LA PROTECCIÓN DE DATOS PERSONALES Y SU INCIDENCIA EN LA ADMINISTRACIÓN TRIBUTARIA NICARAGÜENSE.

Jorge Luis GARCIA OBREGÓN[1]

"La protección de datos personales de los ciudadanos es una obligación para el Estado. Pero, es responsabilidad de su titular hacer valer la importancia de sus datos".

SUMARIO: ***I. Nota introductoria. II. La protección de datos personales en Nicaragua. III. La administración tributaria IV. Bibliografía.***

[1] Catedrático de la Especialización en Derecho Empresarial de la Universidad de Ciencias Comerciales (UCC), Nicaragua. Catedrático de la Maestría en Asesoría Empresarial y Tributaria del Centro de Estudios Tributarios, Administrativos y Empresariales (CETAE), Nicaragua. Miembro de la Red Iberoamericana de Derecho Informático y Miembro del Observatorio Iberoamericano de Protección de Datos (OIPRODAT).

I. Nota introductoria.

El tema de protección de datos personales es un tema novedoso en el sistema jurídico nicaragüense. Tan novedoso que no todas las personas tienen pleno conocimiento sobre qué son los derechos personales, aun las que saben que tipos de derechos son los que se les tutela, indican que no hay mecanismos efectivos, a pesar que la ley prevé las vías correspondientes a seguir.

Este artículo es un acercamiento al origen del tema de protección de datos personales, tanto en el ámbito internacional, como en el ámbito nacional. Se aborda el impacto que posee esta normativa en otras ramas del derecho, así como algunas instituciones, como dependencias del Estado, tales como son la Administración Tributaria.

La Administración Tributaria en virtud de sus funciones recopila una gran cantidad de datos personales considerados por la legislación como sensibles. El contribuyente como tal muchas ocasiones desconoce cuáles son los cuidados que se toman para la protección de sus datos personales, también desconoce la forma eficaz de hacer valer sus derechos frente a un mal uso de esta información. Este artículo trata de eso, de plantear cuales son los derechos de los contribuyentes y las vías que posee para exigir una correcta protección de sus datos personales frente a una institución de naturaleza pública, como es la Administración Tributaria.

II. La protección de datos personales en Nicaragua.

Sobre el tema de protección de datos personales ha sido muy poco lo que se ha escrito en el ámbito nacional, esto derivado a muchos factores, entre los cuales puedo resaltar, a criterio personal, el estancamiento normativo, profesional e intelectual de la gran mayoría de letrados en derecho, que han quedado debatiendo por décadas los casi jurásicos institutos del derecho civil y el derecho penal. También, puedo recalcar la falta de una institución o ente reguladora que vele por la normativa en materia de protección de datos personales. Por último, el lento desarrollo del ecosistema digital

en el país, puesto que somos el país con menor penetración de internet en la población[2].

Por lo que, para poder abordar el tema del origen de la normativa sobre protección de datos personales en Nicaragua, es recomendable primero recurrir a la normativa internacional para posteriormente aterrizarla en el contexto nacional.

i. Antecedentes.

En el ámbito internacional me permito enfatizar que existe un momento preciso donde se puede mencionar la gestación de la normativa en materia de protección de datos personales, la cual mencioné en una obra en la que participé como coautor y donde expresé, textualmente:

> *Poco se ha escrito del origen de la protección de datos personales en el ámbito costarricense, no obstante existen algunos autores que han hecho referencia al verdadero origen de los mismos, ubicando el nacimiento de la institución en Alemania, pues se le atribuye ser el primer país en salvaguardar los derechos a la intimidad de sus habitantes por medio de mecanismos legales que permiten evitar prácticas abusivas y arbitrarias en el tema. En 1970, el Parlamento de Estado alemán de Hesse, fue el primero en promulgar su normativa de protección de datos denominado «Datenshutz».*
>
> *Consecutivamente, la iniciativa llegó hasta el parlamento federal de Alemania donde en el 1977 se creó un Comisario Federal para que interviniera en las situaciones donde se percibiera una lesión a los derechos ligados a la intimidad de las personas. Posteriormente, la Unión Europea (UE), a través del Consejo Europeo, redactó en 1995 un instrumento jurídico —denominado Directiva 95/46 CE— vinculante para los países de la UE, donde sí algún país de otro continente deseaba comercializar información sobre datos personales debía cumplir con lo requerido en el documento.*

[2] Ranking 2013, Penetración de TIC´s en LATAM. Publicado por Infolatam.

Su finalidad fue tan extensiva que se incorporó a los tratados internacionales entre los países de otros continentes. En dicho texto se redactaron algunos de los principios y términos que rigen hoy en día, tales como la calidad de datos, la legitimación del tratamiento, las categorías especiales de tratamiento, información a los afectados por dicho tratamiento, el derecho de acceso del interesado, y el derecho del interesado por oponerse. Estos son aplicables a los datos tratados o no por medios automatizados, de conformidad al Convenio 108, Convenio de la Protección de los Individuos con respecto del procesamiento automático de datos personales[3].

La Organización de la Naciones Unidas (ONU), como un conglomerado de países o una entidad de acción mundial, el 14 de Diciembre de 1990 publicó una directriz conocida como **"Principios rectores para la reglamentación de los ficheros computarizados de datos personales"** que tenía la finalidad de servir como guía para los países miembros de la ONU en el manejo y seguridad de la información personal de los individuos.

Como todo tipo de normas modelos que se aprueban en convenciones, organizaciones de carácter internacional y otras similares, se busca como pactar directrices que sirvan para luego ser "tropicalizadas" al contexto y realidad particular de cada país.

Así fue que aproximadamente en el año 2008, se introdujo a la asamblea nacional el proyecto de "Ley de Protección de Datos Personales".

ii. Ley de protección de datos personales.

