UNIVERSIDAD DE CASTILLA-LA MANCHA (UCLM)

UNIVERSIDAD APEC (UNAPEC)

TRABAJO FIN DE MÁSTER

ANÁLISIS DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES ANTE LA OBTENCIÓN E INTERCAMBIO DE INFORMACIÓN POR PARTE DE LA ADMINISTRACIÓN PÚBLICA

Para optar por el título de:

MASTER EN JUSTICIA CONSTITUCIONAL Y DERECHOS FUNDAMENTALES

Proponente:

Yenevi de Jesús Álvarez García

Director:

María Mercedes Serrano Pérez

Maestría en Justicia Constitucional y Derechos Fundamentales con doble titulación UCLM-UNAPEC, programa 2019-2020.

Santo Domingo, Distrito Nacional,

octubre 2020.

TABLA DE CONTENIDO

INTRODUCCIÓN

El derecho de protección de datos es un derecho fundamental el cual debe ser debidamente garantizado. Dicho derecho es la vía que posee cualquier persona sobre la disposición y control de sus datos personales, facultándolo a decidir cuáles datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, conforme a la definición otorgada por el Tribunal Constitucional español mediante la STC 292/2000 de fecha 30 de noviembre en su fundamento jurídico 7. Además, le permite saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

En ese sentido, la previsión constitucional de la tutela de los derechos frente al uso de la informática se proyecta sobre los datos personales e implica, por un lado, derechos y garantías para los titulares de esos datos de carácter personal. Por el otro, supone para quienes los recogen, tratan, transmiten, ceden o conservan, una serie de obligaciones en lo que se refiere a la calidad y a la seguridad de la información de esa naturaleza que manejan y a las condiciones en que pueden utilizarla, almacenarla, facilitarla o cederla[1].

En República Dominicana la configuración jurídica del derecho de protección de datos era en sus inicios legal, ya que existían diversas leyes sectoriales que regulaban dicho derecho, sin embargo, con anterioridad a la Constitución dominicana del 2010 no existía disposición alguna que de manera expresa estableciera el citado derecho como fundamental. Luego de la promulgación de la Carta Magna en el 2010 se le otorgó un reconocimiento de derecho fundamental en su artículo 44.2. Para el año 2013 se promulgó la Ley No.172-13 sobre protección de datos de carácter personal, lo que significó un gran avance para el fortalecimiento y desarrollo del Estado Social y Democrático de Derecho consagrado por la Constitución en su artículo 7, aunque con sus carencias como estableceremos más adelante.

De manera general, realizaremos un trabajo en base a la realidad de la normativa de nuestro país, y la evolución de las normativas en España en relación al derecho de protección de datos, con la Ley Orgánica 3/2018, de 5 de diciembre, y en el ámbito europeo, con el Reglamento (EU) 2016/679 de 27 de abril, los cuales fueron creados a los fines de ir acorde a los avances de la

[1] MURILLO DE LA CUEVA, Pablo Lucas, "La Construcción del derecho a la autodeterminación informativa", **Revista de Estudios Políticos**, núm. 104, abril-junio 1999, p.36.

tecnología lo que ha provocado, en el orden internacional, la aprobación e implementación de nuevos y más efectivos instrumentos de tutela.

En dicho contexto, el tema a tratar es el "Análisis del derecho de protección de datos personales ante la obtención e intercambio de información por parte de la administración pública". Al respecto, dicho derecho no puede ser considerado absoluto, al igual que otros derechos fundamentales, por ello, ante posibles requerimientos por parte de los poderes públicos, los datos personales en algunas ocasiones deben ser cedidos. En consecuencia, en el presente trabajo, analizaremos el tema de la forma siguiente:

I. Generalidades del derecho de protección de datos personales, verificando su conceptualización y reconocimiento constitucional, así como la naturaleza jurídica del mismo y la normativa aplicada tanto en España como en República Dominicana. Asimismo, los principios del derecho de protección de datos personales, el consentimiento que debe otorgar el titular de los datos y los derechos del mismo;

II. Por otro lado, trataremos el tema sobre la utilización de datos por parte de la administración pública. Se tomará en cuenta tres acápites sobre las actuaciones de la administración pública frente al derecho de protección de datos, tales como: tributaria, sanitaria y estadística. Asimismo, se abordará sobre otras bases legítimas existentes para la obtención de datos personales como excepción al requerimiento del consentimiento, así como la existencia del carácter reservado a los datos obtenidos por parte de la administración pública.

