Protección de datos personales y derecho a la autodeterminación informativa: Régimen jurídico

The allegation and proof of foreign law in Spain after the new international legal cooperation act

May Rubby Pérez Martínez
May.pmartinez@gmail.com
Maestría en Derecho de Empresa. Universidad Centroamericana, Nicaragua

https://doi.org/10.5377/derecho.v0i28.10146

Fecha de recibido: mayo de 2020 / Fecha de aprobación: junio de 2020

Resumen

Dentro del Ordenamiento Jurídico Nicaragüense se encuentra vigente la Ley No. 787, Ley de Protección de Datos Personales, y el Decreto 36-2012, "Reglamento de la Ley No. 787 "Ley de Protección de Datos Personales", que persiguen la tutela de los datos personales como preocupación central para mantener la competitivdad del país en las diversas relaciones comerciales que se realizan día a día. Con este artículo lo que se pretende es conocer los aspectos fundamentales y vacíos de la legislación, asimismo, nos permitirá reconocer la importancia que tiene la protección de los datos personales, el ejercicio del derecho a la autodeterminación informativa entendido como derecho fundamental y autónomo consagrado en la Constitución Política de Nicaragua, el aviso informativo y la obtención del consentimiento, como elementos esenciales y requisitos formales en el tratamiento de los datos personales contenidos en la Legislación de la materia. De tal forma que podremos determinar los derechos de los titulares y las obligaciones de los responsables de los ficheros de datos derivadas del tratamiento de los datos personales, permitiendo al titular de los datos ejercitar los derechos Arco (derecho de acceso, rectificación, cancelación y oposición) como una forma de garantizar y controlar el uso de la información brindada al empresario.

Palabras Clave

Datos personales / tratamiento / autodeterminación informativa / consentimiento / responsable de los ficheros de datos

Abstract

The Law No. 787, Law of Protection of Personal Data and Decree 36-2012, "Regulation of Law No. 787" Law of Protection of Personal Data ", which pursue the protection of citizens, are in force within the Nicaraguan legal system. Personal data as a central concern to maintain the competitiveness of the country in the various commercial relations that are carried out day by day. With this article, what is intended is to know the fundamental and empty aspects of the legislation, it will also allow us to recognize the importance of the protection of personal data, the exercise of the right to self-determination information as a fundamental and autonomous right enshrined in The Political Constitution of Nicaragua, information notice and obtaining consent, as essential elements and formal requirements in the treatment of personal data contained in the legislation of the matter. So that we can determine the rights of the owners and the obligations of those responsible for the data files derived from the processing of personal data, allowing the data subject to exercise the rights Arco (right of access, rectification, cancellation and opposition). As a way to guarantee and control the use of the information provided to the entrepreneur.

Key words

Personal data / treatment / informational self-determination / consent / responsible for the data files

Tabla de contenido

1. **Consideraciones previas** 1.1 *Marco normativo de la protección de datos en Nicaragua 1.2 Conceptos básicos 1.2.1 Sujetos intervinientes 1.2.2 Datos personales 1.2.3 Ficheros de datos y tratamiento 1.2.3.1 Fichero de Titularidad Pública 1.2.3.2 Ficheros de Titularidad Privada 1.3 Principios. 1.3.1 Calidad de Datos 1.3.2 Consentimiento Informado 1.5.3 Seguridad de datos* **2. El Derecho a la autodeterminación informativa** *2. 1 Contenido 2.2 Derechos Arco 2.2.1 Condiciones Generales del ejercicio de los derechos Arco 2.2.2 Medios para acceder y procedimiento 2.2.3 Derecho de Acceso 2.2.4 Derecho de Rectificación 2.2.5 Derecho de Cancelación 2.2.6 Derecho de Oposición* **3. Obligaciones del empresario** 3*.1 Aviso de informativo 3.2. Consentimiento 3.2.1 Tipos de consentimiento 3.3 Obligaciones previas al tratamiento de los datos personales 3.4 Obligaciones durante el tratamiento de los datos personales 3.5 Obligaciones posteriores al tratamiento de los datos personales* **4. Conclusiones. Lista de Referencias**.

Introducción.

Los datos personales y su protección están inmersos en la diversidad de relaciones que día a día surgen, entre personas naturales, jurídicas y/o la administración pública. Debido a que el flujo de información en el tráfico de bienes y servicios es uno de los elementos primordiales para realizar las distintas actividades, desde adquirir un servicio básico hasta solicitar atención médica, así como contratar un crédito o comprar algún bien mueble o inmueble.

De este modo, el avance tecnológico, la rapidez y efectividad con la que se realizan las relaciones comerciales hoy día, hace indispensable que exista de parte del Estado, la promulgación y aprobación de leyes que protejan los intereses superiores de los sujetos intervinientes, debido a los riesgos que pueden surgir con el tratamiento de los datos personales.

Por ello, esta investigación, se divide en tres capítulos que comparten un escenario en común, como lo es la protección de los datos personales de los titulares y el derecho a la autodeterminación informativa, de tal forma que se pueda conocer y entender el alcance que actualmente dispone el ordenamiento jurídico ante esta temática, las fortalezas y limitantes que tiene, así como determinar los derechos de los titulares y las obligaciones que nacen para el empresario en virtud del tratamiento de los datos personales.

En el primer capítulo se abordará el marco normativo vigente en la protección de datos personales, se definirán los principales conceptos que abarcan esta temática y los principios bajo los cuales se rige el tratamiento de los datos personales.

En el segundo capítulo se desarrollará el derecho a la autodeterminación informativa, como derecho fundamental que da lugar a exigir ante los responsables de los ficheros (públicos y privados), la tutela de los derechos de los titulares de los datos, siendo una de las principales obligaciones que el empresario debe resguardar, sobre todo los derechos Arco.

En el tercer capítulo haremos referencia a la creación del aviso informativo y la obtención del consentimiento como elementos configuradores que se deben priorizar en el tratamiento de los datos personales, estableciendo de manera enunciativa las obligaciones que debe cumplir el empresario en el tratamiento de los datos personales, señalando como recomendación la autorregulación de parte del empresario frente a esta temática.

Asimismo, la presente investigación, se realizará bajo el método de análisis – síntesis, y de la lectura de la normativa vigente, legislación comparada como lo es la legislación de Costa Rica, México y España, la doctrina y jurisprudencia (Colombiana, Española, Salvadoreña y Costarricense), de forma tal que permitirá establecer los lineamientos básicos sobre la creación, modificación, funcionamiento y extinción de los datos personales recogidos en los ficheros de datos, el derecho a la autodeterminación informativa, la elaboración del aviso informativo, la obtención del consentimiento y la forma de ejercicios de los derechos ARCO como una obligación del empresario frente al tratamiento de los datos personales.

Hoy día la difusión de los datos comerciales y la pérdida de control de la información que ha sido suministrada por el titular de los datos, implica que el empresario emplee estrategias y medios para el cumplimiento de dichas normativas, que permitan al titular de los datos ejercitar los derechos Arco como una forma de garantizar la privacidad de la información brindada, así como los mecanismos de defensa cuando consideren que su derecho a la autodeterminación informativa ha sido violentado de parte del responsable de los ficheros.

1. Consideraciones previas

En un mundo globalizado donde la circulación de la riqueza va de la mano con el avance social y tecnológico, implica garantizar al individuo la salvaguarda de intereses superiores y el reconocimiento de derechos fundamentales, como lo es la vida personal, privada, familiar, que se materializa al ser parte interviniente en el tráfico de bienes y servicios, siendo de suma importancia asegurar la privacidad de los datos que el individuo exterioriza y sobre todo resguardar su identidad, bajo la premisa de que el uso de sus datos pueda desarrollarse de forma adecuada y dentro de los límites que para tal fin el ordenamiento jurídico dispone.

Actualmente nos encontramos en la sociedad de la información donde el tratamiento masivo de datos personales en el desarrollo de las relaciones comerciales, no sólo implica la facilidad de proveer información, sino, el riesgo de ser afectado por la mala utilización o el uso ilegítimo de estas, aunado a ello, el desconocimiento del usuario (titular de los datos) de los derechos que ostenta al proporcionar sus datos y de obligaciones las empresas (responsables de los ficheros) en la recopilación y utilización de los mismos.

Por ello, hoy por hoy, surgen diversidades de conflictos con nuestro datos personales, recibimos correos o llamadas de diversas empresas o casas comerciales, ofreciendo algún producto o servicio, sin siquiera saber cómo obtuvieron nuestros datos y desconocemos que garantías tenemos para cancelarlos o para revocar nuestro consentimiento, asimismo, firmamos contratos y aceptamos todos los términos y

condiciones, sin dedicarle tiempo a leer el aviso informativo, política de privacidad o de confidencialidad donde entenderíamos el alcance del uso de nuestro datos personales proporcionados.

Es importante señalar que los datos personales han adquirido un valor añadido para los negocios, bajo esa línea Valerio (2008, p. 32) señala que "La sociedad percibe el valor que tienen sus datos personales, y por tanto, la protección de los mismos por parte de las empresas supone un plus de calidad que el cliente percibe".

Siguiendo esa línea de pensamiento Tapia Sánchez (2016) expresa que para los consumidores existe diversidad de riesgos, al facilitar su información personal cuando requieren de los servicios de empresas del sector comercial o financiero, ya sea en la venta de un producto o un servicio. Además, las mismas empresas corren riesgos en la información que estos pueden facilitar y en cuyo caso pueden ser víctimas de hackers o crackers.

Asimismo, este autor señala que "al no brindar seguridad en la información personal de sus clientes, las mismas empresas tienen efectos adversos y/o concomitantes, lo que repercute en su reputación vinculada a la competitividad y rentabilidad en el mercado." (2016, p. 35).

Debemos concluir que el titular de los derechos desconoce de los riesgos que corre al facilitar sus datos, y no es necesariamente por un tema de desprotección o desregulación, sino que, es difícil que el mismo cliente conozca para qué y cómo serán utilizados los datos que ha proporcionado, si serán transferidos a terceros o no. Por ello, no podemos olvidar que la información que facilitamos nos identifica como persona titular de derechos y obligaciones, y es y debe ser personal.

1.1 Marco normativo de la protección de datos en Nicaragua.

Hoy día, en materia de protección de datos personales, Nicaragua dispone de un marco normativo que despliega su regulación desde el ámbito constitucional, en materia penal, civil, constitucional, hasta la aprobación y entrada en vigencia de la normativa especial.