Luego de pasar por más de cuatro años en el proceso de formación de ley de la asamblea nacional de Nicaragua en el año 2012, se aprobó la Ley 787, Ley de protección de datos personales, marcando un hito en el avance de la normativa

[3] García Obregón, Jorge Luis. et. al., "Protección de datos y habeas data: una visión desde Iberoamérica". Accésit 2014, XVIII Edición Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. España, AEPD, Obra Ganadora en Investigación Grupal. 2014, p. 53 y 54

nicaragüense en materia de derecho informático, Por primera vez, se trajo a la realidad jurídica instrumentos válidos para tutelar el manejo responsable de datos personales.

Previo a la existencia de la ley 787, no existía en el país una ley ordinaria o especial que normara el tratamiento de los datos personales. Muchos de los derechos constitucionales, como el derecho a la privacidad, quedaban en una ineficacia jurídica ante la ausencia de métodos de tutela efectiva. La mayoría de los reclamos en materia de protección de datos no tenían mayor asidero que la ética y la moral. El poder judicial tampoco tenía muchas herramientas legales eficaces para tutelar los derechos de los ciudadanos.

En el momento de la promulgación de la normativa, se dieron una serie de acontecimientos y denuncias que hicieron que los diputados de la asamblea nacional dieran mayor importancia al proyecto de ley, tales como la falta de una normativa que regulara responsablemente el manejo de los datos por parte de los buros de crédito[4]. En un principio las empresas de buró de créditos funcionaban en la medida correcta; servían como una base de datos para las empresas, que primeramente subían el historial crediticio de sus clientes, para así tener una referencia comercial sobre los mismos. Pero, luego de subir las referencias negativas de los clientes, estas no se preocupaban por restablecer la referencia a "solvente" una vez que se normalizaba la situación crediticia. Cuando estos buró de créditos fueron utilizados no solo en la referencia para un crédito sino hasta como parámetro evaluativo para fines laborales, la falta de normalización del *status* crediticio por parte de las empresas y la pasividad de los buró de créditos, trajeron consigo una serie de reclamos fuertes por parte de focos de la población.

Otras de las denuncias que en su tiempo sopesaron y hasta hoy en día se resienten por parte de la población, han sido el tráfico de datos con fines comerciales que los funcionarios públicos han hecho. Ejemplo, el caso de la base de datos del

[4] Empresas que se dedican a la venta de servicios de datos sobre la situación crediticia de las personas.

Instituto Nicaragüense de Seguridad Social (INSS), donde los empleados comercializaron la información a otras empresas, tales como las empresas de telemercadeo, los que a su vez ocuparon la información para poder tener referentes de ingresos de los ciudadanos y poder efectuar campañas agresivas de créditos, especialmente la venta de tarjetas de créditos. La información obtenida por estas empresas fue utilizada de manera irresponsable, pues sobrevino en un sobre endeudamiento de los ciudadanos, quienes a su vez por su falta de educación financiera y en su mayoría bajo índice de escolaridad, no previeron los problemas futuros.

En la exposición de motivos de la normativa sobre protección de datos se planteó como objetivo fundamental:

> *(…) la protección de la persona frente al tratamiento de sus datos personales, ya sea que estén almacenados en ficheros de datos públicos o privados, automatizados o no. Garantizándole sus derechos constitucionales establecidos en el Artículo 26, de la Constitución Política de Nicaragua, al mismo tiempo esta ley, regulara y facilitara los procesos legales y administrativos, para que el ciudadano pueda protegerse frente al tratamiento de sus datos (…)*[5].

SI analizamos el artículo 26 Cn[6], expresa que:

> *Artículo 26: Toda persona tiene derecho: A su vida privada y la de su familia; A la Inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo;(…). A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información*.

[5] Texto tomado de la exposición de motivos de la ley de protección de datos personales de Nicaragua. Website: http://legislacion.asamblea.gob.ni/Diariodebate.nsf/76ed72912dd57e570625698c00773f5d/f72538fe50a5946706257a1e0060d734?OpenDocument

[6] Constitución Política de Nicaragua.

Este artículo en particular es el principal fundamento de la normativa sobre protección de datos en el ámbito nacional, así como el recurso de *habeas data*, que abordaremos más adelante.

El término "vida privada" que en el referido artículo se menciona, en el derecho nicaragüense carece de claridad, puesto que el derecho tradicional civilista de origen romano, que tiene impregnado el derecho nacional, no lo aborda ampliamente. De igual manera, desinteresada, la jurisprudencia nacional no ha hecho esfuerzo por unificar criterios sobre este concepto, es más podría atreverme a mencionar que ni a definirlo. Mientras tanto en el derecho comparado ya se ha abordado ampliamente este tema, abordando diferentes concepciones, no unificándose criterios y con significados distintos en el tiempo y espacio para los diferentes sistemas jurídicos. Esta dicotomía la plantea de una manera muy veraz, el profesor constitucionalista **Christian Suárez Crothers** al decir:

> *Se trata ciertamente de una noción compleja, que se encuentra en plena etapa de elaboración, y que debido a esta misma complejidad ha dado lugar a manifestaciones diversas en el derecho comparado. En el Derecho angloamericano, como veremos, irá extendiendo su irradiación, por vía jurisprudencial, hacia ámbitos que pudieron haber parecido insospechados para los primeros sostenedores de la moderna teoría de la privacy, y su misma evolución presenta en el derecho americano problemas variados y muy discutidos por la doctrina. En el derecho continental europeo ha recibido distintas denominaciones y así se habla de "riservatezza", "derecho a la vida privada", "derecho a la intimidad", "derechos pertenecientes a la esfera de la vida privada", etc*[7].

