruebas, y luego, en el plano que nos ocupa, con las restricciones al tratamiento automatizado de datos, que se vio también plasmado en el plano legal con la *Fair Credit Reporting Act* de 1970, la cual según indica FROSINI[16], estaba destinada a proteger al cliente de las casa de crédito contra *difamation, invasion of privacy, or negligence* ... por parte de agencias de informació; así como también, la *Privacy Act* (Acta de Privacidad) de 1974, y en otras normas federales, como la *Right to Financial Privacy* (Norma para Privacidad

[16] FROSINI,citado por Piccinelli, Oscar. Ibídem. Pág. 89.

Financiera) de 1978 y la *Privacy Protection Act* (Acta de Protección de la Privacidad) de 1980, en un proceso que se trasladó casi coetáneamente, a los Estados Federales y al Reino Unido.

En lo que se refiere a normativa dirigida directamente a la Protección de Datos Personales, en el año de 1969 el Parlamento Inglés aprueba un acta de protección de las informaciones privadas, conocida como “Data Surviellance Bill”, la cual principalmente permitía declinar las intromisiones en la vida privada de las personas a través del uso indebido de informaciones del servicio electrónico; no obstante, es hasta en 1983 que se aprueba la Ley Inglesa de Protección de Datos Personales. Así mismo, la primera ley específica que surge con este fin es la Ley del Estado de Hesse, en Alemania en el año de 1970; luego surge la figura del Comisionado en la Protección de Datos, con la idea de ser una institución jurídicamente independiente y con la capacidad efectiva de controlarla actividad estatal, a fin de observar el respeto al derecho a la autodeterminación informativa. En 1977, el Parlamento Federal aprueba la Ley Federal de Protección de Datos (Bundesdatenschutzgesetz), la cual regula toda la Federación.

En Suecia se promulga una ley con el fin de la protección de datos personales contenidos en registros o bases de datos, y se instaura la figura del Comisionado para la Protección de Datos, dicha ley es la conocida como

Data Lag Sueca de 1973; en esta ley se instaura, además, una autorización especial para el procesamiento automático de los datos en el extranjero. En esa misma línea, en el año de 1965 en América pueden ser percibidas la raíces del Acta de Privacidad de 1974, cuando se llevaron a cabo algunas audiencias por el Subcomité Especial sobre Invasión de la Privacidad del Parlamento Legislativo de los Estado Unidos de Norte América.

Portugal fue el primer país europeo en constitucionalizar el derecho a los ciudadanos de controlar las informaciones que sobre ellos circulan, en el artículo 35 de su ley fundamental (1976); además, esta disposición prohíbe la creación de un documento único de identidad. Así mismo, en una reforma en el año de 1982 en el punto 1 del mismo artículo, se reconoce la Libertad Informática, prohibiendo también, en el apartado segundo, el acceso de terceros a ficheros con datos personales, así como su respectiva interconexión.

En 1978, en Francia nace un ente dedicado a la protección de datos personales, conocido como la Comisión Nacional de Informática y de las libertades, creada por la Ley 78-17 del 6 de febrero de 1978 “Informática, archivos y libertades”, estableciendo en su artículo primero que: “*La informática debe estar al servicio de los ciudadanos, su desarrollo debe operarse dentro del marco de la cooperación Internacional. No debe*

conllevar un atentado contra la identidad humana, los derechos humanos, la vida privada, ni las libertades individuales o públicas"[17]. La Constitución Española de ese mismo año, en su artículo 18.4 introduce una protección señalando que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"[18]; de igual manera, el artículo 105. b) presupone el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas; a principios de la década de los 90's que se crea la Ley Orgánica 5/1992 de 29 de octubre, regulando el tratamiento automatizado de los datos de carácter personal, y en la cual nace la Agencia de Protección de Datos Española, ente encargado de vigilar el cumplimiento de dicha ley. Siempre en el año de 1978, el 18 de octubre, en Austria se cre la Ley de Protección Datos, retomando la idea de Suecia y poniendo énfasis en el tráfico internacional de datos, y además introduce ciertas normas penales.

Ante la necesidad e importancia de proteger los datos personales reforzando a través de tratados comunitarios, en el marco de la Comunidad Europea se crea la **Convenció para la Protección de Individuos con**

[17] Loi n▫ 78-17 du 6 janvier 1978 Informatique, fichiers et libertés, citada por Alfaro Escoto, D. A., y otros. Ob. Cit. Pág. 6.
[18] Loi n▫ 78-17 du 6 janvier 1978 Informatique, fichiers et libertés, citada por Alfaro Escoto, D. A., y otros. Ob. Cit. Pág. 6.

respecto al procesamiento automático de Datos Personales[19], en Estamburgo, Francia el 28 de enero de 1981, creando el Comité Consultivo, cuya finalidad era facilitar la aplicación estricta de la Convención.

En 1990, la ONU dicta los Principios Rectores para la reglamentación de los Ficheros Computarizados de Datos Personales, adoptados por la Asamblea General en resolución 45/95 del 14 de diciembre de ese año[20]; principios en los cuales se recomienda enfáticamente a las legislaciones domésticas adoptarlos para asegurar una mayor eficacia a los derechos a que se dirige su protección.

El Parlamento Europeo y el Consejo de la Comunidad Europea adoptan la Directiva 95/46/CE de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, protegiendo especialmente la transfronterización de dichas informaciones en el flujo de capital humano en la Comunidad.

1.2.2 Protección de Datos en Latinoamérica.

La Constitución de Costa Rica de 1949, en su artículo 30 regula la garantía de libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público, dejando fuera de estas

[19] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 7.
[20] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 7.

posibilidades los secretos de Estado[21]. Así mismo, la Constitución de Guatemala de 1985, en su artículo 31 establece el derecho de acceder a archivos y registros estatales.

Lo que constituye un hecho reciente y novedoso concerniente a garantizar la protección de datos personales, es la incorporación en la Ley primaria de Brasil de la figura del Hábeas Data, la cual fue bautizada así por el Profesor de la Universidad de São Paulo, José Alfonso da Silva, con la idea de proteger derechos que se establecen con relación a la Libertad Informática. Es así como la Constitución Brasileña de 1988[22], en el artículo 5 inciso LXXII, fue la primera en utilizar esta figura y llamarla con este nombre, pues en otros países recibe denominaciones distintas, como en el caso de Estados Unidos en donde se hace referencia a ella como “The right to be let alone” (el derecho a ser dejado en soledad); así mismo, la Doctrina sentada por el Tribunal Constitucional Alemán se permite hablar de “Derecho a la Autodeterminación Informativa”.

Como ya se dijo antes, la Constitución Brasileña dispone: se concederá Hábeas Data: a) para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público, b) para la rectificación de datos, cuando no se prefiera hacerlo en proceso reservado

[21] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 8.
[22] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 9

judicial o administrativo[23]. En Brasil ocurre algo muy curioso; si bien es cierto que la figura en estudio fue introducida en 1988, se esperaba que su procedimiento como garantía fuera regulado en una ley ordinaria, pero no se fió así, ya que otorgado el derecho, permanecía ausente de procedimiento apropiado; aparentemente, esto no importó a los juristas brasileños, quienes le reconocieron plena eficacia a la norma constitucional; es así como, en determinado momento, el Juez pasó a actuar como legislador, ocurriendo que el Juez Federal de la Décima Sección Judicial del Estado de São Paulo, Paulo Octavio Baptista Pereira, concedió la primera decisión de Hábeas Data, adoptando el proceso (Rito) del mandato de seguridad por semejanza, señalando que: "la ausencia del procedimiento no lleva a la obstaculización del derecho. La laguna ausencia de la ley procesal que se presenta deberá ser suplida por integración de la norma analógica (lo que permite el artículo 126 del Código de Proceso Civil brasileño) que por las razones expuestas, entiendo que es la más apropiada frente a la cognición sumaria en el alcance de la prestación judicial postulada, aplicándose el rito de mandato de seguridad a la tramitación de hecho"[24]. Es hasta el año de 1997 que, con la Ley No. 9.507/97, se regula el derecho de Acceso a la Informaciones Personales y Disciplina el Rito de Hábeas Data.

[23] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 9 y 10.
[24] Baptista Pereira, Paulo Octávio: "Hábeas Data", citado por Alfaro Escoto, D. A., y otros. Ibídem. Pág. 10.

Así mismo, la Constitución de Paraguay del 20 de junio de 1992, establece expresamente el Hábeas Data en su artículo 135, disponiendo lo siguiente: "*Toda persona podrá acceder a la información y a los datos que sobre sí misma o sobre sus bienes en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad, para solicitarse ante el magistrado competente la actualización, rectificación o la destrucción de aquellos, si fuesen erróneos o afectaren ilegítimamente los derechos*"[25]. En Paraguay, la figura en comento se extiendo no sólo para proteger derechos personalísimos, sino también derechos patrimoniales.

La Constitución Argentina de 1994, en su artículo 43 regula que: "Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista «otro medio judicial más idóneo», contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un Tratado o una Ley"; además, en el inciso tercero establece: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados o proveer informes, y en caso de falsedad o discriminación, para

[25] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 11.

exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística"[26]. Como puede observarse, en Argentina no se incluye literalmente la figura como tal; sin embargo, en algunos fallos de sus tribunales se le ha llamado Hábeas Data, al amparo.

1.2.3 Protección de Datos en El Salvador.

En nuestro país, hasta el momento no existe una ley especialmente dirigida a brindar protección a los datos personales, pero existen normas dispersas en el ordenamiento normativo jurídico, tanto a nivel constitucional como legislativo.

A nivel constitucional, se da un mecanismo específico de control de las informaciones personales, en la constitución de 1983, en su artículo 6 llamado Derecho de Respuesta; otra norma constitucional a la que se le pudiese inferir dicha protección es el artículo 2 de la Constitución, en cuanto contempla el derecho al honor, intimidad familiar y propia imagen. A nivel internacional existen algunos instrumentos suscritos y ratificados por El Salvador y que pasan a formar parte de sus leyes internas de acuerdo al

[26] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 11.

artículo 144 CN, estos instrumentos pueden ser divididos en Universales y Regionales[27].

En lo que respecta a los INSTRUMENTOS UNIVERSALES: La Declaración Universal de los Derechos Humanos, acarrea obligaciones jurídicas, como los tratados que están sujetos a suscripción, adhesión, aceptación y ratificación; en su articulo 12 establece que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, familiar, su domicilio o correspondencia, ataques contra su honra o reputación. En el mismo marco de la ONU, se aprueba la Convención sobre el Derecho Internacional de Rectificación, el cual tiene mayor énfasis en aspectos tales como: hacer efectivo el derecho de los pueblos a estar plena y fielmente informados, mejorar la mutua comprensión entre los países mediante la libre circulación de las informaciones y opiniones entre otros. En la misma línea de ideas, el articulo 14 del Pacto Internacional de Derechos Civiles y Políticos establece una protección para quienes intervienen en los juicios, en el sentido de facultar a los jueces de aplicar reservas totales o parciales en procesos donde por consideraciones de moral, orden publico o seguridad nacional en una sociedad democrática, o cuando lo exija el interés de la vida privada de las partes. De manera especial para los menores de edad, la Convención Sobre los Derechos del Niño establece que ningún niño será objeto de

[27] Alfaro Escoto, D. A., y otros. Ibídem. Pág. 12 y 13

injerencias arbitrarias o ilegales a su honra y reputación; en el articulo 14, La Convención garantiza al niño el acceso a la información que tenga por finalidad promover su bienestar social, espiritual y moral y su salud física y mental.

En lo relativo a los INSTRUMENTOS REGIONALES: El Preámbulo de la Declaración Americana de los Derechos y Deberes del Hombre, establece que la moral y las buenas costumbres constituyen la floración más noble de la cultura, por lo que es deber de todo hombre acatarlas siempre[28]; de igual manera, el artículo 5 establece la protección a la honra, la reputación personal y la vida privada y familiar. En ese orden de ideas, el articulo 5 de la Convención Americana sobre Derechos Humanos, reconoce el derecho a la integridad personal en el sentido físico, psíquico y moral, y presupone además, la publicidad de los juicios, estableciendo la salvedad en aquellos que sea necesaria su reserva por razones de preservar los intereses de la justicia. Otro derecho considerado importante, es el reconocido en el artículo 13, con respecto a la libertad de pensamiento y expresión el cual conlleva también la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, en las formas que en él se expresan[29].

[28] Alfaro Escoto, D. A., y otros. Ibídem. Pág. 15
[29] Alfaro Escoto, D. A., y otros. Ibídem. Pág. 16

En lo que se refiere a la protección de los derechos al honor, intimidad personal y familiar y propia imagen, se encuentran disposiciones en el código penal; cuerpo normativo en el cual se desarrolla el Titulo VI denominado Delitos relativos al honor y la intimidad, dentro del cual, el capitulo I , De la Calumnia y la Injuria comprende del articulo 184 al 191. Asi mismo, el Código Procesal Penal en el artículo 272 establece la publicidad del proceso penal y aquellas causales de excepción como la moral, el interés público y la seguridad nacional. De igual manera, el artículo 327, establece que la audiencia será pública cuando se refiere al juicio, estableciendo las mismas causales de excepción que se mencionaron anteriormente.

Otras normas Jurídicas relacionadas con el tratamiento de datos personales, la vida privada y los derechos son: El Código de Procedimientos Civiles, el cual regula lo referente a los actos previos a la demanda, dentro del cual el articulo 156 establece el derecho que tiene toda persona, cuando va demandar a otra, de pedirle que se exhiba ante el juez, los documentos públicos o privados objetos de la demanda o la defensa en su caso; una disposición similar es la que se contempla en el Código de Trabajo en el articulo 406 al permitir la exhibición de planillas o recibos.

Además, se cuenta con algunas normas tendientes a la rectificación de datos erróneamente procesados, dentro de las cuales se encuentran: la

Ley del Ejercicio Notarial de la Jurisdicción Voluntaria y de otras diligencias, la cual en su articulo 11, en lo que respecta a las omisiones u errores en partidas de nacimiento en el Registro del Estado Familiar, así como en el articulo 31, en lo relativo al establecimiento de la identidad personal.

El artículo 3 de la Ley Transitoria del Registro del Estado Familiar y de los Regímenes Patrimoniales del Matrimonio, establece la publicidad de la información y la obligación de tomar medidas tendientes a la protección de la misma, y su artículo 17 presupone la rectificación y subsanación de los asientos.[30]

Como se ha señalado, El Salvador, al igual que Costa Rica y Panamá, se incluye dentro del bloque de países que carece de disposición constitucional relativa al Hábeas Data, pero que han concentrado sus esfuerzos regulatorios en la creación de leyes procesales sobre este instrumento; y aunque en nuestro país no existe aún un reconocimiento constitucional ni legislativo del Hábeas Data, este ha sido aceptado por la Sala de lo Constitucional de la Corte Suprema de Justicia[31], la cual en sentencia de fecha 2 de marzo de 2004, señaló: "*El hábeas data constituye un mecanismo o instrumento que protege al individuo contra el uso ilegal o*

[30] Alfaro Escoto, D. A., y otros. Ibídem. Pág. 18
[31] Proceso de Amparo Constitucional No. 118-2002, citado por Ayala, José María y otros: "La Protección de Datos Personales en El Salvador". Pág.59.

indebido de los datos personales de un individuo por parte de entidades públicas o privadas, tutelando de una forma eficaz el derecho a la autodeterminación informativa. De tal manera que constituye una garantía cuyo fundamento en la normativa constitucional responde a la necesidad de los sujetos de proteger sus derechos ante la amenaza del acceso y uso indiscriminado de sus datos personales".

De esta forma, el derecho a la Autodeterminación Informativa, como manifestación del derecho a la Intimidad, no queda totalmente desprotegido, pues, como ya se dijo antes, se reconoce este recurso a partir del principio general del inciso primero del artículo 2 de la Constitución, en cuanto expresa que "Toda persona tiene derecho a [...] y a ser protegida en la conservación y defensa de los mismos"; así mismo, el artículo 247 de la Constitución, en su primer inciso señala que "Toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución". De esto se infiere que los derechos reconocidos, tanto explícita como implícitamente, deben ser garantizados a toda persona a través de los mecanismos de protección establecidos para su ejercicio. De tal manera que, aún y cuando no se disponga hasta el momento de una Ley que prescriba los presupuestos procesales para materializar la figura en estudio, puede decirse que la protección del derecho en mención puede (y debería ser así) efectuarse a

través del proceso constitucional de amparo, sin importar la naturaleza de la empresa o el ente a quien se le atribuya la vulneración de dicho derecho.

En ese orden de ideas, aún y cuando en nuestro país el derecho a la Autodeterminación Informativa se encuentra resguardado en el Art. 2 Cn., formando parte del contenido esencial del derecho a la Intimidad de la persona, por ser uno de los países latinoamericanos que no cuenta aún con una regulación de la Libertad Informática, ha intentado hacer surgir el Hábeas Data de la Tutela Constitucional del derecho a la Intimidad,[32] pero no lo ha logrado. Esto puede deberse a que, como la Libertad Informática y principalmente la Autodeterminación Informativa se ha concebido como manifestación del derecho a la Intimidad, esta se ha dejado a la atención de los operadores jurídicos; debido a que *el derecho a la intimidad tiene un contenido amplio, surgiendo posturas diversas para enumerar su contenido e independizar o mantener unidas sus manifestaciones*[33]. En ese sentido, a pesar que dentro del Art. 11 de la Constitución de la República, se reconoce las garantías que toda persona tiene para protegerse ante violaciones de sus derechos como la Intimidad, señalando al Hábeas Corpus a utilizar ante detenciones arbitrarias o ilegales, y el Amparo para violaciones al derecho a la Intimidad propiamente dicho, ante la falta de regulación expresa del Hábeas Data como figura autónoma, es que se utiliza el Amparo ante la

[32] Ayala, José María y otros. Ob.Cit. Pág. 27
[33] Ayala, José María y otros. Ibídem. Pág. 25

violación del derecho a la Intimidad por posibles abusos en el tratamiento de datos personales, dejando a la atención de los operadores jurídicos la decisión: si estos casos de abusos en el tratamiento de datos personales se ubican o no dentro del contenido del derecho a la Intimidad. Así mismo, no existen sentencias de la Sala de lo Constitucional por violaciones al derecho a la Libertad Informática o Autodeterminación Informativa, no porque en la práctica no existan violaciones a ese derecho, sino por el poco conocimiento o total desconocimiento que la mayoría de los salvadoreños tienen sobre este. No obstante que la Jurisprudencia de la Sala, ha reconocido el derecho a la Autodeterminación Informativa, entendido como manifestación del derecho a la Intimidad, esto se hizo mediante interpretación constitucional, señalando la necesidad de establecer una garantía reforzada para su eficacia, siendo esta el Hábeas Data; aclarando, además que no existe una disposición constitucional que regule expresamente la facultad de limitar el uso de la informática para preservar los derechos fundamentales, mucho menos una normativa secundaria eficaz que contenga los principios básicos del tratamiento de datos personales con la garantía del Hábeas Data. En consecuencia, es importante y necesario reformar nuestra Carta Magna con el fin de limitar el uso de la informática para garantizar el derecho a la Libertad Informática o Autodeterminación Informativa y el pleno ejercicio de los derechos relacionados con este.

No se trata de definir un nuevo derecho, sino de reconocer que el avance de las nuevas tecnologías y el uso de la información en las sociedades deja la puerta abierta a áreas que no han estado sujetas, hasta ahora, a ninguna regulación normativa en nuestro país. Si bien es cierto que la aplicación de las nuevas tecnologías de información en El Salvador es particularmente inferior a la de otros países, eso no significa que el acceso y la protección de datos personales no deban ser considerados como prioridad en el manejo de la información, ya sea en registros automatizados o manuales, tanto públicos como privados.

En definitiva, y tal como lo señala JOSÉ MARÍA AYALA[34], "*la Autodeterminación Informativa y su garantía constitucional, el Hábeas Data, constituyen elementos indispensables para la protección contemporánea de la vida privada, en tanto que, a través de los mismos se definen y se protegen aquellas informaciones que no deben ser objeto de tráfico, transmisión o uso, sin conocimiento y consentimiento de su titular*".

1.3 EL HABEAS DATA EN EL SALVADOR.

Como ya se ha dicho en apartados anteriores, frente a todo el avance informático en El Salvador, que representa una prioridad gubernamental, por

[34] Ayala, José María y otros. Ibídem. Pág. 61.

representar el progreso social y la competitividad de su economía, y la utilización cada vez mayor de la informática por empresas nacionales y extranjeras y por la administración pública, y un incremento en el tratamiento de datos personales en el país, debido a esto nace la pregunta sobre cómo controlar la difusión de la información personal, si es posible este control y que tipo de barreras pueden oponerse al avance de la divulgación de la información.

Sin ninguna duda, deberían existir límites ya que no toda información que puede originar una persona es relevante social o públicamente. Incluso, información referida a situaciones exclusivamente personales, puede llegar a ser utilizada en forma discrimatoria y conculcatoria de sus derechos personales y garantías individuales. Así, junto al progreso tecnológico deben nacer leyes que eviten los abusos de la tecnología. En ese sentido, se tratará de realizar un análisis acerca de la necesidad de proteger los datos en El Salvador; además se expondrá, en su momento, el marco político, legislativo y jurisprudencial actual en el cual se enmarca una regulación de datos personales.

1.3.1 Fundamentación de la necesidad de proteger los datos en El Salvador.

La protección de la información en El Salvador, específicamente en materia de tratamiento de datos o informaciones personales, no está definida en una Ley o norma que reúna o trate de analizar, en forma sistemática, el tema, sino que, al contrario, existe un alto de grado de dispersión.

En El Salvador existen instituciones que poseen y gestionan bases de datos, desde el Servicio Nacional de Estadísticas, las instituciones encargadas de registrar y proteger la propiedad intelectual, hasta los servicios de administración de justicia y policíaca, quienes también gestionan información diversa sobre víctimas, imputados, condenados, etc. Diversas instituciones han tratado, en los últimos años de efectuar investigaciones y aportar elementos para el desarrollo de políticas públicas vinculadas con la protección de datos personales, así como también para evitar la concentración de información o la negación de la misma tanto a particulares como a instituciones privadas o públicas.

Sin embargo, las iniciativas han sido parciales en diversos aspectos. En primer lugar, han implicado el desarrollo de ciertas áreas del acceso a la información y la protección de datos, pero se han quedado cortas en su desarrollo en otros contenidos. Por otra parte, han sido iniciativas que pretenden abrir o generar una cultura de acceso a la información y respeto o

protección de la información o de los datos personales dentro de sectores o instituciones específicas, por lo que tampoco existe un marco amplio que regulen los ficheros de titularidad pública y, sobre todo, que detalle cómo debe ser la relación entre el acceso a la información y la protección de datos personales.

Por otra parte, diversos escándalos, nacionales y regionales relacionados con el tratamiento de datos han despertado inquietud entre la opinión pública. Recientemente, una empresa estadounidense compró los datos personales de millones de ciudadanos de Argentina, Colombia, El Salvador, Guatemala, Honduras, Nicaragua, Venezuela y Brasil, que incluyen información sobre nombres, nacimiento, filiación, domicilio, números telefónicos, antecedentes legales, cuentas bancarias y propiedad de viviendas. Estos datos fueron a parar diversas agencias de seguridad americana. El lucro de la empresa fue muy elevado, mientras que a los titulares de los datos pudieran denegárseles sus visas para viajar a Estados Unidos[35].

Es indudable la inquietud que despiertan, también en El Salvador, las empresas dedicadas a la venta de información o a la creación de ficheros o archivos, públicos y privados, con información obtenida para el manejo de las

[35] Ayala, José María y otros. Ibídem. Pág. 139.

instituciones o la toma de decisiones empresariales. Los titulares de los datos ignoran quién posee esta información[36].

Ante esta situación de incertidumbre, la regulación de la protección de datos o Autodeterminación Informativa en El Salvador, podría ayudar a establecer criterios garantías ligados a la tutela de la persona y a la construcción democrática. Por ello, la protección de datos es, a la vez, un compromiso político y un instrumento de política pública, que deben plasmarse en una norma específica cuidadosamente elaborada y puesta en práctica.

1.3.2 Fortalecimiento de la Democracia.

La regulación de los datos personales y la sujeción de los tratamientos a los principios de calidad, información, consentimiento, y a derechos de acceso, rectificación, cancelación y oposición constituye un elemento más en el proceso de fortalecimiento de la democracia en El Salvador.

Hay que tener presente que la protección de datos mejora el acceso a la información que está en poder de instituciones públicas que incluye tres grandes áreas[37]:

[36] Ayala, José María y otros. Ibídem. Pág. 139 y 140.
[37] Ayala, José María y otros,. Ibídem. Pág. 140.

a) El derecho de cada uno a acceder a la información personal propia almacenada en los archivos o documentos del Estado.

b) El derecho de acceso a información relevante para la persona, la cual se halle almacenada en archivos, registros o documentos públicos.

c) La posibilidad de tratar y divulgar la información pública de forma que el acceso a los concursos públicos sea lo más transparente posible.

El afán de promover el máximo acceso a la información posee diversos fines. Por una parte, se relaciona directamente con políticas de transparencia de la Administración, transparentar el Estado, lo cual favorece la confiabilidad en las instituciones frente a terceros, ya sean empresas privadas, instituciones públicas o entes internacionales, en tanto que dicho acceso facilita o, mejor dicho, permite un trato igualitario al brindar la información sin ningún tipo de elementos discrecionales o discriminatorios. Por otra parte, también permite un mayor control de la gestión pública por parte del ciudadano o de la ciudadana, lo cual facilita una especie o variante de las políticas de rendición de cuentas. Estas han sido señaladas como elementos beneficiosos para establecer mayores índices de legitimidad, transparencia y confianza de la ciudadanía hacia las instituciones.

En este contexto, se está utilizando el concepto de Información en un sentido amplio, incluyendo noticias, declaraciones, datos, opiniones, proyecciones, etc. Tal vez la característica fundamental de la información es

su carácter de medio o instrumento para el ejercicio de otros derechos, por lo que su tutela permite también la mejor realización de los derechos de la persona. Además, la información puede tener un carácter de bien público o colectivo, pues no se limita a generar un bien individual, sino que cobra un marcado carácter público o social. Funcionalmente, ese carácter público o social tiende a relevar el empleo instrumental de la información no como – o no sólo como – factor de autorrealización personal, sino como un mecanismo o andamiaje de control institucional, tanto frente a autoridades públicas como frente a particulares, cuya situación de poder de injerencia o inducción permite la determinación de conductas de otros particulares o su misma subordinación.

ABRAMOVICH y CURTIS[38] señalan que existen evidentes vínculos entre esta concepción, una noción participativa de la democracia y la consideración del respeto de los derechos fundamentales como fuentes de legitimación del ejercicio del poder. En este sentido, el acceso a la información pública es un derecho fundado en una de las características principales del gobierno republicano que es el de la publicidad de los actos de gobierno y la transparencia de la Administración.

[38] Ayala, José María y otros. Ibídem. Pág. 63

Esta característica se explica a partir de los propios cimientos del ejercicio del gobierno representativo: la representación democrática tiene carácter temporal, y el ejercicio de las funciones públicas, en nombre de la representación otorgada por el pueblo soberano, esta abierta al refrendo o escrutinio de la población en cuyo nombre se gobierna a través del voto. Por ello, la publicidad de los actos de gobierno constituye el mejor factor de control, o bien de legitimación del ejercicio del poder por parte de los representantes[39].

No cabe duda entonces, de que el acceso a la información en sentido amplio es un derecho necesario dentro de los Estados contemporáneos, el cual ha sido recogido en innumerables declaraciones y pronunciamientos de entes internacionales y de derecho comparado.

Por otro lado, los organismos garantes de la tutela internacional de los Derechos Humanos se han pronunciado, en el sentido de que el acceso a la información constituye un área fundamental del derecho a la libertad de expansión. Así, en 1999, la Asamblea General de las Naciones Unidas aprobó la "Declaración sobre el derecho y el deber de los individuos, los grupos y las instituciones, de promover y proteger los derechos humanos y las libertades fundamentales universales reconocidas", y, dentro de dicha

[39] Ayala, José María y otros,. Ibídem. Pág. 142.

declaración, en su articulo seis, establecido lo siguiente: " Toda persona tiene derechos individualmente y con otras: a) a conocer, recabar obtener, recibir y poseer información sobre los derechos humanos y libertades fundamentales, con inclusión del acceso a la información sobre los medios por los que se da efecto a tales derechos y libertades, en los sistemas legislativos, judicial y administrativo internos; b) conforme a lo dispuesto en los instrumentos de derechos humanos y otros instrumentos internacionales aplicables, a publicar, impartir o difundir libremente a terceros, opiniones, informaciones y conocimientos relativos a todos los derechos humanos y libertades fundamentales; c) a estudiar y debatir si esos derechos y libertades fundamentales se observan, tanto en la Ley como en la práctica y a formarse y mantener una opinión al respecto, así como a señalar la atención del público esas cuestiones por conducto de esos medios y de otros medio adecuados[40].

En El Salvador, el derecho de acceso a la información está resguardado o garantizado no por una, sino por diversas disposiciones que coinciden en los objetivos y protección del contenido de acceso a la información. En ese sentido, puede relacionarse el acceso a la información con el derecho contenido en el Art. 6 de la Constitución salvadoreña, en donde se consagra el derecho a la libertad de expresión. De ahí se deduce

[40] Ayala, José María y otros,. Ibídem. Pág. 144.

que el acceso a la información permite el libre flujo de datos e informaciones y facilita el conocimiento de la cosa pública.

Por otra parte, el derecho de acceso a la información está sustentado también en el Art. 2 de la Constitución salvadoreña, en tanto que el escrutinio y la disposición de la información en las instituciones públicas, debe ser del conocimiento de la ciudadanía, especialmente cuando esa información la pueden conocer terceros, es decir, su manejo “podría incidir en la esfera de su intimidad personal y familiar y en la propia imagen.

En forma genérica, el acceso libre a la información también está resguardado por el derecho general de libertad contenido en el Art. 8 de la Constitución de El Salvador, así como en el Art. 12 de la Declaración Universal de los Derechos Humanos de 1948, el Art. 17 del Pacto de Derechos Civiles y Políticos de 1966, el Art. 11 del Pacto de San José de 1969, el Art. 16 de la Declaración Universal de los Derechos del Niño, y en los Arts. 5,9 y 10 de la Declaración Americana de los Derechos Humanos de 1948, todos ratificados por el Estado de El Salvador.

En otras palabras, se trata de apostar por la construcción de un cultura humanista y abierta, que permita la organización de la información y su

accesibilidad por parte de la ciudadanía para que ésta pueda disponer de ella, reflexionar sobre ella y utilizarla.

El acceso a la información puede inducir cambios en las sociedades, ya que influye en los hábitos o las orientaciones de los individuos o de las instituciones, fomenta u orienta la elección de empleo y formación, fomenta la inversión, lleva a introducir nuevos productos en el mercado, promociona servicios como el Turismo, y otras ventajas que permiten abrirse en forma transparente a mercados altamente competitivos. Por lo tanto, el acceso a la información en poder del Estado es, en lo fundamental, un vehículo para el ejercicio de la Democracia.

1.3.3 Fundamento en el Carácter Autónomo de la Protección de Datos.

La protección de datos es un derecho que procede de la misma tutela de la Intimidad, aunque posee connotaciones específicas que le dan cierta autonomía. Este derecho protege las relaciones personales y familiares, afectivas y de filiación, las creencias y preferencias religiosas y sexuales, las convicciones personales y políticas, etc., y es lo suficientemente amplio como para proteger también las agresiones a la vida privada de las personas, que puedan provenir del tratamiento abusivo de sus datos personales. Puede afirmarse que el derecho a la Intimidad es un derecho fundamental, en virtud

del cual se debe excluir o negar el acceso del conocimiento de ciertos aspectos de la vida de cada persona a terceros.

La protección de datos se ha vuelto autónoma respecto del derecho a la Intimidad, de ahí la necesidad de una regulación *ad hoc*, ya que no es suficiente con lo ya regulado sobre la Intimidad. En definitiva, los datos que hay que proteger no son solamente los que atañen a la vida íntima del individuo en el sentido tradicional. La sociedad actual impone ser muy amplios en cuanto a los datos que se protegen, porque un dato cobra importancia ante las posibilidades técnicas, comerciales y psicológicas publicitarias de crear perfiles, prever conductas y anticipar comportamientos. En tal sentido, el bien jurídico que nace en esta sociedad de la información rebasa el bien jurídico de la Intimidad y se conceptualiza como Privacidad.

La tecnología y la capacidad de tratar, cruzar y utilizar datos personales ha gestado, en nuestras sociedades contemporáneas, nuevos derechos, como el de la autodeterminación Informativa, los cuales se relacionan con los derechos tradicionales e incluso permiten fortalecerlos.

La protección de datos y su garantía constitucional, el Hábeas Data, se consideran elementos indispensables para la protección contemporánea de la vida privada, en tanto que, a través de los mismos, se definen y se

protegen aquellas informaciones que no deben ser sujetas de tráfico, transmisión o uso, sin conocimiento de su titular. La autodeterminación Informativa define un ámbito material de protección de la Intimidad, que abarca la revelación, el uso y la protección de datos personales, tanto para la elaboración de registros públicos y privados, como por la posibilidad de su transmisión; de esta manera, siguiendo a ANTONIO ORTI VALLEJO[41], la Autodeterminación Informativa se constituiría en una subdivisión del derecho a la Intimidad que protege a la persona frente a la utilización, la disposición, el registro y la transmisión informática de sus datos personales.

El objeto de una normativa que proteja el ámbito jurídico de la Intimidad, que se puede denominar Autodeterminación Informativa, es doble: que los ciudadanos y las ciudadanas controlen el uso que se hace de sus datos personales, y permitir a estos el acceso a los registros y archivos públicos, para conocer la información que se maneja concerniente a su persona.

1.4 MARCO JURISPRUDENCIAL DE LA PROTECCION DE DATOS EN EL SALVADOR.

La Sala de lo Constitucional de la Corte Suprema de Justicia ya se ha

[41] Orti Vallejo, Antonio, citado por Ayala, José María y otros. Ibídem. Pág. 65.

pronunciado sobre el derecho a la Protección de Datos en El Salvador, en el proceso constitucional de Amparo número 118-2002, en cuya Sentencia Definitiva de fecha 2 de marzo de 2004, señala que 'El *hábeas data* constituye el mecanismo o instrumento que protege al individuo contra el uso ilegal o indebido de los datos personales por parte de entidades públicas o privadas, tutelando de una forma eficaz el derecho a la autodeterminación informativa. De tal manera que constituye una garantía cuyo fundamento enla normativa constitucional responde a la necesidad de los sujetos de proteger sus derechos ante la amenaza del acceso y uso indiscriminado de sus datos personales. En términos generales, se trata de un instrumento judicial que entra en funcionamiento a petición de parte, cuando ésta ha cumplido con el requisito prejudicial de solicitar a la empresa que posee o maneja sus datos personales, le exhiba los mismos con el objeto de verificar los que han sido incluidos en los ficheros automatizados y comprobar la veracidad de los mismos. De no obtenerse la respuesta requerida, el Estado, a través de dicho mecanismo, interviene solicitando la exhibición modificación, supresión, o actualización de los datos, según el caso, con la consiguiente responsabilidad civil para la empresa demandada en caso de comprobarse la vulneración al derecho en cuestión, sin perjuicio de la responsabilidad penal a que hubiere lugar. Países como Brasil o España son ejemplo de tener dicha regulación en su sistema jurídico a través de leyes específicas.

Si bien en el ordenamiento jurídico salvadoreño no aparece la figura del *habeas data* como instrumento diseñado para la protección específica del derecho a la autodeterminación informativa, como manifestación del derecho a la intimidad, ello no significa que tal derecho quede totalmente desprotegido, pues partiendo de lo que establece el inc. 1º del art. 2 Cn., que "toda persona tiene derecho (...) a ser protegida en la conservación y defensa de los mismos" y asimismo el art. 247 de la misma Carta Primaria, también en su primer inciso sostiene: "Toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución"; se infiere que los derechos reconocidos expresa como implícitamente, deben ser garantizados a toda persona a través de los mecanismos de protección establecidos para su ejercicio. De manera que, aunque no se disponga de una ley que prescriba los presupuestos procesales para materializar tal figura, se puede decir que la protección del derecho en mención puede ser efectuada a través del proceso constitucional de amparo, no importando la naturaleza de la empresa o ente a quien se le atribuya la vulneración de dicho derecho(…)[42]

A consideración del honorable Tribunal, el objeto de regulación de protección de datos en El Salvador es doble: que la ciudadanía controle el uso que se hace de sus datos personales, y permitir a ella el acceso a los registros y archivos públicos, para conocer qué información se maneja

[42] Ver primera parte de Anexo Número Tres.

concerniente a su persona. Así mismo, se reconoce los esfuerzos realizados por el demandante, quien interpuso el primer amparo en materia de protección de datos, el cual constituye la única experiencia jurisprudencial con la que cuenta la Sala de lo constitucional en materia de protección jurisdiccional extraordinaria sobre este derecho fundamental, ya que otros intentos de pretensiones relacionadas con el mismo fueron rechazadas.

En relación a lo anterior, la Sala se ha pronunciado también en el proceso de Inconstitucionalidad No. 36-2004, en particular contra los incisos 30 y 40 del artículo 201 de la Ley de Bancos, en cuya Sentencia Definitiva de fecha 2 septiembre de 2005, se señala que "… se advierte que, en los diferentes países en los cuales se ha articulado el hábeas data como mecanismo de protección del derecho a la autodeterminación informativa, se ha proporcionado un tratamiento procesal de diversa índole. Así, existen ordenamientos jurídicos que han creado un proceso específico desarrollado en la ley secundaria; mientras que en otros, se sigue el trámite de la vía de tutela común al resto de derechos fundamentales —v. gr. el amparo—. Asimismo, algunos países aplican al instituto las pautas generales relativas al amparo —aunque con algunas particularidades— creándose una modalidad de este proceso o un amparo especializado.

Por regla general, al analizar la experiencia de estos Estados, la

doctrina coincide en que lo más conveniente para maximizar la protección del derecho a fa autodeterminación informativa es la emisión de una normativa especializada que contemple —entre otros— la articulación de un proceso específico, distinto al resto de procesos constitucionales…"[43]

Las disposiciones impugnadas se vuelven contrarias a la Constitución de la República, ya que la autodeterminación informativa de las personas se anula con aplicación abierta y arbitraria de las normas legales citadas. Esto se debe a que a los titulares de los datos se les niega el derecho de control eficaz de los mismos; lo cual es contrario a lo que ha sostenido la Sala, al expresar que a los titulares se les permite el acceso a sus datos para comprobar su veracidad o requerir su exclusión, cuando lo fines por los que fueron incluidos en la base de datos hayan desaparecido. En primer lugar, porque el derecho de acceso debe ser gratuito para el titular de los datos y, hoy por hoy, hay que pagar por ejercer dicho control; y en segundo lugar, porque no se informa al titular que sus datos son objeto de tratamiento ni qué personas acceden a ellos, además de que dichas bases se usan para fines distintos de los previstos. En consecuencia, tales preceptos legales son indeterminadamente abiertos, que carecen, a parte de una claridad normativa, de toda garantía mínima para preservar el ejercicio de los derechos constitucionales señalados; el cual es requisito indispensable en

[43] Ver Segunda Parte de Anexo Número Tres.

una sociedad democrática, como lo estipula la Constitución

CAPITULO II
2. ELEMENTOS DOCTRINARIOS SOBRE EL DERECHO A LA INTIMIDAD.

La evolución e interacción constante de la sociedad ha avanzado sobre la intimidad de las personas, y se asiste a diario a una solicitud de información y de datos que en muchos casos aparecen innecesarios o sobreabundantes para el tipo de actividad o gestión que se realiza; existe un interés desmedido e incesante de obtener información con la justificación social de que mientras más conocemos al individuo común, mas sabremos de la sociedad en la que vive, lo que lleva a una desmedida búsqueda de información individual, que pone de manifiesto la necesidad de un control en el flujo de información que se encuentra almacenada en ficheros y base de datos.

En el presente capitulo se realizará un estudio de los aspectos básicos del derecho a la intimidad, dado que en virtud de la presente investigación se hace necesario esclarecerlo, por la amplitud en su estructura y desarrollo a si como en su esfera de protección lo abordaremos en relación a la presente

investigación, es decir, al tratamiento automatizado de datos personales en archivos o registros públicos o privados.

2.1 EL DERECHO A LA INTIMIDAD.

2.1.1 Concepto y Diferencia con la Privacidad.

La Intimidad Humana, es una necesidad del hombre en su intento por vivir en una sociedad que le permita un desarrollo integral de su personalidad. La Intimidad conlleva el concepto de lo secreto, de lo reservado. Puede decirse que todo lo íntimo es secreto, aunque no todo lo secreto proviene de lo íntimo.

"En su origen etimológico, Intimidad proviene del término INTUS (dentro), superlativo de interior"[44]. Es decir, se refiere no sólo a los que está adentro, sino a los que está más adentro.

Ahora bien, es de suma importancia abordar la Intimidad ya como un derecho fundamental de la persona. En ese sentido, puede decirse que la Intimidad es un derecho natural del hombre o un derecho humano consagrado en Convenios y Tratados Internacionales, que posteriormente se

[44] C. Méjan, Luis Manuel: "El derecho a la Intimidad y la Informática", citado por Alvarado Bonilla, K.M. y otros: "Hábeas Data como Garantía de Protección de la Persona frente al Tratamiento de sus Datos Personales". Pág. 51.

incorporaron al derecho positivo en constituciones de determinados Estados que convirtieron esta garantía en derecho fundamental.

Así, el derecho a la Intimidad es inherente a la persona humana, ya que para que el hombre se desarrolle o geste su propia personalidad e identidad, es necesario que goce de un área que comprenda diversos aspectos de su vida individual y familiar, que esté libre de la intromisión de extraños. Por lo que se hace necesario establecer qué se debe entender por derecho a la Intimidad; en ese orden de ideas, se dice que el derecho a la intimidad concebido como poder o potestad de tener un domicilio particular, papeles privados, ejercer actividades, tener contactos personales, y pensamientos que no trascienden a terceros, en virtud del interés personal de mantenerlos en reserva y la discreción de quien se entera de no hacerlos públicos, cuando se trata de hechos privados o datos sensibles de las personas, cada vez se encuentra más jaqueado por un interés desmedido e incesante de obtener información.

La pretendida justificación “social” de algunos, afirman que *mientras más se conoce al individuo común, se tendrá un mayor conocimiento de la sociedad en la que vive, sus problemas y posibles soluciones, los lleva a una desmedida búsqueda de información individual; para otros, la justificación es económica y se sustenta en “darle a cada uno el producto que necesita”;*

también cuenta con otros que asientan en un interés político, basado en la supuesta necesidad de dar respuestas al electorado[45]. Ninguna de ellas se basta a sí misma, así como tampoco su sumatoria es relevante para tamaña desproporción de conocimiento y avance sobre la Intimidad de las personas.

A partir de la anterior definición de Intimidad, corresponde averiguar cuál es la relación que existe entre ésta y lo privado; para lo cual, se citará diferentes corrientes y autores al respecto. Para algunos, lo privado es el género que incluye como núcleo central a la Intimidad; la Intimidad sería la parte más reservada de la vida privada. Otra corriente señala que la Privacidad se refiere al ámbito de las acciones privadas que no afectan a terceros, aunque puedan ser conocidas por éstos, y que la Intimidad se refiere al ámbito personal que no es o no debería ser conocido por los demás, por ejemplo, opiniones sexuales, divulgación de fotografías sin autorización, etc.

Por otra parte, ALBERTO S. BIANCHI[46], manifiesta un pensamiento contrario, ya que no encuentra ninguna diferencia relevante entre lo íntimo y lo privado. Ambas opiniones dan una idea de algo reservado a donde sólo tienen acceso ciertas personas. Así por ejemplo, una reunión es íntima o privada cuando asisten a ella algunas personas elegidas.

[45] Pierini, Alicia, y otros:"Hábeas Data, Derecho a la Intimidad". Pág. 238.
[46] Bianchi, Alberto S., citado por Alvarado Bonilla, K.M. y otros. Ob. Cit.. Pág. 55.

Por último, CARLOS COLAUTTI, manifiesta que puede establecerse una diferencia entre Intimidad y Privacidad, sosteniendo que "*entre acciones privadas y acciones íntimas existe una relación de género a especie; por lo que las acciones íntimas son una especie dentro de las acciones privadas; esto porque todas las acciones íntimas son privadas, pero no todas las acciones privadas son íntimas; así por ejemplo, la política, la religión, etc.*"[47]

2.1.2 Objeto del derecho a la Intimidad.

El surgimiento de normas y leyes encargadas de la protección de derechos fundamentales del individuo, sirve para que exista un respeto del propósito u objeto de la existencia o creación de los mismos. Por lo cual, corresponde en este apartado establecer el objeto del derecho a la Intimidad, consistiendo el mismo en "*dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales sin el afán de vedar toda intromisión en las esferas de la vida que el titular se reserva para sí; sino facultándolo para permitir o no controlar el uso que de esa información se haga*"[48].

Cabe mencionar que el derecho a la Intimidad es amplio en su estructura y desarrollo, así como en su esfera de protección. Por lo tanto, en este apartado el objeto aquí planteado es en relación a la situación que

[47] Colautti, Carlos, citado por Alvarado Bonilla, K.M. y otros. Ob. Cit.. Pág. 56.
[48] Ibídem. Pág. 58.

corresponde al presente estudio, el cual está referido al tratamiento automatizado de datos personales en archivos o registros públicos y privados.

2.1.3 Características del derecho a la Intimidad.

Dentro del derecho a la Intimidad, como uno de los derechos de la Personalidad reconocida constitucionalmente en la legislación salvadoreña, como derecho de cada persona a mantener reservada una parte de su vida, es necesario establecer que como derecho posee las características que a continuación se señalan:

A) Es un derecho originario e innato: puesto que la persona ya nace con este derecho, es decir, que corresponde al titular desde el origen de éste.

B) *Es absoluto*: esto es que posee una posibilidad alegatoria *erga omnes*, es decir, ante cualquiera. Sin embargo, esta característica no significa que sea ilimitado sino limitará las libertades de expresión cuando estas atenten contra la vida privada.

C) *Es extra patrimonial*: esto significa que sobre este derecho es imposible hacer negocio jurídico alguno. No obstante, hay casos en que ciertas personas “venden” su vida privada a la prensa, pero la reiteración de una conducta no es un factor de legitimación de la misma en ningún caso.

D) *Es irrenunciable*: el individuo no puede renunciar a este derecho, por ser innato; aunque pueden darse disposiciones sobre manifestaciones puntuales en las que el individuo acepta el conocimiento de terceros sobre ciertos aspectos íntimos de su vida.

E) *Es inembargable e inexpropiable*: el derecho a la Intimidad no puede ser apartado de la vida del ser humano; por lo tanto es intransferible.

F) *Es imprescriptible*: porque no es alcanzado por los efectos del tiempo que no influye en su pérdida, no obstante el abandono del titular. Por su propia naturaleza de derecho de la personalidad, sin embargo cabría remarcar que este derecho no dejaría de serlo si trasciende de la esfera privada, pues existe el secreto por voluntad expresa del individuo.

G) *Es vitalicio*: acompaña al ser humano durante toda su vida.

H) *Es Inalienable*: no es susceptible de enajenación por ningún título, está fuera del comercio.

2.2 TITULARES DEL DERECHO A LA INTIMIDAD.

Es de tener en consideración que no existe sociedad sin la presencia de seres humanos, por lo que se hace necesario estudiar el reconocimiento del derecho de todo ser humano a conservar fuera del acceso general ciertos hechos concernientes a su esfera de Intimidad, el cual tiene por fundamento la necesidad esencial de soledad y recogimiento para el desarrollo pleno de

la personalidad; es así como dentro de los titulares del Derecho a la Intimidad encontramos los siguientes:

2.2.1 Personas Naturales:

No se discute en la Doctrina que el Derecho a la Intimidad corresponde a los seres humanos, negar esta posibilidad sería negar la existencia misma del derecho a la Reserva de la Vida Privada. Algunas legislaciones, como la nuestra, al referirse a la naturaleza humana del derecho a la Intimidad, lo establecen como uno de los derechos fundamentales del individuo, visto como derecho inherente a la personalidad.