III. A su vez verificaremos los mecanismos y garantías por parte del titular de los datos personales, entre los que se destacan: acción de *hábeas data*, derecho de indemnización y procedimiento de tutela del derecho de protección de datos.

IV. Finalmente, se propondrá un tema en relación a la creación de una autoridad única para la protección de los datos personales en la República Dominicana, siendo esto ya una realidad en otros países, tal como es el caso de España.

En consecuencia, respecto al derecho de protección de datos personales la administración pública debe ser considerada como una gran creadora de ficheros que almacenan datos de carácter personal, los cuales son necesarios para cumplir con eficacia sus funciones. Dicha posición de responsable de los ficheros y de los datos obliga al poder público a someterse a todas las prescripciones de la Ley, especialmente aquéllas que tienen que ver con las obligaciones del responsable, con el fin de respetar el derecho a la protección de datos. Aunque también hay que señalar que, tratándose de datos recabados por el poder público, se prevén un conjunto de excepciones al consentimiento, al derecho de información y al ejercicio de los derechos de acceso, rectificación y cancelación[2]. No obstante, dichas excepciones, tal es el caso de España, constituyen limitaciones al ejercicio del derecho fundamental a la protección de datos, lo cual han de realizarse con las debidas cautelas, con el fin de no dejar vacío el contenido esencial del derecho, pues de otra manera se rebasaría el límite constitucional permitido[3].

[2] SERRANO PÉREZ, María Mercedes, **Los Derechos al Honor, a la intimidad personal y familiar y a la propia imagen. La inviolabilidad del domicilio. La protección de datos,** GARCÍA GUERRERO, José Luis, (Coord), Los Derechos Fundamentales: La vida, la igualdad y los derechos de libertad, Tirant lo Blanch, Valencia, 2013, p.492.

[3] STC 292/2000 del Tribunal Constitucional español de fecha 30 de noviembre, F.J.9.

I. DERECHO DE PROTECCIÓN DE DATOS PERSONALES

En el presente capítulo abordaremos el derecho de protección de datos personales, en el cual verificaremos su conceptualización y su reconocimiento constitucional, así como su naturaleza jurídica. Por otro lado, realizaremos un análisis comparativo de la normativa dominicana y española vigente, de los principios de protección de datos personales, la necesidad del consentimiento como forma de proteger el derecho de protección de datos y finalmente los derechos que poseen los titulares.

A. Conceptualización y reconocimiento constitucional

En el contexto europeo, las leyes de la primera generación[4] utilizan de forma genérica el concepto de *hábeas data*, así como parte de la doctrina de los años 80. Sin embargo, más adelante el Tribunal Federal alemán en 1983 emite la sentencia relativa a la Ley del Censo, utilizando el concepto de 'derecho a la autodeterminación informativa'[5]. En los años 80 y 90 se entremezclan el uso del concepto genérico de 'privacy' y el de 'libertad informática'. Posteriormente, con la entrada en vigor del Convenio 108 del Consejo de Europa será el punto de inicio del uso generalizado del concepto de protección de datos, incluso en el ámbito anglosajón, no obstante, el concepto de 'privacy' tenía una pluralidad semántica para referir de forma genérica derecho a la vida privada y protección de datos de carácter personal, circunstancias hoy superada, de tal forma que el uso del concepto de protección de datos, es más conocido[6].

---

[4] REBOLLO DELGADO, Lucrecio y SERRANO PÉREZ, María Mercedes, **Manual de Protección de Datos**, Tercera Edición, Editorial Dykinson, S.L, Madrid, 2019, p. 30. Leyes primera generación: el conocimiento de los datos es difícilmente generalizable o instrumentalizable, por ello la protección se centra sobre el espacio físico en que se ubica la información (ordenador y base de datos) y se lleva a cabo mediante la autorización previa para su acceso y uso. Esta primera generación de normas habría que incluir la Datenschutz del 7 de octubre del 1970, la Data Lag sueca de 11 de mayo de 1973 y la Landesdatenschutzgesetz de 24 de enero de 1974 del Land de Renania-Palatinado.