Al imaginar el término de vida privada dentro de la esfera de las nuevas tecnologías la situación se vuelve demasiado delicada, con la globalización y traslados

[7] Christian Suárez Crothers, "El concepto de derecho a la vida privada en el derecho anglosajón y europeo". Revista de Derecho Valdivia, Vol. XI, diciembre 2000, pp. 103-120.

de los modelos de negocios y servicios a la internet, toda la información está preocupantemente más expuesta.

En la exposición de motivos de la Ley 787, se encuentra como justificación de la normativa este extracto que me permito transcribir:

> *(…) El actual contexto de desarrollo de la sociedad de la información propone circunstancias en las que es necesario repensar el contenido del derecho a la intimidad y a la privacidad, en virtud de los cambios vertiginosos de las tecnologías de la comunicación y de la información y de las necesidades de protección que las personas tienen frente a nuevos y sutiles peligros de abuso de estas tecnologías, que permiten hoy, de manera ineluctable, la conformación de perfiles de las personas, y un seguimiento constante de sus actividades, deseos y aspiraciones, en una verdadera conquista de la vida interior del ciudadano a través de las tecnologías (…)*[8].

No podemos decir, que la exposición de motivos trata de conceptualizar el derecho a la intimidad, y ni por cerca el de vida privada, sino que los mismos quedan abiertos a los cambios y evolución de las tecnologías.

Al igual que en otros artículos que he escrito sobre este tema, me llama la atención que la exposición de motivos de la ley 787, retoma el concepto de "perfiles de personas", término que va interrelacionado en su nacimiento con la psicología y que hoy en día se ha trasladado con mayor uso a las *TIC´s*[9] especialmente las redes sociales. Psicológicamente, perfiles de personas, es un término que denota las características de las aptitudes mentales de los individuos y que son determinadas por medio de pruebas específicas y científicas, muy utilizado en la psicología forense para prever o entender comportamientos de los individuos. Socialmente, lo podemos entender, como la ubicación del individuo dentro de clases o grupos sociales. En informática se ha generalizado desde hace unos años el término perfil, en el campo de

[8] Exposición de motivos de la ley de protección de datos personales de Nicaragua. Op cit.

[9] Anglicismo que significa Tecnologías de la Información y la Comunicación.

las redes sociales es donde se emplea aquel para referirse al nombre, a toda aquella información personal que posee y a la imagen que cada usuario presenta en los citados espacios web para darse a conocer o mostrarse el resto de internautas. Es decir un Avatar[10].

En la ampliamente referida exposición de motivos de la ley 787, se señalan otros aspectos importantes como son;

> *(…) La intimidad y la privacidad de los ciudadanos se desarrollan hoy en muy diversos ambientes, no sólo en el hogar y en el ámbito familiar. Las crecientes facilidades para la comunicación y el intercambio de información, incluso más allá de las fronteras del país, provocan la necesidad de que tales intercambios sucedan sin que haya riesgos de configurar perfiles de los ciudadanos o abusos de sus datos e información más allá del conocimiento y consentimiento de los afectados (…)*[11].

Si analizamos extensivamente esta exposición de motivos, podemos ver que se reconoce implícitamente, a juicio del autor, la importancia de la Internet e incluso el *Cloud Computing*[12]. Entendiendo que no todo lo que ocurre en la Internet es *Cloud Computing*. Pues, abarca hasta los negocios que tienen que ver con el internet, pero que necesariamente no requieren de este, tales como la venta de información.

En la discusión de la normativa sobre protección de datos, se les compara con derechos humanos de tercera generación, al decir que:

> *Se trata de una regulación propia de la tercera generación de derechos humanos, dirigida a alcanzar para el individuo medios para oponerse a los potenciales riesgos y peligros a los que se enfrenta en la sociedad tecnológica.*

[10] Palabra que proviene del sánscrito, nombre que recibían las reencarnaciones de los dioses, en la cultura hindú, cuando se presentaban ante los hombres, sea como ser humano o como animal.

[11] Exposición de motivos de la ley de protección de datos personales de Nicaragua. Op cit.

[12] Concepto tecnológico sobre un modelo de negocio en el que se prestan servicios de almacenamiento, acceso y uso de recursos informáticos relacionados con la Internet.

La base de solidaridad, que es idéntica para todos los derechos humanos de la tercera generación, también contribuye a configurar el derecho a la autodeterminación informativa como un medio de realización de una sociedad más abierta, más democrática, más participativa, resguardando aquellas trincheras donde las posiciones del individuo empiezan a sufrir embates ante las necesidades crecientes de información para la toma de decisiones en los más diversos campos, que pueden promover, junto a sus evidentes beneficios, el enorme peligro de objetivización e instrumentalización del ser humano.

Tal comparación a mí juicio son contradictorios con los intentos de actualizar la legislación nicaragüense con las tendencias mundiales, puesto que hoy en día ya no hablamos de derechos humanos de primera, segunda, tercera o cuarta generación. Sino, que se ven los derechos humanos como uno solo, sin darle un escalafón o lugar pues todos tienen la misma importancia ante la obligación de protección del Estado.

Un punto importante es el reconocimiento de la autodeterminación informativa[13], como un derecho fundamental e indispensable ante la privacidad.