En este sentido, a priori podemos destacar que en el ordenamiento jurídico nicaragüense se vislumbra como primer punto de referencia la Constitución Política de Nicaragua que desde el año de 1987 en el artículo 26 regulaba como derecho de toda persona: 1) A su vida privada y a la de su familia; 2) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones y 3) Al respeto de su honra y reputación.

Con la reforma del año de 1995, se adiciona a este artículo 26, el numeral 4 el cual introduce y establece el derecho de la persona "a conocer toda la información que haya registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información". No obstante, esta reforma limitó este derecho a un ámbito de aplicación únicamente estatal, es decir, a las instituciones del Estado.

En el año 2007, se aprobó la Ley No. 621, "Ley de Acceso a la Información Pública", la cual tiene por objeto normar, garantizar y promover el ejercicio del derecho de acceso que tiene toda persona para acceder a la información pública existente en los documentos, archivos y bases de datos de las entidades o instituciones públicas y otras que la misma norma establece (Art. 1), y en la misma se empieza a definir conceptos

tales como archivos, bases de datos, registro, información pública y privada, entre otros (Art. 4).

Siendo en el año 2012, la aprobación de la Ley No. 787, "Ley de Protección de Datos Personales", y del Decreto No. 36-2012, Reglamento de la Ley No. 787, "Ley de Protección de Datos Personales", con el objetivo de mantener un equilibrio con la Ley No. 621, "Ley de Acceso a la Información Pública", propiciar la implementación de las garantías que se establece en el artículo 26 de la Constitución Política de la República de Nicaragua y mantener la competitividad del país en actividades comerciales donde el tema central sea la protección de datos personales.

Posteriormente, en el año 2014, la Constitución Política sufre una última reforma, la cual introdujo un cambio importante en el tema de la protección de datos personales, al adicionar al artículo 26 el ámbito de aplicación correspondía tanto a entidades públicas como privadas. El cual hoy día en sus partes conducentes establece lo siguiente:

> **Art. 26** Toda persona tiene derecho:
> 1) A su vida privada y a la de su familia.
> 2) Al respeto de su honra y reputación.
> **3) A conocer toda información que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene esa información**. (la negrita es de la autora)
> 4) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.

Finalmente, en el año 2018 se aprueba La Ley No. 983, Ley de Justicia Constitucional, mediante la cual se introduce la regulación del recurso de habeas data como garantía de tutela de datos personales asentado en cualquier tipo de soporte de índole pública o privada.

Así pues, la Ley No. 787 se ordena en 56 artículos estructurados en nueve capítulos. Y su reglamento el Decreto No. 36-2012, se ordena en 63 artículos estructurados en nueve capítulos.

Ahora bien, cuando nos referimos al tema de la protección datos personales debemos partir de del objeto y ámbito de aplicación de la Ley No. 787, en este sentido su objeto es la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados (ámbito de aplicación), a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa (arts. 1 y 3).

Bajo estas disposiciones se desprenden ideas importantes que serán abordadas en el desarrollo de este estudio. Primero, el sujeto puede ser tanto una persona natural o jurídica, de igual forma que lo será el responsable de los ficheros de datos.

Segundo, los datos pueden ser automatizados o no en ficheros de datos, ya sea que estos sean de índole pública o privada, pudiendo ser registrados en soportes físicos o electrónicos que hagan posible el acceso a los datos personales con arreglo a criterios

determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Y tercero, se debe garantizar el derecho a la autodeterminación informativa, como pilar fundamental para ejercitar los derechos y mecanismos que toda la legislación provee cuando se considera que una persona ha rebasado los límites de actuación sobre este derecho.

Es dable destacar, que durante este estudio no serán abordados los ficheros de que corresponden a las Instituciones de la SIBOIF y CONAMI, las cuales por disposición del artículo 54 de la Ley No. 787 se considera materia excluida de aplicación de la Ley. Todo lo anterior es sin perjuicio de los principios generales, los derechos de los titulares de datos, así como las limitaciones establecidas en la Ley.

1.2 Conceptos básicos

1.2.1 Sujetos intervinientes

La Ley No. 787 reconoce como titular de los datos a toda persona natural o jurídica a la que conciernen los datos personales. (Art. 3 inc. m, Ley No. 787). Por su parte, se le conoce como responsable de ficheros de datos, a toda persona natural o jurídica, pública o privada, que conforme Ley decide sobre la finalidad y contenido del tratamiento de los datos personales. (Art. 3 inc. k, Ley No. 787).

Finalmente se reconoce la existencia de un tercero como aquella persona, pública o privada que realice a su arbitrio el tratamiento de datos personales, ya sea en ficheros de datos propios o a través de conexión con los mismos. (Art. 3 inc. l, Ley No. 787).

1.2.2 Datos personales

La Ley No. 787, en su artículo 3 literal e, define a los Datos Personales como "toda la información sobre una persona natural o jurídica que la identifica o la hace identificable."

Estos datos personales se clasifican en 4 categorías:

1. **Datos Personales Sensibles**: sólo pueden ser obtenidos y tratados por razones de interés general en la Ley, o con el consentimiento del titular de datos, u ordenados por mandato judicial. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Los datos personales relativos a los antecedentes penales o faltas administrativas sólo pueden ser tratados por las autoridades públicas competentes, en la esfera de sus competencias (Art. 8 inc. a, Ley No. 787).

2. **Datos personales relativos a la salud y actividades conexas a la salud**: Los datos personales relativos a la salud, en los hospitales, clínicas, centros y puestos de salud, públicos y privados, y los profesionales vinculados a las ciencias de la salud: sólo pueden ser aquellos respecto a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando el secreto profesional (Art. 8 inc. b, Ley No. 787).

3. **Datos Personales Informáticos**: Son los datos personales tratados a través de medios electrónicos o automatizados. (Art. 8 inc. c, Ley No. 787).

4. **Datos Personales Comerciales:** Son los datos sensibles de las Empresas las bases de datos de clientes, proveedores y recursos humanos, para fines de publicidad y cualesquiera otros datos que se consideren información comercial o empresarial reservada fundamentalmente para el libre ejercicio de sus actividades económicas. (Art. 8 inc. d, Ley No. 787).

Respecto al concepto de "Dato" La Corte Constitucional de Colombia en su sentencia No. T-414/92 cita al Experto Ernesto Lleras quien señala:

> El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos.

Al respecto el artículo 4 numeral VI de la Ley Federal de Protección de Datos Personales en posesión de los particulares de México establece que estos datos son aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

1.2.3 Ficheros de datos y tratamiento

La Ley No. 787 define a los ficheros de datos como los archivos, registros, bases o bancos de datos, públicos y privados, que contienen de manera organizada los datos personales, automatizados o no (Art. 3 lit. i), es decir, que son el soporte o base de datos sea este de indole pública o privada donde se recopilan y registran los datos personales obtenidos del titular.

Respecto al tratamiento de los datos personales estos son definidos como las operaciones y procedimientos sistemáticos, automatizados o no, que permiten la recopilación, registro, grabación, conservación, ordenación, almacenamiento, modificación, actualización, evaluación, bloqueo, destrucción, supresión, utilización y cancelación, así como la cesión de datos personales que resulten de comunicaciones, consultas, interconexiones y transferencias. (Art. 3 lit. n. Ley No. 787).

Asimismo, el artículo 9 de la Ley No. 787, establece que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas en la Ley, y señala:

> Los datos personales sólo podrán ser tratados, cuando sean adecuados, proporcionales y necesarios en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan solicitado. Los derechos de oposición, acceso, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación de los datos tratados se ejercerán mediante comunicación por escrito.

> Ninguna persona que solicite la prestación o adquisición de bienes y servicios está obligada a brindar a las instituciones públicas y privadas, mayor información o datos personales que aquellos que sean adecuados, proporcionales y necesarios para la prestación de los mismos.
>
> El tratamiento de los datos personales del usuario o comprador debe tener como finalidad facilitar la mejora, ampliación, venta, facturación, gestión, prestación del servicio y adquisición de bienes.
>
> El responsable del fichero y en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su acceso, uso, alteración, pérdida, revelación, transferencia o divulgación no autorizada.

Como señala Garriga Domínguez (2016), tanto la definición legal de fichero como el tratamiento de los datos personales no debe entenderse como "un simple depósito de datos, sino como el conjunto de procesos y aplicaciones informáticas que se llevan a cabo con los datos registrados, susceptibles en caso de interrelación, de configurar el perfil de una persona" (pp. 168-169).

En este sentido, la aplicación de ambos conceptos nos permite entender por una parte, que además del cumplimiento de las prerrogativas que para ello dispone la legislación, deben identificar o hacer identificable a una persona, ya sea esta persona natural o jurídica, es decir, que la información facilitada permita relacionar a una persona física concreta, en un determinado lugar y condición, y por otra parte, que dichos ficheros (cualquiera que sea su naturaleza) y su tratamiento estén estructurados y organizados ya sea automatizados o no, de forma que puedan accederse a ellos fácilmente.

Por otra parte, a pesar de que la Ley No. 787 no tiene un tratamiento diferenciado respecto a los ficheros de titularidad pública y privada establece una regulación particular respecto tres aspectos que señalaremos a continuación, no obstante, dicho tratamiento hoy día es inaplicable por la inexistencia de la Autoridad competente:

a. Disposiciones comunes para su creación, modificación y extinción (Art. 23 de la Ley No. 787):

Al respecto y como norma general el párrafo segundo del artículo 23 de la Ley No. 787 dispone que los Ficheros de datos públicos y privados deberán estar estructurados y organizados de forma tal que en ellos pueda avizorarse, primero las características y finalidad del fichero de datos; segundo, las personas respecto de las cuales se pretenda obtener datos y tercero el carácter facultativo u obligatorio de su suministro por parte de aquéllas. En este punto es importante señalar que estas disposiciones generales, tendrán relación con el aviso informativo que deberá crear el responsable de los ficheros cuando desee realizar el tratamiento de los datos personales del titular, tal y como se desarrollará en el capítulo tercero.