Todos los seres humanos, sin distinción entre los individuos capaces e incapaces, tienen derecho a la tutela en el ordenamiento jurídico en cuanto a hechos, datos o situaciones que integran su vida privada. Cuando se trata de autorizar ciertos actos de intromisión en la esfera de Intimidad, el derecho a la Reserva de la Vida Privada es parcial y relativamente disponible, habrá que aplicar reglas diversas, ya sea que se trate de personas capaces o incapaces. En ese sentido, cuando una persona plenamente capaz pretende disponer de su derecho, dentro de los márgenes legales, bastará su sólo consentimiento expreso o tácito. Cuando se trata de personas incapaces, hay que distinguir a la vez si tiene o no discernimiento; de no tenerlo, bastará el consentimiento otorgado por su Representante Legal; en cambio, si el

incapaz tuviera discernimiento no bastará el consentimiento manifestado por su Representante Legal para autorizar la conducta violatoria de la Intimidad. En tales casos, será necesario obtener el consentimiento del Representante y del incapaz representado. Así mismo, la afección no impide su discernimiento, lo que le permite juzgar y elegir lo que desea para su vida; tendría derecho, en consecuencia, a que se consulte su opinión en la materia. En cuanto a los casos de incapaces sin discernimiento, y siempre en aras de lograr una mayor y mejor protección de la Intimidad, se dispone que al consentimiento del Representante Legal debe agregarse la autorización judicial.

2.2.2 Personas Jurídicas: distintas posturas:

En cuanto a esta situación, se plantean diferentes posturas sobre las cuales versan una serie de interrogantes para determinar si las personas jurídicas gozan de este Derecho a la Intimidad, entre las cuales se encuentran: ¿pueden los entes ideales gozar de la protección a la Intimidad?, ¿debe extenderse la protección de datos de las personas físicas a las personas jurídicas?, o ¿gozan estas últimas de un Derecho a la Intimidad, que justifique la aplicación de la garantía del Hábeas Data en su defensa?; las respuestas a estas interrogantes no han sido coincidentes, ya que el planteo tiene detractores pero también ha cosechado adhesiones.

"*La noción de persona jurídica se mantuvo en un plano secundario hasta el siglo XIX, en que el Capitalismo moderno la usó como un resorte fundamental de su expansión y predominio*"[49]. La utilización de la "forma" de la persona jurídica permitió la reunión de grandes capitales con los cuales se afrontó la realización de empresas económicas inaccesibles, para los individuos aislados. La cuestión fue siempre compleja y problemática.

Desde los comienzos del Derecho común, la idea de que existan otras personas distintas de las de carne y hueso, despertó todo tipo de resistencia entre los juristas. Por lo que a continuación se explican dos posturas, que a nuestro juicio son las más representativas:

+ *Primera Postura*: la tesis mayoritaria, en el Derecho Comparado afirma que "las personas Jurídicas no tienen Derecho a la Intimidad". La razón fundamental que sustenta este criterio radica en que estos entes no pueden sufrir daños morales, los cuales surgen de la violación de la vida privada. Se argumenta también que la naturaleza intrínseca del derecho a la Intimidad descalifica a las personas ideales para ser titulares del mismo; el respeto a la vida íntima, la mención a la publicación de retratos, a la mortificación en las costumbres o sentimientos revela con elocuencia la

[49] EKMEKDIJIAN, Miguel Ángel Y PIZZIOLO, Cologero: "Hábeas Data, el Derecho a la Intimidad Frente a la Revolución Informática". Pág. 77.

índole del bien jurídico tutelado que solo puede ser concebido con referencia al ser humano, como portador natural de la intimidad.

Se manifiestan partidarios de la corriente antes descrita, Novoa Montreal, Rivera, Mosset Iturraspe, Cifuentes y Carranza, entre otros; afirmando que " *fuera de la persona humana no es posible sostener un derecho a la intimidad. Los entes ideales no la tienen, puesto que son instituciones con fines específicos y carecen de tales derechos innatos."*[50]

Otra argumentación para sostener esta postura es la establece que "*la persona jurídica es una institución creada por el hombre como legislador; no parece, entonces, de una sana lógica jurídica sostener que la criatura goza de los mismos derechos que su creador."*[51]

Así también, existe otro argumento, es el que establece que dentro del esquema de derechos y garantías, la persona física nunca se disuelve, como puede ocurrir en algunos casos con la persona jurídica, por dicha razón es que se reconoce al derecho a la intimidad como uno de los derechos personalisimos del ser humano, junto con el honor y la propia imagen.

[50] Ferreira Rubio, Delia Matilde, citado por Alvarado Bonilla, K.M. y otros. Ob. Cit.. Pág. 65.
[51] EKMEKDIJIAN, Miguel Ángel Y PIZZIOLO, Cologero: "Hábeas Data, el Derecho a la Intimidad Frente a la Revolución Informática". Pág. 87.

+ *Segunda Postura*: esta postura corresponde al criterio minoritario sosteniendo que "las personas jurídicas están tuteladas en su vida privada"[52]; aclarando que el contenido que se dará a la esfera de reserva protegida deberá ser diverso del que se atribuye a las personas físicas. Este criterio es apoyado por los autores Jean Dabin y Velu, siendo este último quien afirma que "*si las personas jurídicas tienen derecho a un nombre, al honor y a la reputación, porqué razón no podrían utilizar la protección que surge del derecho al respeto de la vida privada*"[53], sosteniendo, así mismo, que debido al desarrollo de las técnicas del espionaje industrial, las compañías comerciales deberían estar capacitadas para ampararse en el derecho al respecto de la vida privada, al igual que los individuos particulares.

Los juristas del siglo XIX, bajo el flujo del Iluminismo y de los principios de la Revolución Francesa, gestaron toda la teoría de los derecho subjetivos y de las personas jurídicas, teniendo una realidad distinta de la actual. Ellos jamás, hubiesen imaginado la magnitud que alcanzaría esta criatura jurídica, y de qué manera influiría en la sociedad contemporánea.

Desde la Dogmática difícilmente se puede hablar de la persona jurídica como titular de derechos subjetivos; pero, algo muy diferente ocurre

[52] Alvarado Bonilla, K. M. y otros: "El Hábeas Data como garantía de protección de la persona frente al tratamiento de sus datos personales". Pág. 65.
[53] Ferreira Rubio, D.M.: "El Derecho a la Intimidad". Pág. 157.

en la dimensión práctica, ya que en esta se demuestra cómo determinadas conductas afectan al Honor y a la Intimidad de la persona moral, de similar manera que afectan a una persona jurídica.

En el sentido que una falsa o inexacta información sobre la solvencia de cualquier entidad financiera afecta su prestigio y reputación en el mundo de los negocios, de la misma manera que la falsa imputación de un delito puede afectar el honor de un individuo frente a la sociedad en general.

En el mismo orden de ideas Estadella Yuste, sostiene, que "*La justificación de la protección de datos de las personas físicas se desprenden del resguardo concedido a los derechos humanos individuales; y la protección de personas jurídicas tiene sus raíces, en gran parte de los casos, en derechos económicos.*"[54] Por lo tanto, en ocasiones, el uso incorrecto de información económica hace tan vulnerables a los individuos como a las entidades jurídicas. Ejemplo: Un balance crediticio negativo fruto de información errónea puede perjudicar la estabilidad financiera de una empresa o de un individuo.

Parece lógico, entonces, que las entidades jurídicas puedan disfrutar de un derecho de acceso o de corrección sobre información que hace

[54] Ekmekdjian, M.A. Ob. Cit. Pag. 83.

referencia a esa entidad. En otras palabras, si los individuos pueden ejercer un derecho de acceso a los bancos de datos personales almacenados en una entidad; ¿Porque no podrían hacerlo las personas jurídicas? Ya que esto le permitiría corregir datos inexactos u obsoletos que, como en el caso de las personas físicas, les provocan un perjuicio.

Cabe señalar que, en el ordenamiento jurídico salvadoreño se distingue entre "el respeto a la vida privada" y "el ataque a la intimidad de la vida privada" y "*se pone de manifiesto el que ambas expresiones significan cosas distintas y así se afirma que mientras que la vida privada merece el respeto de los demás y la protección judicial, el núcleo íntimo de la misma suscitará la adopción de medidas judiciales excepcionales."* [55] En realidad lo que el legislador ha querido garantizar es el núcleo íntimo de la vida privada de las personas en su esfera personal y familiar. Quedan por lo tanto, fuera de la tutela constitucional las esferas laboral, profesional comercial, etc. Y en principio no cabria hablar en momento alguno, de intimidad de la persona jurídica.

Sin embargo, debido a la realidad actual con los avances tecnológicos, esa situación jurídica podría variar, en el sentido que si bien es cierto el derecho a la intimidad es un derecho de la personalidad; las personas

[55] Bertrand Galindo, F. y otros: "Manual de Derecho Constitucional". Tomo II. Pag. 742.

jurídicas pueden verse afectados por situaciones que se relacionen a su ámbito privado afectando el buen nombre de dicho ente si se llega a publicar información falsa sobre la calidad y Confiabilidad de la misma, situación que desmejoraría su estado financiero, causando pérdidas en todo ámbito.

Finalmente, de acuerdo a las posturas antes planteadas, podríamos determinar que las personas jurídicas tienen derecho a la intimidad en su vida privada, así como derecho al honor comercial; por lo que es posible considerar a las personas jurídicas no como titulares de derechos personalísimos de manera permanente, como es el caso de las personas físicas, sino en un determinado contexto y en situaciones o condiciones concretas en que sea necesaria su protección. Es decir, la protección no se otorga “en sí misma “, sino “para sí”, según el caso de que se trate.

2.3 LIMITES AL DERECHO A LA INTIMIDAD.

Todos los derechos de las personas están sometidos a ciertos límites y restricciones; la limitación surge como requisito indispensable para la convivencia armónica de todos los miembros de la comunidad.

Aun los llamados derechos humanos están sujetos aun límite esencial que es el respeto de los derechos de los demás miembros de la

sociedad. En la Declaración Universal de Derechos Humanos de 1948, reconoce restricciones en el artículo. 29, en el que se autoriza la imposición de limitaciones en los derechos fundamentales, con el fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás y satisfacer las exigencias justas de la moral, del orden público y el bienestar general.

El derecho a la intimidad no escapa a esta regla, puesto que entonces las limitaciones a este derecho como las que se imponen para los otros, no deben atentar contra la dignidad física, intelectual o moral de la persona humana.

2.3.1 Limitaciones de Base Conceptual.

Son las que se aplican en el caso de personajes; el fundamento de la restricción al derecho a la intimidad, varía en estos supuestos según la categoría de persona célebre de que se trate, así como los hombres de la historia contemporánea, los políticos, etc. En cambio, tratándose de personas que adquieren popularidad, sin que sus conductas afecten la situación global de la colectividad, el fundamento de las limitaciones radica en la búsqueda de popularidad por parte de estos sujetos.

2.3.2 Limitaciones Generales.

Estas limitaciones no tienen fundamento en el carácter que revisten las personas, por lo que se aplican sin consideración a los sujetos concretos, es decir en relación a:

A) La Seguridad del Estado: La defensa y seguridad del Estado justifica que en ciertas situaciones se limite el derecho a la intimidad de los particulares. Así por ejemplo, en tiempos de guerra o de emergencia nacional que ponga en peligro las bases mismas del Estado, se restringen todos los derechos y, entre ellos están el derecho a la intimidad; en estas circunstancias el Estado tendrá derecho a entrometerse en la vida privada de las personas; no se trata del ejercicio del derecho a la información, sino del derecho a la investigación.

Aunque la protección de la Seguridad del Estado no queda reducida solo en época de guerra, también en tiempos de paz, ya que puede inmiscuirse en la vida privada de las personas a fin de mantener el orden publico, la paz social, prevenir los delitos y reprimir los cometidos.

B) El Bienestar General: La protección de la moral pública y de las buenas costumbres justifica ciertas intromisiones del Estado en la vida privada de las personas. A manera de ejemplo, y entender lo que se ha dicho, la salud publica justifica la injerencia de la autoridad en aspectos de la intimidad de las personas. La obligatoriedad de las vacunaciones, la

necesidad de someterse a ciertos estudios y chequeos, están legitimados por el interés general del Estado en mantener un nivel de vida sanitaria digna entre la población.

2.4 PROTECCION O GARANTIA A LA INTIMIDAD PERSONAL.

Fue hasta la Constitución vigente que este derecho a la Intimidad apareció consagrado por primera vez en el inciso segundo del artículo dos (junto con el Honor y la Propia Imagen). Es en este que el Estado reconoce a todas las personas por igual el derecho a la Intimidad, refiriéndose a la personal y familiar; esto es, a que nadie se entrometa en la vida íntima de la persona y su familia.

Una de las proyecciones de la Intimidad se relaciona con el derecho al silencio y al secreto. "*El primero es la faz negativa del derecho a la libre expresión y difusión del pensamiento, y al igual que el derecho al secreto, implica la facultad de reservarse ideas, sentimientos, conocimientos y acciones que el sujeto no desea voluntariamente dar a la publicidad o revelar a terceros o cumplir*"[56].

[56] Bertrand Galindo, F.y otros. Ibídem. Pág. 742.

En la actualidad, recibimos frecuentemente en nuestro medio, propaganda de lugares o locales en los que no hemos estado nunca, o propaganda de entidades que se dedican al marketing (comercio), situaciones que ponen en riesgo la Intimidad. Por eso es necesario que se protejan esas bases de datos y toda aquella información de carácter personal que tienen las empresas que se dedican a vender estos datos.

El atentado contra la Intimidad por el uso de la Informática puede provenir, tanto de la recolección de datos como de aquellos que pueden afectar a la esfera más personal. Por ello, es necesario que se cree en El Salvador una Agencia de Protección de Datos que sea la encargada de atender las peticiones y reclamaciones formuladas por los afectados, y que tenga la facultad de ordenar la cesación de tratamiento de datos o cancelación de ficheros.

Además, en la recolección y almacenamiento de datos para constituir un archivo o fichero, los afectados tendrían el derecho a ser informados previamente a la recolección. También existe el derecho a verificar la exactitud de los datos que figuren en dicho archivo y su actualización, de ser necesaria. Se tiene derecho por parte del responsable del fichero, en caso de que se produzca una lesión en sus bienes o derechos, debiendo indemnizar al que los ha sufrido.

A menudo nos preguntamos hasta qué punto puede llegar una persona a sobrepasar la Intimidad de otra, sobre todo en la última década más innovadora que nunca. Ya no son sólo las personas públicas las que reivindican este derecho fundamental (derecho a la Intimidad), sino que cualquier ciudadano sabe que sus datos, teléfono y demás información estrictamente privada, se encuentra dentro de la esfera interior, reservada e imprescindible que cada individuo necesita para desarrollarse personalmente.

Con la gran oleada de avances tecnológicos nos cuestionamos nuestro derecho a la Intimidad, con respecto no sólo a los medios de comunicación (Libertad de expresión y de Información), sino que ahora también referido en el ámbito de la llamada era de las comunicaciones y tecnología de punta, referidos a los medios informáticos y a los datos que se mueven por este.

La persona, a lo largo de su vida, va dejando una enorme estela de datos dispersos y que, hoy en día, con la aplicación de los medios tecnológicos, es posible agrupar y tratar en forma conjunta, relacionándolos y analizando significados e interpretaciones conexas, creando o estudiando a

voluntad aquellos aspectos del individuo que sea de interés contratar o conocer.

Mediante la utilización de los medios informáticos de los medios informáticos se puede ejercer un control social, incluso sin que la persona note que alguien pueda estar interfiriendo en su vida. La invasión de la Intimidad de los medios informáticos se ve claramente en la utilización indiscriminada de nuestros datos.

En cuanto a los mecanismo de protección del derecho a la Intimidad, en relación con los datos personales, en El Salvador las personas no están protegidas, esto es por el hecho de que no se cuenta aún con una figura específica como medio de protección de derechos fundamentales de las personas por el tratamiento automatizado de sus datos personales, como lo es el Hábeas Data.

Por tanto, este derecho fundamental de máxima protección cada vez más compleja por los avances desmesurados en la tecnología, se tiene muy presente en una sociedad de la información a la que nuestro ordenamiento jurídico se debe adecuar, si pretende ver cumplida la misión de no permitir que se vulnere el derecho a la Intimidad.

2.5 AVANCES TECNOLOGICOS DE LA INFORMATICA Y SU INCIDENCIA EN LOS DERECHOS FUNDAMENTALES.

2.5.1 Los Derechos Fundamentales frente a la Tecnología.

La formulación de los derechos fundamentales como tales es una expresión relativamente reciente, surgida en el año de 1770 en los "*droits fondamentaux"* de Francia, dentro del movimiento que condujo a la Declaración de los Derechos del Hombre y del Ciudadano de 1789, y constituye una fase más avanzada del proceso de positivación de los derechos naturales en los textos constitucionales del Estado de Derecho, según explica Pérez Luño[57].

El factor histórico resulta determinante para conocer y comprender el catálogo de derechos fundamentales de una sociedad democrática en particular. En la actualidad, estos presentan rasgos novedosos que permiten hablar de una tercera generación de derechos humanos complementaria de dos fases anteriores. Respecto a esta tercera generación, Frosini mencionado por Sánchez Bravo, señala que "*está estrechamente vinculada a la sociedad tecnológica, en su calidad de derechos positivos, por lo que ya no pueden calificarse de innatos"*[58].

[57] Alvarado Bonilla, K. M. y otros. Ob.Cit. Pág. 76.
[58] Alvarado Bonilla, K. M. y otros. Ibídem.

Suñé Llinás[59], por su parte, vincula estos derechos de tercera generación con los valores inherentes a la cultura post materialista que ya no responden a la necesidad de seguridad física o económica, como en las dos generaciones anteriores, sino que se relacionan con la auto realización personal, adoptando un carácter más de expresivo que instrumental.

Para Pérez Luño, los derechos de Tercera Generación responden al fenómeno de la contaminación de las libertades que alude a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de la tecnología[60].

Dentro de los rasgos innovadores de esta fase menciona el hecho de que la solidaridad constituye el valor guía de los derechos, porque se hallan aunados entre sí por su incidencia universal en la vida de todos; y para realizarse, exigen esfuerzos y responsabilidades comunes a escala mundial.

Por otra parte, y siguiendo la línea argumental de este autor, a través de un análisis funcional de los derechos fundamentales, es posible distinguir dos cometidos complementarios: por un lado, reconocen determinadas facultades o posibilidades de actuación a los ciudadanos; y por el otro,

[59] Alvarado Bonilla, K. M. y otros. Ibídem.
[60] Alvarado Bonilla, K. M. y otros. Ob. Cit. Pág. 77-

propenden hacia un equilibrio de poderes políticos, sociales y económicos al interior de las sociedades democráticas a que pertenecen.

Si esas sociedades presentan un nivel de desarrollo tecnológico importante, es posible prescindir, cada vez más, de la coacción física para dar paso a complejas amenazas a los derechos y libertades mediante el uso de la información, para influir y controlar la conducta de las personas. Por lo tanto, la armonía que se busca, a través del reconocimiento constitucional de los derechos de las personas, en este tema, pasa por el establecimiento de un sistema de protección de datos personales, considerados como garantía básica para cualquier comunidad que descanse en la libertad e igualdad de sus integrantes.

No obstante, también es fácil que se produzca un tratamiento ilegítimo de datos en el sector público a través de diversas vías, unas más evidentes que otras. Ciertamente aquí se está haciendo referencia, por una parte, al Estado que, en regímenes totalitarios como el Nacional Socialista Alemán durante la Segunda Guerra Mundial, utiliza los datos personales para identificar y oprimir a sus opositores.

En el anterior ejemplo, Hitler, probablemente con el apoyo de los directivos de IBM de esa época, según algunas investigaciones

recientemente publicadas, facilitó su búsqueda de judíos para conducirlos a los campos de concentración y exterminio, tras revisar en los padrones municipales datos tan simple como el nombre y los apellidos de origen semita[61].

Pero el Estado Democrático también puede desconocer las garantías mínimas que, al respecto, fijan los ordenamientos jurídicos modernos; como en el caso del que se dedica a tratar y almacenar información de los ciudadanos como si fuese propia, aplicando medidas de restricción de los derechos fundamentales del titular de los datos, sin la base legal específica, y argumentando en ocasiones, razones tan amplias y ambiguas como el "atender al interés general" o "resguardar el orden público".

No obstante ello, resulta más preocupante el caso en que el Estado Legislador regula la materia, otorgando privilegios excesivos para los órganos públicos, normalmente bajo la forma de excepciones que desnaturalizan esos mismos derechos que viene reconociendo, porque queda encubierta la injerencia ilegítima bajo una apariencia de legalidad en la que confía la ciudadanía.

[61] Alvarado Bonilla, K. M. y otros. Ob.Cit. Pág. 78.

En definitiva, los derechos fundamentales gozan de un régimen de protección jurídica reforzada, manifestada en una serie de instrumentos de tutela diversos, dentro del que destacan las garantías normativas. A través de las cuales, la Constitución busca asegurar su cumplimiento, evitar su modificación y mantener la integridad de su sentido y función.

+ *El Rol de la Protección de Datos Personales en la garantía de los derechos fundamentales*: luego de haber reconocido la necesidad de proteger a la persona natural y sus derechos y libertades fundamentales a través de una regulación de tratamiento de datos personales, corresponde ahora explicar de manera breve la razón justificante de normas específicas que aborden el tema y la estructura que normalmente tienen.

Es de aclarar en un primer momento lo que se debe entender por Protección de Datos Personales. En ese sentido, Pérez Luño señala que dicho termino hace referencia al "*conjunto de bienes o intereses que puedan ser afectados por elaboración de informaciones referentes a personas que pueden ser identificadas o identificables*"[62].

Así concebida, la Protección de Datos de carácter personal encuentra su razón de ser, ya no en el resguardo del ámbito íntimo de la vida privada,

[62] Pérez Luño, A.E.: "Problemas Actuales de Documentación y la Informática Jurídica". Pág. 68.

sino en la posibilidad de controlar esa información para asegurar al individuo frente al riesgo que supone el acopio y la transmisión de sus datos de un modo que lo vuelvan un ser transparente.

Ahora bien, cuando ese poder de control y disposición sobre los datos personales propios se recoge en el Derecho Positivo, las normativas que se dictan suelen seguir tres grandes líneas, según Suñe Llinás[63]. La primera de ellas obedece a la búsqueda de equilibrio entre los derechos fundamentales que se encuentran en juego. De este modo, sea cual fuere la posición doctrinal que se tenga sobre el bien jurídico tutelado por las leyes de protección de datos, los derechos individuales de los titulares se ven limitados en aras del interés general a través de ciertas libertades públicas, en particular, la libertad de información, las necesidades de información del Estado y la Libertad de Empresa. Finalmente, las leyes de protección de datos deben definir su ámbito de aplicación y decidir si abarcarán a los archivos manuales o sólo se extenderán a los automatizados; si su alcance comprenderá a las bases de datos del sector público y privado o sólo a algunos de ellos; y si correctamente sólo resguardarán los derechos de las personas naturales o también los de las jurídicas.

[63] Alvarado Bonilla, K. M. y otros. Ob.Cit. Pág. 80.

Sin embargo, esta particular idea de Libertad Informática, que para la Doctrina corresponde a un derecho fundamental nuevo e independiente y distinto de los tradicionalmente reconocidos, se aproxima luego más a la del derecho a la Intimidad. Así se señala que la garantía de la Intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada Libertad Informática es, así también, derecho a controlar el uso de los mismos datos insertos en un programa informático (Hábeas Data)

2.5.2 Peligros de la Informática en relación con la Intimidad.

En la sociedad de la información, las personas han estado tan expuestas a ojos extraños. Los riesgos no proceden sólo del poder publico sino también de poderosos poderes privados débilmente controlados por aquel, los cuales a través de las nuevas tecnologías de la información pueden penetrar casi sin barreras en la esfera privada y hacerse con el control de datos de miles de personas.

Es preciso, pues, precaverse contra esa amenaza, sobre todo si se tiene en cuenta que estamos comenzando a vivir la fiebre del almacenamiento de datos por parte de estos dos poderes. Esa explosión informática es hecha por los rápidos avances de la tecnología de los ordenadores, lo cual ha permitido la acumulación de un volumen de

información sobre las personas antes inimaginables y en el que pueden acceder, sin su consentimiento ni control, terceros extraños.

De esta manera, no solo se pone en peligro la intimidad, sino que también otros derechos como la identidad del hombre y así mismo la propia imagen, ya que por la novedad de hoy en día es que la difusión de datos personales es prácticamente ilimitada gracias a la informática.

De todo esto dice Pablo Lucas Murillo que existen razones socioeconómicas que favorecen a la acumulación de información en sistemas informáticos. Así, ha señalado tres factores que explican el nacimiento y posterior multiplicación de Empresas que con relación a la tecnología informática, prestan servicio de facilitar datos personales, los cuales son: "*La expansión del uso del crédito y las tarjetas de crédito; la extraordinaria movilidad de la población no solo dentro de un país, sino por todo el mundo; el enorme incremento, en cantidad y calidad, de la fuerza de trabajo*"[64]. Todo esto lleva a que, cada vez, con más frecuencia, tanto las instituciones financieras como las empresas comerciales se afanen en la búsqueda de información en cuanto a la solvencia que posean sus actuales clientes e incluso los que puedan llegar a serlos en un futuro.

[64] Alvarado Bonilla, K. M. y otros. Ob.Cit. Pág. 83.

En definitiva, el progreso ha traído consigo un instrumento extraordinariamente eficaz tanto para su buen uso como también para el malo. De no establecerse medidas efectivas, puede prosperar esa utilización perversa y atraer graves consecuencias. Es necesario evitar o reducir al mínimo peligros de los que se han expuesto, pues, solo de esa manera será posible asegurar a cada uno el control sobre la información personal que afecta la posibilidad de obtener la corrección o cancelación de datos inexactos o falsos sobre sí mismo, incluidos en una base o registros de datos y tener presente que *"el respeto a la intimidad es una condición para el goce de una calidad mínima de la vida humana y que igualmente debe serlo la protección de los datos personales frente a su tratamiento informático."*[65]

[65] Murillo de la Cueva, P.L.: " El derecho a la autodeterminación Informativa". Pág. 115.

CAPITULO III
3. EL DERECHO A AUTODETERMINACION INFORMATIVA Y LA PROTECCION DE DATOS PERSONALES.

En el capítulo a desarrollar se plantea el perfil de un nuevo derecho fundamental, el derecho a la Autodeterminación Informativa, sustentándose en los riesgos que implica el uso de la informática en el Tratamiento de Datos Personales; así mismo, se aborda lo relativo a la Privacidad sobre los datos personales, donde se contempla lo que se entiende por datos personales, la naturaleza jurídica, el fundamento y autonomía, además del bien jurídico tutelado y los mecanismos de protección de los mismos.

3.1 EL PERFIL DE UN NUEVO DERECHO: EL DERECHO FUNDAMENTAL A LA AUTODETERMINACION INFORMATIVA.

Se ha hablado, en páginas anteriores, del derecho a la Intimidad señalando que se trata de un derecho fundamental directamente ligado a la Dignidad Humana caracterizado por un eminente contenido negativo para salvaguardar del conocimiento ajeno una parte de nuestra vida personal y familiar. En cambio, el derecho a la Autodeterminación Informativa tiene un objeto y un contenido diferente, su ámbito es más amplio y los elementos que lo componen más complejos.

El tratamiento de la información personal puede, pero no tiene por qué, afectar a informaciones íntimas o secretas que son el objeto de protección del derecho a la Intimidad. De la misma forma, los datos personales informatizados no tienen necesariamente que precipitar un retrato personal que implique una valoración peyorativa u ofensiva de un individuo y que atente contra su buen nombre o fama.

El tratamiento automatizado de los datos personales no afecta de forma general y habitual al derecho a la Intimidad y, mucho menos, al derecho al Honor, tal y como parece opinar el Constituyente Español cuando exige que la Ley limite el uso de la informática para garantizar el Honor y la Intimidad Personal y Familiar de los ciudadanos y el pleno ejercicio de sus derechos[66]. No existe, por supuesto, unanimidad sobre esta cuestión; una posición distinta es la defendida por Carlos Ruiz Miguel, quien considera que el derecho a la autodeterminación Informativa no sería un nuevo derecho, sino se trataría "*del mismo derecho a la Intimidad auxiliado de nuevas técnicas y aplicado a un objeto nuevo, la Informática*"[67].

[66] Garriga Domínguez, Ana: "Tratamiento de Datos Personales y Derechos Fundamentales". Pág. 23.
[67] Ruiz Miguel, Carlos: "En torno a la Protección de Datos Personales Automatizados", citado por Garriga Domínguez, Ana. Idem. Pág. 23.

A través del análisis de los nuevos riesgos que el uso de la tecnología informática supone para las personas y sus derechos y, seguidamente, a través del estudio del contenido y de las funciones que, específicamente, el derecho a la Autodeterminación Informativa pudiera realizar para garantizar la Dignidad y la Libertad de las personas frente a reales o potenciales abusos en el tratamiento de informaciones personales.

3.1.1 Los Riesgos.

No sólo los datos que hacen referencia a aspectos más próximos, secretos o sensibles de nuestras vidas van a quedar dentro del ámbito de protección del derecho a la Autodeterminación Informativa; porque no es únicamente el deseo de mantener nuestra vida privada lejos de miradas ajenas lo que fundamenta la consagración de este nuevo derecho fundamental, sino que los peligros son varios y para todos los demás derechos fundamentales.

El actual desarrollo de las tecnologías de la información hace posible recoger y almacenar, sin límite de espacio, infinidad de datos sobre un mismo individuo, realizar un auténtico catálogo de informaciones personales sobre él y, además, interrelacionar todos los datos existentes sobre una misma persona, con independencia de que se encuentren en archivos

distintos, relativos a diferentes etapas de su vida, o que estos hayan sido recogidos incluso en lugares lejanos.

Los datos personales o el perfil de la personalidad, serán usados normalmente para adoptar todo tipo de decisiones, favorables y desfavorables, por entidades privadas y públicas. Así, esa información puede servir para conceder o denegar un seguro de vida o para el automóvil, un crédito, el acceso a una vivienda, a un empleo, o para enviarnos publicidad de productos que, según nuestro perfil, probablemente adquiriremos. Además, este ensanchamiento de la posibilidad de indagación sobre la vida de las personas se traducirá en una mayor influencia y presión, aunque sólo sea psicológica, sobre sus propias decisiones y también sobre las acciones u omisiones, consecuencia de esa influencia y presión. La libertad de elección y decisión de los individuos se verá directamente afectada ante el desconocimiento de quién, para qué, y qué informaciones sobre nosotros están archivadas, limitándose nuestra capacidad de actuación, ante la incertidumbre de que si nuestras comunicaciones, actividades o elecciones van a ser registradas por entidades que desconocemos y para finalidades que igualmente ignoramos. Por ello, y especialmente por el grado de perfeccionamiento actual de la tecnología, este proceso "*podría degenerar en*

el más implacable fenómeno de control y manipulación que pueda imaginarse"[68].

Los datos pueden utilizarse de forma más o menos aislada, o bien reunirse y confrontarse. Esta interrelación de las informaciones personales permitirá la obtención del perfil de cualquiera y servirá para que se adopten decisiones que le afecten sin que las personas " sean tenidas en cuenta o consultadas". El perfil permite obtener una radiografía de toda o de parte de su vida, así como prever o al menos intuir sus reacciones o comportamientos futuros. El tratamiento de los datos personales hace posible una vigilancia de hecho de la vida cotidiana del individuo, al permitir el registro de una serie de datos que separadamente carecen de importancia, pero que adecuadamente relacionados permiten obtener el perfil de una persona.

No debemos olvidar tampoco, que el uso exclusivamente del perfil informático en la toma de decisiones que afecten a un individuo significará normalmente su discriminación en muchas de las actividades de la vida cotidiana. Ante este hecho nos encontraremos indefensos al desconocer que, quien decide, conoce informaciones que consideramos olvidadas o secretas, o bien que la decisión se basa en el perfil obtenido a través del tratamiento

[68] Pérez Luño, A.E.: "La contaminación de las libertades en la sociedad informatizada y las funciones del defensor del pueblo", citado por Garriga Domínguez, Ana. Ibídem. Pág. 25.

automatizado de datos públicos que aisladamente considerados son inofensivos.

En ese sentido, algunos autores consideran que las modernas técnicas de penetración en las aptitudes profesionales o de comportamiento individual se apoyan hoy, en los métodos informáticos que establecen correlaciones entre determinadas características y comportamientos concretos a los que se les confiere una apariencia de rigor científico. Basándose en estas correlaciones se construye el perfil de una persona, cuya utilización presenta una estrecha similitud con el racismo: se sirve de un perfil consistente en imputar a un individuo ciertas pautas de comportamiento, comunes al grupo en que le hemos censado y que distinguimos del resto de la población global. Entonces se establecen normas de conductas y tratamientos diferenciados para los determinados grupos en los que hemos dividido la población. Tales previsiones serán, generalmente, discriminatorias y, sobre todo porque, "*en la creencia de descubrir en el sujeto ciertos signos anunciadores de su comportamiento futuro, este perfil instaura una forma de determinismo incompatible con el atributo más preciado de la libertad, la elección de un futuro autodeterminado*"[69]. Un ejemplo claro de lo anteriormente señalado es el caso de los latinos y negros en los Estado Unidos de Norteamérica, quienes

[69] Rigaux, F.: "La protección de la vie privée et des autres biens de la personalité" citado por Garriga Dominguez, Ana. Ibídem. Pág. 26.

al comprar casas "*pagan más por sus préstamos hipotecarios que los blancos, de acuerdo con un informe divulgado por la Reserva Federal (Fed)"*. Según dicho informe, "*los negros que solicitan préstamos tienen más probabilidades de ser rechazados que los latinos y blancos"*[70].

La obtención del "perfil" implica encasillar a una persona, en función del resultado del tratamiento automatizado de sus datos, en un determinado grupo al que se le atribuyen unos determinados comportamientos futuros, cuya utilización en la toma de decisiones, que afecten a los sujetos de tales operaciones, pueden suponer una valoración desfavorable de sus rasgos y características personales, lo cual, al final, podría significar una discriminación para la obtención de un crédito, de un empleo, de un ascenso, etc., o la haría acreedora de una *especial vigilancia y control*, al encajar su radiografía informática en el perfil del posible delincuente, terrorista o disidente de la ideología mayoritaria.

Los anteriores efectos perjudiciales son más evidentes en aquellos casos en los que el ciudadano aparece identificado en relación con unos hechos o una situación determinados, incorporándose su identidad y sus datos personales a las denominadas "listas negras" (listas de morosos, de infracciones criminales o administrativas, de carácter laboral, de carácter

[70] "Fed: Tasas más altas para negros y latinos": El Diario de Hoy, Sección Negocios, 11de septiembre de 2006. Pág. 32.

ideológico o sobre comportamientos políticos, sobre datos relativos a la salud, sobre informaciones genéticas, etc.) pero que tiene en común que la inclusión el algunas de esta listas implicaría, generalmente, consecuencias adversas y perjudiciales para las personas incluidas en el fichero, consistentes en la mayoría de los casos en su discriminación al excluirlas de la posibilidad de acceso a un determinado bien o servicio o, también, en un daño directo a su reputación.

El uso desviado de la tecnología de tratamiento de datos personales supone claros peligros para la libertad, para el derecho a no ser discriminado y para la propia dignidad personal. El perfil informático, instaura un determinismo incompatible con la Autodeterminación, la presión del juicio universal permanente puede producir mermas intolerables en la libertad individual; pues, que las decisiones que nos afecten se tomen en base a un precipitado automatizado de la personalidad supone, no solamente ser juzgado sin poder contradecir el resultado y sus consecuencias, sino también, la posibilidad de ser discriminado y excluido. El ser humano pasa a ser *mero objeto de información, dejando de ser un ser dotado de dignidad y sujeto de derechos fundamentales*[71].

[71] Garriga Domínguez, Ana. Ob. Cit. Pág. 28.

Es importante recordar que los derechos fundamentales *son derechos individuales que tiene al individuo como sujeto activo y al Estado como sujeto pasivo, que garantizan a los ciudadanos un status jurídico o la libertad en un ámbito de existencia*[72]*.* En ese sentido, se habla de dimensión subjetiva de los derechos fundamentales. Pero también, en su dimensión objetiva, los derechos fundamentales actúan como elementos esenciales para establecer el necesario equilibrio entre poderes n las sociedades democráticas. Esta función requiere que en las relaciones entre el Estado y la sociedad o entre los miembros de esta, "*no se den situaciones de marcada desigualdad en el acceso al poder que implique para determinadas personas o grupos humanos una marginación de la libertad*"[73]. Cuando una pocos controlan los grandes bancos de información gozan de una gran ventaja sobre aquellos que no pueden llegar a ella, lo cual va a suponer un más fácil acceso al poder de los primeros en detrimento de los segundos, objeto de vigilancia y control.

Por todo lo anterior, la protección de datos personales en nuestras sociedades debe perseguir, además de la genérica protección de la dignidad, la libertad y el disfrute de los derechos fundamentales, el equilibrio entre poderes y situaciones que es condición indispensable para el correcto

[72] Garriga Domínguez, Ana. Ibídem.
[73] Garriga Domínguez, Ana. Ibídem.

funcionamiento de una comunidad democrática de ciudadanos libres e iguales.

3.1.2 Derechos y bienes afectados: El derecho a la Autodeterminación informativa.

Ante los riesgos y problemas descritos, puede tomarse dos posturas distintas: una primera postura que los identificaría como nuevos y contemporáneos riesgos para el derecho a la Intimidad, al Honor y a la Privacidad, y una segunda postura que, consciente de su novedad y especificidad, sugiere la búsqueda de una solución diferente, nueva y específica. El presente estudio comparte la opinión de ANA GARRIGA DOMINGUEZ[74], al decir que la segunda de las posturas es la opción más acertada, en virtud que la problemática que suscita el tratamiento automatizado de datos personales es tan singular, que requiere una solución jurídica especial, o sea, de un nuevo instrumento de tutela y garantía de la libertad y dignidad humanas; en otras palabras, se requiere de un nuevo derecho fundamental que proporcione la respuesta jurídica adecuada ante la "contaminación" que sufren la libertad individual y los derechos fundamentales de las personas.

[74] Ibídem. Pág. 29

No importa la naturaleza del dato, si es íntimo o no, sino las posibilidades de relacionarlo con otros y la finalidad de ese proceso. La protección de los datos personales no persigue mantener fuera del conocimiento público aspectos de la vida privada de un individuo, sino dotar al ciudadano de los medios necesarios para controlar quién, cómo, dónde y con qué motivo conoce cualquier información acerca de su vida, íntima o no, pública o secreta.

Nos encontramos con nuevas contingencias que no es posible enfrentar con los medios tradicionales. El derecho a la Intimidad, cuyo contenido es predominantemente negativo (protegiendo aquella parte de la vida personal y familiar que queremos mantener a salvo de la injerencia ajena), no nos proporciona una respuesta adecuada que permita garantizar la libertad y dignidad de los individuos frente al tratamiento de informaciones personales.

La constatación de esta insuficiencia ha llevado a la elaboración doctrinal y, más tarde jurisprudencial, de un nuevo derecho fundamental con un contenido propio y distinto del derecho a la Intimidad, con un carácter marcadamente positivo frente al predominantemente negativo de aquél. La distinción entre ambos derechos ha tenido, en cierta medida, su reflejo en la legislación sobre protección de informaciones personales, así por ejemplo, la

primera Ley española de protección de datos personales, la LORTAD[75], se hizo eco de esta distinción entre Intimidad y una nueva libertad; en su "Exposición de Motivos" diferenciaba Intimidad de lo que se dió en denominar "privacidad", considerando la segunda más amplia que la primera, ya que la Ley decía: "*En tanto la intimidad protege la esfera en que se desarrolla las facetas más singularmente reservadas de la vida de la persona – el domicilio donde realiza su vida cotidiana, las comunicaciones donde expresa sus sentimientos, por ejemplo -, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.*"

Pero, tal vez, el reflejo normativo más evidente de esta distinción entre Intimidad y Autodeterminación Informativa lo encontramos en la consagración de ambos derechos de forma claramente diferenciada en la Carta de los Derechos Fundamentales de la Unión Europea bajo la denominación de "respeto de la vida privada y familiar"[76] en el artículo séptimo y de "protección de datos de carácter personal en el artículo octavo. La Carta de los Derechos Fundamentales de la Unión Europea ha consagrado como un derecho

[75] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
[76] Carta de los Derechos Fundamentales de la Unión Europea, artículos siete y ocho, citada, por Garriga Domínguez, Ana. Ob.Cit. Pág. 30.

fundamental autónomo e independiente, tanto del derecho a la Intimidad como del derecho al secreto de las comunicaciones, el derecho a la protección de los datos personales o, lo que es lo mismo, el derecho a la Autodeterminación Informativa.

El Tribunal Alemán configuró a partir del derecho general de la personalidad garantizado en la Ley Fundamental de Bonn, "*la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida*"[77]. Puede notarse que el Tribunal extrae del derecho al libre desarrollo de la personalidad la facultad de cada individuo de disponer sobre la revelación y el uso de datos, entendiendo el derecho a la Autodeterminación Informativa como la facultad general de disponer de los datos propios.

Según E. DENNINGER, el Tribunal Alemán puso el acento de forma decisiva en la cuestión más importante, al entender que "*la autodeterminación informativa no sólo depende de los datos sino de su elaboración*"[78]. Por lo tanto, la necesidad de proteger mediante los

[77] Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Alemán, en Garriga Domínguez, Ana. Ibídem. Pág. 31.
[78] Denninger, E.: "El derecho a la autodeterminación informativa", citado por Pérez Luño, A.E.: "Problemas Actuales de Documentación y la Informática Jurídica". Editorial. Tecnos. Madrid, 1987. pág. 273.

adecuados instrumentos jurídicos los datos relativos a las personas, no dependen tanto de si pertenecen o no a su ámbito íntimo, "*cuanto a las posibilidades de elaboración e interrelación propias de la tecnología informática*"[79]. El riesgo, para las libertades depende de unas posibilidades de interrelación prácticamente limitadas; pues como destaca TRAVERSI, si la nota peculiar de cualquier sistema de elaboración electrónica es que permite la memorización de un número elevadísimo de información de cualquier tipo, seleccionarla, agregarle otra o confrontarla con la contenida en otro banco y transmitirla a cualquiera y todo esto, en tiempo real y sin límites de espacio ni fronteras[80]. De tal manera que, un dato carente de interés aisladamente considerado, bajo las condiciones de la elaboración automática de datos, puede adquirir un nuevo valor de referencia, por lo que ya no existe, ninguno sin interés. Lo importante es "*la finalidad con la cual se reclaman los datos y qué posibilidades de interconexión y de utilización existen"* y, sólo cuando estén claros estos puntos "*se podrá contestar la interrogante sobre la exactitud de las restricciones del derecho a la autodeterminación informativa*"[81].

[79] Ibídem.
[80] Traversi, A.: "Il Diritto dell'informatica", Seconda Edicione, Ipsoa Informática, citado por Garriga Domínguez, Ana. Ob. Cit. Pág. 32.
[81] Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional Alemán, en Garriga Domínguez, Ana. Ibídem.

Por otro lado, y dentro de la línea de ponderación de los bienes, PEREZ LUÑO señala que "*el Tribunal Constitucional de Karlsruhe advierte que el derecho a la autodeterminación informativa no carece de límites*"[82]. El ciudadano de un Estado Social de Derecho no tiene un poder absoluto e ilimitado sobre sus datos personales, al ser una persona que se desenvuelve en una comunidad social en la cual la información y la comunicación resultan imprescindibles.

El derecho a la Autodeterminación Informativa pone el acento en el uso que se haga de las informaciones resultantes de interrelacionar determinados datos personales y del perfil que se obtenga; por lo que, lo que se encuentra en juego no es propiamente la Intimidad de las personas, es su identidad. En ese sentido, VITTORIO FROSINI señala que la libertad informática "*representa una nueva forma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del right of privacy, consiste también, en la libertad de informarse, es decir de ejercer un control autónomo sobre los datos propios, sobre la propia identidad informática*"[83].

3.2 PRIVACIDAD SOBRE LOS DATOS PERSONALES.

[82] Pérez Luño, A.E.: "La defensa del ciudadano y la protección de sus datos, en Jornadas Internacionales sobre Informática y Administración Pública, citado por Garriga Domínguez, Ana. Ibídem.
[83] Frosini, V.: "Informática y Derecho". Pág. 23.

La privacidad sobre la información de carácter personal conlleva el establecimiento de reglas que rigen la protección y tratamiento de Datos Personales, así por ejemplo, informaciones crediticias y los archivos médicos; además, facultan al titular de los datos para que pueda tomar conocimiento de ellos a fin de poder ejercer ulteriores acciones sobre sus informaciones, como rectificar, complementar o eliminarlas de los registros o bases de datos que las contengan.

Este aspecto de la Privacidad, hasta el momento, no está contemplado expresamente en el ordenamiento jurídico salvadoreño, ni en los tratados suscritos y ratificados por El Salvador, aunque existen ciertas normas que dispersamente a ellos se refieren. Como ejemplo de ello tenemos, a nivel constitucional, el artículo 19 permite que se realicen pesquisas de la persona para la prevención o averiguación de delitos o faltas; tomando en cuenta que la pesquisa es una indagación o investigación que se realiza para crearse un juicio razonado de algo o de alguien, estamos ante una situación que amenaza nuestra privacidad, ya que, "*sería sencillo que bajo esa justificación, cualquier persona pueda solicitar información de alguien, que indique sus comportamientos u otros aspectos de su vida privada*"[84].

[84] Alfaro Escoto, D.A. y otros: "Hábeas Data : La Autodeterminación sobre las Informaciones Personales". Pág. 45.

En vista que, y tal como se ha mencionado antes, en el sistema normativo jurídico salvadoreño no se encuentra expresamente lo relativo a la privacidad de los datos personales, se hace necesario definir algunos aspectos generales inmersos en ellos.

3.2.1 ¿Qué son los Datos Personales?

En un primer momento, se debe partir de una definición separando las dos palabras; en ese sentido, de conformidad al Diccionario Iter Sopena de la Lengua Española, la palabra Dato significa "documento, fundamento; antecedente. Puede notarse, entonces, que "*Dato es sinónimo de información, algo que permite conocer un ente en todas sus partes, y nos permite, además individualizarlo, crearnos un juicio acerca de ello*"[85]. En lo que respecta a "personal", el diccionario antes citado define este término de la siguiente manera: "relativo a la persona".

De las dos definiciones mencionadas se desprende que los datos personales son informaciones que se refieren a un individuo de la especie humana, que permiten identificarlo y además formarse una idea de cómo es él en todas sus dimensiones; de igual manera se expresa la Ley francesa de 78-17 del 6 de enero de 1978 informática, registros y libertades, cuando en el artículo 4 establece que se reputan nominativos (datos personales) "*las*

[85] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 46.

informaciones que permiten, bajo la forma que sea, directamente o no, la identificación de personas físicas a las que se les aplique, no importando que el tratamiento sea efectuado por personas físicas o morales"[86].

La Convención para la protección de personas con respecto al procesamiento automatizado de datos personales, en su artículo dos dice que Datos Personales significa: *cualquier información sobre una persona identificada o identificable*[87]. La magnitud en el nivel de conocimiento que adquiramos de las informaciones de una persona dependerá de la cantidad o calidad de datos que tengamos. Se establece, entonces, una relación causa – efecto, entre la información que poseamos y el juicio que nos creamos de alguien. De esto se desprende la preocupación acerca de la protección de dichas informaciones, en virtud que el grado de aceptación que le brindemos a una persona dentro de la sociedad depende de los juicios que nos formemos a través de los perfiles que resultan de sus datos personales.