Al reconocerse la autodeterminación informativa como un derecho fundamental e indispensable ante el derecho constitucional de la privacidad, es comparable a un derecho constitucional, gozando de todas y cada una de las prerrogativas que ley concede para la protección de estos derechos.

iii. **El Habeas Data**

En todo Estado de Derecho, uno de los pilares más importantes para una plena democracia es la protección de los derechos fundamentales de los individuos. Con los avances tecnológicos que hemos venido abordando y el uso de las *TIC´s*, se cambió el matiz o la visión de lo que constituye esa amalgama de derechos fundamentales. Por eso, es que la normativa en el derecho procesal y sustantivo tiene la difícil

[13] Facultad de todo individuo para ejercer control sobre su información personal, contenida en registros públicos o privados, específicamente -pero no excluyente – los contenidos en cualquier medio informático, pudiendo pedir su cambio, actualización supresión o publicación.

obligación de actualizarse constantemente para poder estar atento a cualquier violación que pudiere surgir a los referidos derechos fundamentales, con especial atención en este artículo, a los que tienen que ver con la protección de las bases de datos o *habeas data*. Son muchos los derechos fundamentales en juego, cuando de bases de datos hablamos, entre los que podemos mencionar: la libertad de información, de expresión, de acceso a la justicia, de privacidad e intimidad.

El habeas data, de similar manera que la protección de datos personales, tiene un origen, aunque mayor, el cual podemos remontarlos a los tiempo de Juan sin Tierra[14], donde aparece la primera medida de protección al derecho a la intimidad, el *habeas corpus*, que se refería cuando se encerraba a una persona sin justa causa. Por ello, conocemos el *habeas corpus* como *traer el cuerpo*.

Cuando aparecieron en la historia de la humanidad los computadores y la internet como tal la conocemos hoy en día, hay un enorme flujo de información personal que circula con creciente intensidad, sin que muchas veces los titulares de esa información tengan conciencia o noticia de ello. Así justificadamente es que aparece el habeas data como un mecanismo de protección a la información personal.

Como referimos anteriormente el concepto de vida privada es más amplio que lo que desarrolla la legislación nacional, pues se reconoce internacionalmente el derecho a la intimidad personal y familiar, derecho a la imagen propia y el derecho al secreto de las comunicaciones, siendo este último uno de los más protegidos.

El habeas data como significado etimológico, podríamos conceptualizarlo como *traer los datos*, sirviendo como una herramienta para garantizar los llamados excesos del denominado *poder informático*. En Alemania, con la promulgación de la *Hessiches Datenschutzgesetz* del 7 de abril de 1970, como indicamos anteriormente, este territorio se convirtió en el primero con una norma dirigida a la protección de datos,

[14] Rey de Inglaterra, perteneciente a la dinastía Plantagenet (Oxford, 1167 - Newark, Nottinghamshire, 1216). Era el quinto hijo de Enrique II, quien le dejó sin territorio en el reparto de la herencia (de ahí procede el sobrenombre que le puso su propio padre). Sin embargo, pronto se hizo con un patrimonio y se convirtió en un importante señor de vasallos.

que tiene como fin impedir la lesión de bienes dignos de tutela de las personas interesadas, garantizando los datos relativos a su persona de abusos cometidos con ocasión de su almacenado, transmisión, modificación o cancelación.

En Suecia, el 11 de mayo de 1973, se promulgó el *Data lag*, con la misma finalidad de proteger a los individuos del mal uso de los datos y de la información personal, por medio de registros y archivos.

El 31 de diciembre de 1974, con el escándalo *Watergate* y con el temor sobre el uso que el Gobierno pudiera hacer de los ordenadores y de los sistemas informáticos, el Congreso norteamericano promulga el *Privacy Act*. Teniendo como premisa la protección de los individuos frente el asalto a su intimidad por sistemas de acopio y almacenamiento de datos derivados del uso de la tecnología informática por las agencias federales.

En Portugal en 1976 establecen en su Constitución el artículo 35 indicando que todos los ciudadanos tienen derecho a tomar conocimiento de los datos contenidos en ficheros o registros informáticos a su respecto, pudiendo exigir su rectificación y actualización, sin perjuicio de lo dispuesto por las leyes sobre secretos de Estado (...)

En 1978, Francia estableció la Comisión *Nationale de la Informatique et des Libertes*, una institución colegiada, encargada de elaborar un registro o archivo de archivos en el que se inscriben los diversos bancos de datos, así como su naturaleza, su funcionamiento y sus finalidades. Los ciudadanos pueden ejercer su derecho a la información sobre sus datos.

También en 1978, la Constitución española incorporo por medio del inciso 4 del artículo 18, lo que se lee: La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos (...).

En 1984, el Parlamento británico promulgó el *Data Protection Act*, cuerpo legal destinado a proteger una parte especial de la intimidad de las personas: la que tiene que ver con sus datos personales.

En 1984, la Constitución de Brasil, en su artículo 5, inc. 72, incorporó la norma que expresa: se concederá el habeas data para: a) asegurar el conocimiento de información relativa a la persona del demandante, que consiste en registros o bancos de datos de entidades gubernamentales o de carácter público y b)rectificar datos cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo. En Brasil se presenta el habeas data como un procedimiento independiente del amparo.

En Perú, la Constitución de 1993 prohíbe expresamente que los servicios informáticos, computarizados o no, públicos o privados, suministren informaciones que afecten la intimidad personal o familiar (artículo 2, inciso 6.) Posteriormente, el artículo 200 establece el procedimiento del habeas data. En este último caso, la Constitución peruana presenta como instrumento innovativo para regular esta materia al Habeas Data.

En Argentina, con la Constitución Federal de 1994, el artículo 43 declara: (...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad que conste en registros o bancos de datos públicos destinados a proveer informes, y en caso de falsedad y discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto a las fuentes de información periodísticas. (...)

En Nicaragua se ha desarrollado el habeas data con base al artículo 26 Cn que dice:

> *Toda persona tiene derecho: A su vida privada y la de su familia; A la Inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo;(…). A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información*.

La inclusión de esta figura de *habeas data*, se hizo dentro la ley especial con rango constitucional denominada Ley de Amparo. Al incluir un artículo 5 bis, que dice:

El Recurso de Habeas Data se crea como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya una invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar. El Recurso de Habeas Data procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales y su publicidad indebida.