Ya que tal y como prescribe el artículo 9 párrafo tercero de la Ley No. 787 la finalidad del tratamiento de los datos es facilitar la mejora, ampliación, venta, facturación, gestión, prestación de los servicios y adquisición de bienes

b. Obligatoriedad de la inscripción ante en el registro de ficheros de datos (Arts. 22 y 40 de la Ley No.787):

La inscripción se realiza ante el Registro de ficheros de datos que para tal efecto cree de la Dirección de Protección de Datos Personales (DIPRODAP), quien emitirá su resolución en el término de treinta días (art. 22 Ley No. 787), en la cual se debe recabar la siguiente información:

> a) Nombre y domicilio del responsable, ya sea persona natural o jurídica con toda la descripción de la razón social, fecha de constitución, objeto y representante legal;
> b) Naturaleza de los datos personales contenidos en cada fichero de datos;
> c) Forma, tiempo y lugar de recolección y actualización de datos;
> d) Destino de los datos y personas naturales o jurídicas a las que pueden ser transmitidos;
> e) Modo de interrelacionar la información registrada;
> f) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar nombre y domicilio de las personas que intervienen en la colecta y tratamiento de los datos;
> g) Tiempo de conservación de los datos; y
> h) Forma y procedimientos en que las personas pueden acceder a los ficheros de datos personales para realizar la rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los mismos según concierna.

Respecto al tema de la inscripción quisiéramos puntualizar que la Ley No. 787, establece en su artículo 53 una vez que haya trascurridos seis meses desde la publicación de la Ley No. 787 y su decreto, los responsables de los ficheros de datos tienen la obligación de inscribirse en el registro de ficheros de datos, no obstante, dicha obligación dista de la realidad por cuanto el recurso institucional DIPRODAP no existe, por lo que esta es una de las debilidades de nuestra legislación, desde el punto vista de la falta de eficacia de la norma, lo que no quiere decir que no puedan llevarse a cabo el tratamiento de datos personales o que el mal actuar del responsable del fichero de los datos quedará impune o que los derechos de los titulares serán transgredidos sin ninguna garantía de restitución.

c. Procedimientos de inspección (Arts. 31-33 Ley No. 787 y Arts. 49 -55 Decreto 36-2012).

Este procedimiento puede ser solicitado de oficio o a petición de parte ante la DIPRODAP, quien nombrará un inspector. Las inspecciones son actividades de visita, verificación y control, mediante las cuales los inspectores debidamente identificados, están facultados para revisar los ficheros de datos de acuerdo al programa de visitas con el objetivo de establecer el grado de cumplimiento de las normas regulatorias o de brindar a las autoridades de la Dirección de Protección de Datos Personales mayores elementos de juicio para la adopción de una resolución con afectación a terceros o no. El inspector levantará la correspondiente acta.

Por otra parte, es menester desctacar que la Ley No. 787 y el Decreto No. 36-2012, no establecen ninguna definición para cada figura, es decir, frente a los ficheros de titularidad pública y de titularidad privada, ni dispone de ningún tipo de regulación específica y diferenciadora para su creación, modificación, actualización, extinción y procedimiento sancionador. Es allí donde encontramos unos de los vacíos en nuestra legislación nacional.

No obstante, es de nuestra consideración que ante la evidente falta de regulación deberá atenderse a las normas mínimas establecidas en la Ley. No. 787 y el Decreto No. 36-2012, los que deberán armonizarse para su creación según el giro de cada responsable de fichero de datos, sea institución pública o empresa privada, y deberán garantizar las medidas de seguridad pertinentes, cumplir con los principios de calidad de datos, consentimiento informado, así como el derecho a la autodeterminación informativa y derechos Arco. Es decir, que toda creación, modificación, actualización, extinción no deberán atentar contra la ley, la moral y el orden público.

1.2.3.1 Fichero de Titularidad Pública

Para Pineda Quinteros (2007), "los bancos de datos públicos comprenden el registro de la información que hace una dependencia del Estado en el cumplimiento de sus fines" (p. 25). Es decir, que es un órgano administrativo, el que está encargado del tratamiento de los datos personales.

Bajo ese orden de ideas, en España el artículo 5 numeral 1 literal m) Real Decreto 1720/2007 "Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal" los define como los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

Según Reyes Valenzuela (2013), estos ficheros deben realizarse por medio de una disposición general, es decir un acuerdo del órgano competente, el cual según el órgano emisor deberá revestir diversas formas, en caso que se refiera a la administración general del Estado u organismo dependientes de las mismas o a los órganos de las comunidades autónomas.

Podemos entender que los ficheros de titularidad pública se refieren a aquellos que pertenecen al Estado o que tienen una dependencia del mismo, y que en virtud de la naturaleza de las funciones públicas que ostentan en sus relaciones con la población, requieren de la recopilación y uso de los datos personales. Los que deberán en todo tiempo adecuar sus actuaciones y cumplir con las solemnidades que le Ley No. 787, así como del ordenamiento jurídico en general.

1.2.3.2 Ficheros de Titularidad Privada

Hoy día para el buen funcionamiento y el desarrollo de las actividades del objeto social de las empresas, es necesaria la recopilación y registros de grandes cantidades de información relativas a personas sean estas naturales y jurídicas.

Así, como señala Garriga Domínguez (2009), la información se ha convertido en un activo más de las empresas, e incluso en el más valioso. En unos casos se trata de empresas que almacenan datos personales por la existencia de relaciones contractuales con el titular de los datos y, en otros, las empresas recogen e informatizan datos de carácter personal para otras empresas; en este caso la finalidad de la empresa no es proporcionar un servicio al afectado sino a otras empresas.

Pineda Quinteros (2007), indica que los bancos de datos privados existen dos tipos de categorías, primero aquellos que se refieren a los propios de la empresa para facilitar el cumplimiento de su finalidad económica, como el de una base de datos referida a sus clientes, y aquella base de datos a proveer informes sobre los cuales debe versa la institución ya que los datos están sujetos a tráfico y ello puede producir la afectación o menoscabo en las personas.

Respecto a este tipo de ficheros, debemos entender que a diferencia de los de titularidad pública, estos surgen en razón de facilitar el desarrollo de las relaciones comerciales, por consiguiente, explotar el objeto social de cada empresa, con el fin de obtener mayor rentabilidad, ingresos, y permitir el desarrollo comercial de cada sector de mercado y del país en general.

En definitiva, consideramos que al referirnos a los ficheros de titularidad pública o ficheros de titularidad privada, estos se diferencian primero en la razón de su titular y segundo en la razón de sus funciones, ya que ambas titularidades tienen distinta naturaleza, sin embargo, para la creación, modificación y extinción de los ficheros o bases de datos, deberán atender a la normativa mínima que implica el respeto de los principio de calidad de la información, consentimiento, seguridad de datos, así como establecer el funcionamiento y administración del fichero, debiendo contener además:

1. Identificación del responsable del fichero de datos, si es público o privado,
2. identificación del fichero, sus finalidades y los usos para el que fue creado, así como los datos que serán recopilados,
3. Identificación como los datos serán tratados, así como definir su tratamiento y la forma en cómo serán recopilados, y
4. Indicar las medidas de seguridad del fichero.

1.3 Principios

Antes de abordar esta temática es dable destacar que nuestra legislación carece de un apartado especial que regule los principios sobre la protección de los datos personales, no obstante, se hará referencia a artículos en específicos donde estos se pueden subsumir.

1.3.1 Calidad de Datos

Para Valerio (2008) este principio indica que los datos deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, específicas y legítimas para las cuales se han obtenido. Además, que estos datos deben ser exactos y puestos al día, de forma que respondan con veracidad a la situación actual del titular de los datos.

Por su parte, Garriga Domínguez (2016) agrega que son normas que regulan la recogida, registro y uso de los datos personales y están encaminados a garantizar tanto la veracidad de la información contenida en los datos, como la congruencia y racionalidad de su utilización.

En este sentido, la Ley No. 787 menciona este principio en los artículos 5 y 9, en cuanto a la forma de obtención y de tratamiento de los datos personales. Ya que tal y como

hemos indicado no existe un articulado especial que se dedique específicamente a la regulación de este principio.

Sin embargo, para mayor claridad sobre este principio y como forma de Derecho Comparado debemos recurrir a nuestra legislación hermana en Costa Rica, que mediante la Ley No. 8968, "Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales" en su artículo 6 describe al principio de calidad de la información indicando que solo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean **actuales, veraces, exactos y adecuados** al fin para el que fueron recolectados.

Según el artículo precitado de la legislación costarricense podemos entender que la actualidad se refiere a la obligación que tiene el responsable de la base de datos de eliminar los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados.

Por su parte, la **veracidad** indica que el responsable de la base de datos está obligado a modificar o suprimir los datos que falten a la verdad. De la misma manera, velará por que los datos sean tratados de manera leal y lícita.

La **exactitud** requiere tomar las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

Y finalmente la **Adecuación al fin**, que los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines.

Con este principio de calidad de datos, lo que se pretende es garantizar una determinada calidad en los datos personales que sean recopilados, de tal forma que estos sean pertinentes y utilizados para una finalidad concreta y no para un uso distinto e incompatible para el cual fueron recabados, y que dicha obtención sea de forma legítima. Además, que estos sean actualizados según las situaciones que se presenten en cada caso en concreto. Asimismo, este principio permite al titular de los datos ejercer los derechos conocidos como derechos Arco, los cual serán abordados en el siguiente capítulo.

1.3.2 Consentimiento Informado

Es una manifestación de la autodeterminación informativa que según Zeledón Arancibia (2013) significa "una condición indisponible sobre la que se asienta la licitud del tratamiento de datos personales de la empresa y su legitimidad" (p. 16), se encuentra regulado en el artículo 4 literal C del Decreto No. 36-2012.

Este principio nos permitirá entender a lo largo de este estudio, el papel fundamental y decisivo que tiene el titular de los datos personales al consentir y permitir el uso o no de los datos personales, el que facilitará la diversidad de relaciones comerciales y determinará la responsabilidad del empresario (responsable de los ficheros de datos) de recopilar dicho consentimiento dentro de los límites y prerrogativas que la legislación dispone. Es decir, que la legislación exige que la obtención de los datos personales y su tratamiento sean con el consentimiento expreso e inequívoco de parte del interesado.

1.3.3 Seguridad de datos

Este principio se encuentra regulado en el artículo 11 de la Ley No 787, el cual obliga al responsable del fichero de datos a adoptar las medidas técnicas y organizativas que resulten necesarias para: garantizar la integridad, confidencialidad y seguridad de los datos personales, para evitar su adulteración, pérdida, consulta, tratamiento, revelación, transferencia o divulgación no autorizada, y que permitan detectar desviaciones, intencionales o no, de información privada, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Del Paso Navarro & Ramos González citados por Garriga Domínguez (2009, p. 82), señalan que el principio de seguridad de datos va a estar orientado en tres direcciones debiéndose adoptar las medidas necesarias para garantizar, en primer lugar que los destinatarios legítimos de los datos personales puedan recibirlos a tiempo y acceder a ellos; en segundo lugar, que no se altere o pierda la información y tercero, que sólo las personas autorizadas tengan conocimiento de los datos de carácter personal registrados.