Algo que es importante tener presente es que cuando se habla de Datos Personales, se puede tomar desde un doble enfoque:[88]

[86] Ley Francesa de 78-17, Informática, Registros y Libertades, Artículo 4, citado por Alfaro Escoto, D.A. y otros. Ibídem. Pág. 46.

[87] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 46 y 47.
[88] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 47.

A) En cuanto datos que se refieren o ligan aspectos meramente de la persona inherentes y consubstanciales a ella, son condiciones que forman parte de su ser como individuo de la especie humana y que, en primer momento, están alojados en el interior de su titular, puesto que es donde se originan; lo que podemos definir como datos personalisimos; siendo algunos de ellos, los datos sobre comportamientos sexuales, religiosos, el nombre, la nacionalidad, etc.

B) Aquellos datos relacionados a la persona, pero que no dibujan aspectos que forman parte integrante de ella, la información que brindan son ajenas a su humanidad, y pueden desprenderse de ella sin afectar sus funciones orgánicas, como por ejemplo, datos sobre sus bienes, la cantidad de impuestos que paga al Fisco, el número de cuenta y su ubicación en los bancos donde depositan el dinero, número de teléfono, etc. Estos datos lo podemos llamar datos sobre la persona.

3.2.2. Información Sensible.

Se denomina así a la "*información cuyo contenido se refiere a cuestiones privadas y cuyo conocimiento general puede ser generador de perjuicio o discriminación*"[89]. Así, toda publicidad respecto de información relacionada con preferencias y comportamientos sexuales, religión, filiación política o gremial, raza, etc., encuadra exactamente en los parámetros a

[89] Pierini, A. y otros: Ob. Cit. Pág. 25

proteger para evitar que la información en cuestión sea borrada y/o evitada su publicidad, salvo que existan actividades claras de la persona que determinen que las cuestiones no son “sensibles” para ella o que la misma se encargue de exponerlo públicamente. El presidente de una asociación que nuclea a homosexuales hace pública su condición de tal; razón por la cual, deja de ser privada o sensible dicha opción en cuanto al conocimiento general, debiéndose cuidar que tal dato no se transforme en discriminador. Para cualquier otra persona, el registro de ese dato en sí mismo implica una “cuestión sensible” y privada, la cual debe ser resguardada y protegida.

El derecho a la Intimidad, al Honor, a la Imagen, a la Identidad, a la libre elección sexual y al resto de los derechos personalisimos que son inherentes a la esencia misma del hombre deben preservarse y guardarse con absoluto recelo, respeto y secreto, en idénticos términos a los que todo el mundo convino sobre la existencia del secreto bancario, del secreto profesional, del secreto de confesión, etc.

La finalidad del Hábeas Data es impedir que en bancos o registros de datos se recopile información que está referida a aspectos de su personalidad directamente vinculados con su intimidad que no pueden encontrarse a disposición del público o ser utilizados en su perjuicio por órganos públicos o entes privados. Se trata, particularmente, de información

referida a la filiación política, las creencias religiosas, militancia gremial, el desempeño en el ámbito laboral o académico, etc.

Este criterio también es recogido por la legislación, jurisprudencia y doctrina internacionales; en todos los casos, se tiende a preservar el derecho de Intimidad y el respeto sobre la información "sensible", en el convencimiento de que la misma no debe utilizarse para su almacenamiento en base de datos alguna, por no pertenecer la información más que a la propia persona.

Tanto es así, que la Asamblea General de las Naciones Unidas en el Art. 45 de la Declaración sobre la Regulación de Datos Personales Automatizados "Directrices para la Regulación de Ficheros Automáticos de Datos Personales", establece que los "*datos sensibles son cierto tipo de datos personales cuya utilización puede dar lugar a discriminaciones ilegales o arbitrarias, fijando entre los datos que no deben ser recogidos expresamente los referidos a raza, origen, etnia, color, vida sexual, opinión política, religión, filosofía y otras creencias, así como el ser miembro de asociaciones o uniones sindicales*"[90].

[90] Pierini, A. Ibídem. Pág. 26.

3.2.3 El derecho a la Protección de Datos Personales.

El derecho a la Protección de los datos es un derecho de reciente consagración. Por tal motivo, existe consenso en cuanto a su ubicación dentro del conjunto de la tercera generación de derechos, pese a un precedente contenido en la Constitución de Weimar, que de atenderse, lo colocaría dentro de los derechos de la segunda generación.

Desde el ángulo lexicológico, este nuevo derecho ha recibido una serie de denominaciones que, ciertamente, no reflejan de manera clara su contenido. Entre las denominaciones utilizadas por la doctrina y coincidentes en cuanto a sus contenidos esenciales, HONDIUS se refiere a la Protección de Datos como "*aquella parte de la legislación que protege el derecho fundamental de libertad, en particular el derecho individual a la Intimidad respecto del procesamiento manual o automático de datos".*[91]

WESTIN, bajo la denominación similar de Information Control, define a esta como "*el derecho de los individuos, grupos e instituciones para determinar por sí mismos cuándo, cómo y con qué extensión la información acerca de ellos es comunicada a otros"*. FRIED, con la misma denominación y en la intención de superar la definición de WESTIN, entendió que "*es el*

[91] F. Hondius: "A decade of internatiomal Data Protection", citado por Pucinelli, Oscar: "Hábeas Data en Indoiberoamérica". Pág. 66.

control de la información sobre uno mismo, o la habilidad individual de controlar la circulación de la información referente a la persona"[92].

Por derecho a la "Autodeterminación Informativa"[93], fórmula utilizada por el Tribunal Constitucional Alemán en un célebre caso resuelto en 1983, se ha entendido aquél derecho que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones que les concierne, archivadas en bancos de datos; controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, disponer sobre su transmisión.

Con la denominación "Libertad Informática", PEREZ LUÑO alude a un nuevo derecho fundamental, propio de la Tercera Generación, que tiene por finalidad "*garantizar la facultad de las personas de conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos, controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su transmisión*"[94]; FROSINI, se refiere a ella como una nueva forma presentada por el derecho a la Libertad Personal, que emplea el derecho de controlar las informaciones

[92] Estadela Yuste, Olga: "Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales", citado por Pucinelli, Oscar. Ibídem. Pág. 66Ibídem.
[93] Puccinellu, Oscar. Ibídem. Pág. 66.
[94] Pérez Luño, Antonio E.: "Los Derechos Humanos en la Sociedad Tecnológica", citado por Pucinelli, Oscar. Ibídem. Pág. 67.

sobre la propia persona, es decir, el derecho de Hábeas Data; y LUCAS MURILLO la define como "*el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo, la propia identidad, nuestra dignidad y libertad*"[95]. Ese concepto de libertad informática, si bien mayoritario, no es unívoco. A nuestro criterio, debería significar aquella proyección del principio – valor "libertad" que, aplicado a la actividad informática, se traduce en el derecho de los operadores de estos sistemas de colectar, procesar y transmitir toda la información cuyo conocimiento, registro o difusión no esté legalmente restringido por motivos razonables, fundados en la protección de los derechos de las personas o en algún interés colectivo relevante que justifique tal limitación.

Con el nombre de Hábeas Data, EKMEKDJIAN y PIZZOLO se refieren al instrumento diseñado para controlar la calidad de la información personal contenida en bancos de datos, corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su posible transmisión; y, entre otros, la doctrina Española y particularmente la Corte Constitucional de Colombia, al derecho autónomo y fundamental que permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas y

[95] Murillo, Lucas, citado por Pucinelli, Oscar. Ibídem. Pág. 67

privadas, en defensa de sus derechos fundamentales a la intimidad, a la honra y al buen nombre[96].

Como se advierte, salvo por la distinta concepción que tenemos sobre lo que debe entenderse por “libertad informática”, y por la disímil naturaleza (derecho o garantía) que se le otorga al Hábeas Data, las diferencias entre los distintos términos mencionados son sutiles, y ciertamente, no reflejan con precisión el contenido del nuevo derecho; por lo que, es preferible establecer algunas diferencias entre ellos, para definir aspectos particulares de la cuestión en estudio y, consecuentemente, adoptar la expresión Derecho a la Protección de Datos para definir a aquél, y ello pese a que no se mejora de manera sustancial el panorama desde esta perspectiva lexical, toda vez que pareciera atender a la protección de los datos en sí, cuando en realidad pretende indicar que estos poseen una trascendencia especial y que, por ello, deben ser sometidos a un régimen particular protectivo.

Así, por derecho a la Protección de Datos se propone entender la suma de principios, derechos y garantías establecidos a favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos nominativos a ella referidos, con lo cual, al decir de PEREZ LUÑO, “la protección de datos personales tendría por objeto prioritario asegurar el

[96] Pucinelli, Oscar. Ibídem. Pág. 68.

equilibrio de poderes sobre y la participación democrática en los procesos de la información y la comunicación a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos", con lo cual tutelaría "el conjunto de bienes o intereses que puedan ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables"[97].

Aun admitiendo las definiciones dadas por la Doctrina a los términos precitados, se propone mantener al derecho a la Protección de Datos como denominación genérica por tener la aptitud mencionada para englobar todas las otras rotulaciones y conceptos; con lo cual, el derecho a la Autodeterminación Informativa bien podría ser una especie de él, y por haber sido así receptado en las principales normas internacionales sobre la materia, para evitar ambigüedades en el manejo de este vocablo.

En el esquema propuesto, la Autodeterminación informativa sería entonces un aspecto del derecho a la Protección de Datos, y el Hábeas Data su garantía, su instrumento procesal, que no alcanzaría como medio tutelar al derecho a la Protección de Datos, pues este incluye aspectos que exceden a las posibilidades del accionar judicial por la vía sumarísima y contradictoria del Hábeas Data.

[97] Pérez Luño, Antonio E.: "Los Derechos Humanos en la Sociedad Tecnológica", citado por Pucinelli, Oscar. Ibídem. Pág. 68.

3.2.4 Naturaleza Jurídica, Fundamento y Autonomía.

El reconocimiento del derecho a la Protección de los Datos encuentra su fundamento en la necesidad de tutelar una amplia gama de bienes jurídicos, que pueden verse afectados por el tratamiento de los datos nominativos, mediante una regulación con pautas propias que exceden del marco de aquellos derechos a los que pretende proteger. Por tal motivo, entendemos que se trata un derecho de carácter instrumental y autónomo. En efecto, pese a que muchos de los denominados "derechos" que poseen tal carácter instrumental son, en realidad, garantías, en virtud que constituyen en sí el medio técnico de tutela de ciertos derechos para cuya protección han sido creados (el derecho de réplica y el derecho de huelga), en este caso el derecho a la Protección de Datos contiene reglas de fondo propias y es tutelable mediante ciertas garantías, específicamente creadas para ello.

En este sentido, resulta clarificador lo señalado recientemente por BIDART CAMPOS, al sostener que dentro del ámbito tutelar de los derechos personales, y en afinidad con las garantías clásicas frente al Estado, hay "derechos" denominados tales que, en rigor, sirven y se usan para la defensa de otros derechos; a aquellos denominados derechos que se dirigen a proteger otros derechos se les asigna la categoría y la naturaleza de garantías[98].

[98] Pucinelli, Oscar. Ibídem. Pág. 69.

En definitiva, es de carácter instrumental, porque sirve de medio para la tutela de los derechos implicados, pero no pierde la categoría de derecho (y en ello está de acuerdo la doctrina) pues no alcanza a reunir las notas de la moderna concepción de las garantías.

Ya se dijo que el derecho a la Protección de Datos es autónomo. Aunque len la doctrina no hay unanimidad al respecto, se entiende que ello es así porque su contenido esencial, aunque se nutre en aspectos parciales con los de otros derechos que coadyuvan a su integración, es exclusivo de él.

Relata ZUNIGA URBINA que, desde el reconocimiento que hizo la jurisprudencia del derecho a la Autodeterminación Informativa en el sonado caso resuelto en 1983 por el Tribunal de Karlsruhe, por el cual se confería un poder jurídico a los individuos para disponer de la información personal en todas las fases de elaboración y uso, se produjo un amplio debate en la doctrina alemana, en especial entre quienes defienden el derecho como fundamental, autónomo o nuevo y los que ven en este una concreción del derecho general a la personalidad[99]; en este punto, parece acertada la observación de PEREZ LUÑO por cuanto "*aceptar un derecho a la*

[99] Zúniga Urbina, F. Citado por Pucinelli, Oscar. Ibídem. Pág. 70.

Autodeterminación Informativa como derecho fundamental autónomo acarrea el peligro de consagrar una especie de propiedad privada sobre datos personales, que niega la dimensión social y comunitaria de los derechos, pero pese a ello cabe defender la autonomía del nuevo derecho, con fundamento en la evolución y dinamicidad del derecho a la Intimidad, ya que negarla, para englobarlo en el derecho al libre desarrollo de la personalidad, soslayaría el carácter dinámico de los derechos fundamentales y dificultaría su relación con otros derechos de tal rango, puesto que una libertad apéndice de valores constitucionales y un derecho general tendría menor consistencia, y su fuerza dependería de estos".[100]

De otro lado, su carácter autónomo se justifica adicionalmente por la necesidad de reforzar la garantía, diseñando instrumentos específicos de tutela, como el Hábeas Data brasileño, que demuestran su entidad de derecho fundamental[101].

Sea como fuere, aunque se sostiene la autonomía del derecho, a nuestro criterio la protección de los datos personales no estriba tanto en añadir un nuevo derecho fundamental al repertorio de los ya conocidos, sino en asegurar el disfrute efectivo del conjunto de tales derechos. En ese

[100] Pérez Luño, A. E., citado por Pucinelli, Oscar. Ibídem. Pág. 71.
[101] Zúniga Urbina, F.: "Derecho a la Intimidad y Hábeas Data (del Recurso de Protección del Hábeas Data)", Disertación pronunciada en el Seminario Iberoamericano sobre la Acción de Hábeas Data, Universidad de Talca (Chile, abril, 1997), citado por Ibídem. Pág. 71.

sentido, es de advertir una importante coincidencia respecto de que, si bien puede argumentarse como fundamento de este derecho a otros preexistentes (Intimidad o Privacidad, de cuyas extensiones conceptuales históricamente proviene) el contenido esencial del derecho a la Protección de Datos difiere de aquellos (con lo que pudiera justificarse su autonomía) y requiere garantías específicas para su tutela.

3.2.5 Objeto y Contenido.

En lo que respecta al objeto de la protección los datos personales, comenta ESTADELA YUSTE que el derecho individual a la Protección de Datos puede variar en algunos aspectos entre las leyes nacionales o instrumentos internacionales. En general, se puede decir que el derecho a la Protección de Datos está relacionado con aquellos datos que hacen referencia a una persona física identificada o identificable, y que han sido objeto de una actividad realizada en parte o en su totalidad con ayuda de procedimientos automatizados, es decir, operaciones de registros de datos, aplicaciones a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión"[102].

Entonces, se pretende con su creación brindar una tutela especial a las personas físicas y, en varios sistemas, también jurídicas, frente a las afecciones a los derechos fundamentales que pudieran sufrir estas a partir

[102] Zúniga Urbina, F.: "El Derecho a la Intimidad y sus paradigmas", citado por Pucinelli, Oscar. Ibídem. Pág. 103.

del tratamiento de datos por parte del Estado y, aunque con ciertas restricciones variables según el ordenamiento de que se trate, de los particulares.

En cuanto al Contenido, el derecho a la Protección de Datos es de tipo genérico e instrumental. Por tal motivo, se integra con una serie derechos específicos otorgados al sujeto a partir de ciertos principios que son establecidos para el tratamiento de datos personales, con el fin de cautelar los bienes jurídicos especialmente protegidos por intermedio de aquél, y también de ciertas garantías específicamente diseñadas para la tutela de tales principios y derechos.

Si bien es factible observar que gradualmente se han ido estandarizando las respuestas jurídicas y, por tanto, los principales principios de la Protección de Datos, van encontrando similar alojamiento en los sistemas jurídicos occidentales, desde el punto de vista normativo se observa una diferencia importante entre los países que han dictado leyes específicas al respecto y aquellos que han establecido sólo su garantía jurisdiccional por vía constitucional. Los primeros detallan un conjunto de facultades otorgadas al sujeto que, a su vez, intentan ser tutelados por medio de una serie de garantías institucionales; los segundos, sin establecer principios rectores, reconocen ciertas facultades concretas que pueden ser reducidas, en el

criterio de EKMEKDJIAN y PIZZOLO, a los derechos de conocer, de acceder y de rectificar[103].

Los derechos específicos otorgados a los registrados, a fin de que se pueda hacer efectiva la tutela perseguida, con la creación del derecho a la Protección de Datos, son variadas y dependen de la extensión con que cada sociedad desea admitirlos; cabe recordar que, en muchos lugares, este derecho es todavía desconocido por el lento o nulo acceso a las nuevas tecnologías. Sin embargo, con las variantes mencionadas según el sistema de que se trate y las reglas de fuente internacional que le fueren aplicables, es factible establecer ciertas pautas mínimas, comunes a la mayoría de los ordenamientos jurídicos que lo han contemplado.

Para definir tales contenidos mínimos, a continuación se intentará determinar a groso modo, qué es lo que se protege, de qué y respecto de quién se protege y cómo se hace.

3.2.5.1 *¿Qué se protege?*

Responder a la primera pregunta nos lleva a recordar que en esta materia:

[103] Ekmekdjian, M.A. y Pizziolo C.: "Hábeas Data, el Derecho a la Intimidad Frente a la Revolución Informática". Pág. 63.

a) Si bien no se los protege *per se*, si no a los derechos que su publicidad pudiera lesionar, se tutelan “datos”, entendidos como elementos circunscriptos y aislados, aunque en realidad lo que se protege es la información que pudiera surgir de la relación entre datos. Al considerar ese aspecto, en el “*Lindop Repor”t* se entendió más correcto el uso del término Data que el de Information, pues este último se referiría al resultado final de la elaboración, mientras que el primero denominaría las informaciones iniciales a partir de las cuales se realizan todas las operaciones sucesivas y sobre ellas recaerían los controles y recibirían la máxima protección, ya que de ellas depende cualquier elaboración futura. La información personal se entiende en este sentido como: “*toda información que se refiere a cualquier dato del sujeto, que es o puede ser identificado por medio de informaciones como el nombre, la dirección, la edad, o el número telefónico”*[104].

b) Se protegen datos “personales”, por lo que debe entenderse los relativos a personas identificadas o identificables.

c) Se tutelan los datos de las personas físicas, y si bien existen diferencias respecto de que si debe alcanzar a las jurídicas, a las extranjeras y a las residentes, a nuestro criterio, si bien debe atenderse prioritariamente datos de personas físicas, no deben realizarse las exclusiones mencionadas.

d) Se amparan, para alguna doctrina, sólo cierto tipo de datos, en concreto aquellos vinculados con ámbito cerrado. Nos inclinamos por no

[104] Estadella Yuste, Olga: “La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales”. Pág. 130.

agotar los datos protegibles a ciertas y limitadas categorías, sino promoviendo el establecimiento de categorías especialmente protegidas de evaluarlos en función de la cantidad y calidad que se pretende tratar y los medios técnicos que se utilizan, pues ciertos tipos de datos aparentemente irrelevantes, al ser interconectados y procesados con sistemas inteligentes, permite descubrir aspectos de la persona que no debieran trascender sin su consentimiento.

3.2.5.2 *¿De qué y respecto de quién se protege?*

El derecho a la Protección de los Datos Personales se otorga frente a ciertas actividades respecto de los datos de tal tipo (acceso, registro, tratamiento y transferencia) desarrolladas por determinados sujetos.

a) *¿De qué se protege?* Entre las principales situaciones que se pretenden evitar, se cuentan:

- El acceso a la información personal por parte de terceros no autorizados: se trata de impedir que cualquier persona pueda acceder a datos personales sin causa justificada.
- El registro de ciertos datos: aquí se intenta evitar que determinados datos sean almacenados en sitios de donde puedan ser luego tomados por terceros distintos del registrador, y que se mantengan registrados de manera incorrecta o más allá de un término prudencial.

☻ El tratamiento ilegítimo de los datos registrados: en este supuesto se busca que los datos se mantengan tal como se encuentran registrados (si el sujeto se encuentra habilitado para registrarlos y están correctos) y no sean interconectados con otros o sometidos a operaciones de transformación que lleven a la configuración de perfiles virtuales de las personas, sin que medie causa justificada.

☻ La transferencia no autorizada de los datos: aquí se procura que los datos no sean proporcionados a terceros sin autorización expresa del interesado o de Ley (algunas normas se preocupan especialmente del flujo de datos más allá de las fronteras) y especialmente que no sean almacenados en otros registros sin que medie causa justificada, de manera que por vía de la interconexión de los datos, puedan ser sacadas conclusiones en base a ellos.

b) *¿De quién se protege?* El derecho a la Protección de Datos se formula para ser ejercido contra cualquiera que realice las actividades reseñadas; esto es, las de acceso, registro, tratamiento y transferencia de datos, y que por tal virtud los datos trasciendan a terceros.

No existe uniformidad respecto de qué calidades deben reunir estos sujetos pasivos del control propio del régimen de protección de datos, sobre todo respecto de si deben ser alcanzados sólo los bancos y bases de datos

informatizados (o si por el contrario, pueden incluirse los ficheros manuales); si deben ser incluidos únicamente los públicos o si también cabe incluir los privados, y en tal caso, cuáles podrían ser alcanzados (esto es, si deben estar diseñados y destinados a la provisión de informes o si bien, por el contrario, basta con el hecho de que tal comunicación de los datos sea posible).

3.2.5.3 *¿Cómo se protege?*

El derecho a la Protección de Datos puede ser tutelado de diversas formas, entre las cuales las más comunes son las siguientes:

1) Las normas generales o específicas, convencionales, constitucionales o legales que establezcan:

a. Ciertas reglas mínimas para el Tratamiento de Datos y para la habilitación de las bases y bancos de datos, específicamente limitando sus actividades de tratamiento de datos a las estrictamente necesarias para la finalidad para la cual son autorizadas.

b. Una serie de derechos de los registrados.

c. Sanciones de tipo administrativas y penales para quienes infrinjan ciertos aspectos de las normas (Art. 8º de los Principios de la ONU, Art. 10 del Convenio Europeo de 1981 y Art. 24 de la Directiva Europea de 1995).

d. Mecanismos institucionales de garantía (como una comisión de habilitación y seguimiento de los bancos de datos personales)

e. Recursos frente a esas instituciones u otras vías administrativas idóneas.

f. Vías judiciales de Amparo, específicamente amoldadas a la tutela de los datos (el Hábeas Data del Constitucionalismo Iberoamericano)

g. La remisión a mecanismos procesales que sirvan, de manera genérica, para la tutela de los derechos fundamentales (al Amparo, Tutela o Recursos de Protección)

2) Las normas sectoriales que traten aspectos puntuales (alcances de los secretos impositivos o estadísticos)

3) Los contratos – acuerdos respecto del tratamiento de determinados datos.

4) Los códigos de conducta o de ética.

5) Ciertos convenios internacionales (globales o regionales) que regulen ciertos aspectos comunes, en especial lo relativo al flujo de datos más allá de las fronteras.

3.2.6 Bien Jurídico Tutelado por la Protección de Datos Personales.

Es de todos conocido que la creación de nuevas necesidades, como resultado socio cultural proveniente del desarrollo histórico, es lo que lleva a brindarles un valor a dichas necesidades, las cuales por virtud del pacto social adquieren cierta trascendencia jurídica, es decir, que se les comienza

a brindar protección, puesto que reportan utilidad al conglomerado social, considerándoseles como bienes. De ahí que surgen los bienes jurídicos.

Por bienes jurídicos se entiende los bienes vitales, los valores sociales y los intereses reconocidos jurídicamente del individuo, por ejemplo, la vida, la integridad corporal, la libertad personal, el honor, la propiedad y el patrimonio (bienes jurídicos individuales) Son bienes jurídicos de la colectividad, entre otros, la integridad del Estado y de su régimen de libertad y democracia, la salva guarda de secretos de Estado, la Administración de Justicia, la incorruptibilidad de los funcionarios (bienes jurídicos universales)[105].

La Doctrina en general considera que el bien vital tutelado con la Protección de los Datos Personales es la Intimidad, puesto que es esta la que conlleva el deber del sigilo, y en consecuencia, el deber de no revelar ciertas informaciones de los individuos sin su consentimiento. Las elaboradoras del presente estudio no están de acuerdo con esta posición, en virtud que, como ya se ha mencionado en lo referente a la definición de lo que debe entenderse como datos personales, estos pueden ser considerados desde una doble perspectiva; por lo que existen algunos aspectos protegidos con la tutela a los datos personales, que no están

[105] Wessels, Johannes: "Derecho Penal" (Parte General) citado por Alfaro Escoto, D.A. y otros. Ob. Cit. 49.

ligados directamente con la Intimidad. A manera de ejemplo, y tal como lo manifiesta Pablo Andrés Palazzi, con los datos sensibles que son susceptibles de producir discriminación, lo que se trataría de proteger no es la Intimidad, sino más bien la Igualdad; o cuando se habla de datos que son falsos, lo que se tutela es la verdad[106]. En ese sentido, es que se llevará a cabo el planteamiento sobre el bien jurídico que es tutelado.

En un primer momento, cuando se hace referencia a los datos personales de carácter personalismo, sí se podría aceptar que la protección está destinada a asegurar, por un lado, la integridad del derecho a la Intimidad, pero debe recordarse que los derechos de la personalidad encierran un conjunto de aspectos, los cuales sirven de protección a otros, de ahí que surja la denominada teoría de las esferas de los derechos de la personalidad. Esta teoría presupone que los derechos existen como una espiral, o en esferas, colocándose unos fuera y otros dentro de la espiral, dependiendo de la situación específica.

Así puede afirmarse que lo que se protege con la tutela a los datos personales de carácter personalismo no es la Intimidad en sí, sino más bien el honor; ya este conlleva implícitos dos aspectos básicos que son: uno subjetivo referido a la inmanencia o mismicidad que consiste en la estimación que cada persona hace de sí misma o cualidad moral que se contrae al

[106] Palazzi, Pablo Andrés, citado por Alfaro Escoto, D.A. y otros. Ob. Cit. 50.

cumplimiento de deberes; otro, de carácter objetivo, que consiste en la trascendencia o exterioridad integrada por el reconocimiento que los demás hacen de nuestra dignidad, que es la reputación o fama que acompaña a la virtud, lo que podría ser dañado con la publicación de ciertas informaciones que pongan en grave situación al titular de dichas informaciones; incluso, para muchos el derecho a la Intimidad o a la propia imagen no existe, sino lo que existe es el honor y llaman a aquellas manifestaciones del honor, llegando así a la conclusión, que la función de la vida privada es velar por la integridad del honor.

Otra parte de la doctrina considera que el bien jurídico tutelado es un derecho humano de tercera generación elevado a la categoría de fundamental en algunos países como Alemania; este derecho es el denominado derecho a la Autodeterminación Informativa, consistente en la facultad de disponer sobre la revelación y utilización de datos personales, que abarcan todas la etapas de la elaboración y uso de los datos por medios informáticos, es decir, su almacenamiento, registro, calificación, modificación, transmisión y difusión.

En verdad, es este derecho lo que toma a los datos personales como su objeto y no al contrario, es decir, que este derecho lo que protege es los

datos, como si fuese eso lo que se tratase de proteger en última instancia. En síntesis, consideramos que es un medio para la protección de los datos.

A nuestro parecer la protección de los datos personales de carácter personalisimos, tiene arraigado su objeto en un aspecto más profundo que el de brindar protección al honor, mas bien a lo que brindan protección en todo momento es lo que sostiene el honor; hablamos aquí de la integridad moral aquello que hace de cada uno lo que es y, de esta forma le permite insertarse en la vida social y en la vida publica enlazándose con el principio de la dignidad de la persona y de sus derechos inviolables, reconocidos constitucionalmente como fundamento del orden político y de la paz.

Por el otro lado, con la tutela de los datos sobre la persona, lo que se trataría de tutelar no es un aspecto meramente moral o espiritual, sino la protección se podría dirigir a un campo vasto de derechos de la persona integra, dependiendo de los casos en concreto. Así, podría decirse que con evitar la publicación de información financiera de alguien que tiene mucho dinero, se podría evitar un posible secuestro, salvaguardando la libertad ambulatoria, o incluso la vida misma; o bien, con el acceso a cierta información en donde se contengan datos de que establezcan que el accionante pertenece a un sindicato, lo que en realidad es falso, y puede ser borrado posteriormente, se garantiza el derecho a la estabilidad laboral.

3.2.7 Mecanismos de Protección de los Datos Personales.

Actualmente, existen varios mecanismos de protección de los Datos Personales, funcionando alrededor del mundo, y, en algunos países, se utilizan uno o más de estos mecanismos, dependiendo de lo que las necesidades dicten. Básicamente los modelos o mecanismos los podemos clasificar atendiendo a su formalismo como jurídicos y no jurídicos.

Los primeros, tienen su fundamento en una regla ya trazada, es decir una ley, la cual describe las funciones de las figuras doctrinarias adoptadas por ese sistema y los principios contenidos en las mismas, y por tener su base en un precepto jurídico son de obligatoria observancia. Tales figuras son:

A) El Comisionado para la Protección de Datos.

B) Leyes Especiales que regulan lo referente a los datos.

C) El Hábeas Data.

Por el otro lado, cuando se habla de Mecanismos no Jurídicos de Protección de Datos, nos referimos a aquellos procedimientos o prácticas voluntarias regidas básicamente por un carácter ético, tendientes a brindar un especial cuidado a las informaciones que son tratadas por determinadas instituciones. Este tipo de mecanismos no son los únicos que existen, pero entre los que con más frecuencia se usan, se encuentran los siguientes:

A) La Autorregulación de la publicidad por parte de las instituciones.

B) El Encriptamiento.

3.2.7.1 *Mecanismos Jurídicos:*

A. El Comisionado para la Protección de Datos.

El modelo adoptado por países como Alemania, Suecia, Estados Unidos de Norte América, Hong Kong, Australia y otros, consistente en una figura de un Oficial Público, encargado de aplicar directamente las leyes, referentes a las informaciones de los individuos que estén en registros o bases de datos de oficinas públicas o aun privadas.

Las facultades concedidas a este funcionario, varían dependiendo del país de que se trate, pero básicamente, la esencia de la función es la misma en todos: “la protección de la información”.

Con el fin de tener un mayor acercamiento con esta figura es oportuno realizar una revisión de la Ley Federal sobre Protección de Datos de Alemania de 20 de diciembre de 1990, contenida en el Código Civil 1.I. Pág. 2954 modificada en la Ley 17.12.1997 contenida en el Código Civil 1.I. Página 3108[107], que es el cuerpo legal que le da vida en este país.

[107] Ley 17.12.1997, citada por Alfaro Escoto, D.A. y otros. Ob. Cit. 54.

En primer lugar, el fin de esta Ley es brindar protección al individuo para evitar dañar sus derechos de la personalidad por medio de la manipulación de la información sobre su persona.

El campo de aplicación de la mencionada ley es extensible al levantamiento, procesamiento y utilización de los datos personales, automatizados o manuales, ya sea por oficinas publicas de la Federación Alemana, por los Estados de la Federación individualmente (siempre que no exista una ley en ese Estado que regule una situación similar) por el Organo Judicial actuando en casos que no sean asuntos de la Administración, por oficinas privadas, y otros que se establecen en las consideraciones generales, Sección 1ra. Se aplica así mismo a la Transferencia de los Datos.

Cabe mencionar que dentro de las definiciones que la Ley da, cuando establece qué debe entenderse por datos personales, señala que estos son informaciones individuales sobre relaciones personales o materiales de una determinada persona natural, por lo que puede notarse que excluye a las personas jurídicas (no obstante ello, en su artículo 19 (3) establece que los derechos fundamentales rigen también para las personas jurídicas con sede en el país, en tanto por su propia naturaleza sean aplicables a las mismas), y es que la Dignidad Humana es intangible ... Es lo que reza la primera frase del artículo uno de la Constitución Federal. El sistema judicial, a través de la

jurisdicción del Tribunal Constitucional Federal, desarrolla y protege la dignidad del individuo por medio del derecho a la Autodeterminación Informativa, es decir, el derecho del individuo por medio del cual decide sobre la revelación y uso de sus datos personales. Desafortunadamente, no fue incluido de manera expresa en la Constitución Federal, lo cual hubiese traído una importancia mayor para dicho derecho fundamental. No obstante, en algunos Estados (Länder) se incluye expresamente el derecho a la protección de los datos personales, como por ejemplo, en el artículo seis de la Constitución del Estado de Mecklenburg – Vorpommern, el cual en su párrafo primero literalmente dice: "*Todos tienen derecho a la protección de sus datos personales. Este derecho está limitado por el derecho de los terceros y por la prevalencia del interés general*"[108].

La Ley Federal concede el procesamiento de datos sólo cuando sea expresamente permitido por la misma, por otra o cuando exista consentimiento por parte de la persona cuyos datos se procesan, para lo cual, tal consentimiento debe constar por escrito; o en el caso del procesamiento para fines científicos, cuando se compruebe que no afecta a su titular y sea necesario para los fines de la investigación. Además, en la Ley se establece el deber de las personas que trabajan con los datos a guardar secreto de ellos, pues recordemos que lo que se trata, es de

[108] Constitución del Estado de Mecklenburg – Vorpommern citada por Alfaro Escoto, D.A. y otros. Ob. Cit. Pág. 55.

resguardar la información en ellos contenida, no importando cuál sea su medio de difusión[109].

En lo que respecta a las cuestiones particulares sobre el Comisionado Federal para la Protección de Datos (Bundesbeayftragter für den Datenschutz), puede mencionarse que, en cuanto a su funcionamiento, "*es el Parlamento Federal a propuesta del Gobierno Federal quien lo elige, con más de la mitad de sus miembros, luego es nombrado por el Presidente Federal y funge para un período de cinco años, permitiéndose solamente una vez su reelección*"[110]. Un punto muy importante es el relativo a la independencia en sus funciones; este ejerce el derecho de vigilancia del Gobierno Federal, encontrándose adscrito y subordinado al Ministerio del Interior, donde se arreglará con el presupuesto destinado al dicho Ministerio para los asuntos financieros. El legislador alemán, previendo los casos de corrupción, impone la obligación al Comisionado, de dar aviso al Ministro Federal del Interior, sobre obsequios que se recibieren, y este Ministro dispondrá de ello como más le parezca; para garantizar una mayor efectividad y disposición de sus actuaciones, no podrá ejercer durante su período ningún otro cargo público remunerado, ni ejercer otra profesión.

[109] Alfaro Escoto, D.A. y otros. Ob. Cit. Pág. 55.
[110] Alfaro Escoto, D.A. y otros. Ob. Cit. Pág. 56.

La finalización de las función del Comisionado es, bien por haber transcurrido el tiempo para el cual fue designado, por despido o renuncia. Este despido es llevado a cabo por el Presidente del Federal a propuesta del Gobierno Federal.

Algo que llama la atención es que en la Ley no se señalan requisitos especiales para ser elegido Comisionado Federal para la Protección de Datos Personales, únicamente se hace referencia a que ”*debe tener treinta y cinco años al momento de su elección*”[111].

Las funciones básicas del Comisionado estriban en:

Ejercer control de vigilancia respecto de las actividades relacionadas con los datos personales llevadas a cabo por las Oficinas Publicas, ejecutando su competencia de la siguiente manera:

En la sección 24 numero (1) se dispone que los datos personales que sean procesados o utilizados serán controlados en su levantamiento, procesamiento y utilización, cuando el afectado demuestre que por ese motivo sus derechos han sido dañados, o el Comisionado tenga la convicción que existe un daño. El Comisionado puede actuar a petición del interesado o de oficio[112].

[111] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 56.
[112] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 57.

Se extiende la protección hacia aquellos datos los cuales están en una oficina donde se almacenan datos de Profesionales o una en concreto, donde por razón de los datos, se deba guardar secreto, como por ejemplo, el secreto tributario. En el caso de las comunicaciones postales (art. 10 de la ley Fundamental Alemana), dicha facultad esta restringida a menos que esté expresamente determinada por la oficina especifica[113].

La ley establece, entre otras excepciones de control por parte del Comisionado, el secreto médico (sección 24 (2) 2.b). Además en la ley se establecen otras funciones como: Brindar asesoría a las personas sobre lo que concierne a la protección de datos, recibir peticiones dentro del derecho que tienen las personas de dirigirse a él, cuando sus datos no sean tratados en la forma que la ley establece; brindar asesoría técnica a las oficinas públicas de los Estados de la Federación, así como dar recomendaciones para el mejoramiento de la protección de los Datos Personales. Establecer criterios generales que ayuden al mejoramiento de la protección, y en especial, la corrección de los datos que estén incorrectos. Así mismo las oficinas públicas, están en obligación de brindar apoyo al Comisionado Federal como a los comisionados designados en su sedes. Con respecto al control en las Oficinas Privadas que se dediquen al procesamiento de datos personales, y que por lo menos empleen cinco trabajadores, se establece en la sección 36 la obligación por parte de éstas a nombrar un Comisionado

[113] Alfaro Escoto, D.A. y otros. Ibídem.

para la Protección de Datos, dentro de un mes luego de haber comenzado con sus actividades.

Las funciones son parecidas a las del Comisionado Federal, y trabajan en cooperación para brindar una mayor efectividad al cumplimiento de las leyes, ya que la cantidad de empresas privadas existentes en este país acumularía de gran trabajo al Comisionado Federal haciendo inoperante su función.

B. Leyes Especiales.

Este tipo de leyes están encaminadas a brindar protección a los individuos de manera específica sobre sus datos personales; así, Estado Unidos de Norte América tiene un conjunto de leyes encaminadas a dicho fin, aclarando que también adopta la figura del Comisionada para al Protección de Datos (Registrar)

El presente estudio se va a enfocar en dos leyes, por considerarlas fundamentales, ya que representan el punto de partida del sistema de Protección de la Privacidad no sólo en este país, sino a nivel mundial; estas son las siguientes: el Acta de la Libertad de Información de 1966 y el Acta de Privacidad de 1974.

En cuanto al *Acta de Libertad de Información* (Freedom of Information Act or FOIA): promulgada en 1966, prevé de manera general el derecho de acceso de las personas, pero sólo a los registros de informaciones de las Agencias Federales; por ejemplo, se puede solicitar y recibir una copia de cualquier registro que esté en los archivos oficiales de las agencias federales que no esté bajo ninguna excepción, así, si alguien desea información acerca del más reciente reporte sobre inspección de las condiciones de un hospital, la oficina de seguridad social local que lleva tales registros, los que solicitados en debida forma, deberá proveerlos; o si se quiere saber si la Oficina Federal de Investigación (F.B.I.) tiene un archivo que incluye al solicitante. Bajo los criterios de esta Ley se dieron a conocer algunos reportes que eran considerados de máxima seguridad, como el caso Rosswel de Nuevo México o el asesinato del Presidente de los Estados Unidos, John F. Kennedy, que hoy ya pueden ser accesados vía Internet.

Para fines ilustrativos, las excepciones contempladas en el Acta son:

1) Material clasificado como información de Defensa Nacional o información sobre las relaciones internacionales.

2) Reglas y prácticas del personal interno de las agencias.

3) Material prohibido de ser revelado por otra Ley.

4) Tratados secretos y otros negocios confidenciales.

5) Cierta inter – intra comunicación de las agencias.

6) Información personal médica y otros archivos conteniendo información personal privada.

7) Ciertos registros recopilados para efectos judiciales.

8) Cuestiones relacionadas con la supervisión de instituciones financieras.

9) Información geológica sobre bienes petroleros[114].

La acción de este derecho puede ejercerse directamente por el interesado a la oficina correspondiente o bien puede ejercerse por vía judicial cuando en la anterior vía fuere denegado.

Ahora bien, para que la oficina a la que se ha dirigido la solicitud pueda efectivamente encontrar la información se debe especificar lo más exactamente posible, ya que si no es encontrada luego de un período razonable de búsqueda, no está en la obligación de proveer la información; además, la FOIA no obliga a las agencias a investigar o compilar o analizar los datos, ni responder preguntas sobre tal información.

Una crítica que puede hacerse, en relación a las acciones que posibilita esta Acta, es que permite tantas excepciones, que se podría pensar que ellas son la regla general, y la cuestión empeora cuando, en algunos casos, los términos son muy vagos, por ejemplo, el conocido Secreto

[114] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 60.

de Estado, el cual puede ser extremadamente amplio. Así mismo, cuando se solicita información a una oficina y esta considera que los datos proporcionados por el solicitante son insuficientes para localizar lo pedido, y luego de un plazo razonable, de búsqueda, no se encuentra la información. ¿Qué se debería de entender por plazo razonable?

En lo relativo al *Acta de Privacidad*, como se sabe el Gobierno Federal estadounidense es uno de los Estados que más información compila sobre los individuos, y así por ejemplo, si alguien ha prestado servicio militar o ha sido empleado en una agencia federal deben existir registros de su servicio; si ha aplicado para una concesión federal o si ha recibido una beca escolar prestada por el gobierno, sin duda esa información estará en un archivo. Existen registros de cada individuo que paga sus impuestos, o reciben cheques de Estado en concepto de seguridad social o servicios hospitalarios[115].

El Acta de Privacidad, establece ciertos controles sobre qué informaciones personales son recolectadas por el gobierno y de qué manera será usadas. Básicamente el Acta garantiza los derechos fundamentales a:

1. Ver archivos acerca de la persona, fuera de los casos de excepción.

[115] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 61.

2. Derecho a corregir el archivo si no es preciso, o si la información es irrelevante, desfasada o incompleta.
3. El derecho a promover acciones en contra del gobierno, por violaciones a la Ley, incluso cuando se permitan a otros ver los archivos de la persona, a menos que esté específicamente expresado[116].

De igual manera, provee ciertas limitaciones a la práctica de agencias de información, tales como, que el requerimiento o recolección de datos de un individuo se de en toda su magnitud; requerir de las agencias, que aseguren que las informaciones son relevantes, precisas, actuales y completas, y prohibe que las agencias mantengan información acerca de cómo la persona ejerce sus derechos constitucionales, a menos que ella lo consienta, o por virtud de una Ley o de una investigación.

Las informaciones que se pueden invocar con el Acta son sólo aquellos documentos acerca de personas que son mantenidos por las agencias pertenecientes al Organo Ejecutivo Federal, pero aplican sólo si estos se encuentran en el sistema de registros, es decir, que sólo pueden ser localizados por un indicador, como el nombre de la persona, el número del seguro social o alguna otra forma de identificación personal. El Acta de Privacidad no aplica su uso hacia archivos de personas que están

[116] Alfaro Escoto, D.A. y otros. Ibídem.

registrados en otras materias, como por ejemplo, miembros de organizaciones o clubes.

Dentro del Acta se establecen diez excepciones, por las cuales una agencia de información está facultada para retener ciertos datos[117]. Algunos de estos ejemplos son: las informaciones clasificadas como de seguridad nacional o la concerniente a investigaciones judiciales; otra de las excepciones usualmente invocada, es la de impedir el conocimiento de información que permite identificar una fuente confidencial.

Básicamente, la diferencia de la FOIA y el Acta de Privacidad estriba, en que la primera se refiere a cualquier tipo de datos en registros federales, no necesariamente sobre datos personales, y la segunda, se aplica sólo a datos concernientes a los individuos.

Otras leyes federales acerca de la Protección de la Privacidad son: Acta de Privacidad sobre el Derecho de Educación Familiar de 1974 conocida como la Enmienda Buckley 20 USC s.1232g.; Acta de Privacidad de Comunicaciones Electrónicas de 1986 18 USC 2510; Acta sobre Reporte de Créditos Justos de 1992; Acta de Protección de Privacidad del

[117] Alfaro Escoto, D.A., y otros. Ibídem. Pág. 62.

Consumidor por Internet de 1997; Acta de Protección de Privacidad de Videos de 1998 (Bork Bill), 15 USC 1681[118].

C. El Hábeas Data.

Debido a que este mecanismo de protección de datos personales será tratado más adelante en un apartado especial, no se hará mayor comentario al respecto.

3.2.7.2 *Mecanismos No Jurídicos:*

A. Autorregulación en la publicación de informaciones.

Cuando hablamos de Autorregulación en la publicación de las informaciones, nos viene a la mente un conjunto de actos y procedimiento que son adoptados por los encargados y colaboradores de las instituciones dedicadas al procesamiento y publicación de ciertos datos, información, publicidad sobre artículos, etc., cuyo fin es la protección de los titulares de los mismos o algún aspecto hacia quienes se dirigen. Así por ejemplo según José Miguel González Llorente, la Autorregulación de la Publicidad " es lo que se conoce como Autorregulación Publicitaria. Los anunciantes, las agencias publicitarias y los medios de comunicación se ponen de acuerdo, suscriben un código de ética y crean un órgano representativo llamado CONAR, o Consejo Nacional de Autorregulación Publicitaria. El CONAR administrará un sistema de vigilancia de la publicidad para garantizar que se

[118] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 62.

cumpla a cabalidad el código de ética que todos firmaron. Esto asegura una publicidad responsable, regulada por sus propios autores. La autorregulación publicitaria funciona exitosamente en todos los países miembros de la Unión Europea, en Estados Unidos y Canadá. En América Latina opera en Brasil, Chile, Colombia, El Salvador y en México desde fines del pasado año. Además, la autorregulación publicitaria está en vías de implementación en países como Argentina, Honduras, Paraguay, Perú y Uruguay; en Venezuela funciona desde hace años un órgano precursor del ONAE, que es el Código de Etica Unificado Anda – Fevap".[119]

En nuestro país funciona desde el 30 de septiembre de 1999 un código de ética de la prensa, elaborado por la Asociación de Periodistas de El Salvador (APES). El artículo 39 de ese Código presupone que las normas éticas contenidas en el mismo son de aceptación personal, pero se recomienda su cumplimiento a los miembros de la APES y a todo aquél que pertenezca a la empresa de las comunicaciones y esté en condiciones de decidir el manejo de la información y los artículos de opinión. Dicho código se basa en algunos principios básicos tales como la verdad, la justicia, la dignidad humana, el Estado Democrático, la cultura de la tolerancia, el perfeccionamiento de la sociedad y la fraternidad entre los pueblos.

[119] González Llorente, José Miguel citado por Alfaro Escoto, D.A. y otros. Ob. Cit. 64.

Otras de las obligaciones morales que se deben seguir, según el Código, es en cuanto a que la difusión de las informaciones debe estar fundamentada sobre bases sólidas y confiables de lo que se va a dar a conocer, encaminado esto a evitar datos imprecisos que pudiesen ocasionar lesiones o menosprecio en la dignidad de las personas o un descrédito injustificado de las instituciones. Así mismo, prohíbe la utilización de calificativos injuriosos y la descripción morbosa de la violencia y llama a la cordura y consideración para con las víctimas y sus familiares en cuanto a la publicación de imágenes sobre crímenes o accidentes. Se impone una especial importancia a la protección de la imagen e intimidad de las personas y más específica, cuando se tratase de menores de edad; además, señala categóricamente toda publicación que pueda ocasionar discriminaciones, ya sea de sexo, raza, nacionalidad, religión, creencias ideológicas, etc.

B. Encriptamiento.

El avance tecnológico crea nuevas necesidades poniendo en peligro otros del individuo en sociedad. Así surge en ese contexto lo que se conoce, hoy en día, como Encriptamiento, el cual consiste en un “procedimiento que permite asegurar la transmisión de informaciones privadas por las redes públicas desordenándola matemáticamente (encriptándola) de manera que sea ilegible para cualquiera, excepto para la persona que tenga la llave que

puede ordenar (desencriptar) la información"[120]; es decir, que es una manera de codificar la información de un fichero o de un correo electrónico de manera que no pueda ser leído en caso de ser interceptado por una tercera persona mientras viaja por la red. Sólo la persona o personas que tienen software de descodificación adecuado puede descifrar el mensaje. Los dos tipos más comunes de Criptografía son los de "misma llave" y "llave pública".