Podemos indicar que de esta forma por primera vez se abrió en Nicaragua una puerta procesal para el tratamiento de la protección de datos personales, de los cuales hablamos ampliamente en el inciso anterior.

Probablemente en los últimos cinco años, el habeas data ha venido cobrando una importancia relevante en América Latina, puesto que las interrelaciones entre los individuos, desde el punto de vista social, legal y comercial ha venido evolucionando. Últimamente los modelos de negocios han estado migrando de la esfera convencional, *Face to Face*[15] al modelo digital ó *e-commerce*[16]. Similar ocurre en el ámbito institucional donde las administraciones públicas para lograr ser más eficientes han optado por migrar sus servicios u operatividad a la *web*[17], es lo podríamos conocer como la *web 2.0*[18].}

El derecho como ente regulador de relaciones entre los individuos ha tomado participación en las relaciones de los individuos logrando establecer limitantes en los abusos de poder que pudieren o han surgido.

[15] Frase anglosajona que significa cara a cara, se ha adoptado para designar las operaciones o actividades que se hacen con presencia física de las partes.

[16] Acrónimo anglosajón que se refiere al comercio electrónico.

[17] Acrónimo anglosajón que significa World Wide Web ó Internet. En español se traduciría como Red Informática Mundial.

[18] Sitios web centrados en el usuario, la navegabilidad está centrada en la operatividad, su diseño está centrado en el usuario y el dinamismo de servicios.

El Hábeas Data como garantía procedimental de tutela de la autodeterminación informativa del ciudadano pretende crear esta posibilidad de control por parte del ciudadano como un paso más al reconocimiento de nuevas garantías de cara a la era de la información.

Algunos tratadistas, sobre este tema, especialmente en Alemania han criticado el empoderamiento a los individuos sobre el control de sus datos frente al interés del Estado en la investigación de los delitos.

El problema se ha dado de manera específica en los procesos penales donde las autoridades se ven en la necesidad de tener herramientas eficaces que permitan hacerle frente a los retos de la era de la información, sea ampliando las competencias policiales en las investigaciones, por medio de nuevas tecnologías, lo que lógicamente significaría una reducción al amplio terreno que han ganado la protección de datos en Europa.

Por un lado, los defensores de la autodeterminación informativa frente a los abusos de poder de parte de las empresas y el Estado, pero por el otro tenemos a los de la línea populista que en la doctrina penal moderna se apoyan en el *"derecho fundamental a la seguridad"*, que busca conseguir una seguridad pública hacia los ciudadanos, a cualquier costo y con ayuda de las tecnologías que permiten un mayor acceso a la información de los individuos, obteniéndola de sus propias computadoras por medio de las redes de Internet y otras, como también por los más variadas formas como por ejemplo las informaciones contenidas en las tarjetas de crédito. Sin embargo, hay un amplio sector que pregona su oposición a los excesos por parte del Estado y exige la protección de derechos de protección a la persona como el de la intimidad, a la personalidad, a la dignidad y el de autodeterminación de la información.

iv. Regulación penal sobre el manejo de datos personales.

El derecho penal ha venido adaptándose a las nuevas tendencias del derecho penal, logrando mutar sus normas a las nuevas exigencias de la sociedad. Hoy en día se centra más en la eficiencia de métodos preventivos y los nuevos modelos de

negocios. Es por esto que en muchos países se está trabajando en proyectos de reformas a la leyes procesales, como es por ejemplo el caso de Alemania, que en su proyecto ha tomado en consideración cuestiones como los nuevos poderes que gozan los policías con tecnologías de avanzada y su posible extralimitación de estos en perjuicio de los derechos a las personas, así también ha tomado en cuenta la protección de datos en las redes como la INTERNET, por la gran cantidad de consumidores y usuarios que utilizan estas redes, que no solo afectan a individuos sino también a instituciones del estado, empresas privadas y al comercio en general.

Todas las nuevas legislaciones, penales y no penales, en las que la tecnología pueda tener alguna incidencia en su materia, están obligadas a adaptarse. Así por ejemplo se debe entrar a analizar cuestiones como los secretos comerciales que pueden ser robados de los mismas bases de datos de las empresas por personas extrañas o hasta de los mismos empleados, como también los procesos de seguridad transaccional y encriptamiento como posibles formas de cometer crímenes en la red, en donde el estado debe determinar hasta qué grado establecer medidas de control de informaciones en la red y en qué grado dar libertades en virtud de derechos como el de la privacidad.

Dentro de la normativa penal nicaragüense, que tiene relevancia con la protección de los datos personales, o especialmente con delitos de índole informático, que usualmente están relacionados entre sí, encontramos de manera diversa y dispersa en todo el código penal, no hay un capitulo único para ellos, por lo que trataremos de mencionar los supuestos penales en los que a juicio del autor pueda haber relevancia con los datos personales.

- La pornografía. El código penal prevé la manipulación de los derechos de imagen de la persona sin su consentimiento, como una forma de proteger la dignidad de la persona, su vida privada y la autodeterminación informativa, puesto que la imagen es parte de los datos sensibles de una persona.

- Registros prohibidos. Se penaliza la facilitación, autorización, creación y comercialización cualquier base de datos o registro informáticos con datos que puedan afectar a las personas naturales o jurídicas.

- Acceso y uso no autorizado de información. Se penaliza al que sin la debida información utilice los registros informáticos de otros, o ingrese, por cualquier medio, a su banco de datos, o archivos electrónicos.

-Estafa. A quien consiga la transferencia no autorizada de cualquier activo patrimonial mediante la manipulación de registros informáticos o programas de computación o el uso de otro artificio semejante.