La finalidad de este principio de la seguridad de datos, es establecer mecanismos de control sobre la confidencialidad, disponibilidad e integridad de los datos personales que han sido obtenidos por el responsable de los ficheros, de forma que se establezcan medidas técnicas y organizativas que garanticen la seguridad de los datos antes las variaciones que pudiesen producirse durante su tratamiento. Permitiendo de esta manera preservar los datos personales de accesos indebidos. Y sobre todo garantizar el derecho a la autodeterminación informativa.

2. El Derecho a la Autodeterminación Informativa.

Según Riquert (2003), el derecho a la autodeterminación informativa fue definido por el Tribunal Constitucional Alemán, a partir de la sentencia sobre la Ley de Censos de 1983, mediante la cual se configura este derecho como la concreción jurídico-fundamental del derecho común de la personalidad garantizado en la Ley fundamental de Bonn, con la que se trató de combatir las amenzas a la personalidad y, en la cual se señala que:

> "…teniendo en cuenta que esta autodeterminación constituye una condición funcional elemental de una democracia en libertad fundada en la capacidad de ser protegido frente a la libertad fundada en la capacidad de acción y concursos de sus ciudadanos, el individuo tiene que ser protegido frente a la ilimitada investigación, el archivo, la utilización y la transmisión de sus datos personales. Esta protección queda garantizada de una forma ilimitada y el individuo no goza de un derecho entendido como dominio absoluto no limitable sobre sus datos; el individuo no es sino una personalidad que se despliega en el seno de una comunidad social a base de comunicación. De ahí que el individuo haya de tolerar los límites a su derecho de autodeterminación informativa o razón de intereses generales. (p. 52)

Al respecto señala Garriga Dominguez (2009), que el Tribunal Constitucional Alemán en esta sentencia extrae del derecho a la personalidad la facultad de disponer sobre la revelación y uso de los datos y por consiguiente, del derecho a la autodeterminación informativa, en la cual establece "*la facultad del individuo derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites decide revelar situaciones referentes a la propia vida*", (p. 32). Posteriormente, se formularon

diversidades de conceptos respecto a este derecho quienes establecen que derivan de la intimidad, de la libertad y otros, consideran que un derecho autónomo.

Para De Alfonso Laso (2002), el derecho a la autodeterminación informativa "se presenta como una reformulación del derecho fundamental a la libertad y a la privacidad" (p. 39). Asimismo, aclara que esta forma de entender la protección de datos personales, considerando la libertad y la opinión del individuo, se verifica en la aprobación de leyes que pretenden desarrollar la idea de un derecho a la defensa informativa del ciudadano frente al Estado, primeramente.

No obstante, ese concepto según el autor precitado, ha sufrido una notable evolución, debido a que el Estado entendido como un recopilador y transformador de la información que le es facilitada por un sujeto, ahora ha encontrado una compañía como lo es las bases de datos creadas por fuentes privadas. Redireccionándose y rediseñandose de este modo el concepto tradicional de la protección de datos a un campo más amplio debido a las nuevas realidades tanto empresariales como tecnológicas.

Por su parte, Eguiguren Praeli (2004) citado por Bazán (2008, pp. 112 y 113), señala que los derechos a la intimidad personal o, incluso, a la autodeterminación informativa, tienen una importancia que trasciende del ámbito meramente individual, alcanzando una dimensión social indispensable para asegurar el respeto de la dignidad y libertad de la persona, que también constituye fundamento insoslayable de un régimen democrático.

Ampié Vilchez (p. 189) aclara que la intimidad no prohíbe toda información sobre determinada persona sino que impide informar de todo y reconocen dos posibilidades de invasión: la de interés público y la que carece de dicho interés, asimismo, destaca la necesidad de superar esa definición, debido a que el avance tecnológico ha permitido que aun cuando estemos solos, nuestra intimidad resulte dañada por el manejo de la información. Por ello, algunos autores han definido la intimidad como el control sobre la comunicación que nos concierne.

Sin embargo, Garrigas Domínguez (2009), señala que es necesario destacar y delimitar que el derecho a la autodeterminación informativa es distinto al derecho a la intimidad, ya que el primero pone el acento en el uso que se haga de la información resultante de interrelacionar determinados datos personales y del perfil que se obtenga. Es decir, que "lo que está en juego no es propiamente la intimidad de las personas sino **su propia identidad**" (p. 33). (la negrita es de la autora)

Vitorio Frosini (1988) establece que la libertad informática "representa una nueva arma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del right of privacy, (…) consiste, también, en la <<la libertad de informarse>>, es decir, de ejercer un control autónomo sobre los datos propios, sobre la propia <<identidad informática>>" (p. 23).

Por su parte, Bazán (2005, p. 134), infiere que la autodeterminación informativa es "un derecho autónomo, con una doble dimensión: sustancial, como derecho en sí mismo; e instrumental, es decir, como soporte para la cobertura tutelar de otros derechos, in*ter alia*, de los de intimidad, honor y dignidad.". Es un derecho a saber y también un derecho a la transparencia del procesamiento de datos, el cual a su vez es una parte fundamental del concepto moderno de democracia.

Además, dicho autor señala que este derecho ofrece una textura que resulta acorde con los modernos desafíos informáticos, puesto que, abandonando el concepto de intimidad como libertad negativa, permite avanzar hacia una fase activa del proceso de circulación de la información personal brindando protagonismo al interesado al posibilitarle el ejercicio de un adecuado control sobre la misma.

Murillo de la Cueva (1990, p. 120) señala que la autodeterminación como bien jurídico tutelado por el Habeas Data está encaminado a "preservar la información individual –íntima y no íntima– frente a su utilización incontrolada, arrancando, precisamente, donde termina el entendimiento convencional del derecho a la vida privada".

Respecto a este derecho la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica mediante sentencia N° 06484, de 10 de mayo de 2013 establece:

> Es la llamada protección a la autodeterminación informativa de las personas, la cual rebasa su simple ámbito de intimidad. Se concede al ciudadano el derecho a estar informado del procesamiento de los datos y de los fines que con el se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso el que se le cause un perjuicio ilegítimo (...) la Sala se refirió al reemplazo del concepto clásico de intimidad por el de autodeterminación informativa. Reiteró que en sentencia número 7201-01 de las 15:40 horas del 24 de junio de 2001, este Tribunal Constitucional definió a la autodeterminación informativa como: "*el derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea pública o privada; así como la finalidad a que esa información se destine a que sea empleada únicamente para dicho fin, el cual dependerá de la naturaleza del registro en cuestión. Da derecho también a que la información sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir*".

Por su parte, la Sala de lo Constitucional de la Corte Suprema de Justicia, de San Salvador, mediante sentencia No. 934-2007, del 4 de marzo de 2011 añade que:

> … la seguridad jurídica sirve de fundamento a la autodeterminación informativa al trazar el rumbo hacia el cual debe orientarse la defensa del individuo frente al poder fáctico o jurídico: la instauración de resguardos eficaces frente a los riesgos del abuso en el flujo ilimitado e incontrolado de la información personal (…), la autodeterminación informativa presupone –frente a las condiciones de la moderna tecnología para el procesamiento de información– que los individuos tienen la capacidad de decidir y controlar las actividades relacionadas con sus datos personales – individuales y familiares–, ante su posible uso indiscriminado, arbitrario o sin certeza sobre sus fines y límites.
>
> Quien no pueda estimar con suficiente seguridad qué informaciones sobre sí mismo se conocen en determinadas esferas de su medio social o comercial y quien no pueda valorar en forma cierta el conocimiento de los posibles asociados en el desarrollo de la actividad de comunicación, estará restringido en su autodeterminación y autonomía personal.

Es de nuestra consideración que el concepto de la Sala Constitucional de Costa Rica es acertado porque no solo es determinante al establecer al derecho a la autodeterminación como un derecho fundamental e independiente de la intimidad, sino

que además su alcance es tanto para las personas naturales o jurídicas a conocer porqué y para que es o será utilizada la información recabada y que se materializa mediante el ejercicio de los derechos Arco. Y aunado a ello un elemento a importante a destacar que declara la Corte Constitucional de El Salvador es la seguridad juridica que presupone el derecho a la autodeterminación informativa como forma de contextualizar la defensa.

Al respecto, la Ley No. 787 define en su artículo 3 literal a) a la Autodeterminación Informativa

> Es el derecho que tiene toda persona a saber quién, cuándo, con qué fines y en qué circunstancias toman contacto con sus datos personales.

A nuestra consideración el derecho de Autodeterminación Informativa, consiste en la facultad que ostentan las personas naturales y jurídicas y que el ordenamiento jurídico le reconoce como derecho fundamental y como un derecho autónomo no derivado de la intimidad, el cual encuentra asidero legal en la Constitución Política y que permite al titular de los datos personales acceder y conocer la información que existe sobre éste en un fichero de datos o cualquier otro medio en automatizado o no, así como controlar y decidir sobre su utilización y tratamiento.

2.1 Contenido

Ruiz García (2012, pp. 26-27) cita a Davara Rodríguez (s.f), quien señala que la información es un bien que no se agota con su consumo, por el contrario, se enriquece con el uso, y ello permite que su expansión se esté produciendo con la creación de la información provocada, en gran medida, por el desarrollo alcanzado en los sistemas de telecomunicaciones que ha permidio que una misma información sea accesible a un número mayor de usuarios.

Murillo de la Cueva (1990, p. 185), señala que:

> El contenido típico del derecho a la autodeterminación informática puede inducirse a partir de la posición que los diferentes ordenamientos positivos atribuyen al sujeto activo de la protección de datos (…) está integrada por las diferentes facultades que se le reconocen para controlar el uso de la información personal que le atañe tanto en el momento de la recogida de los datos, cuanto en el de su tratamiento y conservación, como, en fin, en el de la transmisión.

En este sentido, el contenido a la autodeterminación informativa se configura en nuestra legislación como los derechos de los titulares con el cual se le faculta al para acceder, rectificar, cancelar y oponerse al uso de sus datos, así como el decidir por qué y para qué se utilizan, lo que permitirá hacer uso del habeas data.

2.2 Derechos de los Titulares: derechos Arco

De Alfonso Laso (2002), señala que es necesario el establecimiento de controles públicos y privados de la protección de datos que busquen unificar el estándar de protección, debido a que el concepto de protección de datos no establece únicamente prohibiciones para determinados tratamientos de datos, sino que, además pone a los individuos en condiciones de manejar sus datos personales con autodeterminación y que le garantice a los titulares la transparencia en el tratamiento de su información. En este sentido una forma de control es a través de los derechos Arco.