En la criptografía con la misma llave, un mensaje es encriptado y desencriptado utilizando la misma llave, que se manda en un envío separado. El método de llave pública es más seguro, el cual utiliza un par de llaves diferentes (una pública y una privada) que pueden tener una relación particular entre sí, de manera que un mensaje encriptado con una llave, sólo puede ser desencriptado con la otra y viceversa.

[120] Alfaro Escoto, D.A. y otros. Ob. Cit. 67.

CAPITULO IV

4. EL HABEAS DATA: CARACTERIZACION Y NATURALEZA JURIDICA. REGISTROS DE DATOS PERSONALES Y LA TRANSMISION INTERNACIONAL DE DATOS.

Las distintas revoluciones que vivió la sociedad determinaron cambios referidos a los sistemas políticos, económicos, industriales sobre el control de los medios de producción, distribución, comunicación etc., pero talvez ninguna de ella sea tan importante y general como la revolución de la información y sus consecuencias, frente a esto nacen las preguntas, ¿Como controlar la difusión de la información personal? ¿Es posible este control y que tipo de barreras pueden oponerse al avance de la divulgación de la información? Sin ninguna duda deberían existir límites, ya que no toda la información que pueda originar una persona es relevante social o públicamente. Incluso, información referida a situaciones exclusivamente personales puede llegar a ser utilizada en forma discriminatoria lo que

vulneraría derechos personales; se considera que este ha sido uno de los mayores impactos que el desarrollo informático ha tenido en el derecho a la Intimidad.

Frente al derecho de acceder a la información, ahora mundial, existe el derecho del ciudadano de preservar su intimidad si ésta se ve vulnerada; si los medios para evitar la circulación de la información son escasos, entonces, también se debe evaluar la necesidad de reparar los daños que la circulación de la información puede causar; en este sentido; países como Suecia , Francia, Noruega fueron los pioneros modernos a la hora de legislar acerca del derecho de las personas de acceder a la información que a su respecto contienen los bancos de datos; así nació el concepto actual de Habeas Data, brindando a los individuos la posibilidad de acceder a la información contenida en los bancos de datos, cualquiera que fueran ellos, y de lograr su supresión en caso de que sea errónea, modificándola y/o actualizándola cuando sea necesario o cuando sea discriminatoria.

4.1 CONCEPTO DE HABEAS DATA.

La consecuencia para los Estados del actuar globalizado será la aceptación por la comunidad internacional y publicidad de los actos de gobierno y su revisabilidad. Para el hombre común, por su parte, implicará la

aceptación por la comunidad en la que actúe y una pérdida de su anonimato proporcionalmente mayor en función de la cantidad de actividades exteriores que realice. El fenómeno de la privatización de las empresas públicas y la consecuente presión tributaria de los Estados para obtener recursos que permitan la realización de sus funciones básicas y específicas determina la necesaria registración de comerciales por insignificantes que fueren; a ello hay que adicionarle la existencia y aceptación de nuevas formas de cancelación de operaciones comerciales, tales como cheques, tarjetas de crédito, etc., que determinan que quien realiza una actividad social no sea un ser anónimo, sino una persona que actúa con nombre y apellido.

En proporciones incalculables, los datos de los individuos van ingresando al conocimiento y registros de otros en forma espontánea y constante, y los que son anónimos socialmente no lo son tanto respecto de aquellos que poseen las bases o registros informáticos.

Al hablar de Hábeas Data, nos viene a la mente, por analogía, la locución latina Hábeas Corpus, que quiere decir “que tengas el cuerpo” y que *marca el origen de un conocimiento especial que se exige respecto de causas cuando no se sabe dónde está el detenido o por qué razones fue privado de su libertad*[121]; el Hábeas Data es un híbrido de voces, la primera

[121] Pierini, Alicia y otros: “Hábeas Data. Derecho a la Intimidad”. Pág. 21.

tomada del latín “Hábeas” que significa “tráigase”, y el segundo tomado del inglés “Data”, que significa “Dato”. Puede decirse entonces, que así como el Hábeas Corpus intenta traer el cuerpo de la persona de que se trata la acción, el Hábeas Data significa “que tengas los datos” o “que vengan los datos” o “que tengas los registros”, es decir, implica tomar conocimiento de datos propios en poder de otro[122].

El Hábeas Data no está referido a una situación relacionada con lo corporal o ambulatorio como la libertad personal, sino que alude al interés del magistrado y/o de las personas de conocer en forma directa la registración de los hechos, es decir, el dato o la información. De ahí la posibilidad de ordenar la remisión de los registros o archivos de datos para constatar la autenticidad o corrección de lo expresado. En consecuencia, respecto de la locución latina que le da el nombre propio al instituto en estudio, se podría referir alguna crítica en su elección, pero hay que reconocer que la expresión es feliz como composición latina para un derecho de fin de siglo de la informática. En ese sentido, *Hábeas*, segunda persona del presente subjuntivo de *habeo... habere,* significa aquí “*tengas en posesión*”, que es una de las acepciones del verbo, y *data* es el acusativo plural de *datum*, que los diccionarios más modernos definen como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación

[122] Pierini, Alicia y otros. Ibídem.

y procesamiento por medios automáticos. Entonces: que tengan los registros, los datos[123].

El Hábeas Data es una figura nueva; configura un mecanismo de los consagrados como garantías constitucionales, dirigidas a la protección de la Intimidad de datos personales, del derecho a las informaciones respecto del interesado y de la oportunidad de su eventual rectificación. Es posible conceptuarlo como un remedio constitucional o instrumento para sanar o corregir, el abuso en razón de informaciones constantes en archivos o bases de datos.

Como esta figura es una garantía, trata de tutelar un derecho, pero aun no existe uniformidad en la doctrina. En un inicio se establecía que era la Intimidad, para lo que la doctrina Alemana[124] argumentaba que no podía ser esta, ya que no sólo conformaba una garantía de negación, o sea impedir que se dieran a conocer públicamente las informaciones sobre la persona; en ese sentido, posteriormente se erigió, en virtud de la amenaza que representaba el desarrollo tecnológico, el derecho a la Libertad Informática. Al igual que la Intimidad, este permitía al titular impedir la divulgación por medios informáticos de los datos personales; sin embargo, en razón de la doctrina alemana, dicha facultad negativa no era suficiente, sino que además

[123] Pierini, Alicia y otros. Ibídem. Pág. 22.
[124] Pierini, Alicia y otros. Ibídem. Pág. 69.

debía existir una facultad positiva, consistente en tener el acceso a los soportes de las informaciones, y aún más allá, poder ejercer otras acciones sobre estos datos allí contenidos.

Es así como con la resolución dictada por el Tribunal Constitucional Federal de Alemania sobre Ley de Censos de 1983[125], surge una nueva doctrina y nace el derecho a la Autodeterminación Informativa, posibilitando tanto impedir que se publiquen los datos de una personas sin su consentimiento (facultad negativa), como permitirle el acceso con el fin de que sepa qué informaciones hay sobre ella en determinado banco o registro de datos, para poder ejercer ulteriores acciones (facultad positiva)

4.2 OBJETIVOS DEL HABEAS DATA.

Entendido como un derecho reconocido, individualizado y protegido por la Constitución, se le debe permitir a una persona acceder a todo registro de datos, sea público o privado, a ella referido y sin importar su finalidad, para tomar conocimiento de los mismos, y en caso de existir falsedad o discriminación contar con un medio legal expedito y urgente que le permitirá suprimir, rectificar, modificar, actualizar, en todo o en parte, el dato en

[125] Tribunal Constitucional Federal de Alemania sobre Ley de Censos de 1983, citado por Pierini, Alicia y otros. Ibídem. Pág. 70.

cuestión, para que se subsane la falsedad y el menoscabo que pudiera implicar.

En consecuencia, el Hábeas Data presupone la existencia "...*de cinco objetivos principales: a) que una persona pueda acceder a la información que sobre ella conste en un registro o un banco de datos; b) que se actualicen los datos atrasados; c) que se rectifiquen los inexactos; d) que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros; y e) supresión en los procesos de obtención de información del requisito de la llamada "información sensible", entre la que cabe mencionar la vida íntima, ideas políticas, religiosas o gremiales*"[126]. A lo que debería adicionarse un sexto objetivo referido a la información con contenido discriminatorio o que induzca a la discriminación. De estos objetivos, los más importantes para resaltar son; a) acceso y control de datos, y b) derecho a accionar en los casos en que la Ley lo prescribe.

El Doctor Liévano Chorro[127] establece que el Habeas Data es un instituto jurídico procesal especial, cuyos objetivos específicos son: el acceso a la información, viabilizando el derecho que tiene la persona de saber que se dice de ella en el registro; actualizar los datos registrados que se

[126] CNFed. Cont.-adm., Sala IV, "Farrel, D.A. c/Banco Central y otros", JA, 1995-IV-350, citada por Pierini, Alicia, y otros. Ob.Cit. Págs. 16 y 17.
[127] Dr. José Gerardo Lievano Chorro, "Amparo e Inconstitucionalidad, Sugerencia para una nueva normativa", citado por Alfaro Escoto, D.A. y otro. Ibídem. Pág. 71

encuentran atrasados (piénsese aquí en datos de mora de una persona o de antecedentes penales de ella, cuando ya ha solventado la deuda u obtenido la rehabilitación); la corrección de datos inexactos, de rectificar información desacertada y la eliminación de información denominada sensible, que aunque sea cierta, la persona tiene el derecho a que sea excluida.

Así tenemos que las acciones que posibilita el Hábeas Data en virtud de la protección del derecho de la Autodeterminación Informativa con referencia a los datos personales, abarca en un primer momento el derecho a conocer, o como lo denomina la doctrina española "*el derecho a la información", entendiéndose por este, el derecho que tiene toda persona a ser informada de la existencia de registros en bancos de datos de carácter personal, de la identidad del titular o responsable, de la finalidad que se persigue con la recolección, tratamiento y transmisión de los mismos y del destino de dicha información*"[128]. Este derecho representa el pilar básico de la Autodeterminación del tratamiento de los datos personales, ya que es difícil o casi imposible el hecho de poder controlar algo cuando no se sabe ni siquiera que existe.

Luego tenemos un derecho que abarca ulteriores posibilidades de control de información, surgiendo de esta manera el derecho de acceso,

[128] Lujan Fapiano, Oscar: "Hábeas Data: una aproximación a su problemática y a su posible solución normativa". Págs. 619-650.

considerado como aquel en virtud del cual, toda persona, acreditando su identidad, tiene derecho a tomar conocimiento de los datos personales referidos a ella, consignados en Registros o Bancos de Datos Públicos o privados y conocer la finalidad para la cual han sido recogidos. Obviamente que la sola acción de conocer y tener acceso a los datos no sirve de nada cuando estos datos son inexactos, incompletos, sensibles o falsos. Este derecho es el corolario de otros derechos que posibilitan otras acciones una vez ejercido el derecho de acceso, del cual, posteriormente surge la posibilidad de intervención sobre el dato, en cuya virtud el titular puede exigir:

a) La rectificación de datos almacenados cuando fueren inexactos. Cuando se habla de rectificación se entiende por esta la corrección de datos que sean incorrectos o erróneos, pero nunca se podrá hablar de la rectificación de datos falsos, puesto que los datos de este tipo no son susceptibles de ser corregidos, más bien habría que suprimirlos.

b) Que se completen las informaciones que hubieren sido total o parcialmente omitidas. Esto está contenido en el principio 2 de los Principios Rectores para la Reglamentación de los Ficheros Computadorizados de Datos Personales[129], en cuanto establece que los responsables de los

[129] Lujan Fapiano, Oscar. Ob.Cit. Pág. 652.

registros o bases de datos deben cerciorarse que los datos ahí contenidos sean lo más completos posible.

c) La cancelación de datos que hayan de ser necesarios y pertinentes para la finalidad para la cual fueron recabados y registrados; de datos falsos; de los que se refieren a hechos que hubieran acaecido años atrás, siempre que sus efectos no se hubieren prolongado en el tiempo y carecieren de relevancia actual, y de los datos cuya recolección, almacenamiento y tratamiento estén prohibidos, es decir, los llamados datos sensibles. En esta acción se reflejan dos de los principales principios del tratamiento de datos personales: el principio de necesidad, que se manifiesta a través de la necesaria recolección de los datos para lograr lo que se ha estipulado con ellos (Art. 5 Literal C de la Convención para la Protección de Individuos con respecto al Tratamiento Automatizado de Datos Personales); y el otro es el principio de sujeción al fin, que regula que los datos no puedan ser utilizados para otros efectos diferentes que para los que fueron recolectados (Art. 5 Literal B de la Convención para la Protección de Individuos con respecto al Tratamiento Automatizado de Datos Personales), es necesario establecer que los datos falsos son aquellos datos los cuales nunca han sido verdaderos, y describen una conducta o características no verídicas de su titular.

Por otro lado, con referencia a los datos que hubieran acaecido años atrás, en un caso resuelto en Argentina en el fuero civil, “la Sentencia de Primera Instancia, con excelente fundamento, había hecho lugar a la pretensión de la actora. El fallo se basó en el Derecho Comparado, señalando que ciertos ordenamientos jurídicos establecen la eliminación del dato por el transcurso del tiempo. También cita en apoyo de su tesis la opinión de Doctrina y de Certámenes Jurídicos y Proyectos de Reforma del Código Civil que se inclinan por aceptar la supresión del dato antiguo o caduco, al que define como “aquél que por efecto del tiempo ha perdido virtualidad, ha devenido intrascendente a los efectos de cualquier efecto jurídico relativo a la ejecutabilidad”. Y agrega que “es innegable que en el caso el dato es caduco, si se piensa en términos de prescripción civil superaría el plazo de prescripción liberatoria” (en nuestra legislación, la prescripción liberatoria equivale a la prescripción extintiva, Art. 2253 C.), de aquí que surja el derecho al olvido sobre el que funda el derecho del actor de ordenar y cancelar “el dato caduco”[130].

Y es que el tratamiento de datos automatizado representa una amenaza por su accesibilidad, rapidez y eficacia, lo cual acorta espacios territoriales vastos, y acercan acontecimientos que suceden en diferentes

[130] Palazzi, Pablo Andrés: “El Hábeas Data en el Derecho Argentino”, citado por Alfaro Escoto, D.A. y otro. Ob.Cit. Pág. 74.

etapas de la historia poniendo en descubierto ciertas esferas del individuo que se quieren mantener al resguardo de la Intimidad.

d) Existen datos que son ciertos, pero que no reflejan la realidad actual, o más bien, debería decirse que fueron ciertos, pero por el hecho de que en este momento no describen una situación que se está viviendo en el presente, no quiere decir que sean falsos, sino obsoletos; por lo que es necesario que ellos sean puestos al día, se requiere "la actualización de datos atrasados"[131]. La diferencia con los datos caducos estriba en que los datos atrasados, si bien es cierto contienen información que fue cierta en un momento de la historia, es necesario que sean actualizados, puesto que todavía son útiles al fin que se persigue.

e) "A que no sean accesibles los datos almacenados cuando no se pudiera determinar si son exactos o inexactos", ya que si se permitiere el acceso se estaría atentando contra la certeza que deben ofrecer los registros, puesto que debe recordarse que los solicitantes al obtener los datos podrían transmitirlos a terceros, a quienes probablemente no se les pueda comunicar su posterior corrección.

[131] Lujan Fapiano, Oscar, citado por Alfaro Escoto, D.A. y otro. Ibídem. Pág. 75.

f) “A que los datos sean utilizados de acuerdo a la finalidad prevista, debiendo guardarse la confidencialidad de los mismos a fin de que terceras personas no tengan acceso a ellos”[132], aquí se enmarca el principio de sujeción y se contempla el deber de sigilo que conlleva el derecho a la Intimidad.

g) A impugnar todo aquello que implique una valoración de su conducta, cuyo único fundamento sea un tratamiento automatizado de datos que ofrezca una definición de sus características o de su personalidad, en ese sentido está dirigido el Art. 2 de la Ley Francesa número 78 – 17 de 6 de enero de 1978, Informática, Ficheros y Libertades, cuando dispone que “ninguna decisión de justicia que implique una apreciación sobre un comportamiento humano puede tener por fundamento un tratamiento automatizado de informaciones que den una definición del perfil de la personalidad del interesado”[133].

h) “A que se comunique a los usuarios que hayan recibido previamente la información, el contenido de la intervención sobre el dato”, es decir, que deberá informarse a las personas que hubiesen tenido acceso a un registro o base de datos los cambios por motivos de rectificaciones,

[132] Lujan Fapiano, Oscar, citado por Alfaro Escoto, D.A. y otro. Ibídem. Pág. 75
[133] Lujan Fapiano, Oscar, citado por Alfaro Escoto, D.A. y otro. Ibídem. Pág. 76.

supresiones u otros realizados en ellos, con el motivo de evitar la difusión de información errónea o desactualizada.

En el otro sentido a que se refiere al Juez Gounçalves, los objetivos del Hábeas Data estriban en "la garantía a los derechos de la personalidad en cuanto patrimonio personal de contenido moral, como los constituidos por la honra, imagen, nombre, vida privada, intimidad, tranquilidad"[134].

Pero además, otro objetivo podría ubicarse a nuestro criterio, en el sentido de que esta acción sea ejercida contra una autoridad pública, como forma de tutelar un derecho subjetivo de naturaleza pública como sería el caso del derecho de acceso a las informaciones, y especialmente de lo que acaece en la Administración Pública; esto estaría reflejando un principio básico del sistema democrático referente a la transparencia de las actuaciones de estos servidores y, en general, de los actos de gobierno, por lo que puede afirmarse que uno de los objetivos del Hábeas Data está encaminado a configurar un mecanismo de control del ciudadano a las actuaciones del poder estatal, es su que hacer propio.

4.3 CARACTERISTICAS.

[134] Gounçalves de Oliveira, L.: "Rito Procesal de Hábeas Data", citado por Alfaro Escoto, D.A..Ibídem. Pág. 76.

El Habeas Data, como figura autónoma, presenta las siguientes características:[135]

a) *Es una garantía específica* para la protección de derechos que pueden ser violados por medio de la divulgación de informaciones personales. El Hábeas Data es una garantía *Sui Generis*, la cual se ocupa especialmente de la protección de derechos los cuales se ven amenazados por el adelanto tecnológico, específicamente la Telemática, ya que ésta hace posible la recolección, tratamiento (en todas sus fases) y divulgación de los datos de una manera increíblemente rápida y extendida o extensible hacia muchas personas, sin que pudiese existir un verdadero control de cómo o a quiénes se envía la información, ni tampoco de la calidad de la información que es enviada.

b) *El proceso debe ser ágil y rápido*. El proceso que ventile el Hábeas Data debe ser un proceso sin dilaciones, para que pueda tener efecto real lo que se pretende al instaurar esta garantía, en una legislación determinada. Como bien sabemos, los derechos que están en juego, igual que todos los derechos, son susceptibles de ser dañados si no hay una rápida justicia, y podría ser que no se restituyesen; además, los medios con que son lesionados, permiten que este daño sea extremadamente amplio, tanto que

[135] Alfaro Escoto, D.A. y otros. Ibídem. Pág. 77-79.

quizá se podría afirmar que no existe reparación alguna cuando fueren transgredidos.

c) *Sencillez y Carencia de Formalismos*. Esta es una característica que va apegada a la agilidad y rapidez del procedimiento; y es que en el cúmulo de formalismos presentes en proceso, favorecen su dilatación y retardo, además de que dificulta de cierta manera, el acceso a la jurisdicción por personas no letradas en Derecho, en primer momento, porque no toda persona que es lesionada en un derecho tiene los recursos para solicitar los servicios de una letrado y, en segundo lugar, porque todo ello intimida al impetrante.

d) *La resolución debe ser inmediatamente obedecida*. Como se decía antes, por lo delicado y susceptible de los derechos en cuestión, la dilatación en obedecer o llevar a cabo el cumplimiento de lo preceptuado en la resolución que conceda el Hábeas Data, no permite vacilar en el mandato impuesto a cumplir; y es que, por ejemplo, la retardación en la supresión de un dato falso que aparecerá en el periódico del día siguiente, puede tener efectos catastróficos para el titular, no obstante que existan mecanismos de posterior rectificación.

e) *Acción personalísima*. Esta acción es susceptible de ser ejercida sólo por el titular del derecho en cuestión, y excepcionalmente, otros que la Ley expresamente determine; y es que, recuérdese que por lo personalísimo de las informaciones de que se trata, sólo su titular puede saber si estas le dañan o no, o si son o no ciertas, o lo son de manera total o parcial, u obsoletas. Además, se debe tener presente que básicamente el Hábeas Data, lo que trata de proteger son derechos subjetivos de tipo privado, lo cual excluye de la facultad de ejercer una acción por otro, en virtud de la legitimación procesal activa en sentido material.

f) *Prioridad sobre otros actos jurisdiccionales*. Esta es una característica que pone de manifiesto la importancia de que se lleve a cabo de manera rápida y con celeridad el proceso, fundado en la importancia que representa el objeto tutelado; y en este sentido, podemos encontrar de manera expresa esta característica en el articulo 19 de la ley Brasileña que Regula el acceso a informaciones y disciplina el Rito Procesal de Hábeas Data, pero no obstante su prioridad, se establecen las excepciones del Hábeas Corpus y del Mandato de Seguridad (conocido con este nombre una figura similar al amparo en EL Brasil)[136].

[136] Gounçalves de Oliveira, L.: "Rito Procesal de Hábeas Data", citado por Alfaro Escoto, D.A. Ibídem. Pág. 79.

4.4 NATURALEZA JURIDICA.

La naturaleza jurídica del Hábeas Data depende, en realidad, de la forma en que ha sido programado en cada ordenamiento jurídico. Si bien es más común encontrarlo diseñado como acción o proceso y más precisamente como proceso constitucional (Brasil, Paraguay, Perú, Argentina), lo cierto es que también ha sido insertado como un derecho constitucional más (Colombia).

Entre los partidarios de la primera concepción, la doctrina brasileña no ha sido renuente al abordar la naturaleza jurídica de Hábeas Data, versión tradicional, y tal vez la expresión más clara es la de ALFONSO DA SILVA, quien menciona que el Hábeas Data es un "*remedio constitucional, un medio destinado a provocar la actividad jurisdiccional y que, por tal motivo, tiene naturaleza de acción, más específicamente de acción constitucional. A su vez, cobija un derecho, el derecho de conocimiento de datos personales y de rectificarlos, que es incorrectamente otorgado en el mismo dispositivo que instituye el remedio de su tutela*"[137]. En similar sentido se han expresado CRETELLA JUNIOR, GRECO FILHO y PINTO FERREIRA; en ese mismo sentido, ZUÑIGA URBINA, refiere que "*el Hábeas Data se erige en la actualidad como instrumento de tutela cautelar de la libertad informática, en*

[137] Da Silva, Alfonso: "Curso de Direito Constitucional Positivo", citado por Puccinelli, Oscar: "El Hábeas Data en Indoiberoamérica". Pág. 213.

una acción – proceso de naturaleza cautelar de amparo constitucional, que con carácter sumario y extraordinario, permite hacer efectivos derechos específicos con relación a información sensible no registrable: derecho de acceso, derecho de actualización de datos, derecho a la rectificación, derecho a la confidencialidad y derecho a la exclusión"[138].

En la doctrina argentina existe coincidencia generalizada respecto de que se trata de una acción procesal constitucional, pero no hay unanimidad en cuanto a su filiación. En efecto, si bien la mayoría de los autores (SAGUES, BIDART, CAMPOS, QUIROGA LAVIE, etc.) indica que se trata de un amparo especializado; para otros se emparenta más con el Hábeas Corpus. Al respecto, SERRA[139] advierte que en una oposición opuesta se considera que el Hábeas Data reconoce cierto paralelismo con el Hábeas Corpus, ya que así como a través de este remedio procesal lo que se reclama es que "se traiga el cuerpo", en aquél lo se intenta es que "se traigan los datos"; su objetivo radicaría en que una persona pueda acceder a tomar conocimiento o enterarse de la información de carácter personal referida a dicho sujeto y contenida en determinado registro; por lo tanto, como en el Hábeas Corpus el fin inmediato es la exhibición del cuerpo, la indagación de los motivos de una privación de la libertad actual e inminente, en el Hábeas

[138] Zúñiga Urbina, Francisco: "El derecho a la Intimidad y sus paradigmas", citado por Puccinelli, Oscar. Ibídem.
[139] Puccinelli, Oscar: "El Hábeas Data en Indoiberoamérica". Pág. 213

Data, la finalidad del proceso radica en acceder a la verificación de la exactitud, actualidad y pertenencia de los datos personales registrados; su objetivo, pues, consiste en hacer cesar el registro inexacto, desactualizado, o bien calificado como público, cuando por su naturaleza debió ser reservado o secreto.

Al analizar la evolución histórica desde la creación del clásico Hábeas Corpus hasta el novísimo Hábeas Data, la diferencia más importante entre ambos es que el primero aparece como uno de los mecanismos procesales básicos para defender la libertad en el marco de lo que la celebre teoría de los *status*, elaborada por JELLINEK[140], serán el *status libertatis* y el *status civitatis;* en tanto que, el Hábeas Data ha sido el fruto de sucesiva ampliación de los *status.* De ahí que la aparición del Hábeas Data no puede entenderse como una sustitución del Hábeas Corpus, cuya función para la defensa de la libertad física sigue siendo plenamente vigente, sino que se trata de una garantía par nuevas agresiones a otras esferas de la libertad.

Finalmente, entre quienes entiendo al Hábeas Data como un derecho personalísimo, cabe recordar a la doctrina española y, en el plano Indoiberoamericano, algunos autores, especialmente de Brasil, Chile y Colombia, que suelen tratar al instituto en estudio como garantía y como

[140] Puccinelli, Oscar. Ob.Cit. Pág. 215

derecho; así, OTHON SIDOU aclara que "*este derecho personalísimo no se confunde con el derecho a la información en general, cuyo acceso se faculta a todos cuando fuera necesario para el ejercicio profesional, resguardando la confidencialidad de la fuente (Constitución Brasileña, Art. 5º, XIV)*"[141].

En lo que hace a la segunda versión de Habeas Data, esto es, el diseñado para acceder a informaciones, aparece claramente como un derecho, salvo en el Perú, donde se le concibe expresamente como garantía, por la generalizada ubicación y formulación constitucional, derecho que, en definitiva, es judicialmente protegible por medio de remedios constitucionales y por lo tanto en algunos países como Colombia, no existiría diferencia en la práctica (el derecho de Habeas Data Colombiano es amparable por vía de la acción de tutela).

En el caso Argentino, y siempre refiriéndonos a las normas de raigambre constitucional, resulta particularmente de interés aquellas contenidas en las diversas constituciones provinciales que se ocuparon, aunque con distintos alcances de esta problemática, en especial las Cartas que: a) regularon el Habeas Data en su versión tradicional, esto, es, como protector de los datos personales, b) establecieron cláusulas genéricas que permiten inferirlo de su remisión a la tutela de derechos y libertades o a las

[141] Othon Sidou, J.M.:"As garantías ativas dos direitos colectivos", citado por Puccinelli, Oscar. Ibídem. Pág. 215.

garantías existentes en el ámbito nacional o por el hecho de ordenar que la ley fije límites a la actividad informática, c) instauraron reglas tuitivas respecto de determinados datos, y d) se ocuparon de garantizar el acceso a la información pública.

En síntesis el Habeas Data aparece regulado en Indoiberoamérica, a veces como derecho y a veces como acción o garantía constitucional. En la doctrina y la jurisprudencia se observa que en líneas generales se ha seguido la fórmula elegida por cada país, aunque en ocasiones se le otorga una naturaleza mixta (acción y derecho) y no se coincide, cuando se lo entiende como acción o proceso, respecto de si se trata de un tipo de amparo o de Habeas Corpus.

Ahora bien, considerando que el Habeas Data, en todos los casos en que fue regulado: a) encierra ciertos derechos de fondo que son expresados de manera exclusiva, esto es, no son reiteración de otras disposiciones y no taxativa; b) que tales facultades integran el derecho a la protección de datos, o el derecho a la autodeterminación informativa, según el punto de vista que escojamos, y que c) las regulaciones que lo consagran están reconociendo un derecho para el cual prevén conjuntamente disposiciones procesales constitucionales ya sean específicas (como ocurre en la mayoría de constituciones) o genéricas, aplicables a todos los otros derechos(Colombia)

consecuentemente se debe colegir que el Habeas Data sería un derecho o un derecho – garantía. Sin embargo, bien podría entenderse de la siguiente manera: dado su carácter instrumental, el Habeas Data constituye en realidad una garantía de los derechos que pretende proteger, estén o no insertos en la norma que lo consagra.

4.5 PROCEDIMIENTO DE HABEAS DATA.

Dado que en nuestro país no existe esta figura procesal, y a fin de tener una idea de la forma en que puede hacerse efectivo el derecho a la Autodeterminación Informativa referida a la Protección de Datos Personales, es que se va a tomar como referencia el procedimiento que en la legislación brasileña se le asigna al Hábeas Data. Así, la Ley Brasileña[142] No. 9.507, de 12 de noviembre de 1997, consiste en veintitrés artículos que regulan el derecho de acceso a informaciones y disciplina, el rito procesal del Hábeas Data.

Dicho procedimiento está dividido en dos etapas; la primera responde a un carácter meramente administrativo y la segunda es la judicial, referida a la figura en sí. A continuación se explica cada una de las mencionadas etapas, a saber.

[142] Gounçalves de Oliveira, L.: "Rito Procesal de Hábeas Data", citado por Alfaro Escoto, D.A..Ibídem. Pág. 79

4.5.1 Procedimiento en Sede Administrativa.

La primera fase, cuyo carácter preliminar o preparatorio (para la segunda), está bien definido, se refiere con mayor medida a la viabilización de tal a través del derecho de petición que se encuentra en el artículo cinco número XXXIV, a) de la *Constitución de la República Federativa de Brasil de 1988*[143]. Este derecho debe ser formulado por medio de un requerimiento o solicitud administrativa, previa al conocimiento de las informaciones constantes en un registro o banco de datos, el cual será dirigido a la entidad en que se contienen tales datos. Y es de hacer énfasis en que el escrito se dirige a la entidad y no al titular de la entidad. Dicho escrito será admitido o no en plazo de cuarenta y ocho horas, luego de las cuales, dentro de las siguientes veinticuatro deberá de serle informada al solicitante (Art. 2 de la Ley que regula el rito procesal de Hábeas Data)[144]. Es de aclarar en este aspecto que la Ley no ha establecido qué sucede en el supuesto que los plazos mencionados sean incumplidos, lo cual a nuestro criterio constituye un vacío de graves consecuencias; lo único que si se puede observar, es que, al existir denegación expresa de la admisibilidad del pedido o al existir silencio administrativo, se cumplen los presupuestos que permiten iniciar la acción de

[143] Alfaro Escoto, D.A. Ibídem. Pág. 81.
[144] Gounçalves de Oliveira, L.: "Rito Procesal de Hábeas Data", citado por Alfaro Escoto, D.A..Ibídem. Pág. 81.

Hábeas Data, puesto que de las decisiones que se tomen o se dejen tomar no cabe la interposición de recurso, sino la iniciación de la vía judicial.

Es importante mencionar que en el artículo 5 número XXXIII de la Constitución del Brasil establece que toda persona tiene derecho de recibir informaciones de las distintas oficinas del gobierno, sobre asuntos privados que le conciernen a ella o a la colectividad o al interés público dentro del plazo establecido por la Ley; continúa señalando el artículo que excepto la información cuyo secreto sea vital para la sociedad o la del Estado.

En el artículo 3 se estatuye que al ser admitida la petición, se establece el día y la hora por parte del ente administrativo para que el requeriente tome conocimiento de las informaciones, debiendo exponer así en la comunicación que se le haga para que pueda ejercer plenamente sus facultades. Los datos no podrán ser mostrados en certificaciones o copias, sino deben serlo en los registros originales o directamente de la base de datos. Así, una vez verificados los datos por el impetrante en el lugar y hora designados, le asisten los subsiguientes derechos; en caso que las informaciones sean inexactas, las que requerirán que se rectifiquen o supriman, u otra de las acciones que él a su juicio solicite, pero acompañando a este nuevo pedido, la documentación que compruebe lo

aseverado por este; y de esta forma, la autoridad administrativa podrá acceder (pudiendo darse el caso que no se acceda a la rectificación).

En caso que no se comprobase la inexactitud del dato, y si el interesado diere una explicación o contestación sobre el mismo, justificando un posible litigio sobre el objeto fáctico del dato, dicha explicación será anotada en el registro o banco de datos. y esta es una facultad otorgada por el legislador, ya que el constituyente sólo se limitó al conocimiento o la rectificación de la información[145]. Esta ampliación no merece censura desde el punto de vista constitucional: lo que la ley ordinaria no podría hacer es estrechar, disminuir, restringir el campo de actuación del Habeas Data, delimitado en la Carta Política. Podría decirse, que a pesar de la diferencia ontológica, si el remedio se presta a la consecución de resoluciones más intensas (rectificación de datos), es razonable admitir a *fortiori*, que se preste a la de resoluciones menos intensas (simple anotación de explicaciones dadas por el requeriente, sin alteración de los asientos existentes).

4.5.2 Procedimiento en Sede Judicial.

El artículo 7 de la ley que regula el Rito Procesal de Habeas Data (LRRHD), establece que “se concede el Habeas Data”:

[145] Gounçalves de Oliveira, L., citado por Alfaro Escoto, D.A. Ibídem. Pág. 82 y 83.

I) Para asegurar el conocimiento de informaciones relativas a la persona del impetrante, constantes en un registro o base de datos de entidades gubernamentales o de carácter público.

II) Para rectificación de datos, cuando no se prefiera hacerlo por proceso reservado judicial o administrativo.

III) Para anotación en los asientos del interesado, de contestación o explicación sobre el dato verdadero pero justificable, y que esté bajo pleito judicial o administrativo[146].

El artículo 8 establece que en el pedido inicial se deben llenar los requisitos que establece el artículo 282 – 285 del Código de Proceso Civil, lo que para fines ilustrativos, se transcriben a continuación:

I) Juez o Tribunal al que va dirigido.

II) Los nombres, apellidos, estado civil, profesión, domicilio y residencia del actor y del reo.

III) El hecho y los fundamentos jurídicos del pedido.

IV) El pedido con sus especificaciones.

V) Valor de la causa (cuantía, que en este caso podría ser de valor indeterminado).

VI) Las pruebas con el actor pretende demostrar la verdad de los hechos alegados.

[146] Gounçalves de Oliveira, L.: "Rito Procesal de Hábeas Data", citado por Alfaro Escoto, D.A..Ibídem. Pág. 83.

VII) El requerimiento de citación del reo[147].

La petición inicial debe ser instruida con prueba de que se ha agotado la etapa preparatoria o administrativa, y para tal efecto, se deberá presentar según sea el caso, la denegatoria de acceso a las informaciones o la manifestación de la carta de contestación de lo pedido por más de diez días; la denegatoria de que fuesen rectificados los datos o la manifestación de la ausencia de contestación por más de quince días y, la denegatoria de que se hubiera hecho la anotación, contestación o explicación, o la manifestación de la falta de contestación dentro de quince días (Artículo 8 LRRHD). Esta petición esta sujeta, como cualquier otra, al control de juez, quien la puede o no aceptar, de lo que se admite recurso de apelación, según el artículo 10 de la Ley en comento.

Admitida la petición, el Juez ordenará que se le de notificación al impetrado del contenido de ésta, a fin de que presente en el plazo de diez días, las informaciones necesarias para terminar el litigio. Terminado este plazo y oído el representante del Ministerio Público, el Juez dará su decisión dentro de cinco días. Tal decisión admite recurso de apelación, la cual concediendo el Hábeas Data, se otorgará en efecto devolutivo. En este caso, el Juez señalará día y hora para que el impetrado presente las informaciones

[147] Gounçalves de Oliveira, L.: "Rito Procesal de Hábeas Data", citado por Alfaro Escoto, D.A..Ibídem. Pág. 84.

al requeriente o presente prueba de las rectificaciones o anotaciones hechas en los asientos.

Un punto importante es el que establece el artículo 18, cuando señala que el pedido de Hábeas Data podrá ser renovado si en la decisión denegatoria no se entrare a conocer de lo principal. Su importancia radica alrededor del estado que cause la decisión o la calidad de cosa juzgada, y es que por ejemplo, el Supremo Tribunal Federal, en casos de mandatos de seguridad, procedimiento que era supletoriamente aplicado al Hábeas Data, se pronunció en que si se denegaba la "segurnaça" por entenderse inexistente, el derecho alegado por el impetrante, la decisión es susceptible de producir cosa juzgada material e impedir cualquier nueva apreciación judicial de la causa.

Pero sería diferente el caso en que se pusiese término al proceso cuando la sentencia que ponga fin a la acción no entre a conocer el asunto de mérito o cosa principal, como cuando quien intentó la acción no era el titular y por lo tanto no tenía la legitimidad procesal para efectuarlo; en ese caso, quedaría expedita la vía para intentar de nuevo la causa y no adquiere calidad de cosa juzgada, en virtud que no se dan las tres identidades: *aedem res, aeden personae et aedem causa petendi.*

4.6 PARTICULARIDADES EN EL PROCEDIMIENTO DE HABEAS DATA.

4.6.1 Sujeto Pasivo.

Las diversas disposiciones constitucionales reguladoras del instituto en estudio indican como sujetos pasivos de las pretensiones por él articulables a los siguientes:[148] bancos de datos y archivos de entidades públicas y privadas (Colombia); archivos, fichas o cualquier otra forma de registros estatales (Guatemala); registros oficiales o de carácter público (Paraguay); registros o banco de datos públicos o privados destinados a proveer informes (Argentina); registros o bancos de datos de entidades gubernamentales o de carácter público (Brasil); entidades públicas o privadas (Ecuador); y servicios informáticos, computadorizados o no, públicos o privados, de cualquier autoridad, funcionario o persona (Perú).

Las diferencias, si bien en algunos casos son sutiles, definen en realidad los verdaderos alcances protectores de cada ordenamiento jurídico que, en ciertos casos, encontrará serias y poco aconsejables limitaciones para extender su radio de acción a los bancos de datos privados.

4.6.2 Sujeto Activo.

Las reglas constitucionales sobre Hábeas Data refieren, por lo general, a “toda persona” (Argentina, Brasil, Colombia, Ecuador, Guatemala,

[148] Puccinelli, Oscar. Ob.cit. Pág. 218.

Paraguay y Perú). Sólo excepcionalmente se alude a "ciudadanos" (Portugal, España); sin embargo, a criterio de PUCCINELLI, y avalado por la doctrina de los países que así lo disponen, "*por tratarse de un derecho fundamental no integrante del conjunto de los derechos políticos, toda persona sin necesidad de considerar si es nacional o extranjera, su residencia y edad (salvo para exigirle que actúe por intermedio de su representante legal), debe poder ejercitar las facultades contenidas en las disposiciones que regulan el instituto*"[149].

4.6.3 El Derecho de Acceso y sus límites.

El derecho de Acceso es parte fundamental del conjunto de derechos que contiene la Libertad Informática, y constituye, la facultad individual que se concede al interesado de requerir al titular del fichero toda información que tenga sobre él y que esté almacenada en sus ficheros.

Existen diversas causas que justifican que la Ley limite el derecho de acceso del interesado, como la salvaguardia de la seguridad del Estado, la defensa, seguridad pública, los intereses económicos y financieros importantes del Estado o la investigación y persecución de los delitos[150]. En la Unión Europea la Directiva permite a los Estados miembros que en sus

[149] Puccinelli, Oscar. Ob.Cit. Pág. 220.
[150] Art. 9 del Convenio 108 del Consejo de Europa citado por Ayala Muñoz, J.M., y otros: "La Protección de Datos Personales en El Salvador". Pág. 77.

legislaciones internas consideren excepciones al derecho de acceso, para proteger la seguridad del Estado, la defensa, la seguridad pública, la prevención, la investigación, la detección y la represión de infracciones penales o de infracciones de la deontología en las profesiones reglamentadas. También se pueden hacer excepciones a este derecho cuando se requiera tutelar un interés económico o financiero de un Estado o de la Unión Europea, lo cual incluye los asuntos monetarios, presupuestarios y fiscales. Por último, el derecho de acceso puede estar sujeto a restricción con objeto de proteger al interesado o los derechos y libertades de otras personas.

En Estados Unidos, la *Privacy Act* de 1974 también limita el derecho de acceso a la información almacenada en determinados archivos públicos. Entre ellos se citan los que siguen: a) los registros de la Agencia Central de información b) los registros gestionados por un órgano que tuviera como función principal o realizara alguna actividad que hiciera referencia a la aplicación de las leyes penales, incluidos en tales actividades los esfuerzos desplegados por la policía para prevenir, dominar o reducir el delito o para aprehender a los delincuentes, así como las actividades de los fiscales, tribunales, autoridades correccionales, autoridades competentes en materia de libertad vigilada, remisión de penas, libertad bajo palabra. c) los registros que contuvieran información recopiladas para identificar delincuentes y delincuentes presuntos, la cual estuviera constituida solo por datos de

identificación y anotaciones de detenciones, naturaleza y estructura de las acusaciones, sentencias, confinamiento, puesta en libertad, situación de libertad bajo palabra y de libertad vigilada; la información recopilada a efectos de una investigación criminal; y, por último, los atestados o informes vinculados aun individuo identificable, recopilados en cualquier estado del proceso de aplicación de las leyes penales, desde la detención o el procesamiento hasta la supresión de toda vigilancia[151].

En América Latina, se pueden destacar los pronunciamientos de la Corte Suprema de Justicia Argentina, en los que se decidió que la ciudadanía puede utilizar la acción del Habeas Data para conocer los datos que posean sobre ella los organismos de seguridad, los cuales podrán negarse cuando se ponga en riesgo la seguridad del Estado[152].

4.7 REGISTROS DE DATOS PERSONALES.

4.7.1 Registros de Solvencia Patrimonial y de Crédito, y Registros Positivos .

Los registros de solvencia patrimonial y de crédito pueden definirse como "*los repertorios que almacenan información sobre la situación financiera o capacidad económica de una persona física*"[153]. El tratamiento

[151] Puccinelli, Oscar: Ob.Cit. Pág. 222.
[152] Puccinelli, Oscar. Ibídem.
[153] Ayala Muñoz, J.M., y otros. Ob. Cit. Pág. 84

de estos datos puede afectar seriamente posibilidades de obtener créditos o la consideración de esa persona con diversos fines. Tal es el caso, por ejemplo, de alguien que a haya pasado situaciones económicas difíciles en una etapa de su vida y que actualmente se encuentre en un período de estabilidad laboral; el acceso a los datos económicos de su pasado puede ser tenido en cuenta por un banco para denegar un préstamo. De igual forma, "*si no son cancelados los datos que revelan una situación económica pasada que no corresponde con la realidad vigente, podrían arrojar un perfil negativo de esta persona, que influyera en que fuera rechazada para un puesto de trabajo concreto*"[154].

Al hilo de los ficheros sobre información relacionada con la solvencia patrimonial y de crédito de una persona, se han ido creando sociedades que gestionan informaciones más completas. Así, se suele distinguir entre los ficheros de "datos negativos" o "negros", que informan sobre el histórico de los incumplimientos e impagos, y los ficheros de "datos positivos" o "blancos"[155], que suministran informes detallados del activo y el pasivo de una persona, sus capacidades, garantías o estadísticas de reembolso, que se conocen como centrales positivas. En la práctica, el funcionamiento de estos ficheros es lo que ocasiona más volumen de vulneraciones a la libertad informática de la ciudadanía.

[154] Ayala Muñoz, J.M., y otros. Ibídem.
[155] Ayala Muñoz, J.M., y otros. Ibídem. Pág. 85.

4.7.1.1 Ficheros de datos negativos: ficheros de mera solvencia patrimonial.

Este tipo de registros se limita a ofrecer información sobre los impagos o incumplimientos contractuales de obligaciones dinerarias. Las empresas consultan estos ficheros para determinar la solvencia del cliente cuando se produce la contratación de algún producto financiero con riesgo económico para ellas (contratación de productos de activo, emisión de tarjetas, concesión de préstamos, etc.). En definitiva, se trata de comprobar que a nombre de quienes intervienen en la operación no figura ningún impagado, así se realiza un análisis del riesgo que entrañan las operaciones en que intervienen. Este tipo de registros es muy común; además, son elaborados por entidades cuya actividad social consiste en la prestación de servicios de información sobre solvencia patrimonial y crédito.

El tratamiento de estos datos está regulado por las leyes generales de protección de datos, en algunos países, o por reglas especiales incluidas en otras normas. Una de las primeras disposiciones que abordaron el, tratamiento de estos fue la estadounidense *Fair Credit Reporting Act (Acta de Reporte de Crédito Justo)* de 1970. Esta norma estableció cautelas ordenadas a la tutela de los derechos de los consumidores frente a las empresas que generan o utilizan estos registros. De acuerdo con esta norma,

los afectados tienen derecho a ser informados (cuando se utilice contra ellos información adversa al denegárseles un crédito, un empleo o cualquier otro beneficio) sobre el origen de la información y la identidad, dirección y teléfono de la empresa que generó el informe[156]. El afectado también tiene derecho a que se le entregue la lista de quienes hayan requerido recientemente sus datos, a que se rectifiquen o cancelen los informes inexactos y a que se notifique dicha rectificación a quienes hubieran podido acceder a ellos.

En América Latina, la Ley argentina número 25.326 de Hábeas Data recoge reglas especiales para este tipo de fichero. Entre ellas se destacan que sólo se pueden archivar, registrar o ceder datos personales que sean significativos para evaluar la solvencia económico – financiera de los afectados, durante los últimos cinco años (o dos años si el deudor canceló su obligación), y que el interesado tiene derecho de acceso a las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas, durante los últimos seis meses, lo cual incluye el nombre y domicilio del cesionario, sin datos obtenidos por cesión.

La utilidad, incluso necesidad, de este tipo de registros parece fuera de toda duda para un correcto funcionamiento del mercado económico, en general, y crediticio, en particular, lo cual contribuye a la mejora de la comercialización de bienes y servicios, ahora bien, el uso indebido de datos

[156] Martínez Martínez, Ricard: "Una Aproximación Crítica a la Autodeterminación Informativa". Ayala Muñoz, J. M., y otros. Ob.Cit. Pág. 86.

personales tratados en esos ficheros puede generar graves repercusiones sociales y económicas para la ciudadanía. La utilización de estos ficheros lleva consigo un indudable peligro para la intimidad y el honor de las personas, por lo que es urgente la observancia de unas reglas de juego por parte de todas las personas que intervienen en su desarrollo.

4.7.1.2 Ficheros de "datos positivos".

En Estado Unidos existen agencias de información de crédito que han creado dicheros positivos, accesibles a toda persona que justifique una finalidad profesional legítima. Estos ficheros incluyen datos sobre la identidad, la situación familiar, el salario y el empleo, y permiten elaborar perfiles muy definidos de millones de individuos. De hecho el noventa por ciento de la población adulta está incluida en estos ficheros, por lo que puede hablarse de la emergencia de una "sociedad vigilada"[157] en Estado Unidos, con los efectos que ello supone de exclusión social y lesiones a la dignidad e intimidad de las personas. El interés por estos ficheros es que hacen más seguras las relaciones contractuales (empleadores, aseguradoras, o entidades de crédito, etc.)

[157] Ayala Muñoz, J.M., y otros. Ibídem. Pág. 82

4.7.2 Registros de Clientes y Registros de Publicidad y Marketing.

La publicidad y el marketing directo son, hoy en día actividades básicas para el comercio y la oferta de bienes y servicios. Su ejecución, sobre todo en el caso de empresas dedicadas a la venta o contratación a distancia, exige el manejo de una base datos que responda a perfiles de posibles interesados y, por ello, posibles clientes. Con carácter general, el tratamiento de datos con fines de publicidad, comprende el alquiler de direcciones a terceros, la publicidad propia o de terceros, la venta directa o a distancia, la recopilación de direcciones, el reparto de documentos, la prospección comercial y otras actividades análogas[158].