-Destrucción de registros informáticos. Comete este delito quien destruya, borre o de cualquier modo inutilice registros informáticos.

-Uso de programas destructivos. Comete este delito quien con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación.

-Apoderamiento de secretos de empresa. Quien, en provecho propio o de un tercero, se apodere por cualquier medio, de información, de datos, documentos escritos o electrónicos, registros informáticos u otros medios u objetos que contengan un secreto empresarial, sin autorización de su poseedor legítimo o del usuario autorizado.

- Acceso indebido a documentos o información pública reservada. Comete este la autoridad, funcionario o empleado público que acceda o permita acceder a documentos o información pública cuyo acceso esté reservado conforme a la ley de la materia.

- Revelación, divulgación y aprovechamiento de información. Comete este delito La autoridad, funcionario o empleado público que revele o divulgue informaciones o documentos declarados como información pública reservada o información privada.

- Denegación de Acceso a la Información Pública. Se castiga a la autoridad, funcionario o empleado público que fuera de los casos establecidos por la ley, deniegue o impida el acceso a la información pública requerida.

- Violación a la autodeterminación informativa. Se penará a la autoridad, funcionario o empleado público que divulgue información privada o se niegue a rectificar, actualizar, eliminar, información falsa sobre una persona contenida en archivos, ficheros, banco de datos, o registros públicos.

- Uso de información reservada. Se sanciona a la autoridad, funcionario o empleado público que haga uso de cualquier tipo de información reservada de la cual ha tenido conocimiento en razón o con ocasión de la función desempeñada con ánimo de obtener un beneficio económico para sí o para un tercero.

III. La administración tributaria.

i. El suministro de información a la administración tributaria.

La Administración Tributaria como un ente descentralizado del poder ejecutivo, está en la obligación de velar por el cumplimiento de lo preceptuado en el artículo 26 de la Constitución Política de Nicaragua. No obstante, la facultad fiscalizadora que posee para hacer cumplir con la obligación de tributación de los ciudadanos está limitada por los derechos fundamentales, especialmente el derecho a la intimidad y el derecho a la privacidad.

Hablar del tema de datos personales, sigilo tributario, autodeterminación informativa, es menester de un estudio más amplio que estas líneas, sin embargo pasaremos de manera somera frente a los puntos más tangenciales sobre ello.

En el referido artículo 26 Cn parte infine se refiere a la facultad fiscalizadora que posee la Administración Tributaria al indicar que:

> *(…) La Ley fija los casos y procedimientos para el examen de documentos privados, libros contables y sus anexos, cuando sea indispensable para*

esclarecer asuntos sometidos al conocimiento de los Tribunales de Justicia o por motivos fiscales.

Las cartas, documentos y demás papeles privados sustraídos ilegalmente no producen efecto alguno en juicio o fuera de él.

El código tributario especifica la obligación de suministrar información, con la salvedad que la misma tiene que ser para fines fiscales, entendiendo que la finalidad fiscal es medir la capacidad contributiva de los individuos.

El artículo 27 Ctr[19] indica sobre la obligación de suministrar información y el valor probatorio de la misma que:

Únicamente para fines y efectos fiscales, toda persona natural o jurídica, sin costo alguno, está obligada a suministrar toda información que sobre esa materia posea en un plazo de diez (10) días hábiles y que sea requerida por la Administración Tributaria. Para efectos de la información de terceros contribuyentes, deberá suministrarse únicamente el número de RUC del contribuyente, o nombre y número de cédula en defecto de éste, fecha y monto de las transacciones. (…). Si la información de terceros contribuyentes solicitada por la administración tributaria se obtiene mediante requerimiento general, la administración tributaria no estará obligada a notificar a las personas naturales o jurídicas sobre la obtención de esa información. En caso que la información de terceros contribuyentes solicitada por la administración tributaria se obtenga mediante requerimiento específico de contribuyentes, la administración tributaria estará obligada a notificar a las personas naturales o jurídicas sobre la obtención de esta información. Toda información obtenida por la Autoridad Tributaria es de irrestricto acceso de la persona natural o jurídica sobre la cual se solicitó la misma.

[19] Código Tributario.

Las autoridades de todos los niveles de la organización del Estado, cualquiera que sea su naturaleza, y quienes en general ejerzan funciones públicas están obligados a suministrar a la Administración Tributaria cuantos datos y antecedentes con efectos tributarios requiera, mediante disposiciones de carácter general o a través de requerimientos concretos y a prestarle a ella y a sus funcionarios apoyo, auxilio y protección para el ejercicio de sus funciones. Para proporcionar la información, los documentos y otros antecedentes, bastará la petición de la Administración Tributaria sin necesidad de orden judicial. Asimismo, deberán denunciar ante la Administración Tributaria correspondiente la comisión de ilícitos tributarios que lleguen a su conocimiento en cumplimiento de sus funciones.

La obligación de los profesionales de facilitar información con trascendencia tributaria a la Administración Tributaria no alcanzará a los datos privados no patrimoniales que conozcan por razón del ejercicio de su actividad, cuya revelación atente al honor o a la intimidad personal y familiar de las personas.

Los profesionales no podrán invocar el secreto profesional a efectos de impedir la comprobación de su situación tributaria.

La Administración Tributaria podrá suscribir Acuerdos Internacionales de Información con otras Administraciones Tributarias en el extranjero que permitan fortalecer la acción fiscalizadora de la Institución. Toda información que por esta vía se solicite y se obtenga, también deberá cumplir con el requisito establecido en el párrafo segundo del presente artículo.

Podemos observar varios elementos en el enunciado anterior, especialmente el principio de autodeterminación informativa. Por cuanto, el contribuyente tiene derecho a saber sobre qué información posee la administración tributaria y con qué fin.