Para ello debemos partir de la idea que toda persona (natural o jurídica) tiene derecho a la protección de los datos personales que provee, para ello puede ejercer el cúmulo de derechos y facultades que para tal efecto le confiere la legislación nacional. Nuestra legislación en materia de protección de datos personales, es válido hacer mención que aunque este derecho carece de una definición legal, tanto la ley como el reglamento lo regulan de forma específica. El artículo 3 literal b del Decreto No. 36-2012, define como derecho del titular a aquel que se refiere a los derechos de acceso, rectificación, oposición y cancelación de datos personales.

El Instituto federal de Acceso a la Información y Protección de Datos Personales de México en adelante IFAI, define a los derechos Arco como el derecho de los titulares de los datos personales a acceder, rectificar y cancelar su información personal en posesión de terceros, así como a oponerse a su uso (IFAI, 2012).

Asimismo, señala que la protección de datos personales es un derecho humano que le da a los individuos el poder de controlar su información personal, decidir con quién se comparte y para qué se utiliza con terceros, así como el derecho a que ésta se trate de forma adecuada, para permitir el ejercicio de otros derechos y evitar daños a su titular.

Al respecto el Tribunal Constitucional de España mediante la Sentencia 292/2000 ha considerado a los derechos arco como el haz de facultades que emanan del derecho fundamental a la protección de datos y lo establece de la siguiente manera:

> … el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a **acceder, rectificar y cancelar** dichos datos. En definitiva, el poder de disposición sobre los datos personales (la negrita es de la autora).

Bajo esa línea tanto la sentencia Tribunal Español como la Sala de lo Constitucional de Costa Rica antes descritas, son coincidentes en que el derecho a la autodeterminación informativa es un derecho fundamental y autónomo que atribuye al titular de los datos facultades que le permitan garantizar un poder de control de sus datos materializado a través de los derechos Arco.

En definitiva, los derechos Arco, son los derechos que la Ley. No. 787 y el Decreto No. 36-2012, dispone en virtud del derecho a la autodeterminación informativa, como un conjunto heterogéneo de mecanismos de defensa de la protección de sus datos personales, regulando de esta forma su tratamiento e impidiendo que los sujetos llamados a la protección de los datos personales, es decir, el responsable de los ficheros lo realice a su libre arbitrio y de forma autónoma, por lo que el titular puede acceder, rectificar, cancelar y oponerse al tratamiento de los datos personales.

En este sentido la protección de los datos personales en Nicaragua, se realiza a través del ejercicio de los derechos Arco, regulados en la Ley No. 787 y el Decreto No. 36-2012, de la siguiente manera:

- ✓ Derecho de acceso: Arts. 9 párrafo segundo y 17 de la Ley No. 787 y artículo 25 al 27 del Decreto No. 36-2012.
- ✓ Derecho de Rectificación: Art. 9 párrafo segundo 19 de la Ley No. 787 y artículo 28 y 29 del Decreto No. 36-2012.
- ✓ Derecho de Cancelación: Arts. 9 párrafo segundo y 19 lit. a) de la Ley No. 787 y artículo 28 y 29 del Decreto No. 36-2012.
- ✓ Derecho de Oposición: Art. 9 párrafo 2 segundo de la Ley No. 787 y artículo 30 y 31 del Decreto No. 36-2012.

2.2.2 Condiciones Generales del ejercicio de los Derechos Arco

Para Valerio (2008) la configuración y ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO), deben contemplarse al menos tres condiciones:

1. Debe ser personalísimos (respecto al titular).
2. Debe ser independiente (respecto a la ejecución de los cuatro derechos).
3. Debe ser gratuito (respecto a ambas partes).

La primera condición, establece que el ejercicio de los derechos Arco debe ser realizado por el afectado o por un representante voluntario debidamente acreditado. (Real Decreto 1720/2007, artículo 23).

En nuestro ordenamiento jurídico se encuentra regulado en el artículo 18 del Decreto No. 36-2012, que establece que pueden acceder al ejercicio de los derechos Arco, las siguientes personas:

a) El titular de los datos, previa presentación del documento de identidad requerido conforme la ley de la materia.
   También podrán ser admisibles los instrumentos electrónicos por medio de los cuales sea posible identificar al titular de los datos, u otros mecanismos de autenticación permitidos por otras disposiciones legales, o aquéllos previamente establecidos por el responsable de ficheros de datos. La utilización del instrumento electrónico que lo sustituya eximirá de la presentación del documento de identificación a que se refiere este inciso, y
b) El representante del titular de los datos, previa presentación del poder de representación suficiente y documento de identidad requerido conforme la ley de la materia.
c) Los padres o tutores del titular de los datos, en el caso de menores de edad, previa presentación de partida de nacimiento del menor y cédula de identidad de los padres. En el caso del tutor, el documento legal que lo acredite como tal.
d) Los sucesores universales del titular de los datos, en el caso de personas fallecidas, previa presentación del documento legal que lo acredite como tal y el certificado de defunción.

La segunda condición presupone que los derechos de acceso, rectificación, cancelación y oposición no pueden entenderse que el ejercicio de alguno de ellos sea requisito previo para el ejercicio de otro (Real Decreto 1720/2007, artículo 24 num. 1.), en el contexto

nicaragüense, no existe ningún elemento normativo tanto en la ley como en su reglamento que indique un grado de prelación o presupuesto legal que obligue a agotar un derecho primero que el otro, cada derecho será aplicado según las condiciones de cada caso en particular. Es decir, que el ejercicio de uno de los derechos no excluye la posibilidad de ejercer primero uno y luego otro, ni puede constituir mucho menos puede ninguno de ellos puede considerarse como requisito previo para el ejercicio de cualquiera de estos derechos.

Y finalmente respecto a la tercera condición debe concederse al interesado un medio sencillo y gratuito (Real Decreto 1720/2007, artículo 24 num. 1) y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan. (Real Decreto 1720/2007, artículo 24 num. 3).

Respecto a nuestra legislación, el artículo 21 del Decreto No. 36-2012, dispone que el responsable del fichero de datos no podrá establecer como única vía para la presentación de las solicitudes del ejercicio de los derechos del titular algún servicio o medio que implique costos. Asimismo, según el artículo 27 del Decreto No. 36-2012, únicamente implicará un cargo por procesamiento respecto al derecho de acceso, cuando se solicita más de una vez al año.

2.2.2 Medios para acceder y procedimiento

Según disposiciones del artículo 19 del Decreto No. 36-2012, el titular de datos personales, para el ejercicio de sus derechos, podrá presentar la solicitud respectiva ante el responsable del fichero de datos conforme a los medios establecidos en la Ley y se ejercerán mediante comunicación por escrito, así como por medios electrónicos, telefónicos, de imagen (Arts. 9 párr. 2 y 18 lit c Ley 787.)

Asimismo, el responsable del fichero de datos podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares de datos el ejercicio de sus derechos, lo cual deberá darlo a conocer a través del aviso informativo. (artículo 19 del Decreto No. 36-2012).

En este sentido y según lo que dispone la Ley No. 787 y su Decreto 36-2012 el titular de los datos personales puede comparecer ante el responsable de los ficheros de datos a solicitar el ejercicio de sus derechos Arco, ya sea un fichero de titularidad pública o un fichero de titularidad privada, es decir, Entidad pública o empresa privada a exigir que sus datos personales sean rectificados, cancelados, entre otros.

Este trámite conocido como solicitud, consiste en tres etapas que de conformidad con el Decreto No. 36-2012 (arts. 22-24), y que se desarrolla de la siguiente manera:

1. Registro de solicitudes: El plazo de atención debe ser dentro de los cinco días hábiles de recibido la solicitud del titular de los mismos, informándole por escrito, o por cualquier otro medio que se le equipare según las circunstancias, de manera completa, clara y sencilla el tratamiento realizado (art. 19 lit b. Ley No. 787);
2. Requerimiento de información adicional: en caso que la información proporcionada sea errónea o incompleta, el responsable del fichero dentro de los cinco días hábiles después de recepcionada la solicitud puede requerir al titular para que presente elementos o

documentos necesario para darle trámite a la misma, quien tiene un plazo de diez días para presentarlo.

3. Respuesta del responsable: deberá referirse exclusivamente a los datos personales que específicamente se hayan indicado en la solicitud correspondiente, y deberá presentarse en un formato legible, comprensible y de fácil acceso. En caso de uso de códigos, siglas o claves se deberán proporcionar los significados correspondientes.

Asimismo, es de nuestra consideración que para el ejercicio de los derechos Arco deberá recurrirse previamente ante el responsable de los ficheros de datos sea este una entidad pública o una empresa privada, y posteriormente recurrir ante la DIPRODAP, según los dispuesto en la Ley No. 787, no obstante, tal y como hemos expresado a lo largo de esta investigación, no existe el recurso institucional, por lo que deberá ejercitarse a través de la sala de lo constitucional, ante la negativa del responsable.

2.2.3 Derecho de Acceso

Murillo de la Cueva (1990), señala que esta facultad implica:

> … la posibilidad de comprobar si se dispone de información sobre uno mismo y conocer el origen del que procede la existente y la finalidad con que se conserva. Del mismo modo, el derecho de acceso conlleva la facultad de exigir y obtener una comunicación escrita en la que conste los anteriores extremos. (p. 187-188).

Por su parte Reyes Valenzuela (2013), agrega que este derecho es la potestad que tiene el interesado para obtener de parte del responsable de los ficheros que se le suministre las informaciones necesarias y sin restricciones de ningún tipo.

Ahora bien, en el contexto nacional, esto implica que el titular de datos personales tiene derecho a solicitar y obtener del responsable de ficheros, sus datos personales, así como información relativa a las condiciones y generalidades del tratamiento de estos. (Art. 25 del Decreto No. 36-2012), a través de los medios que para tal fin proporcione el responsable de los ficheros o por cualquier otro medio y sobre todo deberá ser en formatos legibles o comprensibles para el titular. (Art. 26 del Decreto No. 36-2012).

Los titulares de datos tendrán derecho al acceso de los mismos de la manera siguiente:

a) Cuando solicite información a la DIPRODAP relativa a la existencia de ficheros de datos personales, sus finalidades y la identidad de sus responsables, de manera gratuita; en cual en nuestra realidad es inaplicable por cuanto no ha sido creada la dirección, y

b) Cuando solicite información al responsable del fichero de datos relativa a sus datos personales y al tratamiento dado a los mismos, de manera gratuita una vez al año, y pagando un cargo que cubra el costo de procesamiento, las veces que lo desee. (Art. 27 del Decreto No. 36-2012). Este supuesto permite que el titular acceda directamente ante el empresario a solicitar este derecho.