En este ámbito, la Libertad Informática redunda también en la protección del consumidor, pues los datos empleados para el marketing suelen proceder de una relación contractual previa, de un contrato de consumo en el que el proveedor permite el acceso a cierta información del cliente que abarca sus datos personales, monto de gastos, bienes, costumbres y gustos, comportamiento comercial, nivel de morosidad y cumplimiento. Toda esta información se convierte en un material valioso en el patrimonio del proveedor, pues le permite utilizarlo tanto para promocionar oferta de sus productos como para comerciar con esa información y, así, generar un nuevo producto. En tal sentido, se hace referencia a dos grandes

[158] Ayala Muñoz, J.M., y otros. Ibídem. Pág. 90.

bloques de ficheros, como son: los ficheros de clientes, en particular los que gestionan los datos de fidelización, y los ficheros de correo electrónico y la técnica del spam.

4.7.2.1 *Registros de Clientes: las tarjetas de fidelización.*

Los datos personales que acaban manejando las empresas de bienes y servicios son muchos. Un ejemplo es el de las Tarjetas de Fidelización que tiene auge hoy en día. Este instrumento de marketing tiene implicaciones en materia de protección de datos: en las referidas tarjetas, se almacenan una serie de datos de carácter personal, de los clientes que son socios de los clubes de fidelización promovidos por los propios comercios. La problemática estriba en el origen de los datos, es decir, la fuente de la que se recaban. En gran medida, los datos provienen directamente de los interesados, a través de los formularios específicos que llenan. En dichos formularios, junto con las condiciones generales de uso de la tarjeta, se debería introducir una cláusula de información para garantizar la protección de la Libertad Informática de los interesados. Así mismo, debería incluirse una serie de condiciones generales de uso de la Tarjeta de Fidelización que, además de establecer diferentes reglas de utilización y beneficios para el usuario, informara del constante aumento de los datos almacenados de cada persona, según el uso que de a la tarjeta, ya que la mayoría de programas de fidelización están diseñados para fidelizar al cliente y conocer sus hábitos de consumo; así, identifica cada

producto que el usuario compra, y almacena esos datos. Esta información suele utilizarse para realizar estudios de mercado y para campañas de promociones y lanzamientos de productos.

4.7.2.2 *Registros de Direcciones de Correo Electrónico: la Técnica del Spam*.

Al envío de correo basura se le denomina *spamming*, término que se entiende como "*enviar un mensaje a varios destinatarios*"[159]. Este envío no consentido de mensajes publicitarios por correo electrónico, a una multitud de destinatarios, se vincula con la polémica de las llamadas "comunicaciones comerciales no solicitadas" y queda sujeto a lo dispuesto en la normativa de protección de consumidores y usuarios, y en la aplicación de la normativa sobre protección de datos, en particular al derecho de oposición del interesado al tratamiento de sus datos personales.

Aunque, por lo general el *spamming* se asocia con el envío masivo de correos comerciales, también existe el *spam* cuando se envían correos masivos con propósitos no comerciales, informativos, políticos o de cualquier

[159] Wired, Vol. "Nuevos conceptos para una nueva era: Internet", citado por Ayala Muñoz, J.M., y otros. . ibídem. Pág. 93.

índole. La clave se encuentra en que estos correos llegan a usuarios que no han expresado previamente su interés en recibirlos e ignoran cómo sus direcciones han llegado a formar parte de la lista de ese correo electrónico. De esta forma, acaban recibiendo, a diario en el buzón electrónico un ingente número de mensajes publicitarios sin saber como impedirlo. El spam puede interferir seriamente los servicios y la gestión diaria de los correos electrónicos, comprometiendo la disponibilidad de los recursos. También es de tomar en cuenta que el costo los asume el usuario.

4.7.4 Registros Policiales y Registros de Penados y Rebeldes.

4.7.4.1 *Registros Policiales*.

Los ficheros policiales comprenden el conjunto de bases de datos creadas por las autoridades policiales para la prevención y la represión de las infracciones penales y el mantenimiento del Orden Público[160]. Estos ficheros son un claro ejemplo de supuestos especiales en los que las legislaciones introducen limitaciones a la protección de datos.

El peligro de estos ficheros se puso de manifiesto en el asunto Leander, ventilado ante el Tribunal Europeo de Derechos Humanos (TEDH), por la violación del artículo ocho del Convenio Europeo de Derechos

[160] Ayala Muñoz, J.M., y otros. Ibídem. Pág. 95.

Humanos[161]. Se consideró que la Policía había violado dicho artículo por poseer información relativa a Leander, ciudadano sueco, que había militado en el Partido Comunista Sueco en la asociación editora de un periódico contestatario y en sindicato de soldados. El conocimiento de estos hechos motivó que fuera rechazado para un empleo en el Museo Naval, próximo a una base naval militar, en donde se alegaron motivos de seguridad nacional.

En la Sentencia TEDH no se opone a la posibilidad de una actuación secreta de la Policía ni a un mayor margen de apreciación de los poderes públicos del Estado en este campo, pero se exige que exista una regulación apropiada que resulte mínimamente accesible al ciudadano y, por lo tanto, previsible. Por ello, no basta con que una norma solo administrativa o reglamentaria lo prevea, sino que debe ser una ley (principio de legalidad) la que dote de certeza y previsibilidad a la injerencia y establezca las condiciones que la hagan razonable o proporcionada en una sociedad democrática.

Una ley en la que se detallen los requisitos que deben cumplirse para que se limite la injerencia al derecho fundamental y en la que también se fijen los límites a los cuales debe ajustarse el órgano de investigación de los delitos es requisito necesario para considerar una injerencia legítima. Así,

[161] STEDH del 26 de marzo de 1987, Caso Leander c. Suede, Serie A, No. 116 (1987), citado por Ayala Muñoz, J.M., y otros. Ibídem. Pág.96.

pues, los ficheros creados por las Fuerzas y Cuerpos de Seguridad del Estado que contengan datos de carácter personal, deben de estar sujetos a una ley y ser objeto de un registro permanente.

Como reglas concretas, la Ley debe prever una recolección de datos sin consentimiento del afectado, limitada a aquellos supuestos y categorías de datos que resulten necesario para la prevención de un peligro real, para la seguridad pública o para la represión de infracciones penales debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

4.7.4.2 *Registros de Penados y Rebeldes*.

Los registros de antecedentes penales tienen como principal objetivo informar, a las autoridades responsables del sistema de justicia penal, sobre los antecedentes del justiciable que se tienen en cuenta en la sentencia. El peligro de estos ficheros es el uso que, con otras finalidades, puede hacerse del mismo, por ejemplo, un puesto de trabajo puede exigir conocer los antecedentes para tener confianza en la persona que se contrata. Contra este segundo uso de los ficheros de penados se han alzado algunas voces internacionales, como el *Consejo de Europa en su Recomendación* No. R

(84) 10[162], que considera que ello puede poner en peligro las oportunidades de reinserción social del condenado y que, por tanto, debe limitarse lo más posible.

4.7.6. Registros de la Hacienda Pública.

Los registros de la Administración Tributaria recogen datos directamente del afectado (datos propios) y también de otras fuentes (datos referenciados), esto es, se instaura un auténtico deber de colaboración con la Hacienda Pública en materia de tributos. Este deber de información viene recogido en las legislaciones nacionales, como la española, que disponen que toda persona natural o jurídica, pública o privada, estará obligada a proporcionar a la Administración Tributaria toda clase de datos, informes o antecedentes con trascendencia tributaria, deducida de sus relaciones económicas, profesionales o financieras con otras personas.

En consecuencia, la Hacienda Pública se ve beneficiada en su actividad con la posibilidad de cruzar estos datos para una gestión más eficiente en materia tributaria. También se ve beneficiada con determinadas excepciones a los derechos acceso, rectificación o cancelación, cuando dicho ejercicio obstaculice las actuaciones administrativas tendentes a

[162] Recomendación del Consejo de Europa No. R(84)10, adoptada por el Comité de Ministros el 21 de junio de 1984, citada por Ayala Muñoz, J.M., y otros. Ibídem, pág. 97.

asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras[163].

Las garantías que se establecen para la protección de datos personales en el ámbito tributario, además del cumplimiento de los principios generales y los derechos, con las limitaciones expresadas, son el Control Interno de la Información articulado a través de tres vías[164]: primera, la obligación de secreto y sigilo del personal al servicio de la Hacienda Pública; segunda, el control de acceso a las bases tributarias de forma que se generen registros sobre los accesos a la base; y tercera, la utilización de la información sólo para los fines para los cuales fue solicitada.

4.8 LA TRANSMISION INTERNACIONAL DE DATOS PERSONALES.

En virtud que el tema a desarrollar es relativamente nuevo para las legislaciones latinoamericanas vigentes, se hace necesario, tomar como referencia la *Ley Orgánica 15 de 1999 que regula la Transmisión Internacional de las Informaciones de carácter personal*[165], cuya regulación legal está en sintonía con la norma recogida en el Art. 12 reguladora del "flujo

[163] Artículo 23 de la Ley Española 15/1999 de Protección de Datos, citada por Ayala Muñoz, J. M, y otros. Ibídem. Pág. 107.
[164] Ayala Muñoz, J.M., y otros.ibídem. pág. 107.
[165] Gárriga Domínguez, Ana: "Tratamiento de Datos Personales y Derechos Fundamentales". Pág. 177.

transfronterizo de datos” del Convenio 108 del Consejo de Europa; la finalidad de los Artículos 33 y 34 de la Ley Orgánica de Protección de Datos Personales (LOPDP) es conciliar la protección de la integridad de la información personal, con el libre tránsito de los datos. lo que no puede ser de otra manera, ya que la Transmisión Internacional de Datos constituye una auténtica necesidad de la vida actual y de suma importancia en el ámbito económico de los Estados, tal y como evidencia la gran cantidad de inversiones que en los últimos años han venido realizándose en relación con el entorno de la libre circulación de informaciones y de datos, marco necesario para su funcionamiento.

La norma general en la Transmisión Internacional de Datos es la de exigir un sistema de protección equiparable al español para los datos exportados, cuyo sentido último es lograr compatibilizar el principio de libre circulación de la información con el Principio de Defensa del derecho humano a la Intimidad de los particulares sobre sus datos. Este principio responde, por una parte, a las necesidades de garantizar una protección semejante en la Transmisión Internacional de Datos Personales, a las de la comunicación en el interior de un Estado y, por otra, a las exigencias de los convenios y tratados internacionales a los que España es parte.

También la *Directiva sobre Protección de Datos Personales*[166] exige, para la Transmisión de Información Personal a terceros países, un nivel de protección adecuado. La transferencia de datos personales entre Estados miembros, sin embargo, se adecuará a un criterio deferente, el de un nivel equivalente de protección. No es casual la utilización de un criterio distinto para la Transmisión de Datos dentro de la Unión Europeo o fuera de los Estados miembros y no parece que tenga el mismo significado los términos equivalente y adecuado. Pues, mientras a los Estados miembro se les exige, para que los datos puedan circular libremente por sus territorios, alcanzar el nivel equivalente al del Estado transmisor, cuando la transmisión de datos se produce a un país no comunitario, sólo se exige que satisfaga un estándar mínimo de protección, para evitar las reticencias como países como Canadá y Estados Unidos que ven en este tipo de legislaciones barreras a la transmisión internacional de datos que pudieran dañar sus intereses económicos, por lo tanto, el requisito general para la Transmisión Internacional de Datos es que en el país de destino exista un nivel de protección equiparable al español; sin embargo, no es esta la única condición que se debe cumplir para la Transmisión Internacional de Datos Personales, pues como en el caso de cualquier otra sección deberán respetarse los

[166] Directiva sobre Protección de Datos Personales, citada por Gárriga Domínguez, Ana. Ob.cit. Pág. 78

principios de calidad de datos[167] y los derechos de los afectados. Esto supone que para que se puedan exportar legalmente datos personales, tendría que haberse previsto entre sus finalidades de recolección y tendría que haberse informado al afectado de esta posibilidad y de la identidad de sus destinatarios, en el momento de la recogida de estos cumpliendo, además, con los restantes requisitos que para la sesión de datos personales exige la Ley.

La regulación española ha sufrido determinados cambios como consecuencia de la transposición de los artículos 25 y 26 de la Directiva 95/46/CE[168]. El apartado segundo del artículo 33 recoge prácticamente de manera idéntica las precisiones y circunstancias enumeradas en el artículo 25.2 de la Directiva que nos permitirán saber, si un Estado cuenta o no con un nivel adecuado de protección.

En primer lugar, se determina que éste se evaluará por la Agencia de Protección de Datos " atendiendo a todas las circunstancias que concurran en una transferencias de datos " personales, por tanto, parece que, en principio, se favorece un sistema casuístico y no un criterio general en relación con la transmisión de datos a determinados países, debiéndose evaluar en relación con cada transferencia o categoría o clase de

[167] Ver "Principios de Calidad de Datos y Derecho de los Interesados: el núcleo del derecho a la Autodeterminación Informativa en la LOPDP", Garriga Domínguez, Ana. Ob. Cit. Págs. 77 y siguientes.
[168] Directiva 95/46/CE, citada por Garriga Domínguez, Ana. Ob. Cit. Págs. 178

transferencias, si un tercer estado ofrece o no un nivel de protección adecuado sobre la base de los criterios que enumera, el segundo apartado del artículo 33. Es decir atendiendo a la naturaleza de los datos, la finalidad y duración del tratamiento, el país de origen y el país del destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dicho países y los informes de la Comisión de la Unión Europea.

En el artículo 34 de la LOPDP se establece una larga lista de excepciones al régimen general de exigencias de un nivel equiparable de protección. Las excepciones enumeradas seguidamente son mas numerosas que en la LOARTAD y en algunos casos exceden lo previsto en la Directiva 95/46/CE. Así, será libre la transmisión internacional de datos personales y no será necesario que el país destinatario acredite un nivel de protección equivalente, ni la autorización previa del Director de la Agencia de Protección de Datos, en los siguientes casos:

1- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España. No necesitaran cumplir con las condiciones del artículo 33, por ejemplo, las transmisiones de datos personales registrados en ficheros de los Cuerpos y Fuerzas de Seguridad en función de una investigación concretas hechas. Tampoco, las transmisiones de datos personales realizadas en virtud del

Convenio de Aplicación del acuerdo de Schegen, con destino a la unidad de apoyo del sistema de información Schegen, cuando una investigación policial en curso requiera la utilización de datos del sistema, ni las comunicaciones de datos personales contempladas en Título VI del Tratado de la Unión Europea, en el que se establecen las " Disposiciones relativas a la cooperación en los ámbitos de la Justicia y de los Asuntos de Interior" entre los Estados miembros o las cesiones de datos personales en virtud del Convenio Europol de 26 de julio de 1995.

2 – Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

3 – Cuando la transferencia sea necesaria para la prevención o para el diagnostico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios. A pesar de las modificaciones sufridas por la LOPDP, esta excepción parece excesiva por la naturaleza de los datos objeto de la cesión a un Estado que no cuenta con un nivel de protección semejante al Español y especialmente injustificada, cuando la causa de la comunicación de las informaciones referentes a la salud sea la simple gestión de los servicios sanitarios. Además, esta excepción supone y como siempre en la LOPDP en detrimento de los derechos fundamentales de los ciudadanos una adecuada transposición de la directiva, ya que ésta sólo autoriza la transmisión de datos personales cuando esté en juego el interés vital del interesado.

4 – Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

5 – Cuando el interesado haya dado su consentimiento inequívoco a la transferencia prevista.

6 – Cuando sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

7 – Cuando la comunicación internacional de datos personales sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del afectado, por el responsable del fichero y un tercero.

8 – Cuando la transferencia sea necesaria o venga legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración Fiscal o Aduanera para el cumplimiento de su competencia.

9 – Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

10 –Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un registro público y aquella sea acorde con la finalidad del mismo.

11 – Y finalmente, cuando la comunicación de datos tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del

cual la comunicación de la Unión Europea haya declarado que garantiza un nivel de protección adecuado.

CAPITULO V
5. ANALISIS DE LOS RESULTADOS DE LA INVESTIGACION.

En este capítulo se plantea el problema objeto de la investigación y las hipótesis establecidas en nuestro diseño, así como la metodología utilizada para obtener respuestas a través de las técnicas de investigación documental y de campo; además del respectivo análisis e interpretación de los resultados de los instrumentos aplicados, y la comprobación de las hipótesis planteadas.

5.1 FORMULACION DEL PROBLEMA DE INVESTIGACIÓN.

“Entidades privadas de procesamiento de datos personales (DICOM e INFORNET) ocasionan graves violaciones al derecho a la Autodeterminación Informativa y la Libertad Informática, debido a la falta de regulación jurídica referente a la protección de datos personales y al tratamiento informatizado

de los mismos. Lo anterior, propicia que no haya un control en el uso que se le da a los datos personales por los encargados de su procesamiento; no pudiendo determinarse qué responsabilidades acarrea a los encargados de los registros o bases de datos el manejo no regulado de ellos, haciendo imposible establecer qué responsabilidades Civiles y Patrimoniales acarrean el uso no regulado de los datos personales. A esto se suman cuestiones técnicas como: la forma en que afecta el tratamiento automatizado de los datos personales en la Intimidad Personal y familiar o en la privacidad de las personas; así como también, el procesamiento inadecuado de los datos personales, la falta de actualización en los equipos informáticos, y quién controla el manejo de los datos personales. En esto cobra importancia determinar qué rol juega la Sala de lo Constitucional en la regulación jurisprudencial del Derecho a la Autodeterminación Informativa y Libertad Informática, qué procedimientos legales existen para el resarcimiento por daños morales, por el uso ilegal o arbitrario de los datos personales; qué figura legal es la más adecuada para la regulación del uso irresponsable de datos personales, cómo afecta la falta de regulación legal en los operadores del sistema informatizado de datos en entidades publicas o privadas; finalmente cómo incide el uso que las personas le dan a los mecanismos legales para defenderse ante la violación de su Intimidad personal y familiar, así como a su privacidad".

5.2 SISTEMA DE HIPÓTESIS.

5.2.1 Operacionalización de Hipótesis.

a) Hipótesis General: “Incorporar la figura del Hábeas Data en la Legislación constitucional salvadoreña constituye una necesidad jurídica debido a que, en la actualidad, el tratamiento automatizado de datos personales sin regulación jurídica expresa provoca violaciones graves a los derechos constitucionales regulados en el Art. 2 de la Constitución de la República, relacionados con la Autodeterminación informativa o Libertad Informativa”.

VARIABLE INDEPENDIENTE		VARIABLE DEPENDIENTE	
CAUSA INMEDIATA	Inexistencia del Hábeas Data en la Legislación Nacional.	EFECTO	Graves violaciones a la Autodeterminación Informativa y Libertad Informática
Indicador	Tratamiento Automatizado de Datos Personales	Índice	- Bases de datos - Entidades Públicas y privadas. - Recolección y Almacenamiento de Datos.
Indicador	Falta de regulación jurídica expresa.	Índice	Normativa Constitucional.
Indicador	Violación de Derechos Constitucionales	Índice	- Artículo Dos de la Constitución. - Derecho a la Autodeterminación Informativa. - Libertad Informativa. - Derecho a la Intimidad.

b) Hipótesis Específicas:

Hipótesis Específica Uno: “Incorporar la figura del Hábeas Data, mediante una reforma legal, en la Constitución de la República salvadoreña podrá hacer efectivo el cumplimiento y protección del Derecho a la Intimidad personal y familiar, contenido en el Art. 2 Cn. respecto al tratamiento automatizado de datos personales”.

VARIABLE INDEPENDIENTE		VARIABLE DEPENDIENTE	
CAUSA MEDIATA	Reforma Legal en la Constitución para incorporar el Habeas Data	EFECTO	Base legal para el cumplimiento y la protección del Derecho a la Intimidad, respecto al tratamiento automatizado de datos personales.
Indicador	Hábeas Data como figura autónoma.	Índice	Agregar inciso en el Art. 11 de la Constitución.
Indicador	Protección de Datos Personales.	Índice	- Deducción de responsabilidades civiles y patrimoniales en los encargados de registros o bases de datos. - Entidades públicas y privadas.

Hipótesis Específica Dos: “La creación de una Ley Especial de Protección y Tratamiento de Datos Personales o la incorporación del Procedimiento de Hábeas Data en la Ley de Procedimientos Constitucionales vigente, haría efectivo la protección del derecho constitucional de la Intimidad personal y familiar contenido en el Art. 2 Cn”.

VARIABLE INDEPENDIENTE		VARIABLE DEPENDIENTE	
CAUSA MEDIATA	Creación de Ley Especial o Incorporación del Procedimiento de Hábeas Data en la Ley de Procedimientos Constitucionales	EFECTO	Base legal para la efectiva protección del derecho a la Intimidad familiar y personal.
Indicador	Reforma Legal.	Índice	- Ley de Procedimientos Constitucionales. - Figura Autónoma de Hábeas data.
Indicador	Existencia de Normativa Secundaria.	Índice	- Desarrollo de Principios Básicos del Tratamiento de Datos Personales. - Límites en el uso de la Informática.

Hipótesis Específica Tres: "La garantía del Hábeas Data tiende a proteger los derechos constitucionales relacionados a la Autodeterminación Informativa frente a posibles abusos en el tratamiento de datos personales, por el manejo ilegal y arbitrario por parte de los responsables de los archivos o bancos de datos personales".

VARIABLE INDEPENDIENTE		VARIABLE DEPENDIENTE	
CAUSA MEDIATA	El Hábeas Data como garantía constitucional autónoma.	EFECTO	Protege la Autodeterminación Informativa frente al manejo ilegal e irresponsable de datos personales.
Indicador	Control en el Tratamiento de Datos Personales.	Índice	- Reducción del uso ilegal o arbitrario de datos personales. - Deducción de Responsabilidades de los Encargados de los

Indicador	Existencia de disposición constitucional con la Garantía Hábeas Data.	Índice	Registros o Bases de Datos. Factibilidad en el ejercicio del derecho de acción ante posibles violaciones a la Autodeterminación Informativa y el derecho a la Intimidad

Hipótesis Específica Cuatro: "La falta de regulación jurídica del Hábeas Data en la legislación salvadoreña influye en la existencia de violaciones de los derechos constitucionales relacionados con la Autodeterminación Informativa, ya que posibilita la manipulación de los datos personales contenidos en registros o bancos de datos".

VARIABLE INDEPENDIENTE		VARIABLE DEPENDIENTE	
CAUSA INMEDIATA	Falta de Regulación Jurídica del Hábeas Data en la Legislació0 salvadoreña vigente.	EFECTO	Existencia de violaciones al Derecho de la Autodeterminación Informativa.
Indicador	Vació Legal	Índice	Ineficacia de los mecanismos jurídicos existentes (Hábeas Corpus y Amparo) en cuanto a protección de Datos Personales.
Indicador	Manipulación de Datos Personales.	Índice	- Obligaciones del Responsable del Sistema de Datos Personales. - Responsabilidades en el Tratamiento de Datos Personales. - Competencias atribuidas a los entes públicos y privados que llevan registros o bases de datos.

Hipótesis Específica Cinco: “La legislación constitucional comparada servirá de base para hacer un propuesta de reforma o readecuar la legislación constitucional nacional, para que se pueda incluir el Hábeas Data, como figura autónoma, encaminada a la protección de los derechos constitucionales frente al tratamiento automatizado de datos personales”.

VARIABLE INDEPENDIENTE		VARIABLE DEPENDIENTE	
CAUSA MEDIATA	Legislación Comparada será base para incluir el Hábeas Data en la Legislación nacional.	EFECTO	Protección eficaz de derechos constitucionales respecto al tratamiento automatiza de datos personales.
Indicador	Derecho Comparado	Índice	Efectividad del Hábeas Data.

5.3 METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN.

5.3.1 Metodología de la Investigación.

El abordaje del fenómeno de la Protección de Datos Personales a través del Hábeas Data, ha tratado de hacerse manteniendo una armonía y equilibrio entre dos modelos: a) Jurídico – dogmático, y b) Jurídico – Realista; en donde el primero tiene un enfoque formalista, cuyo objeto es el Derecho Normativo, viéndose éste como una variable independiente en su propia dimensión y en el cual se utiliza básicamente la Lógica Deductiva; y el segundo viene a complementar el enfoque Jurídico – dogmático, siendo su

enfoque Social y su objeto recae en la Investigación de Factores Sociales de todo tipo que influyen en el Derecho; para el caso, se trata de la Influencia de los Avances tecnológicos, principalmente de la Informática, en el Derecho, se trata de una visión integradora. La idea es que, a través del aspecto metodológico, se puedan integrar los dos enfoques, para así obtener los mejores resultados. Se pretende, así mismo, manejar una Teoría explicativa en base a la información y el conocimiento que se obtenga del tema objeto de estudio.

Debido a que toda investigación requiere de un registro estadístico, para lo cual se hace necesario hacer uso de diferentes instrumentos para el acopio de información, se ha hecho uso de la siguiente fórmula: Fr = Fa x 100/N, en donde Fr es igual a Frecuencia Relativa, Fa es igual a Frecuencia Absoluta y N es igual al Total de la Población.

Las Unidades de Análisis a consideradas para la investigación realizada son las siguientes:

Unidades de Análisis	Población	Muestra
Magistrados de la Sala de lo Constitucional de la Corte Suprema de Justicia	5	2
Colaboradores Judiciales de la Sala de lo Constitucional de la Corte Suprema de Justicia	32	32
Gerentes o Jefes de entes encargados de		

Registros o Bancos de Datos públicos y privados.	8	8
Profesionales del Derecho.	------	50

El diseño de la Muestra utilizada se hizo mediante el procedimiento de Muestro Aleatorio Simple, en el cual las unidades de análisis (personas) se seleccionaron al azar y cada elemento tenía la misma probabilidad de ser elegido, haciéndose posible conocer el *Error de Muestreo.* La Entrevista Estructurada estaba dirigida a Magistrados que conforman la Sala de lo Constitucional de la Corte Suprema de Justicia, a quienes no fue posible entrevistar, justificándose en el hecho de no poder anticipar criterio; la misma circunstancia se aplica a la Encuesta de opinión dirigida a los treinta y dos Colaboradores Judiciales de la referida Sala; tomando en cuenta que, no se cuenta con un dato exacto de la población total de los entes públicos y privados encargados de registros o bases de datos en nuestro país, teniendo como base los criterios doctrinarios para clasificar los registros de bases de datos, estableciendo ocho tipos, se seleccionó indistintamente ocho instituciones, una de cada tipo de registros, en las cuales la Entrevista No Estructurada se dirigió a sus gerentes, de los cuales se pudo entrevistar únicamente a cinco, debido a la actitud burocrática de algunas de las referidas instituciones; finalmente, respecto de los Profesionales en Derecho en nuestro país, por no tenerse un dato exacto de la población total, se entrevistó a cincuenta.

La recopilación de datos toma también en consideración las siguientes fórmulas:

$$\frac{Nc}{NT} \times 100$$

Nc = Número de casos.
NT = Total de casos.

Fórmula Complementaria:

$$\frac{Fa}{NT} = Fr\ \%$$

Fa = Frecuencia Absoluta.
NT = Total de casos.
Fr = Frecuencia relativa.

La presentación, descripción e interpretación de resultados necesita de la elaboración de cuadros estadísticos y gráficas respectivamente; por lo que, se ha elegido gráficas circulares para facilitar el análisis e interpretación de los resultados obtenidos, pues permiten visualizar mejor las tendencias de las variables. Es de aclarar que el universo considerado es de naturaleza dirigida, por lo cual asume la calidad de muestra, en virtud que el tema objeto de estudio es una figura no regulada en la legislación salvadoreña, lo que hace exigible que las unidades de análisis sean de carácter selectivas.

5.3.2 Técnicas de Investigación.

a) Técnicas de Investigación Documental:

► Con las *Técnicas de Investigación Documental de Aco*pio se maneja fichas bibliográficas y Hemerográficas seleccionando la información

en: Fuentes Primarias, las cuales son instrumentos jurídicos, así como libros que desarrollan temas como la Protección de Datos Personales, la Autodeterminación Informativa y Libertad Informativa, y principalmente el Hábeas Data, así como Manuales de Derecho constitucional e Informática Jurídica; y en Fuentes Secundarias, como son Revistas, Periódicos, Boletines y otros documentos con información relevante extraída de Internet.

► Con las *Técnicas de Investigación Documental de Análisis de Contenido Jurídico*, se realizó el análisis de Sentencias de Amparo de la Sala de lo Constitucional de la Corte Suprema de Justicia, referentes a la Protección de Datos Personales y Autodeterminación Informativa, así como Jurisprudencia de la Sala.

b) Técnicas de Investigación de Campo:

Para la realización de la investigación de campo se utilizó la técnica de la Observación Indirecta, la cual se hizo a través de:

► Entrevista: con la modalidad de ser Dirigida Individual, y se realizó a personas clave, como Magistrados de la Sala de lo Constitucional de la Corte Suprema de Justicia y Encargados de Registros de Datos Personales en nuestro país.

► Encuesta: este es un instrumento estructurado y controlado, mediante el cual se recopiló opiniones de una muestra; es decir la opinión pública de Colaboradores Judiciales de la Sala de lo Constitucional de la Corte Suprema de Justicia y de Profesionales del Derecho. El diseño de la

Muestra utilizada se hizo mediante el procedimiento de Muestro Aleatorio Simple, en el cual las unidades de análisis (personas) se seleccionaron al azar, con la misma probabilidad para cada elemento de ser elegido, haciéndose posible conocer el *Error de Muestreo.*

5.4 ANALISIS E INTERPRETACION DE RESULTADOS DE LA INVESTIGACION DE CAMPO.

5.4.1 Resultados de las Entrevistas No Estructuradas Dirigidas a Encargados de Registros o Bases de Datos.

Este tipo de instrumento se ha utilizado con el propósito de obtener un mayor conocimiento acerca de la realidad de los registros o bases de datos personales en nuestro medio, por lo que se hace necesario establecer el tratamiento de datos personales en los registros, y de las entidades que, en alguna medida, se relacionan con el almacenamiento y tratamiento de datos personales.

Entrevista número uno:

Dirigida a: Lic. Rolando Fagoaga.

Cargo: Jefe del Registro y Control Penitenciario, Dirección General de Centros Penales.

Fecha: martes veinte de junio del año dos mil seis.

Hora: nueve horas.

A continuación se presenta las preguntas efectuadas al entrevistado, así como las respectivas respuestas.

Pregunta 1: ¿Cuál es el mecanismo o la forma utilizada para la recolección de datos personales contenidos en el registro o base de datos a su cargo?

Respuesta:

Aquí la información se obtiene a través del Jurídico de cada uno de los Centros Penitenciarios del país, ya que inmediatamente que el reo ingresa a dicho centro, el Jurídico le toma sus datos generales, los cuales son: nombres y apellidos, alias, dirección, edad, profesión u oficio, fecha de nacimiento, nacionalidad, el delito, el Tribunal que lo condenó.

Pregunta 2: ¿Cuál es la finalidad de la existencia del registro o base de datos a su cargo, y el destino que se le da a los datos personales contenidos en ella?

Respuesta: La finalidad es llevar un control de la información de cada uno de los detenidos, cuando se ordena la Medida Cautelar de la detención Provisional, en el caso de los reos que aún está en proceso penal, y en consecuencia, no tienen una condena; así como el registro de las sentencias condenatorias y absolutorias, incluso, de las Conciliaciones.

Pregunta 3: ¿El titular de dichos datos tiene conocimiento de la existencia de la base de datos, de la finalidad de la existencia de la misma, y

que sus datos están contenidos en ella, así como el destino que se le da a los mismos?

Respuesta: Si, recordemos que nadie puede alegar ignorancia de la Ley.

Pregunta 4: ¿La base de datos a su cargo cuenta con un sistema de protección de datos?

Respuesta: Sí.

Pregunta 5: Si la respuesta anterior es positiva: ¿En qué consiste dicho sistema y que tan eficaz es?

Respuesta: por cuestión de seguridad no le puedo explicar en qué consiste el sistema; pero si le puedo decir que contamos con mecanismos legales de protección que son del artículo 109 al 113 del Código Penal, que regula el Régimen de los Antecedentes Penales, así como en la Ley Penitenciaria, en los artículo 40, 41 y 310 en lo que respecta al manejo de la información. De igual manera, contamos con una base de datos principal, un Back up, un sistema en el cual cada usuario tiene su password, a través del cual se identifica quién ha ingresado al sistema, si ha cambiado un dato o introducido uno nuevo...; hay diferentes niveles de usuario, ... hay unos que sólo digitan, otros sacan solvencias .... Se tiene una actualización con una tasa del 89% de las sentencias remitidas... Se tiene registrado desde 1990 hasta la fecha; además, se tiene un sistema de depuración de sentencias.

Pregunta 6: Dentro del presupuesto asignado al registro o base de datos a su cargo, ¿qué porcentaje está destinado a la protección de datos personales contenidos en el mismo?

Respuesta: No puedo contestarle, por motivos de seguridad.

Interpretación:

En el desarrollo de la entrevista, el Licenciado Fagoaga manifestó que la recolección de datos personales se realiza de una manera directa; sin embargo, por las particularidades especiales de dicho registro esta información directa no necesariamente es del todo voluntaria, por ser obligatoria y el titular de los datos personales no puede negarla ni exigir privacidad, pues desde el momento de ingresar al centro penitenciario se debe realizar la recolección de datos por el jurídico del respectivo centro penitenciario; dicho registro se encuentra legitimado, no sólo por la sociedad en general, sino también por un respaldo legal amparado en los artículos 102 y 113 del Código Penal, ya que resulta necesario para llevar un efectivo control de los reos con condena e incluso, los que no la tienen; no obstante su legitimidad, puede en algunos casos, ser utilizada dicha información de manera discriminatoria, limitando la reinserción de la persona con antecedentes penales en la sociedad, debido a que en nuestro país esta información es requerida por algunas empresas, al momento de contratar

personal. Mientras no exista una normativa secundaria que regule el tratamiento de datos personales, cabe la posibilidad que dicha información sea utilizada con fines discriminatorios por parte de los empleadores al contratar personal. Por otra parte, el entrevistado manifestó que se cuenta con un moderno sistema de protección, el cual no lo explicó, según él, por cuestiones de seguridad; así mismo, manifestó que aunque no existe normativa especial que regule el tratamiento de datos personales, los Arts. Del 109 al 113 del Código Penal regulan el Régimen de los Antecedentes Penales, y los Arts. 40 y 41 de la Ley Penitenciaria regulan el manejo de la información; los cuales constituyen, en su opinión, mecanismos legales de protección de la información.

Entrevista número dos:

Dirigida a: Lic. Ernesto José Castilla.

Cargo: Jefe de la Unidad de Informática, Departamento de Solvencias de la Policía Nacional Civil.

Fecha: jueves veintidós de junio del año dos mil seis.

Hora: nueve horas y treinta minutos.

A continuación se presenta las preguntas efectuadas al entrevistado, así como las respectivas respuestas.

Pregunta 1: ¿Cuál es el mecanismo o la forma utilizada para la recolección de datos personales contenidos en el registro o base de datos a su cargo?

Respuesta: Voluntariamente el interesado llena un formulario con sus datos personales generales. Para el procesamiento de la información, de la persona, se toman los datos del documento original (DUI), luego se ficha a la persona: se fotografía y se le toma las huellas dactilares, si es por primera vez.

Pregunta 2: ¿Cuál es la finalidad de la existencia del registro o base de datos a su cargo, y el destino que se le da a los datos personales contenidos en ella?

Respuesta: La finalidad es La recopilación de datos para futuras investigaciones, por ejemplo, para cotejar las huellas dactilares para identificar cadáveres, en delitos de Secuestro, cuando el Departamento Antisecuestros lo solicita.

Pregunta 3: ¿El titular de dichos datos tiene conocimiento de la existencia de la base de datos, de la finalidad de la existencia de la misma, y que sus datos están contenidos en ella, así como el destino que se le da a los mismos?

Respuesta: Si, ya que todas las personas, para determinados trámites como por ejemplo para solicitar empleo, tramitan la solvencia de la policía.

Pregunta 4: ¿La base de datos a su cargo cuenta con un sistema de protección de datos?

Respuesta: Sí.

Pregunta 5: Si la respuesta anterior es positiva: ¿En qué consiste dicho sistema y que tan eficaz es?

Respuesta: En primer lugar, la base de datos física está resguardada en el mismo departamento; los expedientes físicos de las personas se van almacenando en cajas, y estas en estantes, en una habitación sellada. Asimismo, se cuenta con un sistema de servidores que evitan la carga del sistema por consulta; hay dos servidores para almacenar la base de datos: un sistema especial de protección contra intrusos, y el otro es un Muro de Fuego “Router”, el cual protege la base de datos. Hay un DNS, el cual es una clase de acceso a la red que consiste en que si una persona no tiene usuario creado en al computadora, no puede accesar a la información; además de tener un usuario creado, tiene que tener un determinado perfil. El encargado de la base de datos puede restringir el acceso a la base determinando que el servidor pueda ingresar desde una unidad determinada o de cualquiera de las de la base. El único que puede modificar o borrar información de la base de datos es el administrador de la misma, ya que este tiene un terminal desde la cual administra la base.

Pregunta 6: Dentro del presupuesto asignado al registro o base de datos a su cargo, ¿qué porcentaje está destinado a la protección de datos personales contenidos en el mismo?

Respuesta: Por ser este una institución en la cual las personas tramitan sus solvencias de la policía, servicio por el cual, dan un aporte económico, contamos con un presupuesto propio; yo, como administrador de esta base de datos, puedo solicitar lo necesario para adquirir determinado equipo, si es requerido. Del presupuesto general de la PNC, como institución, sólo se puede aspirar para cosas básicas.

Interpretación:

En el desarrollo de la entrevista se observó cierta evasión de responsabilidad por parte del entrevistado, ya que manifiesta que las personas proporcionan sus datos de manera voluntaria llenando formularios; pero es de todos conocido que para optar a un empleo, por ejemplo, en la mayoría de empresas exigen a los aspirantes una solvencia de la Policía, y para tramitarla se debe llenar un formulario, en cual se hacen constar datos personales, si no se llena dicho formulario no se le extiende la solvencia, y sin esta no se podrá obtener el empleo; por lo que puede observarse que no es del todo voluntaria la forma en que los sujetos proporcionan sus datos personales. De igual manera, el entrevistado manifestó que la información contenida en la base de datos a su cargo es compartida con otras entidades

públicas para la investigación de delitos, y en cuanto al almacenamiento de la misma, la única persona que puede modificarla o cancelarla es él, por ser el administrador de la base de datos, debido a lo delicado de la información; sin embargo, manifestó que cuentan con servidores que evitan la carga del sistema por “consulta”, por lo que puede deducirse que sí se puede tener conocimiento sobre la información contenida en el registro a su cargo, además el entrevistado reconoció que, por ser personas naturales las que almacenan y manejan la información, cabe la posibilidad que en determinado momento, al contarse con el usuario, clave y perfil determinado, se puede manipular, de alguna manera dicha información, de lo cual únicamente se deducen responsabilidades administrativas.

Entrevista número tres:

Dirigida a: Lic. Francisco Aguilar.

Cargo: Registrador Jefe, Registro de la Propiedad Raíz e Hipotecas, Primera Sección del Centro.

Fecha: lunes veintiséis de junio del año dos mil seis.

Hora: ocho horas.

A continuación se presenta las preguntas efectuadas al entrevistado, así como las respectivas respuestas.

Pregunta 1: ¿Cual es el mecanismo o la forma utilizada para la recolección de datos personales contenidos en el registro o base de datos a su cargo?

Respuesta: Los datos son dados por el mismo titular de una forma voluntaria.

Pregunta 2: ¿Cual es la finalidad de la existencia del registro o base de datos a su cargo y el destino que se le da a los datos personales contenidos en ella?

Respuesta: Brindar seguridad jurídica a los inmuebles. Nosotros somos un registro Publico, por lo tanto la información es publica, por ejemplo tenemos el servicio de carencia de bienes... si alguien me dice, mire yo quiero saber si fulano de tal tiene inmuebles a su nombre y aquí traigo su numero de NIT y DUI, le damos la información.

*Pregunta 3:¿*Cualquier persona aunque no sea el titular de esos datos puede solicitar una carencia de bienes?

Respuesta:

Si, cualquier persona solo necesita el número de NIT y DUI, la ley no nos exige que nos demuestren el parentesco o la calidad en que actúa.

Pregunta 4: ¿Que mecanismo utilizan para la protección de los datos?

Respuesta: Aquí cada quien tiene sus funciones, tenemos personas que la función de ellos es crear códigos; alguien que por primera vez ha comprado un inmueble no tiene código, no había manera de obtenerlo, para

creárselo lleva un proceso: Presentación, escaneo, distribución y después llega a los equipos, la primer persona que agarra ese documento es la que crea el código de las personas naturales, porque las personas jurídicas las lleva el registro de comercio; cuando se les crea por primera vez el código se incluye su nombre completo, numero de DUI y NIT, donde nació; con el numero de NIT podemos determinar hasta su fecha de nacimiento, ese código la persona lo va a tener siempre y se hace publico. La seguridad que nosotros tenemos consiste en que cada quien esta con su usuario y clave. Puedo ir a informática y preguntar quien creo este código y podemos determinar que fue el usuario fulano de tal.

Pregunta 5: ¿Se puede determinar responsabilidades?

Respuesta: Si, hay responsabilidades de lo que hagan mal, hay responsabilidad administrativa. Pero no todos creamos códigos, yo que soy el jefe no puedo crear códigos, no tengo acceso a eso, hay personas determinadas.

Pregunta 6: ¿Entonces, estas personas son las únicas encargadas de modificar o cambiar datos?

Respuesta: Modificar si se puede... Digamos yo estoy como Francisco Aguilar y después presento un documento que tengo un " conocido por", una identidad, entonces puede modificar el nombre, y esto se da con mayor frecuencia con el nombre de las mujeres, que primero aparecen como

solteras y después como casadas o viudas, lo que nos importa a nosotros es el numero de NIT.

Pregunta 7: ¿A través de Internet se puede tener acceso a estos datos personales?

Respuesta: No, ahí puede hacer consultas, igual aquí en el edificio del registro tenemos en la entrada computadoras para consultas, que si yo quiero digamos saber el numero de matricula de mi inmueble porque se me olvido y perdí hasta el antecedente, me voy a consultar a la computadora, ahí yo pongo mi nombre, le doy buscar y si yo tengo un inmueble me va aparecer y pediré una certificación literal de esta matricula con el numero tal.

Pregunta 8: ¿De igual manera cualquier persona puede buscar información de cualquiera, solo ingresando el nombre?

Respuesta: Si, pero el nombre debe ser exacto, "todo esta conforme a la ley digamos", tampoco se le puede entregar a cualquiera un instrumento inscrito, aunque la persona diga: " yo soy el esposo de ella, démelo", por que la ley ya nos dice a quien se lo vamos a entregar: al notario, al dueño del documento o a su representante, " la consulta es publica cualquiera puede venir hacer una consulta, pero si hay limitantes en cuanto a la entrega.

Pregunta 9: Dentro del presupuesto asignado al registro o base de datos a su cargo, ¿qué porcentaje esta destinado a la protección de los datos personales contenidos en el mismo?

Respuesta: Nosotros somos auto sostenibles, tenemos una partida de Hacienda, ahí va todo, digamos, mejor equipo, compra de equipo, mantenimiento de sistemas, hay una cantidad presupuestada para eso.

Pregunta 10: ¿Como es el Tratamiento de los datos personales?

Respuesta: Aquí a diario se hacen los Back up, porque ya se ha dado el caso que se "perdió" información por los bajones de energía y todo eso, entonces no se que pasó ahí cuando eso, y previniendo desgracias mayores hacemos los Back up a diario.

Pregunta 11: ¿Explique el sistema de protección de los datos personales?

Respuesta: Digamos que si aquí entrara un virus, aunque tenemos todo el equipo antivirus, pero hay unos que son bien fuertes o escurridizos, nosotros entonces a diario hacemos Back up y tenemos antivirus.

Pregunta 12: ¿Existe la posibilidad que se pueda modificar datos?

Respuesta: ¡Ah!, recuerde que todos tenemos un precio, y si se dio antes puede darse ahora que algún empleado modifique los datos incluso si se pide una carencia de bienes le dan algo al empleado y no le aparecen bienes, o cambiarse algún código y de repente su propiedad aparezca con otro código y otro dueño.

Pregunta 13: ¿Entonces hay riesgo?

Respuesta: Si, a nosotros entonces, solo nos queda confiar en nuestros empleados.

Interpretación:

Durante el desarrollo de la entrevista, el entrevistado manifestó que en un registro de contenido patrimonial, como lo es el Registro de la Propiedad Raíz e Hipotecas y el Registro de Comercio, el trámite de los datos es de manera personal y voluntaria, el uso de los mismos es interno, en virtud del Principio de Confidencialidad; sin embargo, reconoció que cualquier persona puede tener acceso a la información debido a que se trata de un registro público, a demás de contarse con computadoras para el uso del público en general, así como también a través de Internet, cualquier persona puede consultar la información de otras personas, pero aclara que no puede ser modificada dicha información; por otro lado manifestó también que por no existir disposición legal que regule el tratamiento de datos personales en nuestro ordenamiento jurídico, no están obligados a tener un sistema de protección de la información, pero que toman las medidas necesarias, reconociendo que siempre existe la posibilidad de que pueda darse una manipulación de la información, ya que son personas las que se encargan del manejo de la misma. Con ello, se observa el peligro que existe de que cualquier persona puede tener conocimiento de la situación de los bienes inmuebles de cualquier otra persona, y el peligro latente del posible uso arbitrario de los datos personales por no existir disposición legal que regule el tratamiento de datos personales, que obligue a los encargados de los

registros o bases de datos personales a garantizar la protección de los mismos.

Entrevista número cuatro:

Dirigida a: Analista de Sistemas Informáticos de Scotiabank, quien no quiso que su nombre fuera mencionado en el presente documento.

Fecha: miércoles veintiocho de junio del año dos mil seis.

Hora: nueve horas.

A continuación se presenta las preguntas efectuadas al entrevistado, así como las respectivas respuestas.

Pregunta 1: ¿Cuál es la forma utilizada para la recolección de datos personales contenidos en el Registro o Base de Datos a su cargo?

Respuesta: Los datos son obtenidos por medio de un formulario que la persona llena al momento de solicitar determinado préstamo o para la apertura de una cuenta de ahorros.

Pregunta 2: ¿Cuál es la finalidad de la existencia del registro o base de datos a su cargo y qué clase de datos personales están contenidos en ella?

Respuesta: Los datos que se almacenan son datos generales, por cada cliente existe un archivo, en el cual se encuentran todos los datos o información relacionada a ese cliente, como dirección, beneficiarios, etc., así

como las transacciones que ha realizado con la institución, cuentas, préstamos, etc.

Pregunta 3: ¿La información o datos personales contenidos en el registro que como institución cuenta, son de uso interno o son compartidos con otra entidad?

Respuesta: Esta información es sólo de uso interno, sólo en el caso que llegue un Juez Ejecutor que necesite información para realizar un embargo, se le proporciona dicha información; de lo contrario, es sólo de uso interno.

Pregunta 4: ¿El registro o base de datos a su cargo tiene alguna relación con la institución privada denominada DICOM u otra institución de esa naturaleza?

Respuesta: Sí, todo cliente que se retrase más de noventa días en el pago de la deuda, va para el registro de DICOM; una vez cancelada toda la deuda, el Banco manda una Constancia de pago a DICOM y en treinta días está corregido su registro. Sólo en los casos de tarjetas de crédito se puede tardar hasta cinco años en actualizarlo.

Pregunta 5: ¿El titular de dichos datos tiene conocimiento de la existencia de la base de datos, de la finalidad de la existencia de la misma y que sus datos están contenidos en ella, así como el destino que se le da a los mismos?