[5] MURILLO DE LA CUEVA, Pablo Lucas, "El derecho a la autodeterminación informativa y la protección de datos personales", **Revista Azpilcueta**, núm.20, 2008, p.44. (…) Hablar del derecho a la autodeterminación informativa es hablar de la protección de los datos de carácter personal, del mismo modo que tratar de la protección de datos de carácter personal es tratar del derecho a la autodeterminación informativa. Hay, pues, plena coincidencia y la diferencia de denominaciones obedece a que una, la primera, acuñada por Alemania y utilizada por su Tribunal Constitucional Federal en su Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo, se fija en la principal facultad que encierra este derecho: la de que su sujeto, su titular, es decir, cualquier persona, decida, consienta de forma informada y libre el uso por terceros de datos que le conciernen. En cambio, la segunda denominación que, como veremos, es la acogida por la LOPD, por nuestro Tribunal Constitucional y por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, utiliza una expresión que pretende denominar el conjunto de medios jurídicos a través de los cuales se satisface aquella facultad.

[6] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.38.

Lucas Murillo ha definido la autodeterminación informativa como: *"el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad, nuestra dignidad y libertad. En su formulación como derecho, implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informáticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito"*[7].

En el ordenamiento jurídico español, el derecho a la protección de datos de carácter personal aparece reconocido en el artículo 18.4[8] de su Constitución. No obstante, del precepto constitucional español no se puede deducir con claridad ni el objeto ni el concepto de dicho derecho, pues como afirma Serrano Pérez, su redacción es deudora, por el tiempo en el que se elaboró la Constitución española, de las carencias materiales del momento. Además, señala que dicho precepto se refiere, aunque no explícitamente, a la necesidad de preservar los datos de los ciudadanos, que pueden afectar a la intimidad o al honor, frente a las posibilidades de la informática[9].

En el caso español ha sido la jurisprudencia del Tribunal Constitucional, recogiendo la interpretación de los convenios y textos internacionales sobre el tema y la jurisprudencia del Tribunal de Justicia de la Unión Europea, la que ha concretado el significado y contenido del derecho contemplado en el artículo 18.4 de la CE, relativo a la protección de datos de carácter personal, diseñando un derecho con los elementos necesario para satisfacer la protección de la persona en lo que respecta a su información personal.

El Tribunal Constitucional español mediante la STC 292/2000 de fecha 30 de noviembre en su fundamento jurídico 5, señala que el artículo 18.4 de la CE y teniendo en cuenta los textos internacionales, *"contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos, que además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a*

[7] MURILLO DE LA CUEVA, Pablo Lucas, "Informática y protección de datos personales", **Cuadernos y Debates Centro de Estudios Políticos y Constitucionales**, núm. 43, Madrid, 1993.
[8] Constitución de España: art. 18.4 *"La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."*
[9] SERRANO PÉREZ, Maria Mercedes, **Los Derechos al Honor, a la intimidad personal…**, ob. cit., p.484.

las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática'."[10]

Además, el Tribunal Constitucional ha establecido que el derecho a la protección de datos del artículo 18.4 de la CE contempla un derecho fundamental cuyo contenido esencial *"consiste en un poder de disposición y de control sobre los datos personales, que faculta a las personas para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"*[11]. Serrano Pérez expresa que el concepto del derecho fundamental a la protección de datos, denominación por la que parece decidirse el Tribunal Constitucional español, es un derecho a controlar y a disponer de los datos de carácter personal que se encuentran en manos ajenas[12].

El contenido del derecho fundamental a la protección de datos, incluye un haz de garantías y facultades que se traducen en determinadas obligaciones de hacer. Se trata del 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 cancelarlos[13].

Son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos[14]. En ese sentido, el derecho a la protección de datos de carácter personal es el derecho a decidir y controlar las informaciones personales que sobre nosotros conocen los demás, con independencia del carácter de íntimo o no del dato, cuestión que no es determinante para la protección del sujeto, tal y como señala el Tribunal de Justicia mediante Sentencia de fecha 20 de diciembre del 2017[15].