2.2.4 Derecho de Rectificación

Murillo de la Cueva (1990), señala que "para asegurar la calidad de los datos, una consecuencia del derecho de acceso es la exigir la rectificación de los datos erróneos o inexactos y de obtener la integración de los que sean incompletos" (p. 187).

Al respecto, los artículos 28 y 29 del Decreto No. 36-2012, señalan que el titular podrá solicitar en todo momento al responsable del fichero de datos que rectifique sus datos personales que resulten ser inexactos o incompletos. Para ello la solicitud de rectificación deberá indicar a qué datos personales se refiere, así como, la corrección que haya de realizarse y deberá ir acompañada de la documentación que sustente la procedencia de lo solicitado. El responsable del fichero de datos podrá ofrecer mecanismos que faciliten el ejercicio de este derecho en beneficio del titular.

Este derecho permite que el titular solicite al empresario o responsable del fichero de datos que corrija los datos que han sido obtenidos, siempre y cuando el titular tenga los medios de prueba que sustenten su petición y por tanto que den lugar a la corrección de los mismo con el fin de evitar posibles daños al titular. Piénsese en el caso particular que contratemos un servicio y nuestro nombre ha sido mal escrito bastará la presentación del documento de identidad para acreditar el error evidente y proceder a su rectificación.

2.2.5 Derecho de Cancelación

Murillo de la Cueva (1990), señala que respecto al derecho de cancelación este se justifica en dos razones bien por la falta de "relevancia actual de la información para los fines del banco de datos o, simplemente, por el propósito de permitir al titular que recupere la disponibilidad sobre cualquier faceta de su personalidad, o sobre todas, que figurase en la memoria informática". (pp. 187-188).

La cancelación implica el cese en el tratamiento por parte del responsable del fichero de datos, a partir de un bloqueo de los mismos y su posterior supresión. (Art. 30 del Decreto No. 36-2012).

El titular de los datos podrá solicitar en todo momento al responsable del fichero de datos la cancelación de los datos personales cuando hayan dejado de ser necesarios o pertinentes para la finalidad que dio lugar a su tratamiento o cuando considere que los mismos no están siendo tratados conforme a la Ley No. 787 y su reglamento.

La cancelación procederá respecto de la totalidad de los datos personales del titular, contenidos en una base de datos, o sólo parte de ellos, según lo haya solicitado. (Art. 31 del Decreto No. 36-2012).

Ahora bien, de resultar procedente la cancelación, se dará paso al bloqueo de sus datos personales, este último implica un deber de conservación de los datos personales de la solicitud de cancelación sea esta parcial o total, con el fin de depurar o establecer las posibles responsabilidades que nacieron del tratamiento de los mismos, y que darán lugar a la supresión de los datos.

En ese sentido, el artículo 3 literal b de la Ley No. 787, define la figura del bloqueo como:

> Es la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto

> de tratamiento y transcurrido éste, se procederá a su cancelación en el fichero de datos en el que se encuentran.

En concordancia con el artículo precitado, el artículo 32 del Decreto 36-2012, señala que el responsable del fichero de datos deberá:

> a) Establecer un período de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo al titular de los datos o a su representante en la respuesta a la solicitud de cancelación;
> b) Atender las medidas de seguridad adecuadas para el bloqueo;
> c) Transcurrido el período de bloqueo, llevar acabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas por el responsable del fichero de datos.

2.2.6 Derecho de Oposición

Reyes Valenzuela (2013), señala que este derecho no solamente debe regular en un sentido estricto, en cuanto se refiere a oponerse al tratamiento de todos los datos, sino también en un sentido más amplio, es decir, oponerse al tratamiento de algunos datos personales.

Bajo esa línea, el Decreto No. 36-2012 en su artículo 34, define el derecho de oposición como el derecho que tiene el titular de los datos y que se materializa de dos formas, primero que no se lleve a cabo el tratamiento de sus datos personales o segundo que cese el mismo, y establece como regla general cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuentes de acceso público.

Ahora bien, si el titular de los datos hubiere prestado su consentimiento, tiene derecho a oponerse al tratamiento de sus datos, si acredita la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho.

En caso que la oposición resulte justificada el responsable del fichero de datos deberá proceder al cese del tratamiento que ha dado lugar a la oposición. No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea requerido por ley.

Los derechos Arco, tal y como lo hemos establecido son las facultades que tienen los titulares de los datos en virtud del derecho a la autodeterminación informativa para acceder a sus datos, rectificarlos, cancelarlos o solicitar su cancelación. Los cuales deberán establecerse en el aviso informativo que el empresario cree para el tratamiento de los datos, en el cual se definirán las reglas para el uso de sus datos personales y posterior cancelación.

3. Obligaciones del empresario

3.1 Aviso de informativo.

Los ejes sobre los cuales se basa tratamiento de los datos personales, es que se le garantice al titular de los datos, primero el derecho a la autodeterminación informativa, para ejercer el control y disposición de los datos y segundo que pueda decidir o

consentir de forma libre, inequívoca e informada sobre el tratamiento de la información que ha proporcionado al responsable de los ficheros, tal y como ya hemos abordado en los capítulos anteriores.

Es aquí donde se torna de suma importancia que el empresario o responsable de los ficheros se encamine en la creación y formulación de los avisos informativos que le permitan recopilar los datos personales que este requiere, garantizándoles a los titulares, seguridad y privacidad y que dicho tratamiento adecuado y de calidad le permita consolidar sus relaciones comerciales.

Ahora bien, el Decreto No. 36-2012, establece disposiciones relativas al desarrollo y aplicación de la Ley No. 787, sobre todo estas adquieren un carácter de obligatoriedad respecto al tratamiento de datos personales que obren ya sea en soportes físicos o electrónicos y que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización (Arts. 1 y 2).

Según el IFAI (2011) de México, el aviso informativo, o aviso de privacidad como es conocido en la Legislación Mexicana, tiene dos propósitos principales que consisten en hacer del conocimiento de titular de los datos personales:

> …primero, que su información personal será recabada y utilizada para ciertos fines, y segundo, las características del tratamiento al que serán sometidos sus datos personales. Lo anterior con el fin legítimo de que el titular tome decisiones informadas con relación a sus datos personales y controle el uso de su información personal. (p. 2)

Bajo ese orden de ideas el artículo 3 del Decreto No. 36-2012, introduce la figura de **aviso informativo**, siendo para este caso en estudio una de las primeras obligaciones que se exige para el cumplimento del tratamiento y protección de los datos personales, la cual también puede ser conocida como política de privacidad o de confidencialidad.

El aviso informativo según el artículo 3 literal a) del Decreto 36-2012, es todo documento físico, electrónico o en cualquier otro formato generado por el responsable del fichero de datos que es puesto a disposición del titular de los datos, previo al tratamiento de sus datos personales. El cual debe caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento. (Art. 15 Decreto, No. 36-2012).

En Nicaragua podemos mencionar a la empresa *Pricesmart*, la cual ha establecido que para la compra y acceso a dicho establecimiento se requiere de una tarjeta de membrecía, por lo que al solicitarla el usuario debe llenar un formato con sus datos personales y firmar la política de confidencialidad la cual puede encontrarse en la siguiente dirección web https://shop.pricesmart.com/ni/sp/privacy. Otro caso es con la empresa *omnilife* que en su página web provee su política de privacidad en la siguiente dirección https://www.omnilife.com/nicaragua/politica-privacidad/

Es dable señalar que el responsable del fichero al recopilar los datos, tiene la obligación de informar al titular de los datos como mínimo la información prevista en el artículo 7 de la Ley No. 787, lo que se realizará mediante el aviso informativo (art. 14 del Decreto No. 36-2012), por lo que al realizar un análisis de la Ley No. 787 y su reglamento el

Decreto No. 36-2012, podemos establecer que el contenido del aviso informativo deberá indicar:

1. Identificación y domicilio de Responsable de los ficheros de datos (Art. 7 lit. b, Ley No. 787);
2. La finalidad del uso de los datos personales y quienes pueden ser sus destinatarios (tratamiento) (Art. 7 lit. a, Ley No. 787);
3. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga; (Art. 7 lit. c, Ley No. 787);
4. Las consecuencias de proporcionar los datos personales, de la negativa a hacerlo o de la inexactitud de los mismos; (Art. 7 lit. d, Ley No. 787);
5. La Categoría de los datos personales que recopila (sensibles o no);
6. La garantía de ejercer por parte del titular el derecho de acceso, rectificación, modificación, supresión, complementación, inclusión, actualización y cancelación de los datos personales; (Art. 7 lit. e, Ley No. 787)
7. Cuáles son los medios y el procedimiento que tiene el titular para ejercer sus derechos de acceso, rectificación, cancelación y oposición, es decir, los derechos Arco. (Arts. 18 lit. a, párrafo 2 y 19 del Decreto 36-2012);
8. Cuando los datos procedan de fuentes accesibles al público y se utilicen para hacer envíos publicitarios o promocionales, en cada comunicación que se dirija al titular de los mismos se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten (Art. 7 lit. f, Ley No. 787);
9. Los datos sólo pueden ser utilizados para los fines que motivaron su tratamiento; y no podrán ser utilizados para otros fines; (Art. 7 lit. g, Ley No. 787);
10. Los datos inexactos, incompletos, o que estén en desacuerdo con la realidad de los que le corresponden a la persona, serán rectificados, modificados, suprimidos, completados, incluidos, actualizados o cancelados según corresponda (Art. 7 lit. h, Ley No. 787);
11. Los datos personales deben ser almacenados de modo que permitan el derecho de acceso del titular a los mismos; (Art. 7 lit. i, Ley No. 787);
12. Los datos personales deben ser cancelados cuando hayan dejado de ser necesarios a los fines para los cuales hubiesen sido tratados (Art. 7 lit. j, Ley No. 787);
13. Están prohibidos los ficheros de datos personales que no reúnan condiciones técnicas de integridad, confidencialidad y seguridad (Art. 7 lit. k, Ley No. 787); y
14. Queda prohibida la creación de ficheros de datos personales que almacenen información de datos sensibles, salvo lo dispuesto en la ley. Sin perjuicio de ello, las diferentes sociedades mercantiles y asociaciones sin fines de lucro, pueden almacenar datos de sus miembros (Art. 7 lit. k, Ley No. 787).
15. Cómo limitar su uso o divulgación; o la aceptación o negativa para autorizar la transferencia de datos a terceros. (Art. 6, Decreto 36-2012)
16. Cómo revocar el consentimiento (Art. 12, Decreto 36-2012);
17. La forma en la que se comunican cambios al Aviso de Privacidad (Art. 6 p. 3, Decreto 36-2012).