Respuesta: El cliente tiene conocimiento de la existencia de la base de datos, ya que al momento de realizar algún trámite con el banco, llena una planilla, y la firma aceptando las condiciones y dando su consentimiento para el uso y destino que el banco les de a los mismos.

Pregunta 6: ¿Cómo institución de qué forma garantiza la seguridad de los datos personales contenidos en su registro?

Respuesta: Por tratarse de información confidencial o secreta, y en virtud del secreto bancario, no se le permite el acceso a cualquier persona que quiera saber algo sobre la información de los clientes; de esa manera se protege la información.

Pregunta 7: ¿Cómo institución, cuenta con presupuesto destinado a la protección de datos personales?

Respuesta: Dentro del presupuesto que se le asigna a la institución, se destina lo necesario para cuestiones de mantenimiento de equipo, actualización de programas y antivirus.

Interpretación:

En el desarrollo de la entrevista realizada, el entrevistado manifestó que los datos son obtenidos de manera voluntaria por parte del cliente, a través de un formulario, en el cual se hace constar datos personales generales como nombre, dirección, número telefónico, lugar de trabajo, hasta preferencias deportivas, etc.; las realizadoras de la presente investigación

consideran que la mayoría de los datos que las instituciones financieras exigen que sean proporcionados son excesivos, puesto que las preferencias deportivas, por ejemplo, son irrelevantes para el record crediticio de una persona, así mismo, los dichos datos irrelevantes le dan la posibilidad a las instituciones financieras de clasificar y estigmatizar a los clientes, con lo cual se les atribuye comportamiento futuros y al mismo tiempo ello produce, en determinado momento, cierta discriminación a la hora de ser sujeto de crédito. Aunado a ello, el entrevistado ha manifestado que, por tratarse de una institución financiera intercambia datos personales con la institución denominada DICOM, cuya base de datos no es actualizada constantemente, puesto que, en el caso específico de las tarjetas de crédito, el cliente puede llegar a formar parte de la referida base de datos hasta por cinco años, periodo durante el cual a los ojos del resto de instituciones financieras, el cliente no es sujeto de crédito confiable aunque ya haya solventado su deuda.

Entrevista número cinco:

Dirigida a: Jefe del Registro de Contribuyentes del Ministerio de Hacienda, quien solicitó que su nombre no fuera mencionado en el presente trabajo.

Fecha: viernes veintinueve de junio del año dos mil seis.

Hora: nueve horas.

A continuación se presenta las preguntas efectuadas al entrevistado, así como las respectivas respuestas.

Pregunta 1: ¿Cuál es la forma utilizada para la recolección de datos personales contenidos en el Registro o Base de Datos a su cargo?

Respuesta: Los datos son obtenidos por medio de un formulario que los contribuyentes llenan a efecto de tramitar su NIT.

Pregunta 2: ¿Cuál es la finalidad de la existencia del registro o base de datos a su cargo y qué clase de datos personales están contenidos en ella?

Respuesta: Llevar un control de los contribuyentes y los datos que se almacenan son datos generales; por cada cliente existe un archivo, en el cual se encuentran todos los datos o información relacionada a ese cliente, como nombre, dirección, ocupación, domicilio, residencia, giro comercial en el caso de las sociedades mercantiles, etc.

Pregunta 3: ¿La información o datos personales contenidos en el registro que como institución cuenta, son de uso interno o son compartidos con otra entidad?

Respuesta: Esta información es sólo de uso interno, sólo por medio de una orden judicial a solicitud de la Fiscalía para efecto de investigación de delitos.

Pregunta 4: ¿El titular de dichos datos tiene conocimiento de la existencia de la base de datos, de la finalidad de la existencia de la misma y

que sus datos están contenidos en ella, así como el destino que se le da a los mismos?

Respuesta: Si, ya que para cualquier trámite las personas necesitan obtener su NIT.

Pregunta 6: ¿Cómo institución de qué forma garantiza la seguridad de los datos personales contenidos en su registro?

Respuesta: Por tratarse de información confidencial o secreta, no se le permite el acceso a ninguna persona, se cuenta con una Unidad de Informática, la cual es la encargada del almacenamiento y tratamiento de información, así como del mantenimiento del equipo y actualización del mismo; dicha unidad tiene el monopolio de la información.

Pregunta 7: ¿Cómo institución, cuenta con presupuesto destinado a la protección de datos personales?

Respuesta: A la institución se le asigna cierta partida procedente del presupuesto general de la nación, de la cual se destina lo necesario para el mantenimiento de equipo, actualización de programas y antivirus.

Interpretación:

Para lograr los objetivos primordiales que persigue la Administración Tributaria, es indispensable adoptar los procedimientos mecánicos que garanticen, con mayor eficacia, el control de los contribuyentes, mediante el procesamiento de datos, utilizando equipos electrónicos; y de acuerdo a lo

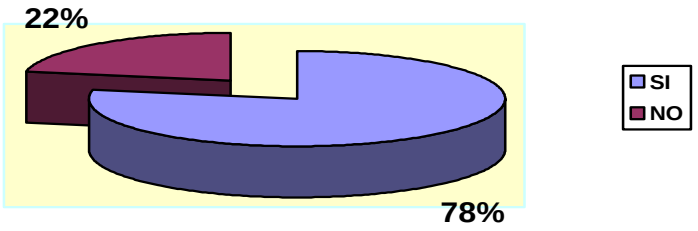
establecido por el entrevistado, el Ministerio de Hacienda cuenta con una Unidad de Informática, la cual es la encargada del almacenamiento y tratamiento de información, así como del mantenimiento del equipo y actualización del mismo; dicha unidad tiene el monopolio de la información.

La administración Tributaria recoge los datos directamente del afectado (datos propios) y también de otras fuentes (datos referenciados) de los cuales existe una obligación expresa por parte de la ley de proporcionarlos, así lo establece el artículo 86 del Código Tributario y la Ley del Registro y Control Especial de Contribuyentes al Fisco, debido a que toda persona natural o jurídica, pública o privada, estará obligada a proporcionar a la Administración Tributaria toda clase de datos con trascendencia tributaria, deducidos de relaciones económicas o financieras con otras personas; así mismo el entrevistado señaló que la información contenida en dicha base de datos es reservada y de uso interno siendo esta una manera eficaz de proteger los datos personales del contribuyente, todo esto lo encontramos reflejado en el artículo 28 inciso primero del Código Tributario.

5.4.2 Resultados de la Encuesta de opinión pública dirigida a Profesionales del Derecho.

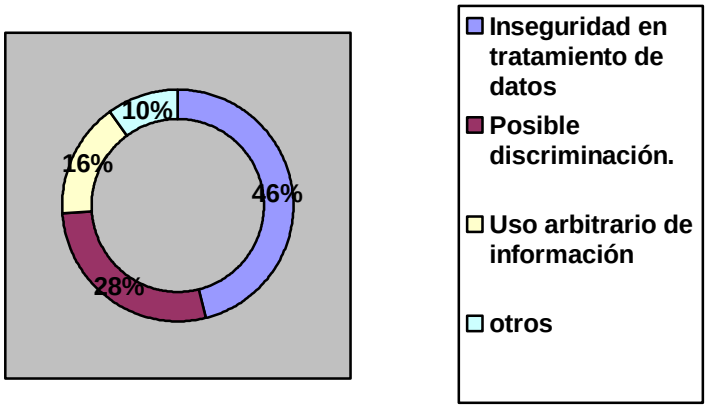
Este tipo de instrumento se ha utilizado con el propósito de conocer la opinión de profesionales en Derecho y que los Datos recogidos puedan ser empleados para su análisis cuantitativo, con el fin de conocer la magnitud del problema en lo relativo a posibles violaciones del derecho a la Intimidad, relacionado con la Autodeterminación Informativa o Libertad Informática, debido a la falta de regulación jurídica del tratamiento de datos personales, contenidos en registros o bases de datos a cargo de instituciones públicas y privadas. Razón por la cual se realizaron las encuestas entre los días 25 al 29 de septiembre, 19, 20 y 23 de octubre eligiendo aleatoriamente una muestra de 50 profesionales como sector representativo de la población a investigarse. Este muestreo por expertos es de gran importancia pues son personas que por su experiencia y conocimiento deciden la representatividad de la muestra. Para la presentación de los resultados se eligió graficas circulares para facilitar el análisis e interpretación de los datos obtenidos, pues permiten una mejor visualización de las tendencias de las variables.

Pregunta Uno: ¿Considera Usted que el uso de la informática en el tratamiento de datos personales vulnera el derecho a la Intimidad Personal y Familiar? SI 78% NO 22%



Interpretación: La finalidad de formular la presente pregunta consistió en conocer la opinión de los profesionales en Derecho acerca de la incidencia de los avances de la informática en el derecho a la Intimidad Personal y Familiar, en relación al tratamiento automatizado de datos personales. Los resultados de la encuesta determinan que el 78% del total considera que el derecho a la intimidad se ve vulnerado, mientras que el 22% considera que no.

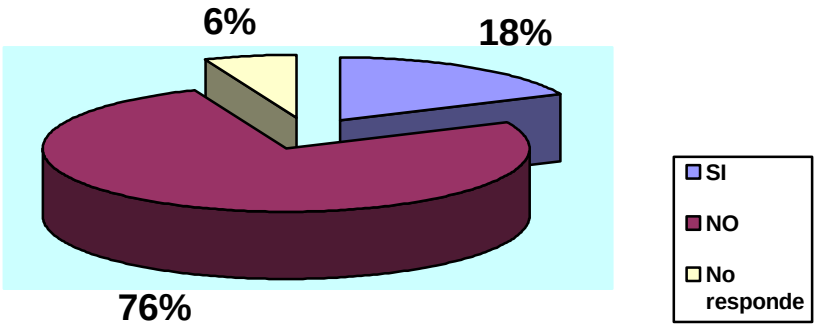
¿Por qué?



Interpretación: Los resultados de la encuesta permiten determinar que de los sujetos que consideran que existe violaciones al derecho a la Intimidad

Personal por el uso de la informática en el tratamiento de datos personales, un 46% del total señala que hay inseguridad en el tratamiento de los datos personales, un 28% señalan una posible discriminación, puesto que se llega a construir un perfil de la persona deduciendo comportamientos futuros de la misma; y un 16% expresan que existe un uso arbitrario de la información; mientras que los sujetos que consideran que el uso de la informática en el tratamiento de datos personales no vulnera el derecho a la intimidad, no justifican dicha negativa, correspondiendo esto al 10% restante del total.

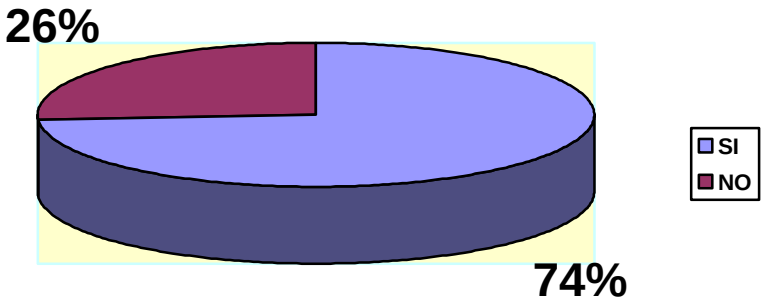
Pregunta Dos: ¿Conoce el uso y destino que se le da a sus datos personales en determinados registros o bases de datos a cargo de instituciones públicas o privadas? SI 18% NO 76% No responde 6%



Interpretación: El objetivo primordial de formular La presente pregunta es establecer en que medida las personas conocen acerca del destino de sus datos, que en la mayoría de casos son proporcionados al momento de solicitar un servicio o adquirir un bien, en este sentido manifiesta el 76% de la

población entrevistada que ignoran el uso final de sus datos personales, lo que pone de manifiesto la inseguridad jurídica a la que estamos expuestos y el peligro latente de una manipulación arbitraria de dichos datos, mientras que solo un 18% dice conocer el destino de sus datos ya que confían en que la institución que los recolecta los utilizará para el fin por el cual fueron dados por su titular, y finalmente un 6% no contestó la pregunta.

Pregunta Tres: ¿Considera Usted que una institución privada, al manejar una base de datos personales puede producir algún tipo de violación al derecho de la Autodeterminación Informativa, relacionado con el derecho a la Intimidad? SI 74% NO 26%

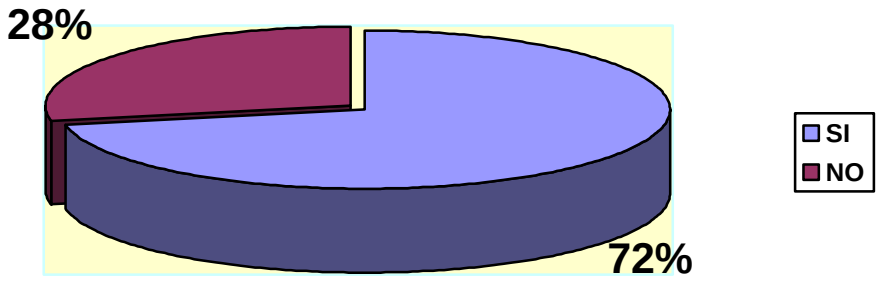


Interpretación: El 74% de los encuestados, coinciden en que estas instituciones encargadas de base de datos personales, que en su mayoría resultan ser, ficheros de datos negativos, vulneran el derecho a la autodeterminación informativa, ya que no permiten el derecho de acceso del afectado para que pueda corregir, modificar e incluso eliminar información

que sobre él se encuentra almacenada, mientras que el 26% considera que no existe tal violación por que la informática en el tratamiento de datos personales solo es utilizada para lograr un efectivo orden en la manipulación de los datos.

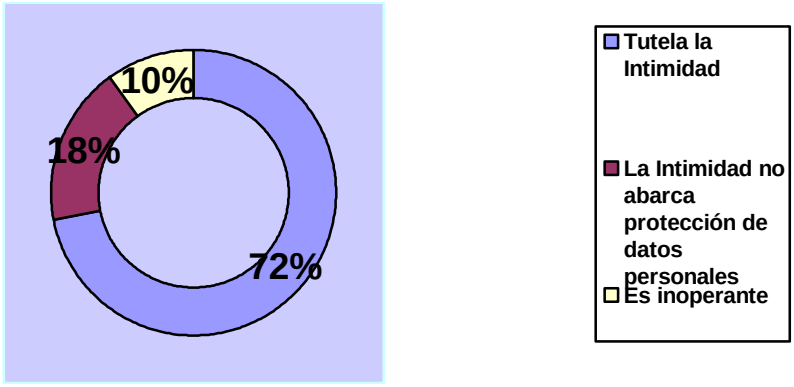
Pregunta Cuatro: ¿Considera Usted que el Amparo es un medio eficaz para tutelar derechos relacionados con la protección de datos personales?

SI 72% NO 28%



Interpretación: Debido a que en nuestro ordenamiento Jurídico, el único mecanismo existente para resarcir daños ocasionados por posibles violaciones a nuestros derechos relacionados con la autodeterminación informativa es el Amparo, por lo cual se hace necesario conocer la efectividad de dicha figura y en este sentido un 72% de los profesionales del derecho la consideran eficaz, mientras que solo un 28% no confían en ella.

¿Por qué?



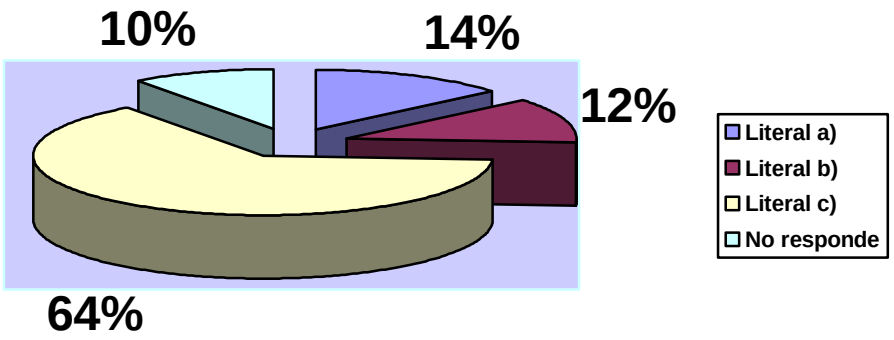
Interpretación: De los resultados de la encuesta puede deducirse que el 72% de los sujetos que respondieron que el Amparo es eficaz para tutelar derechos con la protección de datos personales, justifican su respuesta en que el mismo tutela la Intimidad, debiendo entender que consideran que la protección de datos personales está contenida en el derecho a la Intimidad; sin embargo, de los sujetos que consideran ineficaz al Amparo, el 18% justifican su respuesta en el hecho que la protección de datos personales está fuera de la esfera de tutela de la Intimidad, y el 10% lo consideran inoperante, por ser tardío o lento, además que de los Amparos interpuestos hasta la fecha relativos a violaciones de derechos en el tratamiento de datos personales ninguno de ello ha dado los resultados esperados por los sujetos afectados, en el sentido de resarcir los perjuicios causados.

Pregunta Cinco: En el supuesto que una institución pública o privada comercialice con datos personales con otra institución, ¿a quién considera Usted que se debe demandar?

a) A la institución encargada del registro o base de datos.

b) A la institución que adquirió los datos de la otra.

c) Ambas.

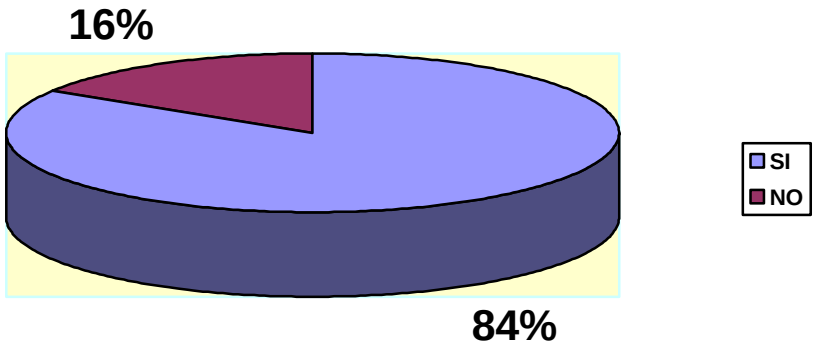


Interpretación:

Esta pregunta tiene como finalidad primordial establecer, la problemática existente a la que los sujetos afectados por el uso indebido o arbitrario de datos personales, afrontan al momento de interponer un amparo, es decir, no esta determinado contra quien se va a dirigir la acción y por lo tanto no se puede deducir responsabilidades, a lo cual un 64% establece que se debe demandar tanto a la institución que vende información personal como la que compra, un 12% piensa que se debe demandar a la institución que compro los datos, el 14% afirma que debe de demandarse a la

institución que vendió los datos, por ser esta la encargada de la seguridad de los mismos, y finalmente un 10% no contesta.

Pregunta Seis: ¿Considera Usted necesario que exista una disposición constitucional con la garantía del Hábeas Data, como figura autónoma que regule expresamente la facultad de limitar el uso de la informática en el tratamiento de datos personales, para preservar derechos fundamentales? SI 84% NO 16%



Interpretación:

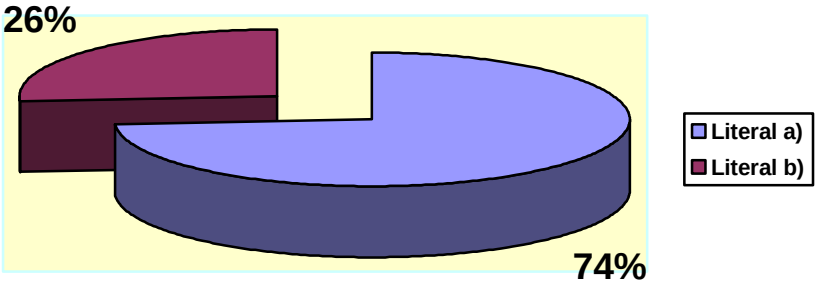
El 84% de los encuestados coinciden, en que nuestro país necesita una disposición constitucional que regule expresamente la figura del Habeas Data, mientras que el 16% restante considera que no es necesario. Con lo cual se sustenta la necesidad de la existencia de una disposición legal, que establezca limites en el uso de la informática en el tratamiento de

datos personales, para una mayor eficacia en la tutela de derechos constitucionales, relacionados con la autodeterminación informativa.

Pregunta Siete: Para una mayor eficacia de la garantía del Hábeas Data ¿Cómo debería ser desarrollada la normativa secundaria que contenga los principios básicos del tratamiento de datos personales?

a) Creación de una Ley Especial de Protección de Datos Personales.

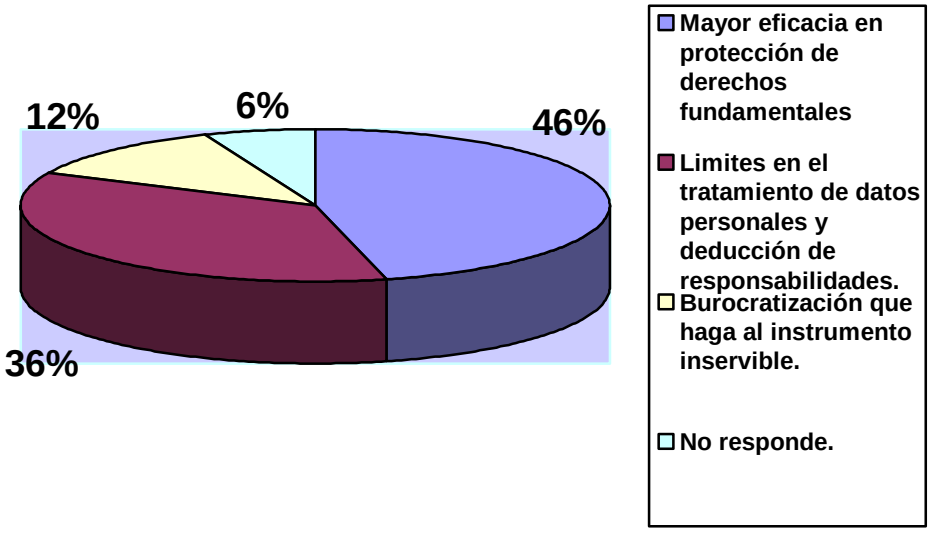
b) Reforma de la Ley de Procedimientos Constitucionales, incorporando en ella el Procedimiento de Hábeas Data.



Interpretación: Los resultados de la encuesta permiten determinar que el 26% de los encuestados consideran la normativa secundaria debería ser desarrolla mediante la creación de una Ley Especial de Protección de Datos Personales, sustentando su posición en que la Autodeterminación Informativa respecto de los datos personales constituye un derecho autónomo, por lo que necesita de una mecanismo de tutela especial regulado

en una Ley Especial que contenga los principios básicos del tratamiento de datos personales; mientras que el 74% consideran que, es suficiente una reforma en la Ley de Procedimientos Constitucionales vigente incorporando el procedimiento de Hábeas Data.

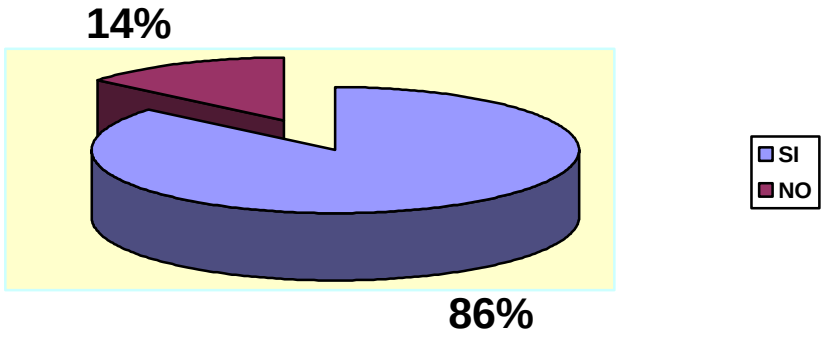
Pregunta Ocho: En el supuesto que se incluya el Hábeas Data en nuestra legislación, ¿Cuáles considera Usted que serían las ventajas y desventajas?



Interpretación: El 82% de los sujetos encuestados consideran que existen más ventajas que desventajas en la incorporación de la figura del Hábeas Data en nuestra normativa constitucional; un 12% considera que la burocratización haría al instrumento inservible; mientras que un 6% se abstuvieron de responder. De lo anterior se desprende que los profesionales

del Derecho de nuestro país ven con buenos ojos la posibilidad de incorporar la figura en nuestra normativa.

Pregunta Nueve: ¿Considera necesario que los estudiantes de la Carrera de Ciencias Jurídicas de las universidades de nuestro país estudien la figura del Hábeas Data en la Materia de Procedimientos Constitucionales, aunque no esté aún regulada en nuestra normativa vigente?



Interpretación: Claro está que la mayoría de los encuestados están de acuerdo en que aunque no esté regulada la figura del Hábeas Data en nuestra normativa, es importante que los futuros abogados de nuestro país se vayan familiarizando con la figura, ya que es una forma de desarrollar el Derecho en esta área y formar al estudiante frente a una posible incorporación de tal figura al ordenamiento jurídico interno.

5.5 DEMOSTRACION Y VERIFICACION DE HIPOTESIS.

a) Hipótesis General: “Incorporar la figura del Hábeas Data en la Legislación constitucional salvadoreña constituye una necesidad jurídica debido a que, en la actualidad, el tratamiento automatizado de datos personales sin regulación jurídica expresa provoca violaciones graves a los derechos constitucionales regulados en el Art. 2 de la Constitución de la República, relacionados con la Autodeterminación informativa o Libertad Informática”.

Como consecuencia de los resultados obtenidos de los instrumentos de investigación de campo aplicados, se ha planteado la necesidad de incorporar el Hábeas Data en la legislación salvadoreña, con lo cual el equipo investigador está de acuerdo, en virtud de considerar que dicha incorporación constituye una necesidad jurídica, puesto que la Autodeterminación Informativa respecto de la protección de datos personales no cuenta con la suficiente garantía. Ello se desprende de la Encuesta de opinión pública dirigida a los Profesionales en Derecho, quienes son determinantes en considerar que dicha incorporación traería una mayor protección de derechos constitucionales.

b) Hipótesis Específicas:

Hipótesis Específica Uno: “Incorporar la figura del Hábeas Data, mediante una reforma legal, en la Constitución de la República salvadoreña podrá hacer efectivo el cumplimiento y protección del Derecho a la Intimidad personal y familiar, contenido en el Art. 2 Cn. respecto al tratamiento automatizado de datos personales”.

Se logro establecer la necesidad de la incorporación del Habeas Data a nuestra legislación, por los resultados obtenidos de la investigación de campo, en la cual la mayoría de personas encuestadas y entrevistadas coinciden en que para una efectiva protección de nuestros datos personales necesitamos la figura del Habeas Data pues constituiría un gran avance en nuestro sistema jurídico, en cuanto ofrece la posibilidad de reclamar el restablecimiento del derecho a la intimidad cuando se ha sufrido un menoscabo en el ejercicio de este, con el uso indebido de la información de carácter personal.

Hipótesis Específica Dos: “La creación de una Ley Especial de Protección y Tratamiento de Datos Personales o la incorporación del Procedimiento de Hábeas Data en la Ley de Procedimientos Constitucionales vigente, haría efectivo la protección del derecho constitucional de la Intimidad personal y familiar contenido en el Art. 2 Cn”.

El resultado de nuestras encuestas y entrevistas, así como la inexistencia de sentencias de la Sala de lo constitucional por violaciones al derecho a la libertad informática o autodeterminación informativa, no porque en la practica no existan violaciones a este derecho, sino por el poco conocimiento que la mayoría de los Salvadoreños tienen sobre este tema, nos pone de manifiesto la necesidad de legislar en materia de protección de datos, independientemente de la técnica jurídica a utilizar, ya que ante la falta de regulación expresa del Habeas Data, como figura autónoma, es que se utiliza el Amparo ante la violación del derecho a la intimidad por posibles abusos en el tratamiento de datos personales, dejando a la atención de los operadores jurídicos la decisión si estos casos de abusos en el tratamiento de datos personales se ubican o no en el contenido del derecho a la intimidad.

Hipótesis Específica Tres: “La garantía del Hábeas Data tiende a proteger los derechos constitucionales relacionados a la Autodeterminación Informativa frente a posibles abusos en el tratamiento de datos personales, por el manejo ilegal y arbitrario por parte de los responsables de los archivos o bancos de datos personales”.

De los resultados de la entrevista no estructurada dirigida a encargados de registros o bases de datos, así como de la encuesta de

opinión pública dirigida a Profesionales en Derecho, se desprende que debido a la falta de regulación jurídica expresa del tratamiento de datos personales en nuestro país, se facilita el manejo ilegal y arbitrario por parte de los referidos encargados de las bases de datos; puesto que lo mismos han reconocido que en el tratamiento automatizado de datos personales, se facilita corregir errores en el almacenamiento de la información e incluso desaparecerla, manipulándola de tal manera que no quede rastro de su existencia; en virtud de lo cual, y en opinión de la mayor parte de los profesionales en Derecho encuestados, el Hábeas Data vendría a garantizar una mayor protección de los derechos relacionados con la Autodeterminación Informativa, ante posibles abusos en el tratamiento de datos personales.

Hipótesis Específica Cuatro: “La falta de regulación jurídica del Hábeas Data en la legislación salvadoreña influye en la existencia de violaciones de los derechos constitucionales relacionados con la Autodeterminación Informativa, ya que posibilita la manipulación de los datos personales contenidos en registros o bancos de datos”.

Lo inexistencia de la figura del Hábeas Data en la legislación salvadoreña conlleva a que se susciten casos en los cuales se vulnere el derecho a la Intimidad por el uso arbitrario de datos personales. Esta práctica indebida no será sancionada hasta que no se regule expresamente el medio

de tutela en estudio; de lo contrario, el mal manejo de datos personales quedará impune. Lo anterior se ha establecido con la entrevista no estructurada dirigida a Encargados de Registros o Bases de datos, dejándose constancia que algunos de ellos han reconocido que existe el peligro inminente de un uso indebido o arbitrario de la información, ya que se han dado casos, por ejemplo, de extravío de folios en el libro de registros de instrumentos en el Registro de la Propiedad Raíz e Hipotecas o la transferencia de inmuebles de un sujeto a otro, por el cambio códigos asignados; así mismo, ellos han reconocido que dentro de la cadena de seguridad de la información, el eslabón más débil siempre es la persona a cuyo cargo se encuentra el almacenamiento y tratamiento de los datos personales, posibilitando estas que terceros tengan acceso a los datos y puedan disponer de ellos.

Hipótesis Específica Cinco: “La legislación constitucional comparada servirá de base para hacer un propuesta de reforma o readecuar la legislación constitucional nacional, para que se pueda incluir el Hábeas Data, como figura autónoma, encaminada a la protección de los derechos constitucionales frente al tratamiento automatizado de datos personales”.

Después de haber hecho un estudio, principalmente de legislación constitucional de países, tanto europeos como latinoamericanos, en donde

se desarrolla la Garantía del Hábeas Data, al hacer una comparación con nuestra normativa vigente, puede deducirse que la misma puede ser la base para realizar una reforma constitucional en nuestro país para incorporar el Hábeas Data, como figura autónoma; en virtud de ello, se ha establecido que países como Brasil han considerado que no es suficiente el reconocimiento del derecho a la protección de datos personales y la Autodeterminación sobre el destino de los mismos, ni la protección a través del Amparo, sino que se hace indispensable incorporar a la legislación el Hábeas Data como garantía constitucional, para brindar una mayor protección de los derechos constitucionales.

CAPITULO VI
6. CONCLUSIONES Y RECOMENDACIONES.

6.1 CONCLUSIONES.

Luego de haber realizado la anterior Investigación, se ha llegado a las siguientes conclusiones:

1. La Teoría de los Derechos Fundamentales es esencialmente dinámica y esto ha llevado a una redefinición de los derechos clásicos, en particular, el derecho a la Intimidad, sin que esto implique una anulación de sus manifestaciones tradicionales, sino la ampliación del mismo. El derecho a la Intimidad constituye realmente una expresión del valor de la Dignidad Humana; sólo desde una posición de libertad respecto a su cuerpo, a sus datos, a su identidad, es que el ser humano puede alcanzar niveles de excelencia.

2. El derecho a la Intimidad, elevado a la categoría de derecho fundamental, ya no puede ser tomado sólo como una simple facultad de negación, es decir, declinante de la intromisión en la esfera privada de las personas, sino también, debe ser entendida como una facultad positiva por medio de la cual se pueda actuar en pro de una mejor tutela que esté alejada del campo de acción de su titular; en ese sentido, no sólo debe tomarse como la posibilidad de impedir la publicación de los datos personales, sino que, además que permita tomar conocimiento de las informaciones que versan en los archivos o bases de datos sobre una determinada persona, para poder así, ejercer las ulteriores acciones que posibiliten una verdadera salvaguarda al bien jurídico que se trate de proteger.

3. Con respecto al reconocimiento de las Personas Jurídicas como sujeto activo del Derecho a la Intimidad, el equipo investigar se adhiere a los argumentos de extender la titularidad del Derecho a la Intimidad y, por ende, a la Autodeterminación Informativa a las Personas Jurídicas, en razón a que cualquier dato relativo a una persona jurídica, lo es en cierta medida referente a cada uno de los miembros que la integran, ya sea como socios, ya sea a través de una relación contractual de cualquier tipo, por cuanto la obtención de datos relativos a aquella puede constituir un eslabón más en la construcción del perfil personal de estos últimos; además, esta justificación de protección de datos personas jurídicas tiene sus raíces, en gran parte, en

los derechos económicos, en el cual uso incorrecto de información económica hace tan vulnerables a los individuos como a las entidades jurídicas. Puede decirse entonces, que es posible considerar a las personas jurídicas, no como titulares de derechos personalísimos permanentes, como es el caso de las personas naturales, sino en n determinado contexto y en situaciones concretas en que sea necesaria su protección.

4. En relación al bien jurídico tutelado por la Protección de Datos Personales, no existe unanimidad entre los doctrinarios, ya que unos establecen que es la Intimidad, pues esta conlleva el deber del sigilio y, en consecuencia, el deber de no revelar ciertas informaciones; otros lo atribuyen al Honor; sin embargo, en nuestra opinión, el bien jurídico tutelado es un derecho humano propio de la Tercera Generación que, en algunos países, ha sido elevado a la categoría de fundamental, y es el denominado Derecho a la Autodeterminación Informativa, consistente en la facultad de disponer sobre la revelación y utilización de datos personales que abarca todas las etapas de las elaboración y uso de los datos por medios informáticos, es decir, su almacenamiento, registro, calificación, modificación, transmisión y difusión; este nuevo derecho, pretende amparar la libertad y dignidad humana frente a los riesgos y abusos derivados del tratamiento automatizado de datos personales que se concreta en el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, ya sea íntima o no, para preservar de este modo y, en último extremo, la propia

identidad, nuestra dignidad y libertad, o dicho de otra manera, con la Autodeterminación Informativa lo que se pretende proteger es la personalidad del individuo, de manera mediata, a través de la protección inmediata de la información que le concierne, posibilitando su control.

5. Podemos afirmar que, en definitiva, con la tecnología existente y las posibilidades de interconexión, desde un “modesto” ordenador domiciliario ubicado en el lugar más recóndito de la tierra se puede invadir la privacidad de una persona; podemos violar sus derechos y libertades fundamentales al difundir información “sensible” y afectar su dignidad sin control y, en ocasiones, sin que jamás se entere de ello. Está situación determina un desequilibrio; por un lado, el poder de la tecnología informática para la acumulación de datos y, por otro, el “ciudadano común”, que ve que frente a estas nuevas herramientas de transmisión de información a nivel mundial nada puede hacer para defenderse. Es ahí donde surge la necesidad legislativa de proteger determinados datos esencialmente privados de los hombres a fin de restablecer el equilibrio perdido, o bien reconocer un nuevo derecho, el de ser resarcido por los perjuicios producidos por la utilización de los medios informáticos masivos.

6. La Interpretación constituye una herramienta jurídica que permite la tutela de los derechos, pero puede convertirse en un mecanismo peligroso, puesto que su uso puede responder a ciertos intereses, tomando así, el carácter de medio de manipulación de las resoluciones, afectando el principio de Seguridad Jurídica y con ello, creando desconfianza frente al ente encargado de la protección de los derechos; es por ello que se considera que las normas expresas constituyen una garantía más sólida que la Interpretación. En virtud que el derecho a la Autodeterminación Informativa no está contemplado en nuestra Ley fundamental, se colige que por ser un derecho humano de Tercera Generación que permite garantizar los derechos del individuo ante los adelantos tecnológicos y por consagrar uno de los medios que permiten asegurar la Dignidad Humana a través de la protección a la Integridad Física y Moral, se le debe otorgar una tutela real y efectiva, mediante una mecanismo o garantía específica de protección como es el Hábeas Data, lo cual, por el momento, sólo puede ser realizado a través de la Jurisprudencia, hasta que no sea regulado mediante una reforma constitucional y en una normativa secundaria eficaz que desarrolle lo principios básicos del Tratamiento de Datos Personales.

7. En nuestro país no existe un marco normativo general respecto al acceso a la información pública o privada, y al régimen de protección de datos a pesar de la existencia de numerosos registros, informáticos y

manuales que contienen información personal, el tema de la protección de datos personales no se ha debatido lo suficiente en el ámbito nacional ni se ha dimensionado su importancia; en ese sentido, puede decirse que no existe ningún tipo de normativa general que limite su manejo o que controle su uso. De ahí que no exista ningún tipo de regulación que permita al interesado conocer el uso y destino de la información brindada.

8. En nuestra legislación no existen leyes especiales para regular el tratamiento de datos personales que permita limitar el uso abusivo y las arbitrariedades que a través de ellos se pueda cometer y las normas jurídicas dispersas que tímidamente tratan al respecto, no son suficientes para garantizar plenamente los derechos en juego. En consecuencia, el Amparo, siendo la única herramienta jurídica vigente a la cual se pueden abocar los sujetos afectados por el uso arbitrario o ilegal de sus datos personales, se advierte que en determinados casos, y tal como se ha establecido en el desarrollo de la investigación realizada, su uso se ve limitado y restringido. Y es aquí donde se pretende hacer énfasis en la trasgresión de derechos fundamentales a través de la comercialización de datos personales, como en el caso de las compañías dedicadas a telemarketing, al igual que las encargadas de bases de datos negativos como DICOM, que por la falta de actualización de su base de datos, se le puede negar el derecho a obtener un crédito a determinada persona.

9. Muchas son las confusiones que se dan respecto a la utilización de las garantías procesales establecidas en las Ley de Procedimientos Constitucionales. En ese sentido, y a fin de aclarar algunos conceptos, puede concluirse que el instituto de Hábeas Corpus determina la situación de una persona en lo relativo a su libertad personal o ambulatoria, bien por estar detenida en condiciones no satisfactorias o bien por existir órdenes restrictivas de libertad que sean ilegítimas. La expresión latina Hábeas Corpus, que quiere decir *que tengas el cuerpo*, marca el origen de un conocimiento especial que se exige respecto a causas, cuando no se sabe donde está el detenido. Análogamente, Hábeas Data significa *que tengas los datos*, es decir, el Hábeas Data no está referido a una situación relacionada con lo corporal o ambulatorio, sino alude al interés de las personas de conocer en forma directa la inscripción de los hechos, es decir, el dato o la información. En nuestro país, ante la falta de regulación expresa del Hábeas Data como figura autónoma, es que se utiliza el Amparo ante la violación del derecho a la intimidad por posibles abusos en el tratamiento de datos personales, dejando a la atención de los operadores judiciales la decisión si estos abusos en el tratamiento de datos personales se ubican o no dentro del contenido del derecho a la intimidad; de esta manera, se ha intentado hacer surgir el Habeas Data de la tutela constitucional del derecho a la intimidad, pero no se ha logrado.

6.2 RECOMENDACIONES.

De todo lo anteriormente señalado, las realizadoras de la presente investigación consideran necesario establecer las siguientes recomendaciones:

1. Que la Corte Suprema de Justicia de El Salvador actúe con agilidad en la protección de los derechos inherentes de las personas por medio de los mecanismos existentes, tales como el Amparo; y al darse la creación de una Ley Especial de Protección de Datos Personales, hacer un efectivo cumplimiento de la misma, como medio de tutela jurídica.

2. La Asamblea Legislativa debe crear una Ley Especial que regule el Tratamiento de Datos Personales, dirigida a tutelar la Autodeterminación Informativa, principalmente en lo relativo a la protección de los datos personales, contenidos en registros o bases de datos a cargo de instituciones, tanto públicas como privadas, obtenidos a través de negocios jurídicos, que le permita al titular de los mismos conocer, acceder, rectificar o suprimir información de carácter personal que considere perjudicial; lo anterior, en virtud que el Amparo, como mecanismo constitucional vigente, en cuanto a posibles violaciones de derechos constitucional ante el tratamiento de datos personales, es tardío y casi inoperante.

3. Que la Superintendencia del Sistema Financiero, como ente fiscalizador, exija a las instituciones financieras la implementación de medidas de Seguridad de la Información basadas en la versión más actualizada de la norma británica de nombre VS6799, en la cual se describe diferentes controles que toda institución, independientemente del tamaño y del giro, deben seguir para crear un programa de seguridad en una institución; ello con el fin de garantizar al ciudadano un mejor control en el tratamiento de sus datos personales de parte de las instituciones financieras, que tienen a su cargo bases de datos personales. Así mismo, que exija a las instituciones financieras que en los contratos de adhesión, el consentimiento, por parte del titular, de que sus datos personales sean transferidos a bases de datos a cargo de empresas dedicadas al intercambio de información, como DICOM, conste en documento aparte, firmando esa autorización específica a la institución; y que además del consentimiento expreso, se le faculte al titular de los datos personales para que, en determinado momento, pueda tener acceso a los mismos, modificarlos o exigir su supresión, así como que se le informe quién solicita tener acceso a ellos.

4. Que las Instituciones públicas o privadas encargadas de registros o bases de datos personales mantengan informado al titular de los datos que consten en sus registros, sobre el manejo y destino de los mismos, así como también informar constantemente a las entidades con las cuales mantienen

intercambio de datos personales, cuando se efectúe algún tipo de cambio o actualización en la misma.

5. Que las Universidades del país, incluyan dentro del Plan de Estudios de la Carrera de Ciencias Jurídicas la figura del Hábeas Data, haciendo referencia a la aplicación en legislaciones similares a la nuestra, ya que la normativa salvadoreña carece de doctrina sobre la misma. Lo anterior, debido a que, no obstante no estar regulada aún, es una forma de desarrollar el Derecho en esa área, siendo importante también formar al estudiante frente a una posible incorporación de tal figura al ordenamiento jurídico interno.

6. La comunidad jurídica salvadoreña ha de investigar y analizar la influencia de los avances tecnológicos, principalmente la Informática, ejercen en las relaciones jurídicas y la medida en que responde a las necesidades de la sociedad actual. En ese sentido, el Programa de estudios de la carrera de Licenciatura en Ciencias Jurídicas de las Universidades de nuestro país debe incorporar en la materia de Procedimientos Constitucionales el estudio de la Figura del Hábeas Data como mecanismo autónomo de tutela del derecho a la protección de datos personales y la Autodeterminación Informativa, así como se ha estudiado las figuras del Amparo y el Hábeas Corpus; ello, le

brindará al estudiante la perspectiva general sobre las relaciones existentes entre el Derecho y la realidad tecnológica del presente.

Listado de Siglas Utilizadas

A.P.E.S. Asociación de Periodistas de El Salvador.

C.O.N.A.R. Conejo Nacional de Autorregulación Publicitaria. Funciona en países miembros de la Unión Europea, Estados Unidos y Canadá.

F.B.I. Federal Buro Investigation (Oficina Federal de Investigación)

F.O.I.A. Freedom of Information Act (Acta de Libertad de Información)

l.R.R.H.D. Ley que Regula el Rito Procesal del Hábeas Data.

L.O.R.T.A.D. Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

L.O.P.D.P. Ley Orgánica de Protección de Datos Personales.

T.E.D.H. Tribunal Europeo de Derechos Humanos.

BIBLIOGRAFÍA.

LIBROS.

1) ALLENDE O., JORGE, y otros: “Manual de Informática Jurídica”. Editorial Astrea, de Alfredo y Ricardo de Palma. Argentina, 1996.

2) AYALA MUÑOZ, JOSÉ MARÍA, y otros: “La Protección de Datos Personales en El Salvador”. 1ª. ed. UCA Editores. San Salvador, El Salvador, 2005.

3) BARBOSA MOREIRA, JOSÉ CARLOS: “O Hábeas Data Brasileiro e sua lei Regulamentadora” en Hector Fix Zamudio: “Liber Amicorum” Vol I Secretaria de la Corte Interamericana de Derechos Humanos San José, 1998. Traducción Libre del Portugués.

4) BERTRAND GALINDO, FRANCISCO, y otros: “Manual de Derecho Constitucional” Tomo II, 4ta. Edición. El Salvador, 2000.

5) C. MÉJAN, LUIS MANUEL: “El Derecho a la Intimidad y a la Informática”. Editorial Porrúa, S.A. México, 1994.

6) CESARIO, ROBERTO: “Hábeas Data. Ley 25.326, Régimen de Bancos de Datos de Informática sobre la persona, derecho de los titulares, acción protectora”. Editorial Universidad, Rivadavia 1225. Ciudad de Buenos Aires. Impreso marzo 2001.

7) EKMEKDIJIAN, MIGUEL ÁNGEL Y PIZZIOLO COLOGERO: “Hábeas Data, el Derecho a la Intimidad Frente a la Revolución Informática”. Editorial Desalma. Buenos Aires, Primera Edición, 1996.

8) ESTADELLA YUSTE, OLGA: “La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales”. Editorial Tecnos. Madrid, 1995.

9) FERREIRA RUBIO, DELIA MATILDE: “El Derecho a la Intimidad”. Editorial Universidad S.R.L B.A 1982.

10) FROSINI, VITTORIO: “Informática y Derecho”. Trad. Jorge Guerrero y Marino Ayerra Redín. Editorial Temis. Bogotá, Colombia, 1988.

11) GARRIGA DOMÍNGUEZ, ANA: “Tratamiento de Datos Personales y Derechos Fundamentales”. Editorial Dykinson, S.L. Madrid, 2004.

12) GONZÁLEZ SEPÚLVEDA, JAIME: “El Derecho a la Intimidad Privada”. Universidad de Chile. Editorial Andrés Bello. Santiago de Chile, 1979.

13) HASSERMAN, WINFRIED Y CHIRINO SÁNCHEZ, ALFREDO: “El Derecho a la Autodeterminación Informática y los Retos del Procesamiento Automatizado de Datos Personales”. Editorial del Puerto. Buenos Aires, 1997.

14) LOSANO, MARIO G. y otros: “Libertad Informática y Leyes de Protección de Datos Personales”. Centro de Estudios Constitucionales. Madrid, España, 1989.

15) MURILLO DE LA CUEVA, PABLO LUCAS: “El Derecho a la Información Informática”. Editorial Tecnos, S.A. Madrid, España, 1990.

16) PÉREZ LUÑO, A.E.: “Problemas Actuales de Documentación y la Informática Jurídica”. Editorial. Tecnos. Madrid, 1987.

17) PÉREZ NOYO, JAVIER: “Curso de Derecho Constitucional”. Novena Edición, Ediciones Jurídicas y Sociales, S.A.

18) PIERINI, ALICIA, LORENCES, VALENTÍN Y TORNABENE, MARÍA INÉS: ”Hábeas Data, Derecho a la Intimidad”. Editorial Universidad, Primera Edición. Buenos Aires, 1999.

19) POLO SABAN, JOSÉ RAMÓN: “Libertad de Expresión y Derecho de Acceso a los Medios de Comunicación”. Centros de Estudios Políticos y Constitucionales. Madrid, 2002.

20) PUCCINELLI, OSCAR: “El Hábeas Data”. Editorial Temis, S.A., Santa Fe de Bogotá – Colombia, 1999.

21) PUCCINELLI, OSCAR: “El Hábeas Data en Indoiberoamérica”. Editorial Temis. Colombia, 1999.