A criterio personal, podría referirme que la información no solo es un elemento importante dentro de las actividades de fiscalización, sino el más importante de todos. Siendo el activo más importante de una administración tributaria moderna.

La información coadyuva a la comprobación del cumplimiento de las obligaciones tributarias. Las obligaciones tributarias como tales son unos indicadores de riquezas muy acertados, así como indicadores comerciales reales y poderosos.

Una Administración tributaria moderna necesita la mayor cantidad de información necesaria, vinculada a los efectos fiscales, pero aún esa necesidad encuentra un *stop*, con los derechos fundamentales como son el derecho a la intimidad y la privacidad.

El artículo 126 Ctr. Parte infine del inciso 5, prevé que las limitantes al requerimiento de información, al decir:

> *Son infracciones administrativas tributarias por incumplimiento de deberes y obligaciones de los contribuyentes y responsables (…):*
>
> *5. (…); y no suministrar las informaciones que les fueren solicitadas en base a la ley y documentación respectiva de respaldo, cuando la Administración Tributaria así lo requiera.*

Podemos observar que si bien existe la obligación de información esta tiene que ser solicitada en estricto apego a la ley, lo que en síntesis debe ser que la información solicitada sea de índole fiscal y que la misma sea para fines fiscales.

ii. Deber de confidencialidad y el sigilo tributario.

En la normativa nicaragüense se expresa de manera clara los deberes de confidencialidad y de guardar el sigilo tributario para las autoridades de la administración tributaria.

Los términos de confidencialidad y sigilo tributario no son nuevos y menos inventados en la normativa nacional, pues responden a las exigencias y directrices internacionales, tales como el modelo de código tributario para Latinoamérica,

publicado por el CIAT[20], el que sirvió de base para la elaboración del actual código tributario nicaragüense.

En doctrina española al sigilo tributario se le conoce como secreto tributario, lo cual constituye el régimen de protección y reserva de la información obtenida por la Administración tributaria frente a su revelación a terceros y uso desviado de la misma[21]. Dicho término proviene término *Stuergeheimnis, Tax Secrecy*[22], que indica un régimen de confidencialidad y reserva de la información obtenida por la administración tributaria.

Sin embargo este sigilo tributario o secreto tributario, tiene una reserva de ley y es que la información sea de índole fiscal y la misma solo sea utilizada para fines fiscales, sancionando –como vimos en la normativa penal- el uso de la información para otros fines.

El artículo 68 Ctr. establece este derecho a la confidencialidad de manera expresa al decir:

> *Los contribuyentes o responsables tienen derecho a la privacidad de la información proporcionada a la Administración Tributaria. En consecuencia, las informaciones que la Administración Tributaria obtenga de los contribuyentes y responsables por cualquier medio, tendrán carácter confidencial. Sólo podrán ser comunicadas a la autoridad jurisdiccional cuando mediare orden de ésta.*
>
> *La Administración Tributaria mediante la normativa Institucional correspondiente, establecerá la implementación de programas de control y*

[20] Organismo internacional, sin fines de lucro que provee asistencia técnica especializada para la actualización y modernización de las administraciones tributarias. Así como en temas de valores de integridad, transparencia y ética, con la disposición de prevenir y combatir todas las formas de fraude, evasión y elusión tributaria facilitando el cumplimiento voluntario.

[21] Sanchez Serrano L. Comentarios al artículo 112 LGT, , en comentarios a las leyes financieras y tributarias. Edersa, Madrid, 1987, p.124.

[22] Calderón Carrero, Jose Manuel, El derecho de los contribuyentes al secreto tributario. Fundamentación y consecuencias materiales y procedimentales. Universidad de Coruña. España. Netbiblo, S.L. 2009. Pág 19.

programas de computación específicos para la administración y control de la información de los contribuyentes y responsables.

La Administración Tributaria deberá proporcionar al Ministerio de Hacienda y Crédito Público, mensualmente o cuando lo requiera, la información necesaria correspondiente para fines de evaluación de la política fiscal.

Podemos observar en la normativa también cuales son las excepciones específicas para el traslado de información a una persona distinta a la autoridad tributaria; entendiéndose que serán las autoridades judiciales y el Ministerio de Hacienda y Crédito Público para poder evaluar la política fiscal (aunque este caso muy difícilmente se brinden los datos a nivel individualizados que permitan la identificación particular de cada contribuyente, por lo general de hace de manera macro).

En materia tributaria sustantiva, especialmente en el tema de precios de transferencia, se aborda la confidencialidad de los datos que se suministren a la administración tributaria –por ser estas fiscalizaciones o comprobaciones más intensas que las fiscalizaciones comunes- al decir en su artículo 99 párrafo segundo, con respecto a los análisis de comparabilidad:

(…) Toda la información suministrada por el contribuyente, deberá ser catalogada como confidencial a la hora de que la Administración Tributaria lleve a cabo dichos estudios y será manejada como tal para tales efectos (…).

Este tipo de fiscalizaciones son de mucho más cuidado para las empresas y los contribuyentes particulares, por cuanto tiene trascendencia internacional, con respecto a las operaciones de los mismos.

Igualmente, en el Título VI, referente a la Administración Tributaria, Capítulo I, Facultades y Deberes de la Administración Tributaria, Sección III, se habla del Sigilo Tributario. Se habla de manera textual del sigilo tributario y se indica en el artículo 151:

Los funcionarios y las personas naturales y/o jurídicas que intervengan en los diversos trámites relativos a la aplicación de las disposiciones tributarias, estarán obligados a guardar sigilo tributario.