En definitiva, el aviso informativo es todo documento que puede ser físico, digital o de cualquier tipo, creado por el empresario, como mecanismo previo a la obtención y tratamiento de los datos personales, y cuya función es poner a disposición del titular de los datos una declaración que informe, quien recaba la información, cuales son los datos, sus finalidades, su uso y alcance, así como las garantías del ejercicio de los derechos Arco, si se acepta su comunicación a terceros, entre otros.

3.2. Consentimiento

Tal y como se ha mencionado, el empresario en el desarrollo de su actividad empresarial (ficheros de titularidad privada) o en el cumplimiento de las funciones propias de la entidad de administración pública (ficheros de titularidad pública), día a día se encuentran frente al trato de los datos personales con los individuos que se relacionen, puede ser en los supuestos más básicos en relación con sus proveedores, clientes o incluso sus propios trabajadores.

Valerio (2008) señala que "la obtención de estos datos se legitiman por su propia necesidad de desarrollo empresarial, pero además resulta necesario el **consentimiento** del afectado o interesado para su almacenamiento, tratamiento y, en su caso, cesión a un tercero (p. 70). (La negrita es de la autora).

Como se puede apreciar el consentimiento es un presupuesto y constituye un elemento integrante para el tratamiento de los datos personales, es decir, que es una exigencia que forma parte de la misma para llevar a cabo los procedimientos de obtención, utilización y demás actividades conexas.

Al respecto, el artículo 3 literal d, de la Ley No. 787 define al consentimiento del titular como "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular de los datos consiente el tratamiento de sus datos personales".

Del cual se desprende y según el artículo 4 del Decreto 36-2012 que el consentimiento que otorgue el titular de los datos deberá cumplir con las siguientes características:

> a) Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;
> b) Específico: referido a una o varias finalidades determinadas que justifiquen el tratamiento, y
> c) Informado: que el titular tenga conocimiento del aviso informativo previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

Es decir, que el consentimiento además de ser libre y específico, debe ser informado, esto último indica que el titular deberá recibir de parte del responsable de los ficheros de datos, información clara, abundante y en términos comprensibles y accesibles, que capacite al titular de los datos para participar de manera voluntaria, consciente y activa en la adopción de decisiones respecto a la obtención y tratamiento de sus datos, conociendo previamente de esta manera sobre el motivo, alcance, consecuencias, beneficios de permitir el uso de sus datos.

Ahora bien, es importante añadir que el consentimiento tiene un papel fundamental en todas las relaciones jurídicas y comerciales, y en específico en temas de consumo, ya que según la Ley No. 842, si este no se obtiene de forma legal, se considera como cláusula abusiva que se tendrán por no pactadas a aquellas que en los contratos:

> Obliguen a la persona consumidora a dar consentimiento para utilizar sus datos personales con fines mercadotécnicos. (Art. 37 numeral 17).

En este sentido, respecto al manejo de información sobre las personas consumidoras y usuarias con fines mercadotécnicos, el artículo 25 de la Ley No. 842, exige que las personas proveedoras están obligadas a proteger la información que recibe de las personas consumidoras y usuarias y no podrán compartirla con terceros, salvo cuando estos lo autoricen de manera voluntaria y en forma expresa a través de una adenda al contrato. Asimismo, esta ley considera como prohibición para las personas proveedoras el divulgar información sin el consentimiento del usuario o el envío de la información publicitaria ante la negativa del mismo. En los casos de violaciones a las disposiciones contenidas en el artículo 25 de la Ley No. 842, se procederá conforme la Ley No. 787.

3.2.1 Tipos de consentimiento

Respecto a las diversas formas en que se exprese el consentimiento, ya sea tácito, verbal o escrito, el responsable del fichero de datos deberá facilitar al titular de datos un medio sencillo y gratuito para que, en su caso, lo pueda manifestar según la forma de su otorgamiento. Pudiendo ser este consentimiento:

a) Expreso: El responsable del fichero de datos deberá obtener el consentimiento expreso del titular de datos cuando:
   a) Lo exija una ley o reglamento;
   b) Se trate de datos financieros o patrimoniales;
   c) Se trate de datos sensibles;
   d) Lo solicite el responsable para acreditar el mismo, o
   e) Lo acuerden así el titular de datos y el responsable del fichero de datos. (Art. 7, Decreto 36-2012).

Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por ley. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento. (Art. 10, Decreto 36-2012)

b) Verbal. Es cuando el titular lo externa oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral. (Art. 9, Decreto 36-2012).
c) Tácito, por regla general y según lo establecido en el artículo 5 del Decreto 36-2012, el consentimiento se entiendo como tácito, salvo los casos en que la Ley exija otro tipo de consentimiento.

Es importante destacar que los titulares de los datos tienen derecho a no otorgar su consentimiento para el tratamiento de los datos personales proporcionados, en este sentido, el responsable de los ficheros debe ser claros en su aviso informativo, estableciendo el mecanismo habilitado para otorgar su negativa, según la forma por la cual fueron obtenidos ya sea de manera directa o personal o indirecta y para las finalidades que serán utilizadas.

En este sentido cuando el aviso informativo no se haga de forma directa y sea para finalidades distintas, el titular tiene un plazo de cinco días hábiles para expresar su negativa, en caso de vencerse el plazo se entenderá que el titular ha otorgado su consentimiento para el tratamiento de los mismos. (Art. 6 Decreto 36-2012).

Para la revocación del consentimiento el titular puede realizarlo en cualquier momento, para ello el responsable de los datos debe establecer mecanismos sencillos y gratuitos que permitan al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó (Art. 12, Decreto 36-2012).

En definitiva, el consentimiento del titular en el tratamiento de los datos personales constituye en la actualidad un presupuesto de la relación entre el responsable de los ficheros y el titular de los datos, una exigencia legal para el responsable de los ficheros, y un derecho que el titular de los datos ostenta, puesto que el primero para poder tratamiento los titulares deben estar previamente informados de modo expreso, preciso e inequívoco sobre qué van a consentir y cuáles son las repercusiones que ello ocasiona en cada caso en particular.

3.3 Obligaciones previas al tratamiento de los datos personales:

1. La creación del aviso informativo y el mecanismo por el cual se pondrá a disposición del titular.
2. Establecer las formas por la cual se obtendrá en consentimiento informado, y señalar los casos en que se requiere el consentimiento expreso y en cuales existe el consentimiento tácito, verbal. Poniendo a disposición del titular los formularios necesarios (arts. 8 -10 Decreto 36-2012).
3. Establecer mecanismos sencillos y gratuitos que permitan al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó (art. 12 Decreto 36-2012).
4. Creación de los ficheros de datos según los datos recabados.
5. No divulgar a terceros la información privada sobre las personas consumidoras o usuarias con fines mercadotécnicos o publicitarios sin su consentimiento, así como enviarles publicidad que expresamente les hubieren manifestado su voluntad de no recibirla (Art. 10 numeral 2 Ley 842).

3.4 Obligaciones durante el tratamiento de los datos personales

1. Cumplir con el aviso informativo.
2. Utilizar los datos para los fines para los cuales fueron recabados.
3. Mantener los datos personales actualizados.
4. Implementar medidas de seguridad (técnicas, físicas, administrativas y tecnológicas) que garanticen la integridad y confidencialidad de los datos.
5. Actualizar los datos, así como garantizar el ejercicio de los derechos Arco.
6. Responder al recurso de habeas data, y derechos arco.

3.5 Obligaciones posteriores al tratamiento de los datos personales

1. Suprimir los datos personales una vez que los datos personales para el fin que fueron recabados.
2. Responder al recurso de habeas data, y derechos arco.

Asimismo, es importante señalar que el empresario, como garante de los derechos y del establecimiento de relaciones sólidas y confiables, puede optar por la elaboración de buenas prácticas, políticas internas, o de autorregularse en la materia de protección de datos personales.

Respecto a este último término, la Legislación mexicana introduce el término de autorregulación como una forma de que los responsables de los ficheros creen sus propios lineamientos y regulaciones a partir de la normativa vigente. No obstante, aclaramos que este estudio no pretende abarcar esa temática, pero si insta a su profundización pues es un tema de gran relevancia, que permitirá salvaguardar los intereses de todas las partes. Por lo que nos remitiremos a dar pinceladas de esta figura.

Respecto a la autorregulación el Artículo 44 de la Ley Federal de Protección de Datos Personales en posesión de los particulares de México establece:

> Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento.
>
> Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto.

Según los Parámetros de Autorregulación en materia de Protección de Datos Personales de México, la autorregulación es el conjunto de principios, normas y procedimientos, de adopción voluntaria y cumplimiento vinculante, que tiene como finalidad regular el comportamiento de los responsables y encargados respecto a los tratamientos de datos personales que lleven a cabo.

Ornelas Núñez & Higuera Pérez (2013), señala que la autorregulación pura es entendida como aquellas normas creadas por los propios sujetos regulados, la cual no puede o debe sustituir a la ley o regulación emitida por el Estado, sino que se considera como una medida complementaria para la protección de datos personales. Cuyos beneficios están definidos a:

> i) Distinguirse frente a sus clientes como organizaciones seguras y preocupadas por garantizar la seguridad de la información de aquellos, lo que fortalece su reputación;
> ii) Contar con mecanismos de prueba adicionales que les permitan acreditar ante las autoridades de privacidad o protección de datos el debido cumplimiento de la ley, (…)
> iii) En los casos de empresas transnacionales, la autorregulación permite unificar la política de protección de datos en todo el mundo, y con ello la simplificación de procesos y la eficiencia de los recursos; y
> iv) La autorregulación podría representar para las autoridades un elemento a considerar para disminuir el monto de sanciones económicas derivadas de algún incumplimiento a la normatividad en la materia (pp. 15 y 16).

En nuestro contexto jurídico encontramos el tema de la autorregulación la Ley No. 787 en el artículo 29 literal i, lo determina como una función asignada a la Dirección de Protección de Datos Personales, que podrá ser utilizado como mecanismo adicional para garantizar el derecho a la autodeterminación informativa.