22) RIGAUX, FRANÇOIS.: “La protección de la vie privée et des autres biens de la personalité”. Bruylant, Bruxelles, 1990.

23) SALGADO, ALÍ JOAQUÍN Y VERDAGUER, ALEJANDRO CÉSAR: "Juicio de Amparo y Acción de Inconstitucionalidad". Segunda Edición Actualizada y Ampliada. Editorial Astrea de Alfredo y Ricardo Desalma, La Valle 1208. Ciudad de Buenos Aires 2000, impreso en Argentina.

24) TÉLLEZ VALDÉS, JULIO: "Derecho Informático". México: UNAM, 1987.

TESIS.

1) "Hábeas Data : La Autodeterminación sobre las Informaciones Personales": ALFARO ESCOTO, DAYSI ASTRID y otro, T-UES San Salvador, 2000.

2) "Hábeas Data como Garantía de Protección de la Persona frente al Tratamiento de sus Datos Personales": ALVARADO BONILLA, KARLA MARÍA y otros. T-UES, San Miguel, 2004.

3) "Derecho a la Intimidad y Protección de Datos Personales": ZALDIVAR ESPINAL, KARLA MARÍA. Ibarra Rafael Antonio (Asesor) San Salvador: UCA, 1997.

ARTICULOS DE PERIODICOS.

1) GUTIÉRREZ, EDWARD: "Infornet seguirá en El Salvador". Diario de Hoy, miércoles 21 de mayo 2003. Págs. 6 y 8.

2) GUTIÉRREZ, EDWARD: "País esperará base de datos de Infornet". Diario de Hoy, jueves 22 de mayo 2003. Pág. 18.

3) GUTIÉRREZ, EDWARD: “Ingenieros demandarán a Infornet ante la Corte hoy”. En el Diario de Hoy. Martes 13 de mayo 2003. Pág. 12.

4) GUTIÉRREZ, EDWARD: “Piden frenar la venta de datos”. Miércoles 14 de mayo 2003. Pág. 16.

5) GUTIÉRREZ, EDWARD: “Piden a Guatemala ver archivos de Infornet”. En el Diario de Hoy. Sábado 02 de agosto 2003. Pág. 24.

6) GUTIÉRREZ, EDWARD: “Infornet reanuda operaciones”. El Diario de Hoy. Martes 25 de noviembre de 2003. Pág. 21.

7) SILVA, JOSÉ ENRIQUE: “Revista Iberoamericana de Derecho Procesal Constitucional”. El Mundo. Miércoles 07 de junio de 2006. Pág. 15.

8) “Fed: Tasas más altas para negros y latinos”: El Diario de Hoy, Sección Negocios. Lunes 11de septiembre de 2006. Pág. 32.

LEGISLACION.

1) Constitución de la República de El Salvador: Editor Luis Vázquez López, Editorial Lis. El Salvador, 2004.

2) Código Penal (1996): Editor Luis Vázquez López, Editorial Lis. El Salvador, 2004.

3) Código Procesal Penal (1996): Editor Luis Vázquez López, Editorial Lis. El Salvador, 2004.

4) Código Civil: Editor Luis Vázquez López, Editorial Lis. El Salvador, 2003.

5) Código de Procedimientos Civiles: Editor Luis Vázquez López, Editorial Lis. El Salvador, 2003.

6) Código de Familia: Editor Luis Vázquez López, Editorial Lis. El Salvador, 2004.

7) Ley Procesal de Familia: Editor Luis Vázquez López, Editorial Lis. El Salvador, 2004.

8) Ley Transitoria del Registro del Estado Familiar y de los Regímenes Patrimoniales del Matrimonio: Editor Luis Vázquez López, Editorial Lis. El Salvador, 2003.

9) Ley de Procedimientos Constitucionales: Editorial Jurídica Salvadoreña, 3ra. Edición. El Salvador, enero, 2004.

10) Ley del Ejercicio Notarial de la Jurisdicción Voluntaria y de otras Diligencias: Editorial Jurídica Salvadoreña, 3ra. Edición. El Salvador, enero, 2004.

11) Ley del Nombre de la Persona Natural: Editor Luis Vázquez López, Editorial Lis. El Salvador, 2003.

ANEXOS

1) MODELO DE ENTREVISTA DIRIGIDA A ENCARGADOS DE REGISTROS O BASES DE DATOS PERSONALES.
2) MODELO DE ENCUESTA DE OPINION PUBLICA DIRIGIDA A PROFESIONALES EN DERECHO.
3) FRAGMENTOS DE JURISPRUDENCIA DE LA SALA DE LO CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA DE EL SALVADOR.
4) JURISPRUDENCIA ARGENTINA: EL HABEAS DATA Y EL "DERECHO AL OLVIDO". Por PABLO A. PALAZZI.
5) REPORTAJES RELACIONADOS CON EL DERECHO A LA INFORMACIÓN.
6) LEY ORGÁNICA DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL - LEY 5/1992.

7) PROYECTO DE LEY ORGÁNICA POR LA QUE SE MODIFICA LA LEY ORGÁNICA 5/1992, DE 29 DE OCTUBRE, DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL.

Anexo Número Uno:

MODELO DE ENTREVISTA DIRIGIDA A ENCARGADOS DE REGISTROS O BASES DE DATOS PERSONALES.

NOTA: "Esta guía contiene preguntas para recopilar información para el tema: " El Hábeas Data como mecanismo de protección de derechos relacionados con la Autodeterminación Informativa ante el tratamiento automatizado de datos personales", el cual es punto para el trabajo de graduación para obtener el grado académico de Licenciado en Ciencias Jurídicas de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad de el Salvador; dicha información tendrá un manejo confidencial y científico para fundamentar nuestras hipótesis".

Pregunta 1: ¿Cuál es la forma utilizada para la recolección de datos personales contenidos en el Registro o Base de Datos a su cargo?

Pregunta 2: ¿Cuál es la finalidad de la existencia del registro o base de datos a su cargo y qué clase de datos personales están contenidos en ella?

Pregunta 3: ¿La información o datos personales contenidos en el registro que como institución cuenta, son de uso interno o son compartidos con otra entidad?

Pregunta 4: ¿El registro o base de datos a su cargo tiene alguna relación con la institución privada denominada DICOM u otra institución de esa naturaleza?

Pregunta 5: ¿El titular de dichos datos tiene conocimiento de la existencia de la base de datos, de la finalidad de la existencia de la misma y

que sus datos están contenidos en ella, así como el destino que se le da a los mismos?

Pregunta 6: ¿Cómo institución de qué forma garantiza la seguridad de los datos personales contenidos en su registro?

Pregunta 7: ¿Cómo institución, cuenta con presupuesto destinado a la protección de datos personales?

Anexo Número Dos:

MODELO DE ENCUESTA DE OPINION PUBLICA DIRIGIDA A PROFESIONALES EN DERECHO.

NOTA: "Esta guía contiene preguntas para recopilar información para el tema: " El Hábeas Data como mecanismo de protección de derechos relacionados con la Autodeterminación Informativa ante el tratamiento automatizado de datos personales", el cual es punto para el trabajo de graduación para obtener el grado académico de Licenciado en Ciencias Jurídicas de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad de el Salvador; dicha información tendrá un manejo confidencial y científico para fundamentar nuestras hipótesis".

Pregunta Uno: ¿Considera Usted que el uso de la informática en el tratamiento de datos personales vulnera el derecho a la Intimidad Personal y Familiar? SI _____ NO _____ ¿Por qué?

Pregunta Dos: ¿Conoce el uso y destino que se le da a sus datos personales en determinados registros o bases de datos a cargo de instituciones públicas o privadas? SI _____ NO _____

Pregunta Tres: ¿Considera Usted que una institución privada, al manejar una base de datos personales puede producir algún tipo de violación al derecho de la Autodeterminación Informativa, relacionado con el derecho a la Intimidad? SI _____ NO _____

Pregunta Cuatro: ¿Considera Usted que el Amparo es un medio eficaz para tutelar derechos relacionados con la protección de datos personales?

SI _____ NO _____ ¿Por qué?

Pregunta Cinco: En el supuesto que una institución pública o privada comercialice con datos personales con otra institución, ¿a quién considera Usted que se debe demandar?

a) A la institución encargada del registro o base de datos.

b) A la institución que adquirió los datos de la otra.

c) Ambas.

Pregunta Seis: ¿Considera Usted necesario que exista una disposición constitucional con la garantía del Hábeas Data, como figura autónoma que regule expresamente la facultad de limitar el uso de la informática en el tratamiento de datos personales, para preservar derechos fundamentales? SI ____ NO ____

Pregunta Siete: Para una mayor eficacia de la garantía del Hábeas Data ¿Cómo debería ser desarrollada la normativa secundaria que contenga los principios básicos del tratamiento de datos personales?

a) Creación de una Ley Especial de Protección de Datos Personales.

b) Reforma de la Ley de Procedimientos Constitucionales, incorporando en ella el Procedimiento de Hábeas Data.

Pregunta Ocho: En el supuesto que se incluya el Hábeas Data en nuestra legislación, ¿Cuáles considera Usted que serían las ventajas y desventajas?

Pregunta Nueve: ¿Considera necesario que los estudiantes de la Carrera de Ciencias Jurídicas de las universidades de nuestro país estudien la figura del Hábeas Data en la Materia de Procedimientos Constitucionales, aunque no esté aún regulada en nuestra normativa vigente?

Anexo Número Tres:

FRAGMENTOS DE JURISPRUDENCIA DE LA SALA DE LO CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA DE EL SALVADOR.

Fragmentos del Proceso de Amparo Constitucional No, 118-2002, Sentencia Definitiva del 2 de marzo de 2004, de la Sala de lo Constitucional en El Salvador.

Estructuralmente el proceso amparo se encuentra regulado en la Constitución como el instrumento de garantía que tiene por objeto tutelar los derechos constitucionales; lo cual se traduce doctrinaria y jurisprudencialmente como la pieza final del sistema de garantías de los derechos y categorías constitucionales, en cuanto a que corresponde, en primera instancia, a los tribunales ordinarios resolver los casos concretos tomando como parámetro no sólo la ley sino también la propia Constitución e indirectamente solventar, de esa forma, los derechos constitucionales que explícita o implícitamente se constituyan en el centro del litigio. El amparo, como garantía subjetiva, es de larga data en nuestro sistema jurídico y fue concebido con el objeto de poner límites a las actuaciones arbitrarias de quien normalmente ostenta el poder, es decir el Estado. Sin embargo, dada la evolución de las relaciones inter-subjetivas que impone toda sociedad moderna, el Estado o el poder público, único capaz de alterar o menoscabar el ámbito privado de los particulares, en concepción típicamente liberal; fue cediendo espacio a poderes o entidades privados cuyos actos se alejaban de una relación entre iguales con los particulares, para lo cual la legislación civil, o penal –que son la normativa idónea para la solución de los conflictos privados-, resulta insuficiente, pues existe cierto tipo de actividades realizadas por particulares o empresas privadas que por concesión de un servicio público, por ejemplo; o por el tipo de actividad que realizan, son capaces de romper la tradicional igualdad formal y transformar la relación jurídica en una desigualdad material, ubicándose fácticamente una de las partes en una posición de superioridad frente a otro u otros, semejante a la del predominio del poder público, creándose con ello el potencial

peligro que en dichas relaciones entre particulares exista vulneración de sus derechos constitucionales.

En ese contexto, la jurisprudencia del amparo en nuestro país también ha evolucionado al ritmo del progreso de la sociedad y superado la tesis de que el amparo es procedente sólo contra actos de autoridad formalmente considerada; v.gr. concejos municipales, jueces, ministros, alcaldes, magistrados, entre otros. El acto de autoridad entonces, tiene ahora una connotación material, más que formal, en el entendido que el acto contra el que se reclama es capaz de causar un agravio constitucional, independientemente del órgano o la persona que lo realiza. A partir de dichas premisas se replantean los supuestos de la legitimación pasiva y ahora se admite la pretensión constitucional también contra actos y omisiones de particulares de los cuales puedan emanar actos limitativos de derechos constitucionales, como si se tratase de actos de autoridades formales, por encontrarse quienes los efectúan, de hecho o de derecho, en una posición de poder.

La jurisprudencia de esta Sala ha sido constante en establecer como presupuestos básicos para la procedencia del proceso de amparo contra particulares, los siguientes: (a) que el particular responsable del acto se encuentre en una situación de poder, (b) que el acto u omisión sea parte del ámbito de constitucionalidad y (c) que no existan mecanismos judiciales o administrativos de protección frente a actos de esa naturaleza; o que de haberlos, sean ellos insuficientes para garantizar los derechos del afectado o se hayan agotado plenamente para remediar el acto contra el cual reclama. De no cumplirse dichos presupuestos, se estaría frente a una improcedencia de la pretensión de amparo, lo cual se traduce en la imposibilidad jurídica de parte de este Tribunal para conocer y decidir el caso.

[...], atendiendo a los argumentos planteados por el actor respecto de las actuaciones atribuidas a las sociedades demandadas que se resumen en un manejo inconstitucional de su status crediticio en la corriente informática y con ello la violación concreta de su derecho a la intimidad en el tráfico electrónico o autodeterminación informativa; es necesario realizar también algunas consideraciones sobre la validación del proceso de amparo como medio idóneo para conocer de tal derecho, en ausencia de un mecanismo propio como el hábeas-data existente en ordenamientos foráneos.

El *habeas data* constituye el mecanismo o instrumento que protege al individuo contra el uso ilegal o indebido de los datos personales de un individuo por parte de entidades públicas o privadas, tutelando de una forma eficaz el derecho a la autodeterminación informativa. De tal manera que constituye una garantía cuyo fundamento en la normativa constitucional responde a la necesidad de los sujetos de proteger sus derechos ante la amenaza del acceso y uso indiscriminado de sus datos personales. En términos generales, se trata de un instrumento judicial que entra en funcionamiento a petición de parte, cuando ésta ha cumplido con el requisito prejudicial de solicitar a la empresa que posee o maneja sus datos personales, le exhiba los mismos con el objeto de verificar los que han sido incluidos en los ficheros automatizados y comprobar la veracidad de los mismos. De no obtenerse la respuesta requerida, el Estado, a través de dicho mecanismo, interviene solicitando la exhibición, modificación, supresión, o actualización de los datos, según el caso, con la consiguiente responsabilidad civil para la empresa demandada en caso de comprobarse la vulneración al derecho en cuestión, sin perjuicio de la responsabilidad penal a que hubiere lugar. Países como Brasil o España son ejemplo de tener dicha regulación en su sistema jurídico a través de leyes específicas.

Y si bien en el ordenamiento jurídico salvadoreño no aparece la figura del *habeas data* como instrumento diseñado para la protección específica del derecho a la autodeterminación informativa, como manifestación del derecho a la intimidad, ello no significa que tal derecho quede totalmente desprotegido, pues partiendo de lo que establece el inciso primero del Art. 2 de la Constitución, que "*toda persona tiene derecho a (…)y a ser protegida en la conservación y defensa de los mismos."* y asimismo el artículo 247 de la misma Carta Primaria, también en su primer inciso sostiene: *"Toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución";* se infiere que los derechos reconocidos expresa como implícitamente, deben ser garantizados a toda persona a través de los mecanismos de protección establecidos para su ejercicio. De manera que aunque no se disponga de una ley que prescriba los presupuestos procesales para materializar tal figura, se puede decir que la protección del derecho en mención puede ser efectuada a través del proceso constitucional de amparo, no importando la naturaleza de la empresa o ente a quien se le atribuya la vulneración de dicho derecho.

Por todo lo anteriormente expuesto, ha de concluirse que frente a la ausencia de un desarrollo legislativo de la figura relacionada que establezca el procedimiento y los mecanismos de defensa pertinentes, la admisión de la pretensión constitucional del demandante relativa a señalar actuaciones que han supuesto afectación al derecho a la autodeterminación informativa, además de responder a un amparo especializado en cuanto al derecho que se trata de proteger, encaja dentro de la figura del amparo; y, en ese caso específico del amparo contra particulares, por cuanto el mal manejo de sus datos personales, que se atribuye a las autoridades demandadas, comprueba la configuración del primer presupuesto de procedencia; es decir, una especie de situación de predominio de las mismas en relación con la posición del demandante.

Las consideraciones manifestadas evidencian la competencia de la Sala de lo Constitucional para conocer el asunto planteado por el demandante. En consecuencia, se rechaza la pretensión de la sociedad DICOM, de que se dictara sobreseimiento a su favor.

[...] Respecto del derecho a la autodeterminación informativa como manifestación del derecho a la intimidad, es menester realizar algunas consideraciones sobre el contenido jurídico del mismo y su forma de ejercicio en la realidad social actual a efecto de que su conceptualización sirva de marco de referencia para valorar su afectación o no a través de las actuaciones contra las que reclama el demandante.

En cuanto al reconocimiento del derecho relacionado en el texto constitucional, ha de partirse de lo que establece el inciso 2º. del citado Art. 2, que señala: "S*e garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".* En referencia específica a la intimidad personal, es preciso manifestar que el contenido de tal derecho hace referencia al ámbito que se encuentra reservado *ad intra* de cada persona, en el que se originan los valores, sentimientos, etc., vinculados a la propia existencia de su titular y cuyo conocimiento importa únicamente a éste y en su caso, a un círculo concreto de personas seleccionadas por el mismo. Por tanto, en dicho ámbito opera la voluntad del individuo para disponer de todos aquellos aspectos que puedan trascender al conocimiento de los demás.

A pesar de que el derecho a la intimidad parte de la esfera privada del individuo, el mismo no se puede alejar del contexto social donde se ejercita; es decir, que no se desliga completamente del entorno social en el cual adquiere sentido y se relaciona con los otros miembros del colectivo social en forma individual o agrupada, lo que implica que el ejercicio

de tal derecho puede encontrarse limitado por las necesidades sociales y los intereses públicos.

Efectivamente, el derecho en estudio, ha ido perdiendo su carácter exclusivamente individual y asumido con mayor fuerza un papel colectivo y social importante, sin que ello signifique la eliminación de la nota que identifica tal carácter –la individualidad– pues ésta se integra con un contenido público que viene a definirla y a complementarla frente a las nuevas circunstancias que van generándose en el tiempo. Para el caso, el suministro de datos particulares que una persona proporciona a la administración pública mediante el empleo de fichas, solicitudes, entrevistas, es un suceso que le compete a la persona misma; y, sin embargo, es de interés también para los demás miembros de un determinado conglomerado social con una finalidad específica. A pesar de ello, el peligro que puede suscitar tal situación consiste más que en el conocimiento y posesión de los datos, en la posibilidad del uso inadecuado de los mismos.

Frente al peligro anteriormente advertido existe una manifestación del derecho a la intimidad, que es precisamente el derecho a la protección de los datos y consiste en que el individuo pueda controlar el uso o tratamiento de los mismos, a fin de impedir una lesión a su esfera jurídica. Tal derecho ha sido denominado de diversas formas, según el autor que lo formule; y así, se le conoce como derecho a la autodeterminación informativa o derecho a la intimidad informática; pero, indistintamente de su formulación, éste debe ser entendido como *aquel que tiene por objeto preservar la información individual que se encuentra contenida en registros públicos o privados, especialmente la almacenada a través de los medios informáticos, frente a su utilización arbitraria.* De modo que a partir del acceso a la información, exista la posibilidad de solicitar la corrección, actualización, modificación y eliminación de los mismos.

Se puede afirmar entonces que el derecho a la intimidad en el ámbito informático implica lo siguiente: (a) que todo individuo tiene derecho de acceder a la información personal y especialmente a aquella que se encuentre contenida en bancos de datos informatizados; (b) que todo individuo ha de tener la posibilidad y el derecho a controlar, de forma razonable, la transmisión o distribución de la información personal que le afecte, (c) que debe existir, en el ordenamiento jurídico, un proceso o recurso que permita hacer efectivos los puntos señalados. Todo ello con la finalidad de establecer la estructura mínima que permita el manejo fiable de los datos personales de los individuos que se encuentren en banco de datos mecánicos o informáticos para conservar la veracidad, integridad y actualidad de los mismos; así como la regulación sobre la inaccesibilidad de otras instancias que no comprueben la existencia de una finalidad que justifique suficientemente la pretensión de conocerlos.

Ahora bien, en el ámbito público o comercial, algunas instituciones y la mayoría de empresas mercantiles, requieren para su información de ciertos datos personales, que si bien resulta ser una injerencia en el círculo íntimo de una persona, ésta cobra validez cuando se trata de cumplir con una finalidad específica para la que fue creada v. gr. Registro Nacional de Personas Naturales; o cuando, para efecto de alguna negociación financiera o comercial, se pretenda resguardar el capital de la empresa. Y es que, para suscribir contratos mercantiles, ambas partes requieren conocer su situación financiera y crediticia, lo cual, al reflejar su comportamiento en relaciones previas de igual o similar naturaleza, será determinante para la confiabilidad recíproca en el cumplimiento de la obligación que se pretende contraer.

En estas circunstancias, cabe la posibilidad que ante el surgimiento de empresas como DICOM, que a través del tratamiento automatizado de datos hacen referencia exclusiva al comportamiento crediticio de los sujetos, las empresas financieras puedan requerirle tal información, pagando por el servicio prestado. La información no se dispersa; o, más bien, no ha de conocerse por cualquier persona que tenga interés o capricho, sino consultada únicamente por su titular o por quienes realmente comprueben tener facultad o autorización para hacerlo.

No obstante lo anterior, la forma o el tratamiento indebido de los datos, en la tarea de recolección, podría ser generadora de perjuicios para el titular de los mismos por razones de falsedad o discriminación respecto de la información. Iguales perjuicios podrían generarse si la información no se encuentra actualizada, debido a la negativa u omisión de la autoridad correspondiente de completar, verificar o realizar los ajustes necesarios. En todos estos casos, bastará que no exista una correlación directa entre los registros contenidos en los bancos de datos y la realidad del sujeto de que se trate.

Lo expuesto evidencia que frente al poder que la tecnología impone en manos de recolectores y clasificadores de datos, el individuo debe estar dotado también de los medios o mecanismos lo suficientemente eficaces que la ley reconozca para garantizar su derecho de participar en ese proceso asegurando de tal manera que los datos recopilados sean veraces y que no sean más de los que se requiera obtener para fines legítimos. Por tanto, respeto al derecho a la intimidad, existe la obligación para todos aquellos que almacenan y sistematizan datos personales en registros ad-hoc, de seleccionar los datos que reflejen la verdadera situación jurídica del individuo. De allí, que todo banco de datos debe adoptar las medidas de seguridad adecuadas para garantizar la inviolabilidad o inalterabilidad de la información en él contenida, se trate de bancos públicos o privados, debiendo establecerse un régimen de responsabilidad ante su uso indebido.

Fragmentos del Proceso de Inconstitucionalidad por Omisión No, 36-2004, Sentencia Definitiva del 2 de septiembre de 2005, de la Sala de lo Constitucional en El Salvador.

[...] en relación con el derecho a la autodeterminación informativa, se ha construido una institución reciente cuya finalidad es la protección y reparación específica de este derecho: el *habeas data*. Pasamos ahora a examinar los elementos más relevantes de esta institución.

Sobre la *naturaleza jurídica* de la misma, se dice que es una institución, en términos genéricos, ya que dependiendo del tratamiento constitucional que cada Estado decida darle, puede establecerse como un derecho ejercitable mediante una vía de tutela común a otros derechos fundamentales, o bien, como una acción o proceso específico.

Así, haciendo un estudio comparado con el objeto de ejemplicar las situaciones anteriores, se advierte que la Constitución colombiana de 1991 estableció en su art. 15 que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución".

Asimismo, la Constitución guatemalteca de 1985 prescribe en su art. 31 que "toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica". En ambos casos, el habeas data se presenta como un derecho ejercitable por vía de la acción de tutela o del proceso de amparo.

Por otra parte, en Perú la disposición constitucional pertinente reconoce como garantía constitucional "la acción de habeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2°, incisos 5° y 6° de la Constitución". De igual manera, la Constitución paraguaya introdujo el habeas data de la siguiente forma: "toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos". En este último país, la acción fue rotulada como habeas data y se alojó en el tramo de los procesos jurisdiccionales de tutela de los derechos –junto con el amparo y el habeas corpus–, estableciéndose, en consecuencia, la posibilidad de ejercer una acción específica para la tutela de los derechos concedidos por la norma constitucional.

[...] Respecto del *tratamiento procesal* que recibe la institución, se advierte que, en los diferentes países en los cuales se ha articulado el habeas data como mecanismo de protección del derecho a la autodeterminación informativa, se ha proporcionado un tratamiento procesal de diversa índole. Así, existen ordenamientos jurídicos que han creado un proceso específico desarrollado en la ley secundaria; mientras que en otros, se sigue el trámite de la vía de tutela común al resto de derechos fundamentales –v. gr. el amparo–. Asimismo, algunos países aplican al instituto las pautas generales relativas al amparo –aunque con algunas particularidades– creandose una modalidad de este proceso o un amparo especializado.

Por regla general, al analizar la experiencia de estos Estados, la doctrina coincide en que lo más conveniente para maximizar la protección del derecho a la autodeterminación informativa es la emisión de una normativa especializada que contemple –entre otros– la articulación de un proceso específico, distinto al resto de procesos constitucionales. Sin embargo, ello no significa que la adaptación de los procesos constitucionales ya existentes tales como el amparo, no provea dicha protección.

Así, la justificación más importante para crear el proceso de habeas data como vía especializada ha sido la necesidad de establecer un procedimiento sumarísimo que responda a las características de urgencia de los derechos involucrados. Sin embargo, ante dicha postura surge otra que considera que mediante el amparo se protegen –entre otros– derechos como la vida, al salud y el medio ambiente que también exigen una resolución ágil y pronta, además de medidas precautorias capaces de evitar el daño o restablecer la situación menoscabada. Asimismo, al referirse a los países que cuentan con un sistema concentrado de control de constitucionalidad, los expertos en el tema estiman que el establecimiento de un proceso de habeas data con plazos preferentes en relación con el amparo contribuiría a la saturación del órgano con competencia en materia constitucional, en detrimento del resto de derechos fundamentales, al tener que resolver los casos de habeas data con prioridad a los de amparo.

Por lo cual se concluye que *es el legislador quien debe tomar en consideración las circunstancias propias a fin de determinar la necesidad y conveniencia de instaurar una competencia especializada de esta naturaleza. Es decir, en todo caso, dichas razones de conveniencia encajan dentro del ámbito de libertad de configuración del legislador.*

Ahora bien, en relación con las garantías administrativas del derecho a la autodeterminación informativa, tiene especial relevancia, para los efectos de esta sentencia, la garantía de desarrollo y tratamiento legislativo del mismo.

A. En 1970, la República Federal Alemana adoptó la primera ley dedicada específicamente a la regulación del tratamiento de datos personales, la cual, además, desginaba un funcionario encargado de velar por el cumplimiento de la ley. A partir de entonces, otros países europeos fueron elaborando paulatinamente legislación específica sobre el tema.

B. De igual manera, la preocupación por esta problemática comenzó a mostrarse en el ámbito internacional, tanto global como regional.

a. En el plano global, para los países miembros de la Organización de las Naciones Unidas (ONU) rigen las siguientes regulaciones: (i) la *Proclama de Teherán*, aprobada por la Conferencia Internacional de Derechos Humanos el 13-V-1968, en la que se sostuvo que "Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evaluación puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente"; (ii) la *Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad*, emitida por la Asamblea General de la ONU el 10-XI-1975, donde se expresó: "Todos los Estados tomarán medidas apropiadas a fin de impedir que los progresos científicos y tecnológicos sean utilizados, particularmente por órganos estatales, para limitar o dificultar el goce de los derechos humanos y las libertades fundamentales de la persona consagrados en la Declaración Universal de Derechos Humanos, en los pactos internacionales de derechos humanos y en otros instrumentos internacionales pertinentes"; y (iii) los *Principios rectores para la reglamentación de los ficheros computarizados en datos personales*, establecidos por la Asamblea General de la ONU en su Resolución 45/95, el 14-XII-1990, a cuyo tenor se dejan las modalidades de aplicación de los reglamentos relativos a los ficheros computarizados de datos personales a la iniciativa de cada Estado, con sujeción a ciertas orientaciones; dicha norma es de aplicación a todos los ficheros computarizados, tanto públicos como privados y, por extensión facultativa y a reserva de las adaptaciones pertinentes, a los ficheros manuales. Los principios que reconoce son licitud y lealtad, exactitud, finalidad, acceso de la persona interesada, no discriminación y seguridad. A ellos se le agregan normas específicas referidas a la facultad de establecer excepciones a estos principios, lo relativo al control y sanciones, y los requisitos para el libre flujo de datos a través de las fronteras.

[...] Tampoco la legislación nacional cuenta con un cuerpo normativo que contenga, de manera sistematizada, las pautas de regulación del tratamiento de datos de carácter personal. No obstante, existen disposiciones dispersas que contemplan aspectos básicos sobre el tema tales como el art. 3 de la Ley Transitoria del Registro del Estado Familiar y de los Regímenes Patrimoniales del matrimonio, el cual se refiere a la publicidad de la información de tales registros; igualmente, los arts. 2, 3 y 4 de la Ley del Registro de Comercio contemplan, respectívamente, los fines del registro, la presunción de exactitud de la información contenida en él, así como la publicidad del mismo y sus excepciones. Además, la Ley del Menor Infractor se refiere, en su art. 5 letra (b) al derecho a la intimidad

personal de los menores, mientras que los arts. 122 y 123 regulan lo relativo al Libro de Registro de Internamientos y a la confidencialidad de los expedientes. De igual manera, el art. 375 del Código de Familia establece la garantía de reserva en la investigación y decisión de asuntos judiciales y administrativos relativos a menores.

Las disposiciones mencionadas anteriormente constituyen –entre otras– un esfuerzo del legislador por desarrollar el derecho a la autodeterminación informativa y su protección. Ahora bien, es claro que la principal justificación para la emisión de un cuerpo normativo que sistematice la totalidad de regulaciones relativas a la protección de datos, consiste en razones de técnica legislativa, ya que *la ausencia de dicho cuerpo, en todo caso, no afecta la eficacia directa del artículo 2 inc. 2º Cn., estando habilitado el operador jurídico para recurrir a la interpretación constitucional así como a la integración legislativa. En consecuencia, este aspecto también corresponde al ámbito de la libertad de configuración del legislador.*

[...] En cuanto a la creación de un proceso de habeas data, cabe señalar que, tal como se encuentra redactado el art. 2 incs. 1º y 2º, al existir un "derecho a la protección en la conservación y defensa de los derechos de las personas", el habeas data se presenta, de acuerdo con nuestro marco constitucional, como un derecho ejercitable mediante una vía de tutela común a otros derechos fundamentales, a diferencia de otros países en los cuales se establece como proceso específico para la protección del derecho a la autodeterminación informativa.

Anexo Número Cuatro:

EL HABEAS DATA Y EL "DERECHO AL OLVIDO"

Por PABLO A. PALAZZI

Pablopalazzi@yahoo.com

publicado en Jurisprudencia Argentina, 1997-I-33.

I. EL CASO.

El fallo que anotamos incursiona en uno de los problemas que plantea la recopilación de datos personales en registros informatizados.

Un particular interpuso acción de hábeas data a los fines de suprimir los datos que mantenía una agencia de informes comerciales, sosteniendo que los mismos estaban caducos por haber transcurrido un lapso excesivo de tiempo. Los datos consistían en inhabilitaciones para operar con cuentas corrientes que el actor había tenido hacía más de diez años en tres bancos. Argumentó asimismo que la existencia de esa información le causaba un perjuicio en su esfera patrimonial, puesto que le dificultaba el acceso al crédito y la posibilidad de obtener una tarjeta de compras.

La demandada sostuvo que los datos eran dados de baja a los diez años, negándose a suprimirlos pues entendió que (i) la información cuestionada era cierta y (ii) que al difundir los datos a terceros, siempre se aclaraba que las inhabilitaciones estaban vencidas.

II. LA DECISION DE 1ª INSTANCIA.

La juez de 1ª instancia hizo lugar a la pretensión del actor. Primero analizó la aplicación del amparo al proceso de Hábeas Data, la legitimación, tanto activa como pasiva y la competencia. No repetiremos aquí los fundamentos, que han sido prolijamente enunciados en la decisión, a la cual remitimos. En segundo lugar -y esto es lo importante-, el fallo hizo lugar a la demanda, reconoció la caducidad del dato basada en el "derecho al olvido" y la arbitrariedad de la negativa a suprimirlo.

Para así decidir la sentencia recurrió al Derecho Comparado, señalando que ciertos ordenamientos jurídicos -la legislación francesa y alemana-, establecen la eliminación del dato por el transcurso del tiempo o cuando ya no resulte indispensable para la finalidad para la cual fue recolectado.

Seguidamente se citaron las conclusiones de Jornadas y congresos e incluso de proyectos de reforma del Código Civil que se inclinan por aceptar la supresión del dato antiguo o caduco, al que se lo define como "aquel que por efecto del tiempo ha perdido virtualidad, ha devenido intrascendente a los efectos de cualquier efecto jurídico relativo a la ejecutabilidad". La conservación indefinida de este dato caduco -siempre según la decisión de primera instancia-, impide el derecho al olvido, que da lugar al principio según el cual "ciertas informaciones deben ser eliminadas de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede prisionero de su pasado".

Y aplicando lo expuesto al caso concreto razonó que "es innegable que en el caso el dato es caduco; si se piensa en términos de prescripción civil superaría el plazo de prescripción liberatoria...". Se citó también el art. 51 CP., que prohíbe informar la existencia de sentencias condenatorias penales pasado cierto tiempo. Así concluyó que la negativa a suprimir los datos sobre inhabilitaciones no vigentes a más de 10 años era arbitraria, ordenando la supresión en las bases de datos de la demandada de la información referente al actor. La decisión fue apelada por la vencida.

III. EL FALLO DE CAMARA.

La Cámara Civil revocó lo decidido por la juez de 1ª instancia. No queda muy claro cuál fue el fundamento de la decisión, sobre todo porque el fallo no se refiere al "derecho al olvido" que había sido reconocido y tan bien fundado en la instancia anterior. La alzada se basó en las siguientes premisas:

i) la acción de hábeas data es procedente siempre que de los registros surjan inexactitudes o que estos puedan provocarle cierta y determinada discriminación al actor.

ii) los datos cuestionados carecían de inexactitudes, porque contenían expresos agregados con asiento de las fechas en que las tres inhabilitaciones habían vencido. iii) la actora sostiene que la demandada publica datos relativos a su intimidad y con ello genera discriminación, pero no impugnó esos datos por inexactos.

iv) la actividad de la demandada no afecta el honor e intimidad ni resulta discriminatoria a la vida de relación del actor. La sala recuerda: a) la ausencia de reglamentación sobre la materia y b) que la información se orienta a actividades de índole estrictamente comercial y crediticia.

v) Por último, el fallo termina señalando que la entidad demandada es típicamente comercial a la luz del art. 8 CCom. y que guarda sus datos durante 10 años. Entonces la sala concluye que "...no es arbitrario o producto de un excesivo rigor informático, a raíz de concordar con la obligación mercantil derivada del art. 67 CCom., según la cual es el período de conservación de los libros y documentación a su vez exigida por el art. 44 de ese cuerpo legal".

IV. CONSIDERACIONES SOBRE LA CADUCIDAD DE DATOS PERSONALES ALMACENADOS EN REGISTROS INFORMATIZADOS.

Personalmente no compartimos las conclusiones a las que arriba la alzada. Consideramos que la sentencia de primera instancia resolvió en forma razonable la cuestión acerca de si un particular puede solicitar la supresión de información sensible que por el transcurso del tiempo ha devenido obsoleta o caduca, esto es, ha perdido utilidad.

Reconocemos que el tema es complejo, pues plantea la posibilidad de aceptar en el hábeas data otros motivos distintos a la falsedad o discriminación, lo que a nuestro juicio debe tener respuesta afirmativa.

Para arribar a tal conclusión nos basamos en lo siguiente: en primer lugar, en nuestro sistema constitucional no existen derechos absolutos; por lo tanto no podría sostenerse válidamente que un recolector de datos pueda almacenar indefinidamente información sensible y como contrapartida que el registrado no pueda suprimirla pasado cierto tiempo. Asimismo, si bien el art. 43 sólo hace referencia a la falsedad o discriminación, es posible aceptar la caducidad como motivo para habilitar la vía del hábeas data, puesto que la difusión de datos caducos puede originar discriminación por parte de otros sujetos que reciban esos datos sensibles. Añadimos que con esa conducta se afecta el principio de finalidad.

Además, si el hábeas data protege los derechos a la intimidad y a la identidad, cabe recordar que la difusión injustificada de datos del pasado ha sido juzgada como afectación a estos derechos.

Por último, tanto los ordenamientos jurídicos extranjeros como los proyectos de reforma del Código Civil y de reglamentación del hábeas data receptan la caducidad del dato, lo que demuestra que la solución de primera instancia en modo alguno era antojadiza. Desarrollaremos estos argumentos seguidamente.

a) Reglamentación razonable del derecho a recolectar y difundir información nominativa

Sabido es que nuestra Constitución no reconoce derechos absolutos de propiedad y libertad, puesto que estos están sujetos a las leyes que reglamenten su ejercicio. De ahí que la Corte Suprema haya dicho que el ejercicio de las industrias y actividades de los particulares puede ser reglamentado en la proporción que lo requiera la defensa y el afianzamiento de la salud, la moral, el bienestar general y aún el interés económico de la comunidad. No cabe ninguna duda de que estas actividades pueden ser reglamentadas también en aras de preservar la intimidad de las personas registradas.

Si bien es lícito recolectar información crediticia a los fines de resguardar el crédito -lo que en definitiva beneficia a toda la comunidad-, ello no obsta a la posibilidad de hallar un límite a dicho almacenamiento. Por eso la analogía que realizó el fallo de 1ª instancia con las normas civiles y penales nos parece acertada. Las reglamentaciones de esas situaciones demuestran que en nuestro ordenamiento jurídico la imposición de límites temporales al ejercicio de derechos es constitucionalmente válida y forma parte, en definitiva, del balance de valores que encontramos en toda sociedad.

De esa forma se logra conciliar los derechos a trabajar y ejercer una industria lícita (art. 14 CN.) -para el recolector de datos-, y el derecho a la intimidad en cabeza del registrado (art. 19 y 43 CN.). Cierto es que esa limitación debería en principio provenir de la ley, pero nada impide que una sentencia judicial, a través de una interpretación como la que realizó la juez de 1ª instancia lo acepte.

A nuestro entender, el término de 10 años es razonable (art. 28 CN.), pues el plazo es más que suficiente para darle un valor útil a la información y además no se coloca al recolector de información en una situación desigual frente al registrado si se le permite tener ese dato por un plazo determinado. A nuestro juicio se trata de la fijación de límites temporales para el ejercicio de un derecho que en forma alguna vulnera la igualdad constitucional.

b) La difusión de datos pasados puede lesionar el derecho a la privacidad

Si el hábeas data protege la intimidad -y también la identidad-, cabe recordar que cierta jurisprudencia ha reconocido como violación de ese derecho la revelación en forma innecesaria de hechos pasados que estaban olvidados.

Como ejemplo de ello señalamos el leading case estadounidense "Melvin v. Reid". Allí, la actora, cuyo nombre original era Gabriel Darley, había ejercido la prostitución

y había estado involucrada como imputada en un juicio por homicidio. Después de haber sido absuelta logró abandonar la vida licenciosa que llevaba, casarse con un hombre llamado Melvin y con éste comenzó a llevar una vida decente y respetable, entablando nuevas amistades con gente que desconocía su pasado. Siete años después se estrenó una película, The Red Kimono, donde se narraba la verdadera historia, con su nombre original, lo que reveló su pasado a sus actuales amistades y en definitiva terminó arruinando su vida. La actora accionó por invasión a la privacidad y el tribunal, basándose en una cláusula constitucional del estado de California que otorgaba a todos los hombres el derecho de "procurar y obtener la felicidad", hizo lugar a la demanda.

El hecho en definitiva consistió en el uso sin autorización del anterior nombre de la actora para hacer una película sobre su vida pasada. El tribunal entendió que se estaba revelando un hecho que era verdadero, pero juzgó que el uso innecesario del nombre de la actora y la revelación de su pasado a sus nuevos amigos y asociados introdujo un elemento que en sí mismo era una transgresión a su derecho a la privacidad.

Es decir que se concluyó que el uso y difusión de un dato verdadero puede ser violatorio de la intimidad y reserva de un individuo, cuando éste tiene cierta antigüedad.

Análogamente, creemos que la difusión de la información de inhabilitaciones en cuentas corrientes bancarias con la antigüedad que presentaban en el caso, por más que se aclarara que estaban desactualizadas, era lesivo de la intimidad del accionante.

c) La caducidad del dato como motivo de procedencia del hábeas data

Es cierto que el art. 43 CN. permite el hábeas data sólo cuando exista falsedad o discriminación, y ésta fue la postura de la Cámara.

¿La caducidad del dato está contemplada en el texto constitucional? En principio, un dato, por su vejez podría crear discriminación, por ejemplo por impedir a una persona obtener algo que obtienen otros que están en la misma situación, como ser un crédito o una tarjeta de compras (casualmente ésto fue lo que se argumentó en el caso).

El hecho de que la Constitución nada diga sobre la caducidad del dato, no debe impedir pasar por alto el art. 33 CN. (cláusula de los derechos no enumerados) que permite incluir -aun después de la reforma de 1994-, a los derechos no enunciados explícitamente en el texto constitucional. Para ello recordamos que la Corte Nacional tiene dicho que:

"La Constitución, en su condición de instrumento de gobierno, debe analizarse como un conjunto armónico dentro del cual cada parte ha de interpretarse a la luz de las disposiciones de todas las demás".

La doctrina, con anterioridad a la reforma de 1994, había sugerido apelar a la autointegración, es decir recurrir a las demás normas y principios constitucionales para hacer frente a los problemas que las nuevas tecnologías y en especial la informática causaban a la intimidad.

Sentado ello, vemos entonces como posible que si el hábeas data permite el control de los datos personales y la protección de la intimidad, ese derecho se ejerza suprimiendo información caduca, esto es, que ha perdido virtualidad por el transcurso del tiempo (arts. 19, 33 y 43 CN.).

Además, la doctrina ha aceptado la procedencia del hábeas data cancelatorio con fundamento en otros motivos. Así Ekmedkjian y Pizzolo lo aceptan contra los datos obsoletos o los que deban permanecer reservados. Para Gozaíni, la facultad de requerir la cancelación o la corrección de los datos inexactos otorga el denominado "derecho al olvido", esto es, el principio a tenor del cual ciertas informaciones deben ser eliminadas de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede prisionero de su pasado. En igual sentido se han pronunciado la doctrina española, francesa e italiana.

Por último, la situación podría encuadrarse asimismo dentro del abuso de derecho (art. 1071 CC.) porque el recopilador de datos, al difundir un dato antiguo y que ha perdido utilidad, está ejerciendo abusivamente ese derecho a informar y trabajar en detrimento del derecho a la privacidad del registrado.

d) El principio de finalidad en la recolección de datos personales

También creemos que se afecta el principio de finalidad que debe existir en toda recolección de datos. Básicamente, este principio consiste en permitir la recolección de datos en ficheros automatizados siempre y cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para los que hayan sido obtenidos.

Aunque este principio no tiene recepción específica en nuestro ordenamiento, está ampliamente contemplado en las legislaciones del derecho comparado y también en los proyectos de reglamentación del hábeas data.

Y aplicando estos principios al caso concreto, si el dato tiene por finalidad saber quién está inhabilitado, vencida la inhabilitación, que tiene un plazo máximo de sesenta meses (Comunicación "A" 2329 - 21-IV-95 - OPASI-2 - RENOM-1, punto 1.8.), carecería de sentido seguir difundiendo el dato y por lo tanto su conservación devendría arbitraria, esto es sin derecho. ¿Qué sentido tiene saber que hace diez años una persona fue inhabilitada para operar en cuenta corriente bancaria, si desde hace otros tantos es un puntual cumplidor de sus obligaciones comerciales? Aquella inhabilitación no refleja sino un dato pasado que puede o no ser objetivo para determinar su solvencia o su comportamiento futuro.

Nos parece que el registro del dato es más grave aun cuando lo realiza una empresa privada destinada a proveer informes, pues sólo el Banco Central es el autorizado legalmente a poseer esta información, a los fines de que durante esa inhabilitación ninguna entidad financiera del país dé curso a las solicitudes de apertura de cuentas corrientes interpuestas por el inhabilitado (OPASI 2, pto. 1.8.3). Pero sucede en la práctica que eliminado el dato de la base de datos de cuentacorrentistas inhabilitados que posee el Banco Central, la difusión del mismo por parte de una entidad privada produce los mismos efectos que tiene cuando lo realiza la entidad rectora en materia financiera.

e) Existencia de discriminación

Dijimos también que la divulgación de datos caducos puede originar discriminación por parte de otros sujetos. En el caso que anotamos, el actor argumentaba que la difusión de datos por parte de la demandada le causaba un perjuicio en su esfera patrimonial, pues le dificultaba el acceso al crédito y a la posibilidad de tener una tarjeta de compras.

Y bien podría argumentarse que la existencia del dato caduco lo discriminaba en la medida en que no le permite obtener lo que otros obtienen estando en la misma situación. Es decir, que las entidades financieras le deniegan la posibilidad de abrir una cuenta u obtener una tarjeta de compras, mientras que otros sujetos que están en las mismas condiciones (vgr. personas cuya inhabilitación esté vencida pero no registrados) los pueden obtener.

Un primer problema estaría dado por la legitimación pasiva del reclamo, pues en este caso la discriminación no proviene de quien difunde el informe sino de quien lo recibe (el banco). Es decir, si bien la actividad de difundir datos caducos genera discriminación por parte de otras personas, ello no permite encontrar el motivo de procedencia de hábeas data contra el banco de datos.

Sin embargo, nos parece que por más que la discriminación no provenga del banco de datos demandado sino de la entidad financiera, el primero actúa como causa originaria de la misma, pues de no difundir el dato caduco, esta discriminación no existiría. Además, la conducta de proveer información antigua y que no refleja necesariamente el estado patrimonial del registrado, sino un mero dato histórico que pertenece a su intimidad constituye una conducta arbitraria que termina causándole una situación discriminatoria. Y esta discriminación no es sino una violación al principio de igualdad ante la ley (art. 16 CN.).

Recordamos que en la tradicional jurisprudencia de la Corte Suprema de Justicia de la Nación el principio de igualdad consiste en que no se establezcan excepciones o privilegios que excluyan a unos de lo que se concede a otros en iguales circunstancias y que dicha garantía no se afecta en tanto las distinciones establecidas por el legislador no obedezcan a propósitos de injusta persecución o indebido privilegio, sino a una objetiva razón de diferenciación, aunque el fundamento sea opinable.

En el caso "Sejean", la Corte dijo que se encuentra dentro del espíritu del art. 16 CN. y de las leyes dictadas en su ejercicio, "la reinserción en el cuerpo social de quienes han delinquido, y en general, el brindar aun a quienes son víctimas de sus propios desaciertos la posibilidad de recomponer su existencia".

Quizás la alusión al art. 51 CP. que realizó la sentencia de grado sea un claro ejemplo de la existencia de discriminación cuando se trata de la caducidad de datos personales que pertenezcan al pasado. Este artículo establece que el registro de las sentencias condenatorias caducará a todos sus efectos en los siguientes plazos: a) si la sentencia es de carácter condicional, a los diez años del dictado de la misma, b) si la condena es privativa de la libertad de cumplimiento efectivo, la caducidad se produce una vez transcurridos diez años a partir de la extinción de la pena impuesta y c) en los casos de condenas a pena de multa o inhabilitación, la caducidad del registro de la sentencia respectiva se produce una vez transcurridos cinco años de la extinción de la multa o inhabilitación impuestas.