El sigilo tributario no comprenderá los casos en que la Administración Tributaria deba suministrar datos a:

1. Las autoridades judiciales en los procesos de cualquier clase de juicio y a los tribunales competentes;

2. Los restantes organismos que administren tributos, en tanto las informaciones estén estrictamente vinculadas con la fiscalización y percepción de los tributos de sus respectivas jurisdicciones;

3. La Contraloría General de la República cuando se encuentre revisando exclusivamente las declaraciones de probidad de los empleados y funcionarios públicos;

4. Las Administraciones Tributarias de otros países en cumplimiento a los convenios internacionales de intercambio de información tributaria; y,

5. Un contribuyente que solicite por escrito, información sobre sus propias obligaciones fiscales.

Podemos observar cuales son, de manera taxativa, los enunciados en los que se puede faltar al sigilo tributario en la legislación nicaragüense. Cualquier otro fáctico fuera de los enunciados y que no esté sustentado en una ley especial (como ley de alimentos, ley creadora de la Unidad de Análisis Financiero) estaría al margen de la legalidad.

Entonces tomando como premisa el deber de contribuir al sostenimiento del estado versus el derecho a la privacidad o la intimidad. Podemos deducir que el primero priva sobre el derecho a la privacidad o la intimidad.

La Administración Tributaria en virtud de poder obtener datos con fines tributarios, estos podrían incluir a los datos potenciales, indirectos e hipotéticos. Según la normativa esgrimida la Administración Tributaria está habilitada por imperio de ley a solicitar la información que crea necesaria o que considere necesaria para el cumplimiento de las obligaciones tributarias.

Si nosotros analizamos los datos referentes a la actividad económica de los contribuyentes, está por sí no tiene relevancia con la vida privada y familiar del contribuyente. No obstante, podemos considerar como el dato del domicilio del contribuyente constituye una manifestación del derecho a la intimidad. También podríamos considerar el derecho a la privacidad de las comunicaciones, donde la administración tributaria tendría una herramienta indispensable de comprobación del comportamiento del contribuyente frente a la facultad de poder fiscalizar o investigar las comunicaciones de los contribuyentes sin autorización judicial, en Nicaragua es imposible a la autoridad tributaria poder intervenir comunicaciones sin autorización de la autoridad judicial. Por último, como una manifestación del derecho a la intimidad o vida privada de los contribuyentes, se menciona el derecho que tiene la autoridad tributaria sobre corroborar la capacidad contributiva de los contribuyentes por medio de una averiguación de las cuentas bancarias de estos.

A manera conclusiva, podemos inferir que el derecho a la protección de los datos personales, es un principio consagrado en la Constitución Política de Nicaragua, la cual tiene mecanismos de protección específicos y a criterio personal muy eficaces. No obstante, tal protección tiene sus limitantes, en lo que refiere a este artículo, como el deber de contribución con el sostenimiento de la carga pública. Sin embargo, el estado debe de hacer un uso responsable de esa facultad, acorde a la legislación vigente.

La protección de datos personales de los ciudadanos es una obligación para el Estado. Pero, es responsabilidad de su titular hacer valer la importancia de sus datos.

IV. **Bibliografía**

GARCÍA OBREGÓN, Jorge Luis, La protección de datos personales en Nicaragua (Parte 1), revista digital El Derecho Informático No 16, Argentina, Red Iberoamericana Elderechoinformatico.com, 2013.

GARCÍA OBREGÓN, Jorge Luis, La protección de datos personales en Nicaragua (Parte 2), revista digital El Derecho Informático No 17, Argentina, Red Iberoamericana Elderechoinformatico.com, 2014.

GARCÍA OBREGÓN, Jorge Luis, Análisis de la ley nicaragüense de protección de datos personales, artículo, España, Observatorio iberoamericano de protección de datos, oipdrodat.com, 2014.

GARCÍA OBREGÓN, Jorge Luis, La necesidad de la protección de datos personales en Nicaragua, artículo, España, Observatorio iberoamericano de protección de datos, oipdrodat.com, 2014.

GARCÍA OBREGÓN, Jorge Luis, Recurso de Habeas Data en Nicaragua, artículo, España, Observatorio iberoamericano de protección de datos, oipdrodat.com, 2013.

GARCÍA OBREGÓN, Jorge Luis. et. al., Protección de datos y habeas data: una visión desde Iberoamérica. Accésit 2014, España, XVIII Edición Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. AEPD, Obra Ganadora en Investigación Grupal. 2014.

ARIAS Kristy, BALTODANO Fernando, El habeas data, Trabajo Académico. Curso de Derecho Informático DE-2108, Profesor del curso: Lic. Guillermo Augusto Pérez Merayo, Universidad de Costa Rica, Facultad de Derecho. Disponible en: http://www.derecho.ucr.ac.cr/~gapmerayo/cursos/cursoDI/trabajosclase/habdata/habdata.htm

HERRERO DE EGAÑA, Juan Manual, Intimidad, tributos y protección de datos personales. Revista para el análisis del derecho INDRET, España, www.indret.com, 2007.

CALDERÓN CARRERO, Jose Manuel, El derecho de los contribuyentes al secreto tributario. Fundamentación y consecuencias materiales y procedimentales. Universidad de Coruña. España. Netbiblo, S.L. 2009.

ASAMBLEA NACIONAL, Nicaragua, Ley 787, Ley de Protección de Datos Personales. 2012.

ASAMBLEA NACIONAL, Nicaragua, Exposición de Motivos de la Ley de Protección de Datos Personales. 2008.

ASAMBLEA NACIONAL, Nicaragua, Dictamen de Comisión de la Ley de Protección de Datos Personales. 2012.

ASAMBLEA NACIONAL, Nicaragua, Ley No 831, Ley de reforma y adiciones a la Ley No 49, Ley de Amparo, 2013.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, Ginebra. Principios rectores para la reglamentación de los ficheros computarizados de datos personalizados. Resolución 45/95. 1990.