4. Conclusiones

El marco normativo de la protección de los datos personales frente al tratamiento del empresario, se encuentra previsto en la Ley No. 787 y el Decreto No. 36-2012, sin embargo, existen vacíos legales en temáticas específicas como regulación de los principios, la definición y modos de creación, modificación y extinción de los ficheros de titularidad pública o privada, definición de derechos Arco.

Los ficheros de titularidad pública y privada, se diferencian primero en la razón de su titular y segundo en la razón de sus funciones, ya que ambas titularidades tienen distinta naturaleza, sin embargo, para la creación, modificación y extinción de los ficheros o bases de datos, debe atenderse a las generalidades que la Ley No. 787, así como del ordenamiento jurídico en general que implica el respeto de los principio de calidad de la información, consentimiento, medidas seguridad, así como establecer el funcionamiento y administración del fichero. De forma que no se transgreda la ley, la moral, el orden público y las buenas costumbres.

Los datos personales deben ser entendidos como la información que identifica o hace identificable a una persona, ya sea esta persona natural o jurídica, que permite relacionar a una persona física concreta, en un determinado lugar y condición, por ello los ficheros de datos y su tratamiento además del cumplimiento de las prerrogativas que para ello dispone la legislación, para su creación, modificación y extinción, deben estar estructurados y organizados ya sea automatizados o no, de forma que puedan accederse a ellos fácilmente y garanticen medidas de seguridad y confidencialidad.

Para el tratamiento de los datos personales es importante tomar en cuenta que, para su realización, el empresario debe garantizar el derecho a la autodeterminación informativa consagrado en la Constitución Política de Nicaragua, y los derechos del titular o derechos Arco reconocidos en la Ley No. 787 y el Decreto No. 36-2012. De este modo el derecho a la autodeterminación informativa, el aviso informativo y la obtención del consentimiento, son elementos esenciales en el tratamiento de los datos personales, puesto que estos son los requisitos legales para que se proceda a la recopilación, uso y cancelación de los datos personales.

El derecho de Autodeterminación Informativa consiste en la facultad que ostentan los titulares de los datos personales y que el ordenamiento jurídico le reconoce como derecho fundamental y como un derecho autónomo no derivado de la intimidad, el cual encuentra asidero legal en la Constitución Política y que permite a la persona natural o jurídica titular de los datos personales acceder y conocer la información que existe sobre éste en un fichero de datos, así como controlar su utilización y tratamiento, decidir de forma autónoma por qué y para qué serán utilizados sus datos.

Los derechos Arco, son los derechos personalísimos, independientes en su ejecución y gratuitos que la Ley. No. 787 y el Decreto No. 36-2012, dispone en virtud del derecho a la autodeterminación informativa, consagrado en el artículo 26 numeral 3 Cn, como un conjunto heterogéneo de mecanismos de defensa de la protección de los datos personales del titular, regulando de esta forma su tratamiento e impidiendo que los sujetos llamados a la protección de los datos personales, es decir, el responsable de los

ficheros lo realice a su libre arbitrio y de forma autónoma, por lo que el titular puede acceder, rectificar, cancelar y oponerse al tratamiento de los datos personales.

El aviso informativo es todo documento que puede ser físico, digital o de cualquier tipo, creado por el empresario, como mecanismo previo a la obtención y tratamiento de los datos personales, y cuya función es poner a disposición del titular de los datos una declaración que informe, quien recaba la información, cuales son los datos, sus finalidades, su uso y alcance, así como las garantías del ejercicio de los derechos Arco, si se acepta su comunicación a terceros, entre otros.

El consentimiento del titular en el tratamiento de los datos personales constituye en la actualidad un presupuesto legal de la relación entre el responsable de los ficheros y el titular de los datos, una obligación para el responsable de los ficheros, y un derecho que el titular de los datos ostenta, puesto que el responsable para poder realizar el tratamiento de los datos personales, debe obtener previamente el consentimiento del titular de modo expreso, preciso e inequívoco e informado, esto último indica que el titular deberá recibir de parte del responsable de los ficheros de datos, información clara, abundante y en términos comprensibles y accesibles, que capacite al titular de los datos para participar de manera voluntaria, consciente y activa en la adopción de decisiones respecto a la obtención y tratamiento de sus datos, conociendo previamente de esta manera sobre el motivo, alcance, consecuencias, beneficios de permitir el uso de sus datos

La protección de datos personales no debe ser únicamente una realidad jurídica sino una realidad social que debe ser entendida y aplicada, por el mismo individuo, la empresa privada y la administración pública. Las obligaciones que se derivan del tratamiento de datos personales se pueden dividir en tres etapas previa, durante y posterior a dicho tratamiento, asimismo, durante todas estas fases es importante resguardar el derecho a la autodeterminación informativa.

Lista de referencia

Bazán, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. Estudios Constitucionales, 3. Recuperado de http://www.redalyc.org/articulo.oa?id=82030204

Bazán, V. (2008). El derecho a la vida privada y el derecho a la libertad de información en la doctrina y jurisprudencia de la Corte Suprema de Justicia argentina. Estudios Constitucionales, 6. Recuperado de http://www.redalyc.org/articulo.oa?id=82060106

Calero Espinoza, L. A. (2013). El nuevo delito de acceso y uso no autorizado de registros, datos o archivos informáticos introducido por la Ley número 641, Código Penal. (Tesis inédita de Licenciado en derecho). Universidad Centroamericana, Managua, Nicaragua.

Constitución Política de la República de Nicaragua, y sus reformas. Publicada en La Gaceta Diario Oficial No. 26, del 10 de Febrero de 2014.

De Alfonso Laso, D. (2002). Intimidad y protección de datos en el derecho penal. En Morales García (comp.), Delincuencia informática. Problemas de responsabilidad. (pp. 37-75) Madrid

Decreto No. 36-2012. Reglamento a la ley de Protección de Datos Personales. Publicado en La Gaceta Diario Oficial No. 200, del 19 de octubre de 2012. Nicaragua

Decreto Ejecutivo No. 37554-JP. Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. Publicado La Gaceta No. 45, del 05 de marzo de 2013. Costa Rica

Garriga Domínguez, A. (2009). Tratamiento de datos personales y Derechos Fundamentales. España: Dykinson

Garriga Domínguez, A. (2016). Principios de calidad de los datos y derechos de los interesados: el núcleo esencial del derecho a protección de datos personales en la LOPD. Dykinson. Recuperado de: http://vlex.com/vid/principios-calidad-datos-derechos-642494421

IFAI. (2012). Guía Práctica para ejercer el Derecho a la Protección de Datos Personales. Recuperado de http://red.ilce.edu.mx/sitios/tabletas/familia/GuiaPracticaEjercerelDerecho.pdf

IFAI. (2011). Guía práctica para generar el aviso de privacidad. Recuperado de http://www.itei.org.mx/v3/micrositios/privacidad/documentos/privacidadguia.pdf

Ley 842. Ley de Protección de los Derechos de las Personas Consumidores y Usuarias. Publicada en La Gaceta, Diario Oficial No. 129, del 11 de julio de 2013. Nicaragua

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Publicada en el Diario Oficial de la Federación, del 5 de julio de 2010. México

Ley No. 621, Ley de Acceso a la Información Pública. Publicada en La Gaceta Diario Oficial No. 118, del 22 de mayo de 2007. Nicaragua

Ley No. 787. Ley de Protección de Datos Personales. Publicada en La Gaceta, Diario Oficial No. 61, del 23 de marzo de 2012. Nicaragua

Ley No. 8968. Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Publicada en La Gaceta No. 170, del 05 de septiembre de 2011. Costa Rica

Ley No. 983, Ley de Justicia Constitucional. Publicada en La Gaceta Diario Oficial No. 247, del 20 de diciembre del 2018. Nicaragua.

Martínez Atienza, G. (2016). Seguridad Pública y Privada. Editorial Vlex. Recuperado de http://vlex.com/vid/seguridad-proteccion-datos-652193961

Murillo de la Cueva, P. L. (1990). El Derecho a la Autodeterminación Informativa. Madrid: Tecnos

Ornelas Núñez, L.G & Higuera Pérez, M. (2013) La autorregulación en materia de protección de datos personales: la vía hacia una protección global. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 9. Recuperado de http://vlex.com/vid/materia-datos-personales-hacia-global-514190398

Pineda Quinteros (2007). El derecho de acceso a la información pública y el hábeas data en Nicaragua. (Tesis inédita de Licenciado en derecho). Universidad Centroamericana, Managua, Nicaragua.

Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal. Publicado en Boletín Oficial del Estado, No. 17, de 19 de enero de 2008. España

Reyes Valenzuela, S.M. (2013). Protección de Datos de Carácter Personal. Flujo de Datos de Carácter Personal en un Mundo Globalizado. Editorial Académica Española Recuperado de https://app. vlex.com/#WW/vid/424909074

Riquert, M. (2003). Protección penal de la intimidad en el espacio virtual análisis de derecho nacional y comparado. Buenos Aires: Ediar.

Ruíz García, L. R. (2012). La autodeterminación informativa y su regulación en el ordenamiento jurídico nicaragüense. (Tesis inédita de Máster). Universidad Centroamericana, Managua, Nicaragua.

Sentencia T-414, Expediente T-534 Corte Constitucional de Colombia 16 de Junio de 1992. http://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Sentencia No. 292/2000 del Tribunal Constitucional Español, 30 de Noviembre de 2000. Recuperado de https://tc.vlex.es/vid/ri-2000-21-1-24-2-13-106365

Sentencia No. 06484 de la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica, de 10 de Mayo de 2013. Recuperado de http://vlex.com/vid/-499834646

Sentencia No. 934-2007 de la Sala de lo Constitucional de la Corte Suprema de Justicia, San Salvador, del 4 de marzo de 2011. Recuperado de http://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2010-2019/2011/03/915DA.PDF

Tapia Sánchez, L. S. (2016). Riesgos de clientes y de la competitividad empresarial ante la desprotección de derechos relacionados con la autodeterminación informativa en Nicaragua. (Tesis inédita de Máster). Universidad Centroamericana, Managua, Nicaragua.

Valerio, B. (2008). La adecuación a la normativa de Protección de Datos de Carácter Personal. Boletín Oficial del Estado. Recuperado de http://vlex.com/vid/n-normativa-datos-car-aacute-personal-41421372

Zeledón Arancibia, N. (2013). La preparación interna de la empresa de cara al cumplimiento de la nueva ley de protección de datos. (Tesis inédita de Máster). Universidad Centroamericana. Managua, Nicaragua