Este artículo fue introducido al Código Penal en 1984 por la ley 23.057 (LA 1984-A-24). El mensaje del Poder Ejecutivo del 13/12/83 decía que introducía un texto:

"Destinado a evitar uno de los males característicos de nuestra vida jurídica en los últimos años: el etiquetamiento de las personas".

Y agregaba:

"No se prohíbe la existencia de registros, que además de ilusoria puede resultar perjudicial (por ejemplo: registros policiales de modus operandi), pero se prohíbe que, cuando esos asientos dejen de ser legalmente útiles, se informe en base a ellos".

El diputado Lorenzo H. Cortese, por su parte, sostuvo: "Hasta ahora, quien tenía la desgracia de delinquir una vez en su vida quedaba con un estigma que lo perseguía para siempre. De aquí en más tendrá ese hombre la posibilidad de evitar el etiquetamiento por una circunstancia adversa, muchas veces no querida o motivada por factores de esta sociedad, que tiene muchos defectos que debemos reparar. De manera que cuando transcurran los términos que marca la nueva legislación -es decir, diez años a partir del cumplimiento de la pena-, ese antecedente ya no podrá ser informado por ningún instituto que lo tenga registrado".

El senador Felipe Celli, remarcó que las informaciones, para evitar el etiquetamiento, no deben proporcionarse cuando han dejado de ser útiles. Añadiendo textualmente:

"Por otra parte, en un Derecho penal moderno basado en el estado de Derecho, no puede decirse que la pena acompañará al delincuente durante toda su vida, porque ello implicaría establecer que existen ciudadanos de segunda clase. Ya demasiado lo castiga la sociedad cuando lo marca y margina, impidiéndole reingresar a la vida

libre con las mejores posibilidades para no delinquir y en igualdad de condiciones con las demás personas. Este es, en síntesis, el objetivo que persigue este art. 51".

Es evidente cuál es el espíritu del art. 51 CP.: evitar la estigmatización de quien delinquió, considerando que, luego de un plazo, cabe liberarlo de su historia criminal, mediante la caducidad de los registros respectivos. Análogamente, en el caso que comentamos, la caducidad de los datos dispuesta por la juez de 1ª instancia tenía el mismo fundamento: evitar la estigmatización del ciudadano frente al manejo que de sus datos se realizan, más cuando el tiempo transcurrido es más que razonable para restarle validez o utilidad al dato.

f) Proyectos de reforma y reglamentación del hábeas data

En nuestro país, el Proyecto de reformas del Código Civil redactado por la Comisión del Ministerio de Justicia estableció la posibilidad de cancelar los datos caducos -aunque no los definía-, y exigir su utilización conforme a la finalidad para la que fueron recogidos (art. 114 del proyecto).

También los actuales proyectos de reglamentación de la garantía del art. 43 CN. establecen un límite temporal para el almacenamiento de información crediticia.

Por ejemplo el proyecto presentado por el senador Eduardo Menem establece en el inc. 4 art. 25, bajo el título "Prestación de servicios de información crediticia" que "sólo se podrán archivar, registrar o ceder los datos de carácter personal que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos diez años".

El Proyecto, aprobado por la Cámara de Diputados y elevado al Senado de la Nación el 5/6/96, al regular la prestación de servicios sobre solvencia patrimonial y crédito establece en el art. 32 inc. 4 que "sólo se podrá tratar datos de carácter personal que sean determinantes para evaluar y apreciar la solvencia patrimonial y el crédito de su titular con una antigüedad no mayor de cinco años".

Por último, el Proyecto de Ley de Hábeas data del diputado César Arias -siguiendo a la legislación española-, establece en su art. 25 inc. 3 que los registros de titularidad privada "sólo podrán archivar registros o ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los afectados, cuando sean adversos y no se refieran a más de seis años".

g) Derecho comparado

Dijimos que también el derecho comparado presenta legislaciones que se inclinan por aceptar una limitación temporal al almacenamiento de informes comerciales.

Así, la ley francesa -una de las más antiguas en la materia-, establece en su art. 36 que el registrado podrá exigir que sean rectificadas, completadas, clarificadas,

actualizadas o borradas las informaciones que le conciernen que sean inexactas, incompletas, erradas o perimidas o cuya recolección o uso, comunicación o conservación esté prohibida.

España también reglamentó el art. 18 de su Constitución mediante la Ley Orgánica 5/1992 del 29 de octubre de "regulación del tratamiento automatizado de los datos de carácter personal". En su art. 28 inc. 3 establece que "sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los afectados y que no se refieran, cuando sean adversos, a más de seis años".

En Noruega el art. 15 ley 48 sobre registro de datos personales establece que "toda empresa de información crediticia se asegurará de que los datos utilizados para información crediticia sean completos en la medida de lo posible y de que no se utilicen datos susceptibles de inducir a una actitud injustificada o indebidamente negativa frente a la persona a la que se refieran. Los datos que al finalizar el año natural tengan una antigüedad de tres o más años, sólo se podrán utilizar si fuere manifiesto que continúan siendo de significación sustancial para una apreciación correcta de la persona a que se refieran".

En los Estados Unidos, la regulación de datos personales se halla normada por gran cantidad de leyes públicas y privadas. Una ley especial fue sancionada en 1970 para establecer el marco legal de las empresas proveedoras de informes comerciales, denominada Fair Credit Reporting Act (FCRA). La ley entre otros aspectos de interés prohíbe a las agencias de información crediticias "proveer información adversa que tenga más de siete años de antigüedad" (cuando se trate de datos relativos a juicios, sentencias, deudas fiscales, registros de arrestos o antecedentes penales e información adversa en general) y de más de diez años cuando se trate de procesos relativos a quiebras o casos del Capítulo XI (Chapter 11) de la Bankruptcy Act.

V. CONCLUSION.

El tema que abordamos en esta nota demuestra que existen aún muchas cuestiones por solucionar respecto del hábeas data y la regulación de la información económica y financiera. El fallo comentado muestra que en la materia existe un gran vacío legislativo y judicial que reclama una reglamentación urgente.

Una interpretación que se atenga a la lectura literal del art. 43 de la Constitución, dirá que el hábeas data sólo procede frente a la existencia de falsedad o discriminación. La respuesta adecuada a esa objeción pasa necesariamente por una valoración constitucional previa.

Esa valoración previa debe pasar por considerar que el hábeas data -como garantía constitucional-, es una nueva forma de garantizar al ciudadano de una sociedad cada vez más informatizada el pleno ejercicio de sus derechos fundamentales. Por ello, la misma deber ser interpretada en consonancia con el tiempo y la realidad

actuales. En una sociedad de la información como la que vivimos, debemos tomar conciencia de que el hábeas data está destinado a evitar los peligros que el manejo irregular de la información puede generar.

En síntesis, nuestras conclusiones son las siguientes:

1. De lege lata consideramos que una interpretación constitucional conduce a aceptar la posibilidad de que un particular pueda solicitar la supresión de información que por el transcurso del tiempo ha perdido virtualidad. El fundamento de ello quedó plasmado en la resolución de primera instancia que motivó este comentario.

2. De lege ferenda, nos parece que la ley reglamentaria que se sancione debería contemplar un límite temporal para los recolectores de datos.

Anexo Número Cinco:

Reportajes relacionados con el derecho a la información

Opinión: La Ley de Ética Gubernamental
La Prensa Gráfica (El Salvador)
http://www.laprensa.com.sv
4/7/2003
Henry Campos
henrycam2@hotmail.com
Abogado y catedrático, colaborador de LA PRENSA GRÁFICA
Se ha estado discutiendo en la Asamblea Legislativa un proyecto de Ley de Ética Gubernamental que tiene por objeto normar la conducta ética de los servidores públicos. No obstante que resulta inadecuado hablar de Ley de Ética, pues esta última se caracteriza por tener normas que no pueden ser impuestas por la fuerza y que son dictadas por el propio individuo, es de considerar como positiva la regulación de un conjunto de normas que pretendan garantizar una administración pública honesta y transparente. En realidad toda norma ética expresada en una ley es norma jurídica.
Dentro de los aspectos que tienen que ver con la libertad de expresión, el proyecto no es del todo feliz.
El artículo 16 letra "h" del proyecto establece que se prohíbe a los servidores públicos vender o divulgar documentación o informes que hubieren sido declarados secretos o confidenciales por la autoridad competente y a los que el servidor público haya tenido acceso en razón de su cargo.
Sobre la prohibición de divulgación de la documentación o informes, el problema es que se deja en manos de la autoridad declarar si aquellos son secretos o confidenciales. Lo cual viola artículos constitucionales y tratados internacionales suscritos por nuestro país.

El artículo 8 de la Constitución establece que nadie está obligado a hacer lo que la ley no manda ni a privarse de lo que ella no prohíbe. De tal manera que sólo la ley puede limitar derechos subjetivos, y no dejarse arbitrariamente en manos de los funcionarios de turno.
El artículo 19 del Pacto Internacional de Derechos Civiles y Políticos exige que la libertad de buscar, recibir y difundir informaciones e ideas pueda ser restringida para el respeto de derechos de terceros, y para la protección de la seguridad nacional, orden público, salud o moral públicas, de forma expresamente fijada en la ley. Esto significa que las limitaciones de acceso a la información, recepción y difusión solo pueden ser limitadas por las razones apuntadas, siempre que estén fijadas de manera expresa en una ley.
El artículo 22 del proyecto letra b) establece que los particulares tendrán derecho a acceder a la información que por ley el servidor público no debe ocultar. Tal artículo implica que es necesario que una ley específica le permita al funcionario no ocultar la información, cuando en realidad la propia Constitución establece ya como regla general la libertad de expresión, con los límites del mismo artículo 6, y cuando la falta de ley, de acuerdo con el artículo 8 Cn., significa tener derecho.
Por lo anterior, hay que tomar en cuenta la importancia y diferencia de los conceptos acceso a la información, hábeas data e información secreta. El primer derecho es una facultad amplia que se reconoce a todo individuo para conocer información pública en general, o información privada con trascendencia pública, registrada o no en archivos y aun cuando no sea titular de las mismas. El hábeas data tiene por objeto garantizar el acceso a cierto tipo de datos o informaciones nominativas consignadas en bancos de datos o archivos que conciernen a un sujeto para conocerlas, rectificarlas, actualizarlas, eliminarlas o disponer sobre su transmisión. La información secreta del Estado u oficial es aquella relacionada con asuntos que pueden dañar la seguridad y defensa del Estado.
Para que la Ley de Ética Gubernamental sea una herramienta exitosa y genere credibilidad y transparencia en la administración, se requiere asegurar los derechos relacionados con la libertad de expresión e información, mediante la emisión de normativas especiales que regulen el acceso a la información, el hábeas data y los secretos oficiales y del Estado.

Art.16 de Ley de Ética Gubernamental, vulnera trabajo de periodistas.

Gloria Silvia Orellana
Diario CoLatino (El Salvador)
http://www.diariocolatino.com
26 de junio de 2003
Con la presentación de una propuesta de reforma al artículo 16, del Anteproyecto de Ley de Ética Gubernamental, la Asociación de Periodistas de El Salvador (APES), y Probidad, pretenden llamar la atención sobre la redacción de algunos artículos que podrían bloquear el trabajo periodístico, de ser aprobados en la Asamblea Legislativa.
El anteproyecto de ley de Ética Gubernamental, que se encuentra en la mesa de discusión de la Comisión de Legislación y Puntos Constitucionales ha puesto en riesgo, según APES y Probidad, el respeto al derecho a la Libertad de Expresión.
William Meléndez, presidente de APES, y Jaime López, de Probidad, afirmaron que tras un análisis del texto de la ley, se hace necesaria una revisión que evite una

discrecionalidad por parte de los funcionarios públicos en el manejo de la información de las instituciones gubernamentales.
"Creemos que como esta redactado el artículo 16, literal "h" obstaculiza la labor de los periodistas, ya que establece con la palabra "divulgar" , cualquier acción de algún funcionario público de entregar información a los medios de comunicación, para llevar a cabo investigaciones que señalen cualquier incumplimiento por parte de la institución", dijo Meléndez.
Actualmente, la Corte de Cuentas ha redactado que : Son prohibiciones para los servidores públicos, h) Vender o divulgar documentación o informes que hubieren sido declarados secretos o confidenciales por la autoridad competente y a los que el servidor público haya tenido acceso en razón de su cargo.
Para Meléndez, es evidente que vender información es un delito y es antiético, pero se hace necesario esclarecer el manejo de la información oficial y el concepto de qué es información secreta.
"Dado que la información que manejan los servicios públicos es precisamente de carácter público, en razón de qué criterio un informe será declarado secreto, o confidencial; cuál es la autoridad competente con poder discrecional de decretar la condición de secretividad o confidencialidad de un informe, y que legislación ampara estas facultades", afirmó Meléndez.
Para el presidente de APES, la redacción actual, viola el espíritu del artículo 19, de la Declaración Universal de Derechos Humanos, que dispone que : Todo individuo tiene derecho a la Libertad de Expresión, y este derecho incluye el 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.
La propuesta de reforma fue acompañada del diputado Fernando González, del partido CDU, para ser incluida en la correspondencia de la Asamblea Legislativa y ser vista, en la correspondiente comisión legislativa para ser analizada.

Crece Mordaza: Proponen restricciones para obtener documentos Oficiales.
Luis Laínez
El Diario de Hoy
nacional@elsalvador.com
El Diario de Hoy (El Salvador)
http://www.elsalvador.com
26 de junio de 2003
La Corte de Cuentas pretende convertir a los empleados públicos en "guardianes" de documentos. El Anteproyecto de Ley de Ética pretende declarar cierto tipo de informaciones como "secretas" y "reservadas".
Para Hernán Contreras, el presidente de la Corte de Cuentas de la República, el servidor público ideal es aquel que guarde con celo documentos oficiales que, previamente, hayan sido catalogados como "secretos", "reservados" o "clasificados". Si estas disposiciones estuvieran vigentes, jamás se habría conocido la corrupción de la ANDA cuando era dirigida por Carlos Perla.
Los "guardianes de la información" son la piedra angular del Anteproyecto de Ley de Ética Gubernamental, defendido ayer por Contreras frente a los diputados de la Comisión de Legislación y Puntos Constitucionales.

En al menos seis artículos del proyecto (que antes se denominaba "Código de Ética Gubernamental"), se identifican, con claridad, disposiciones que restringen el acceso a escritos gubernamentales.

Así se privilegia la confidencialidad como un "principio" de los servidores públicos, en tanto no divulguen información "secreta o especial para los intereses del Estado".

Además, los trabajadores estatales que entreguen escritos "reservados" serán sometidos a multas que dependerán de la jerarquía que éste tenga en la burocracia, de la "gravedad" de la falta y de su "repercusión social" (Art. 26).

"¿Cuál ley?"

El literal "c", del artículo 12, del anteproyecto mordaza de la Corte de Cuentas, ordena a los servidores públicos "ser transparente en las decisiones adoptadas sin restringir información, excepto cuando la ley lo remita".

-¿A cuál ley se refiere? -preguntó el diputado arenero Gerardo Suvillaga, presidente de la Comisión de Legislación.

-Esto es cuando una ley en concreto lo permita. Si no, se debe restringir la información. En otros puntos remitimos a la Constitución. Si no hay una ley que regule, el artículo tiene validez. Permite restringir, pero por ley general no permite restringir información -explicó Contreras, presidente de la Corte.

La misma observación hizo Suvillaga cuando el literal "h", del artículo 16, prohíbe "vender o divulgar documentación o informes que hubieren sido declarados secretos y confidenciales por la ley y a los que el servidor público haya tenido acceso en razón de su cargo".

"Queda menos malo si dice ley y no 'autoridad competente' (como originalmente estaba propuesto)", justificó Contreras.

Al diputado arenero no le convenció la explicación y consideró que era necesario pedir la opinión de la asociación de periodistas y de la ONG Probidad.

Ambas organizaciones estuvieron en contra del primer borrador de la ley y han sido invitadas para participar el próximo viernes en la discusión del anteproyecto de ley.

Óscar Abraham Kattán, diputado suplente del CDU, indicó que en la Corte Suprema de Justicia hay una iniciativa para establecer el hábeas data como un recurso para obtener documentación oficial, una figura que existe en muchas naciones.

La iniciativa de la Contraloría, empero, señaló Kattán, busca restringir el acceso a la información.

El anteproyecto de Ley pretende crear una "Oficina de Ética Gubernamental", que estará adscrita a la Corte de Cuentas.

Una de sus funciones será la de "velar que los ciudadanos tengan acceso a la información, en base a la Constitución de la República".

La única mención que contiene la Carta Magna a este respecto es en lo referente a la libre expresión (artículo 6).

Suvillaga interrogó a Contreras para conocer si ya tiene una partida presupuestaria para que tal Oficina de Ética Gubernamental funcione en todo el país.

El Presidente de la Corte de Cuentas reveló que no tiene ninguna partida, debido a que la ley no ha sido aprobada.

Los alcances

El nuevo anteproyecto de Ley de Ética Gubernamental contiene prohibiciones expresas para que los servidores o empleados públicos den a conocer información.

Sanciona a los que colaboren y es arbitraria

- Bloqueo

Los requisitos de un empleado modelo
La confidencialidad es parte de los principios del "servidor público". No debe divulgar o proveer información considerada "especial", "confidencial", "reservada" o "secreta".
- Sanciones
"Acciones contra la Ética Gubernamental"
Se considera como digno de sanción a aquel funcionario o trabajador de los diferentes órganos del Gobierno que no sepa custodiar documentos o que revele información "clasificada".
- Sin ley
Acceso a la información
Las prohibiciones para dar documentación están basadas en una ley inexistente. "Es para cuando una Ley lo permita (la restricción)", explicó Hernán Contreras, de la Corte de Cuentas.

Anexo Número Seis:

LEY ORGÁNICA DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL - LEY 5/1992

EXPOSICIÓN DE MOTIVOS

1. La Constitución española , en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación de garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática.

El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su

vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.

Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Uno y otro límite han desaparecido hoy: Las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos. Los más diversos -datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado «dinero plástico», sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner sólo algunos ejemplos- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultar. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: El conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley.

2. Partiendo de que su finalidad es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, la Ley se nuclea en torno a los que convencionalmente se denominan «ficheros de datos»: Es la existencia de estos ficheros y la utilización que de ellos podría hacerse la que justifica la necesidad de la nueva frontera de la intimidad y del honor.

A tal efecto, la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende sólo como un

mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia.

La Ley está animada por la idea de implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información. A tal efecto se estructura en una parte general y otra especial.

La primera atiende a recoger los principios en los que ha cristalizado una opinio iuris, generada a lo largo de dos décadas, y define derechos y garantías encaminados a asegurar la observancia de tales principios generales. Alimentan esta parte general, pues, preceptos delimitadores del ámbito de aplicación de la Ley, principios reguladores de la recogida, registro y uso de datos personales y, sobre todo, garantías de la persona.

El ámbito de aplicación se define por exclusión, quedando fuera de él, por ejemplo, los datos anónimos, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general -como pueden ser los registros de la propiedad o mercantiles-, así como, por último, los de uso estrictamente personal. De otro lado, parece conveniente la permanencia de las regulaciones especiales que contienen ya suficientes normas de protección y que se refieren a ámbitos que revisten tal singularidad en cuanto a sus funciones y sus mecanismos de puesta al día y rectificación que aconsejan el mantenimiento de su régimen específico. Así ocurre, por ejemplo, con las regulaciones de los ficheros electorales, del Registro Civil o del Registro Central de Penados y Rebeldes; así acontece, también, con los ficheros regulados por la Ley 12/1989, de 9 de mayo, sobre función estadística pública, si bien que, en este último caso, con sujeción a la Agencia de Protección de Datos. En fin, quedan también fuera del ámbito de la norma aquellos datos que, en virtud de intereses público prevalentes, no deben estar sometidos a su régimen cautelar.

Los principios generales, por su parte, definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandado constitucional, se pretende limitar.

Por su parte, el principio de consentimiento, o de autodeterminación, otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita; sus contornos, por otro lado, se refuerzan singularmente en los denominados «datos sensibles», como pueden ser, de una parte, la ideología o creencias religiosas -cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2- y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece la prohibición de los ficheros creados

con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España .

Para la adecuada configuración, que esta Ley se propone, de la nueva garantía de la intimidad y del honor, resulta esencial la correcta regulación de la cesión de los datos almacenados. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el repetidamente aludido perfil personal, cuya obtención transgredería los límites de la privacidad. Para prevenir estos perturbadores efectos, la Ley completa el principio del consentimiento, exigiendo que, al procederse la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance. Sólo las previsiones del Convenio Europeo para la protección de los Derechos Fundamentales de la Persona - artículo 8.2- y del Convenio 108 del Consejo de Europa -artículo 9.2-, que se fundamentan en exigencias lógicas en toda sociedad democrática, constituyen excepciones a esta regla.

3. Las garantías de la persona son los nutrientes nucleares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de autodeterminación, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático.

En concreto, los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley. El primero de ellos ha cobrado en nuestro país, incluso, plasmación constitucional en lo que se refiere a los datos que obran en poder de las Administraciones Públicas (artículo 105.b). En consonancia con ello queda recogido en la Ley en términos rotundos, no previéndose más excepciones que las derivadas de la puesta en peligro de bienes jurídicos en lo relativo al acceso a los datos policiales y a los precisos para asegurar el cumplimiento de las obligaciones tributarias en lo referente a los datos de este carácter, excepciones ambas que pueden entenderse expresamente recogidas en el propio precepto constitucional antes citado, así como en el Convenio Europeo para la protección de los Derechos Fundamentales.

4. Para la articulación de los extremos concretos que han de regir los ficheros de datos, la parte especial de la Ley comienza distinguiendo, en su Título Cuarto, entre los distintos tipos de ficheros, según sea su titularidad pública o privada. Con la pretensión de evitar una perniciosa burocratización, la Ley ha desechado el establecimiento de supuestos como la autorización previa o la inscripción constitutiva en un registro.

Simultáneamente, ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que el de aquellos de titularidad pública. En efecto, en lo relativo a estos últimos, no basta la mera voluntad del responsable del fichero sino que es precisa norma habilitante, naturalmente pública y sometida al control jurisdiccional, para crearlos y explotarlos, siendo en estos supuestos el informe previo del órgano de tutela el cauce idóneo

para controlar la adecuación de la explotación a las exigencias legales y recomendar, en su caso, las medidas pertinentes.

Otras disposiciones de la parte especial que procede destacar son las atinentes a la transmisión internacional de los datos. En este punto, la Ley traspone la norma del artículo 12 del Convenio 108 del Consejo de Europa, apuntando así una solución para lo que ha dado en llamarse flujo transfronterizo de datos. La protección de la integridad de la información personal se concilia, de esta suerte, con el libre flujo de los datos, que constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la autorización de la Agencia cuando tal sistema no exista pero se ofrezcan garantías suficientes. Con ello no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias.

5. Para asegurar la máxima eficacia de sus disposiciones, la Ley encomienda el control de su aplicación a un órgano independiente, al que atribuye el estatuto de Ente público en los términos, del artículo 6.5 de la Ley General Presupuestaria . A tal efecto la Ley configura un órgano especializado, denominado Agencia de Protección de Datos, a cuyo frente sitúa un Director.

La Agencia se caracteriza por la absoluta independencia de su Director en el ejercicio de sus funciones, independencia que trae causa, en primer lugar, de un expreso imperativo legal, pero que se garantiza, en todo caso, mediante el establecimiento de un mandato fijo que sólo puede ser acortado por un numerus clausus de causas de cese.

La Agencia dispondrá, además, de un órgano de apoyo definido por los caracteres de colegiación y representatividad, en el que obtendrán presencia las Cámaras que representan a la soberanía nacional, las Administraciones Públicas en cuanto titulares de ficheros objeto de la presente Ley, el sector privado, las organizaciones de usuarios y consumidores y otras personas relacionadas con las diversas funciones que cumplen los archivos informatizados.

6. El inevitable desfase que las normas de derecho positivo ofrecen respecto de las transformaciones sociales es, si cabe, más acusado en este terreno, cuya evolución tecnológica es especialmente, dinámica. Ello hace aconsejable, a la hora de normar estos campos, acudir a mecanismos jurídicos dotados de menor nivel de vinculación, susceptibles de una elaboración o modificación más rápida de lo habitual y caracterizados por que es la voluntaria aceptación de sus destinatarios la que les otorga eficacia normativa. En esta línea la Ley recoge normas de autorregulación, compatibles con las recomendaciones de la Agencia, que evitan los inconvenientes derivados de la especial rigidez de la Ley Orgánica que, por su propia naturaleza, es inidónea para un acentuado casuismo. La propia experiencia de lo ocurrido con el Convenio del Consejo de Europa, que ha tenido que ser objeto de múltiples modificaciones al socaire de las distintas innovaciones tecnológicas, de las sucesivas y diferentes aplicaciones -estadística, Seguridad Social, relaciones de empleo, datos policiales, publicidad directa o tarjetas de crédito, entre otras- o de la ampliación de los campos de utilización -servicio telefónico o correo electrónico- aconseja recurrir a las citadas normas de autorregulación. De ahí que la Ley acuda a ellas para aplicar las previsiones legales a los distintos sectores de actividad. Tales normas serán elaboradas por iniciativa de

las asociaciones y organizaciones pertinentes y serán aprobadas, sin valor reglamentario, por la Agencia, siendo precisamente la iniciativa y participación de las entidades afectadas la garantía de la virtualidad de las normas.

7. La Ley no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento. Ello obedece a que se entiende que la sede lógica para tales menesteres no es esta Ley, sino sólo el Código Penal.

Sí se atribuye, sin embargo, a la Administración la potestad sancionadora que es lógico correlato de su función de inspección del uso de los ficheros, similar a las demás inspecciones administrativas, y que se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos, en cuyo caso procederá la oportuna responsabilidad disciplinaria, o sobre los privados, para cuyo supuesto se prevén sanciones pecuniarias.

De acuerdo con la práctica usual, la Ley se limita a tipificar, de conformidad con lo requerido por la jurisprudencia constitucional y ordinaria, unos supuestos genéricos de responsabilidad administrativa, recogiendo una gradación de infracciones que sigue la habitual distinción entre leves, graves y muy graves, y que toma como criterio básico el de los bienes jurídicos emanados. Las sanciones, a su vez, difieren según que los ficheros indebidamente utilizados sean públicos o privados: en el primero caso, procederá la responsabilidad disciplinaria, sin perjuicio de la intervención del Defensor del Pueblo; para el segundo, se prevén sanciones pecuniarias; en todo caso, se articula la posibilidad en los supuestos, constitutivos de infracción muy grave, de cesión ilícita de datos o de cualquier otro atentado contra los derechos de los afectados que revista gravedad, de inmovilizar los ficheros.

8. Finalmente, la Ley estipula un período transitorio que se justifica por la necesidad de ajustar la utilización de los ficheros existentes a las disposiciones legales.

Pasado este período transitorio, y una vez en vigor la Ley, podrá muy bien decirse, una vez más, que el desarrollo legislativo de un precepto constitucional se traduce en una protección reforzada de los derechos fundamentales del ciudadano. En este caso, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, se está estableciendo un nuevo y más consistente derecho a la privacidad de las personas.

TITULO I Disposiciones generales

Artículo 1. Objeto

La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Artículo 2.Ambito de aplicación.

1. La presente Ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación: a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.

b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales.

c) A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.

d) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.

e) A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

3. Se regirán por sus disposiciones específicas: a) Los ficheros regulados por la legislación de régimen electoral.

b) Los sometidos a la normativa sobre protección de materias clasificadas.

c) Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.

d) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36.

e) Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional.

Artículo 3. Definiciones

A los efectos de la presente Ley se entenderá por: a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero automatizado: Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable del fichero: Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

TITULO II Principios de la protección de datos

Artículo 4. Calidad de los datos

1. Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido.

En su clasificación sólo podrán utilizarse criterios que no se presten a prácticas ilícitas.

2. Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos.

3. Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 15.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos sus valores históricos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho de información en la recogida de datos.

1. Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

e) De la identidad y dirección del responsable del fichero.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Artículo 6. Consentimiento del afectado

1. El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos.

Artículo 7. Datos especialmente protegidos

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de un tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Artículo 8. Datos relativos a la salud

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril , General de Sanidad; 85.5, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y demás Leyes sanitarias.

Artículo 9. Seguridad de los datos

1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto

El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

Artículo 11. Cesión de datos

1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando una Ley prevea otra cosa.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tiene atribuidas.

e) Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad.

3. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente.

4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable.

5. El cesionario de los datos de carácter personal se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley.

6. Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

TITULO III Derechos de las personas

Artículo 12. Impugnación de valoraciones basadas exclusivamente en datos automatizados

El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Artículo 13. Derecho de información

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero. El Registro General será de consulta pública y gratuita.

Artículo 14. Derecho de acceso

1. El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados.

2. La información podrá consistir en la mera consulta de los ficheros por medio de su visualización, o en la comunicación de los datos pertinentes mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Artículo 15. Derecho de rectificación y cancelación

1. Por vía reglamentaria se establecerá el plazo en que el responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.

2. Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario.

4. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado.

Artículo 16. Procedimiento de acceso

1. El procedimiento para ejercitar el derecho de acceso, así como el de rectificación y cancelación será establecido reglamentariamente.

2. No se exigirá contraprestación alguna por la rectificación o cancelación de los datos de carácter personal inexactos.

Artículo 17. Tutela de los derechos y derecho de indemnización

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

3. Los afectados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

4. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

5. En el caso de los ficheros de titularidad privada la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TITULO IV Disposiciones sectoriales

CAPITULO I Ficheros de titularidad pública

Artículo 18. Creación, modificación o supresión

1. La creación, modificación o supresión de los ficheros automatizados de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de los ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal que, en su caso, se prevean.

f) Los órganos de la Administración responsables del fichero automatizado.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación y cancelación.

3. En las disposiciones que se dicten para la supresión de los ficheros automatizados se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 19. Cesión de datos entre Administraciones Públicas

1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso.

2. Podrán, en todo caso, ser objeto de cesión los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b) la cesión de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa.

Artículo 20. Ficheros de las Fuerzas y Cuerpos de Seguridad

1. Los ficheros automatizados creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento automatizado para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 21. Excepciones a los derechos de acceso, rectificación y cancelación

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o la cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores, podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros automatizados mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Artículo 22. Otras excepciones a los derechos de los afectados

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 14 y en el apartado 1 del artículo 15 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero automatizado invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPITULO II Ficheros de titularidad privada

Artículo 23. Creación

Podrán crearse ficheros automatizados de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 24. Notificación e inscripción registral

1. Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero automatizado si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 25. Comunicación de la cesión de datos

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando asimismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d) y e), y 6 del artículo 11 ni cuando la cesión venga impuesta por Ley.

Artículo 26. Datos sobre abonados a servicios de telecomunicación

Los números de los teléfonos y demás servicios de telecomunicación, junto con otros datos complementarios, podrán figurar en los repertorios de abonados de acceso al público, pero el afectado podrá exigir su exclusión.

Artículo 27. Prestación de servicios de tratamiento automatizado de datos de carácter personal

1. Quienes, por cuenta de terceros, presten servicios de tratamiento automatizado de datos de carácter personal no podrán aplicar o utilizar los obtenidos con fin distinto al que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación, a otras personas.

2. Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se prestan tales servicios, porque razonablemente se presuma la posibilidad de ulteriores

encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años.

Artículo 28. Prestación de servicios de información sobre solvencia patrimonial y crédito

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento. Podrán tratarse, igualmente, datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los afectados respecto de los que hayan registrado datos de carácter personal en ficheros automatizados, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

2. Cuando el afectado lo solicite, el responsable del fichero le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección del cesionario.

3. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los afectados y que no se refieran, cuando sean adversos, a más de seis años.

Artículo 29. Ficheros con fines de publicidad

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad o venta directa y otras actividades análogas, utilizarán listas tratadas automáticamente de nombres y direcciones u otros datos personales, cuando los mismos figuren en documentos accesibles al público o cuando hayan sido facilitados por los propios afectados u obtenidos con su consentimiento.

2. Los afectados tendrán derecho a conocer el origen de sus datos de carácter personal, así como a ser dados de baja de forma inmediata del fichero automatizado, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 30. Ficheros relativos a encuestas o investigaciones

1. Sólo se utilizarán de forma automatizada datos de carácter personal en las encuestas de opinión, trabajos de prospección de mercados, investigación científica o médica y actividades análogas, si el afectado hubiera prestado libremente su consentimiento a tal efecto.

2. Los datos de carácter personal tratados automáticamente con ocasión de tales actividades no podrán ser utilizados con finalidad distinta ni cedidos de forma que puedan ser puestos en relación con una persona concreta.

Artículo 31. Códigos tipo

1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo.

Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TITULO V Movimiento internacional de datos

Artículo 32. Norma general

No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

Artículo 33. Excepciones

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epidemiológica de enfermedades o brotes epidémicos.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

TITULO VI Agencia de Protección de Datos

Artículo 34. Naturaleza y régimen jurídico

1. Se crea la Agencia de Protección de Datos.

2. La Agencia de Protección de Datos es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio que será aprobado por el Gobierno, así como por aquellas disposiciones que le sean aplicables en virtud del artículo 6.5 de la Ley General Presupuestaria.

3. En el ejercicio de sus funciones públicas, y en defecto de lo que dispongan la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley de Procedimiento Administrativo. En sus adquisiciones patrimoniales y contratación estará sujeta al Derecho privado.

4. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones Públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

5. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos: a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

6. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 35. El Director

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1 a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo.

Artículo 36. Funciones

Son funciones de la Agencia de Protección de Datos: a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de los datos de carácter personal.

f) Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la presente Ley.

g) Ejercer la potestad sancionadora en los términos previstos por el título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros automatizados de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así

como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 45.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 37. Consejo consultivo

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros: Un Diputado, propuesto por el Congreso de los Diputados.

Un Senador, propuesto por la correspondiente Cámara.

Un representante de la Administración Central, designado por el Gobierno.

Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.

Un miembro de la Real Academia de la Historia, propuesto por la misma.

Un experto en la materia, propuesto por el Consejo Superior de Universidades.

Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.

Un representante de las Comunidades Autónomas, cuya propuesta se realizará a través del procedimiento que se establezca en las disposiciones de desarrollo de esta Ley.

Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 38. El Registro General de Protección de Datos

1. Se crea el Registro General de Protección de Datos como órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos: a) Los ficheros automatizados de que sean titulares las Administraciones Públicas.

b) Los ficheros automatizados de titularidad privada.

c) Las autorizaciones a que se refiere la presente Ley.

d) Los códigos tipo a que se refiere el artículo 31 de la presente Ley.

e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 39. Potestad de inspección

1. La Agencia de Protección de Datos podrá inspeccionar los ficheros a que hace referencia la presente Ley recabando cuantas informaciones precise para el cumplimiento de sus cometidos.

A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior, tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 40. Organos correspondientes de las Comunidades Autónomas

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 36, a excepción de las mencionadas en los apartados j), k) y l) y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, por los órganos correspondientes de cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 41. Ficheros de las Comunidades Autónomas en materias de su exclusiva competencia

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero automatizado de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia, podrá requerir a la Administración correspondiente para que adopte las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración Pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TITULO VII Infracciones y sanciones

Artículo 42. Responsables

1. Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45, apartado 2.

Artículo 43. Tipos de infracciones

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves: a) No proceder, de oficio o a solicitud de las personas o instituciones legalmente habilitadas para ello, a la rectificación o cancelación de los errores, lagunas o inexactitudes de carácter formal de los ficheros.

b) No cumplir las instrucciones dictadas por el Director de la Agencia de Protección de Datos, o no proporcionar la información que éste solicite en relación a aspectos no sustantivos de la protección de datos.

c) No conservar actualizados los datos de carácter personal que se mantengan en ficheros automatizados.

d) Cualquiera otra que afecte a cuestiones meramente formales o documentales y que no constituya infracción grave o muy grave.

3. Son infracciones graves: a) Proceder a la creación de ficheros automatizados de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o diario oficial correspondiente.

b) Proceder a la creación de ficheros automatizados de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible, o sin proporcionarles la información que señala el artículo 5 de la presente Ley.

d) Tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio del derecho de acceso y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto, cuando no constituya infracción muy grave.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria, se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

4. Son infracciones muy graves: a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar de forma automatizada los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar de forma automatizada los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos automatizados de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia, temporal o definitiva, de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar de forma automatizada los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7.

Artículo 44. Tipos de sanciones

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.001 pesetas a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.001 pesetas a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia.

5. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 45. Infracciones de las Administraciones Públicas

1. Cuando las infracciones a que se refiere el artículo 43 fuesen cometidas en ficheros de los que sean responsables las Administraciones Públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 46. Prescripción

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causa no imputable al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquél en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 47. Procedimiento sancionador

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Contra las resoluciones de la Agencia de Protección de Datos, u órgano correspondiente de la Comunidad Autónoma, procederá recurso contencioso-administrativo.

Artículo 48. Potestad de inmovilización de ficheros

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros automatizados de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros automatizados a los solos efectos de restaurar los derechos de las personas afectadas.

DISPOSICIONES ADICIONALES

Primera.-Exclusión de la aplicación de los Títulos VI y VII.

Lo dispuesto en los Títulos VI y VII no es de aplicación a los ficheros automatizados de los que sean titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional.

Segunda.-Ficheros existentes con anterioridad a la entrada en vigor de la Ley.

1. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica deberán ser comunicados a la Agencia de Protección de Datos los ficheros y tratamientos automatizados de datos de carácter personal existentes con anterioridad y comprendidos dentro de su ámbito de aplicación.

2. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica, las Administraciones Públicas responsables de ficheros automatizados ya existentes deberán adoptar una disposición de regulación del fichero o adaptar la que existiera.

Tercera.-Competencias del Defensor del Pueblo.

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

DISPOSICION TRANSITORIA

Unica.-Adaptaciones complejas a lo establecido en la Ley.

Cuando la adaptación de los ficheros automatizados a los principios y derechos establecidos en la presente Ley requiera la adopción de medidas técnicas complejas o el tratamiento de un gran volumen de datos, tales adaptaciones y tratamientos deberán realizarse en el plazo de un año desde la entrada en vigor de la Ley, sin perjuicio del cumplimiento, en todo lo demás, de las disposiciones de la misma.

DISPOSICION DEROGATORIA

Unica.-Derogación de la disposición transitoria primera de la Ley Orgánica 1/1982.

Queda derogada la disposición transitoria primera de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

DISPOSICIONES FINALES

Primera.-Habilitación de desarrollo reglamentario.

El Gobierno dictará las disposiciones necesarias para la aplicación y desarrollo de la presente Ley, y para regular la estructura orgánica de la Agencia de Protección de Datos.

Segunda.-Extensión de la aplicación de la Ley a ficheros convencionales.

El Gobierno, previo informe del Director de la Agencia de Protección de Datos, podrá extender la aplicación de la presente Ley, con las modificaciones y adaptaciones que fuesen necesarias, a los ficheros que contengan datos almacenados en forma convencional y que no hayan sido sometidos todavía o no estén destinados a ser sometidos a tratamiento automatizado.

Tercera.-Preceptos con carácter de Ley ordinaria.

Los artículos 18, 19, 23, 26, 27, 28, 29, 30, 31, los Títulos VI y VII, las disposiciones adicionales primera y segunda y la disposición final primera tienen carácter de Ley ordinaria.

Anexo Número Siete:

PROYECTO DE LEY ORGÁNICA POR LA QUE SE MODIFICA LA LEY ORGÁNICA 5/1992, DE 29 DE OCTUBRE, DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL.-

EXPOSICIÓN DE MOTIVOS

La presente Ley tiene por objeto la adaptación del Derecho español a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Y para ello se procede a introducir en la normativa española reguladora de la materia, contenida en la Ley Orgánica 5/1992, de 29 de octubre, las modificaciones que vienen reclamadas por el contenido de la referida Directiva, a fin de que el conjunto normativo resultante se adapte y acomode a las exigencias de homogeneidad dispositiva establecidas por la Unión Europea.

En el momento de promulgarse la Ley Orgánica 5/1992, de 29 de octubre, que ahora es objeto de modificación, estaba en trámites de discusión y elaboración la Directiva que se transpone, por lo que los contenidos normativos de lo que en aquel tiempo era una mera propuesta se tuvieron en cuenta por el legislador español para dar respuesta a la

problemática derivada de la protección de la intimidad en el tratamiento de datos personales. Ello significa que la mencionada Ley Orgánica 5/1992, se ajusta en la gran mayoría de sus previsiones a las disposiciones contenidas en la Directiva 95/46/CE, siendo necesario únicamente introducir en aquélla las precisas reformas que den como resultado la total adecuación entre dicha Ley y la Directiva comunitaria.

Ahora bien, las modificaciones legislativas que para la necesaria adecuación a la Directiva se introducen en la Ley vigente, no por aparentemente exiguas carecen de una singular relevancia, pues en definitiva afectan a aspectos tan importantes como los siguientes: Se amplía el ámbito de aplicación de la Ley, si bien se mantienen determinados supuestos en que no es de aplicación el régimen de protección de datos establecido en la misma; se incrementa la protección de los afectados, tanto en lo que respecta a su necesaria información en la obtención de los datos como en la constante presencia de su consentimiento en el tratamiento y cesión de sus datos personales; se incorpora el derecho del afectado de oponerse al tratamiento de sus datos en determinados supuestos; se prevén nuevos supuestos de excepción en las transferencias internacionales de datos; y se aplican a los ficheros convencionales o no automatizados las disposiciones de la Ley reguladora del tratamiento de datos.

Artículo único.- **Modificación de la Ley Orgánica 5/1992.**

Los artículos que a continuación se relacionan de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, quedan modificados en los términos siguientes:

Uno. En el artículo 1 se sustituye la expresión "tratamiento automatizado de datos de carácter personal" por "tratamiento de datos de carácter personal".

Dos. El apartado 2 del artículo 2 queda redactado de la forma siguiente:

"El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c) A los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional."

d) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Tres. El apartado 3 del artículo 2 queda redactado de la forma siguiente:

"3. Se regirán por sus disposiciones específicas:

a) Los ficheros regulados por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo de la función estadística pública, sin perjuicio de lo dispuesto en el artículo 36."

Cuatro. Se adicionan al artículo 3 las letras g) y h) con el siguiente contenido:

"g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del fichero.

h) Consentimiento del afectado: Toda manifestación de voluntad, libre, específica e informada, mediante la que el afectado consienta el tratamiento de datos personales que le conciernan."

Cinco. El párrafo primero del apartado 1 del artículo 4 queda redactado de la forma siguiente:

"Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."

Seis. El apartado 2 del artículo 4 queda redactado de la forma siguiente:

"Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos, salvo que el tratamiento posterior de éstos lo sea con fines históricos, estadísticos o científicos."

Siete. El párrafo tercero del apartado 5 del artículo 4 queda redactado de la forma siguiente:

"Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos."

Ocho. La letra e) del apartado 1 del artículo 5 queda redactada de la forma siguiente:

"De la identidad y dirección del responsable del fichero, o, en su caso, de su representante.

Cuando el responsable del fichero no esté establecido en el territorio de la Unión Europea y utilice, en el tratamiento de datos, medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento."

Nueve. El apartado 3 del artículo 5 queda redactado de la forma siguiente:

"No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban."

Diez. Se adicionan al artículo 5 los siguientes apartados 4 y 5:

"4. Cuando los datos de carácter personal no hayan sido recabados del afectado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguiente al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido de los datos, de su procedencia así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando el tratamiento de datos esté expresamente previsto en una Ley, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al afectado resulte imposible o exija esfuerzos desproporcionados a criterio de la Agencia de Protección de Datos, en consideración al número de afectados, a la antigüedad de los datos y a las posibles medidas compensatorias."

Once. El apartado 1 del artículo 6 queda redactado de la forma siguiente:

"El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa."

Doce. El apartado 2 del artículo 6 queda redactado de la forma siguiente:

"No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del afectado; o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos."

Trece. Se adiciona un apartado 4 al artículo 6, con el contenido siguiente:

"4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado."

Catorce. El apartado 2 del artículo 7 queda redactado de la forma siguiente:

"Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado."

Quince. El apartado 4 del artículo 7 queda redactado de la forma siguiente:

"Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o vida sexual."

Dieciséis. Se adiciona un apartado 6 al artículo 7 con el siguiente contenido:

"No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento automatizado los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento automatizado los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento."

Diecisiete. En el apartado 1 del artículo 9 se sustituye la expresión "El responsable del fichero deberá adoptar" por la de "El responsable del fichero y, en su caso, el encargado del tratamiento, deberá adoptar."

Dieciocho. La letra d) del apartado 2 del artículo 11 queda redactada de la forma siguiente:

"Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas."

Diecinueve. Se adiciona un segundo inciso al artículo 12 con el siguiente contenido:

"En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre la lógica utilizada en los tratamientos de datos referidos a aquél."

Veinte. El apartado 1 del artículo 14 queda redactado de la forma siguiente:

"El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados, así como sobre el origen de dichos datos."

Veintiuno. El apartado 2 del artículo 15 queda redactado de la forma siguiente:

"Serán rectificados y cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y en particular cuando tales datos resulten inexactos o incompletos."

Veintidós. El apartado 1 del artículo 19 queda redactado de la forma siguiente:

"Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la cesión hubiere sido prevista por las disposiciones de creación del fichero o por disposición posterior de superior rango que regule su uso o cuando la cesión tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos."

Veintitrés. El apartado 3 del artículo 20 queda redactado de la forma siguiente:

"La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales."

Veinticuatro. En el apartado 1 del artículo 22 se suprime la expresión "o dificulte gravemente".

Veinticinco. El apartado 1 del artículo 29 queda redactado de la forma siguiente:

"Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad o venta directa y otras actividades análogas utilizarán listas tratadas automáticamente de nombres y direcciones u otros datos personales, cuando los mismos hayan sido facilitados por los propios afectados u obtenidos con su consentimiento o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos."

Veintiséis. Se adiciona un artículo 30 bis con el siguiente contenido:

"Artículo 30 bis. Tratamientos destinados a la prospección.

En los supuestos de tratamientos de datos de carácter personal destinados a la prospección, los afectados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, así como a ser informados por el responsable del fichero, antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se les ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización."

Veintisiete. La letra c) del artículo 33 queda redactado de la forma siguiente:

"Cuando la transferencia sea necesaria para la salvaguarda del interés vital del afectado."

Veintiocho. Se adicionan al artículo 33 las letras e), f), g), h), i), j) y k), con el siguiente contenido:

"e) Cuando el afectado haya dado su consentimiento inequívocamente a la transferencia prevista.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público importante. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea."

Veintinueve. El apartado 1 del artículo 42 queda redactado de la forma siguiente:

"Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."

Treinta. La Disposición final segunda queda redactada de la forma siguiente:

"Las disposiciones de la presente Ley se aplicarán a los tratamientos no automatizados de datos de carácter personal contenidos o destinados a ser contenidos en un fichero. Quedan excluidas a estos efectos las carpetas que no estén estructuradas".

Disposición adicional única.- **Ficheros preexistentes**

Los ficheros y tratamientos automatizados que, como consecuencia de las modificaciones introducidas en la Ley Orgánica 5/1992, de 29 de octubre, quedan incluídos en el ámbito de aplicación de ésta, deberán ajustarse a la misma dentro del plazo de tres años, a contar desde la entrada en vigor de la presente Ley Orgánica. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones Públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la Ley Orgánica 5/1992, de 29 de octubre y la obligación prevista en el párrafo anterior deberá cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados".

Disposición final primera.- Carácter de la Ley

Los apartados veintidós, veinticinco, veintiséis y veintinueve del artículo único y la disposición adicional única tienen carácter de Ley ordinaria.

Disposición final segunda.- **Entrada en vigor**

La presente Ley Orgánica entrará en vigor al mes de su publicación en el Boletín Oficial del Estado.

ELÉVESE AL CONSEJO DE MINISTROS

LA MINISTRA DE JUSTICIA

Margarita Mariscal de Gante y Mirón.