---

[10]STC 292/2000 del Tribunal Constitucional español de fecha 30 de noviembre, F.J.5.
[11]STC 292/2000 del Tribunal Constitucional español de fecha 30 de noviembre, F.J.7.
[12]SERRANO PÉREZ, Maria Mercedes, **Los Derechos al Honor, a la intimidad personal...**, ob. cit., p.486.
[13] MARTINEZ MARTINEZ, Ricard, "El derecho fundamental a la protección de datos: perspectivas", **Revista de los Estudios de Derecho y Ciencia Política de la UOC**, núm. 5, 2007, p.50.
[14] SERRANO PÉREZ, Maria Mercedes, **Algunos aspectos del derecho fundamental a la protección de los datos personales a la luz del reglamento general de protección de datos de la UE: Los principios de la protección de datos y los derechos de los sujetos**, Anuario 2018 del Tribunal Constitucional dominicano, impresión Búho, S.R.L., República Dominicana, 2019, pp.237 y 239.
[15] Tribunal de Justicia, Sala Segunda de fecha 20 de diciembre del 2017, Peter Nowak c. Data Protection Commissioner (Asunto C-434/16).

En la República Dominicana, el derecho de protección de datos se encuentra reconocido de manera expresa en el artículo 44.2 de la Constitución Dominicana[16]. Al respecto, el Tribunal Constitucional dominicano ha expresado mediante Sentencia TC/0240/2017 en su fundamento jurídico l que: "*Esta protección de los datos de carácter personal se denomina como el derecho a la autodeterminación informativa, que nace del derecho a la intimidad y lo trasciende, protegiendo el derecho a estar informado del procesamiento de los datos y de los fines que con ello se pretende alcanzar, así como el derecho de acceso, actualización, rectificación o eliminación, en caso de que le ocasione a la persona un perjuicio ilegítimo[17]."*

En consecuencia, el derecho de protección de datos personales tiene su fundamento en otorgar a la persona un haz de facultades positivas dirigidas a mantener un poder de disposición y control sobre los datos. Dichas facultades concretas son el derecho a recabar el previo consentimiento para la recogida y tratamiento de los datos, el derecho a saber y ser informado del uso de los datos y el derecho a acceder, rectificar o cancelarlos, temas que abordaremos más adelante.

B. Naturaleza Jurídica

El derecho de protección de datos constituye un derecho de la personalidad con el fin de proteger la vida privada de la persona. En el caso de España se planteaba si el artículo 18.4 de la CE refleja un auténtico derecho fundamental o se trata de una garantía instrumental de la intimidad. Tal como se indicó, la CE no califica de derecho el contenido del artículo 18.4, ya que ha sido la jurisprudencia española, que ha acuñado el nuevo término, otorgándole un contenido propio y diferente de aquel en el que se le podría considerar incluido, esto es, de la intimidad. Es así como, el Tribunal Constitucional español lo configura como un derecho autónomo, aunque con ciertos aspectos comunes a la intimidad y reconociendo, en sus primeras sentencias, que comparte la consideración de derecho independiente con la de derecho instrumental de la intimidad[18].

[16] Constitución de la República Dominicana: art. 44.2 "*Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos*".
[17] Sentencia TC/0240/2017 del Tribunal Constitucional dominicano de fecha 19 de mayo, F.J.1.
[18] SERRANO PÉREZ, Maria Mercedes, **Los Derechos al Honor, a la intimidad personal…**, ob. cit., p.486.

La STC 254/1993 del Tribunal Constitucional menciona por primera vez la denominada libertad informática, entendida como derecho fundamental autónomo, si bien afirma que tiene su origen en la dignidad de la persona (artículo 10.1 CE) y con clara interacción con el derecho a la intimidad (artículo 18.1 CE). De manera que, se pone de manifiesto con ello que los artículos citados ofrecían un mayor cimiento constitucional que el inicialmente previsto en el artículo 18.4, y que era necesario a partir de aquellos elaborar una nueva estructura, un nuevo derecho fundamental, autónomo, distinto, con finalidades específicas, es decir el derecho de protección de datos de carácter personal, el cual fue materializado conforme a la sentencia STC 292/2000, antes citada[19].

No obstante, es necesario recordar que cuando se proclama la CE en el 1978, en esas fechas no existía la posibilidad técnica, ni estaba generalizado el uso de la informática y de los medios tecnológicos. Sin embargo, una vez comienzan los grandes avances, en el que los datos comienzan a ser parte sensible de los derechos que debe poseer cualquier persona, surge la necesidad de protegerlo, frente a la cantidad de datos que pudieran ser utilizados sin un debido tratamiento, en el que pudieran ser afectados sus derechos. Es así como, conforme a las afirmaciones del Tribunal Constitucional español, en el que manifiesta la intencionalidad del constituyente, cuando manifiesta en relación artículo 18.4 lo siguiente: *"De este modo, nuestra constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distinto derechos fundamentales…"*[20].

En definitiva, el derecho a la protección de datos personales es un derecho fundamental autónomo, lo que implica que una determinada actuación puede conculcar el derecho de una persona a la protección de datos personales sin vulnerar el derecho a la intimidad. Aunque es cierto que, el derecho a la intimidad y el derecho a la protección de datos parten de un tronco común, la vida privada de la persona, que enlaza directamente con la dignidad y la libertad de la persona.

Las diferencias fundamentales con el derecho a la intimidad se refieren a su función, lo que implica también que su contenido y su objeto difiera. A juicio del Tribunal Constitucional español, la función de la intimidad es proteger a la persona de cualquier invasión no consentida en el espacio

[19] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., pp.62 y 63.
[20] STC 254/93 del Tribunal Constitucional español de fecha 20 de julio, F.J.6.

en el que la persona desarrolla su vida privada, excluyendo, por tanto, a los terceros de su conocimiento[21]. Por su parte, el derecho a la protección de datos *"persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado[22]"*.

Asimismo, si el derecho a la intimidad permite excluir ciertos datos del conocimiento ajeno, esto es, los datos considerados íntimos frente a una publicidad no querida, el derecho de protección de datos garantiza a las personas el poder de disposición sobre los datos íntimos y sobre lo que no tienen esa consideración y son calificados de personales.

En cuanto al objeto la protección de datos[23], alcanza tanto a los datos íntimos como a los datos públicos, porque el carácter íntimo de un dato no es el factor determinante para acordar la protección. Lo definitivo es que se trate de un dato personal, revelador de información sobre una persona y que esa información pueda afectar al ejercicio de sus derechos. Es decir, el poder de disposición y control se cierne sobre todos los datos, con independencia de su carácter íntimo o no pues a juicio de Serrano Pérez, el control sobre los datos pretende proteger la vida privada y el espacio de libertad del individuo, de manera que este pueda vivir sin estar limitado por lo que los demás conocen de él[24].

Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento informático o no, de lo datos

---

[21] SERRANO PÉREZ, Maria Mercedes, **Los Derechos al Honor, a la intimidad personal…**, ob. cit., p.486.
[22] STC 292/2000 del Tribunal Constitucional español de fecha 30 de noviembre, F.J.6.
[23] Al respecto la STC 292/2000 define el objeto de protección del derecho que alcanza: *"a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"*[23].
[24] SERRANO PÉREZ, Maria Mercedes, **Los Derechos al Honor, a la intimidad personal**…, ob. cit., p.487.

personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a que uso lo esté sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos[25]. Es decir, el sujeto tiene derecho a recibir información del titular del fichero sobre qué datos posee sobre su persona accediendo a sus registros y asientos, y saber que destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele[26].

C. Normativa aplicada

En el presente acápite trataremos de manera general la normativa dominicana y española con respecto al derecho de protección de datos de carácter personal. Actualmente, la República Dominicana posee la Ley No.172-13[27] que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, de la cual, cabe destacar, que al igual que otras normativas latinoamericanas, se inspiró en la Ley Orgánica 15/1999[28] de Protección de Datos de Carácter Personal de España, que a su vez fue el resultado de la transposición de la Directiva Europea 95/46/CE, hoy derogada en razón de su insuficiencia por el Reglamento General de Protección de Datos 2016/679[29] del Parlamento Europeo y del Consejo de fecha 27 de abril del 2016 y la nueva Ley Orgánica No.3/2018[30] de fecha 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales.

Europa cuenta con el RGPD 2016/679 antes citado, que se aplica de manera directa e inmediata a los países europeos, y en el caso que estamos trabajando, España, posee la referida Ley Orgánica No.3/2018, que busca complementar algunos aspectos dejados abiertos por parte del reglamento antes mencionado.

---

[25] STC 292/2000 del Tribunal Constitucional español de fecha 30 de noviembre, F.J.7.
[26] SERRANO PÉREZ, Maria Mercedes, **Algunos aspectos del derecho fundamental a la protección de…**, ob. cit., pp. 237 y 239.
[27] Ley No.172-13 de 15 de diciembre, sobre Protección de datos de carácter personal.
[28] Ley Orgánica 15/1999, de 13 de diciembre, orgánica de protección de datos de carácter personal (LOPD).
[29] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
[30] Ley Orgánica 3/2018, de 5 de diciembre de 2018, sobre Protección de Datos y Garantías de los Derechos Digitales.

1. Normativa aplicada en la República Dominicana

La protección de datos personales es un derecho fundamental consagrado en el artículo 44.2 de la CD, tal cual indicamos anteriormente. Además, el país es signatario de la Declaración Universal de los Derechos Humanos[31] y del Pacto Internacional de Derechos Civiles y Políticos[32], que hacen referencia al derecho a la vida privada y a las no injerencias arbitrarias, así como el derecho a la protección de la ley contra tales injerencias.

Al respecto, la República Dominicana cuenta con la Ley No.172-13 sobre protección de datos de carácter personal. En ese sentido, debemos de comenzar definiendo los datos de carácter personal, para poder verificar cual es el objeto, alcance, ámbito de aplicación y organismo encargado de que la citada ley se cumpla. Conforme a la Ley No.172-13, los datos de carácter personal son definido como: *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".*

A su vez, el objeto de la referida ley es proteger a la persona y sus derechos frente al tratamiento de sus datos personales, buscando una protección integral de los datos asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, de carácter público o privado, en el que se busca garantizar el derecho al honor o a la intimidad de la persona, y también facilitando el acceso a la información que sobre las mismas se registre, conforme al artículo 44 de la CD. Al mismo tiempo, regula la constitución, actividades, funcionamiento y extinción de las Sociedades de Información Crediticia (SIC), así como la prestación de los servicios de referencias crediticias y el suministro de la información en el mercado, garantizando el respeto a la privacidad y los derechos de los titulares de la misma, promoviendo la veracidad, la precisión, la actualización efectiva, la confidencialidad y el uso apropiado de dicha información.

[31] Declaración Universal de los Derechos Humanos adoptada por la Asamblea General de Naciones Unidas: art. 12. *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".*

[32] Pacto Internacional de Derecho Civiles y Políticos adoptado por la Asamblea General de Naciones Unidas: art. 17. 1. *"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2.Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".*

En ese sentido, se pudiera interpretar que la ley busca garantizar el tratamiento de los datos de las personas, a los fines de que su derecho de protección de datos no le sea vulnerado, sin embargo, este no es el caso, pues dicha ley es muy específica para un determinado sector, como es el de intermediación financiera.

Al respecto, el magistrado Román Berroa Hiciano, en su tesis doctoral señala que: *"El examen exhaustivo de dicha normativa, sin embargo, hace que afloren en la práctica una serie de debilidades, contradicciones, insuficiencias e incongruencias que dificultan a menudo el ejercicio de este derecho y su efectiva tutela. Un ejemplo que permite graficar la anterior afirmación es el siguiente: la Ley No.172-13 no contempla un procedimiento penal administrativo en sentido estricto para el juzgamiento de las infracciones administrativas en que puedan incurrir los responsables y encargados de tratamientos, entre ellos, las propias Sociedades de Información Crediticia, además de que existe un déficit de garantía o tutela administrativa sobrevenido de la configuración de un órgano de control de datos personales, dígase la Superintendencia de Bancos que controla, supervisa y sanciona a las Sociedades de Información Crediticia, no así a los restantes bancos o archivos de datos personales."*[33]

En cuanto a la naturaleza del órgano de control, la citada ley señala que los archivos o bancos de datos, públicos o privados, destinados a proveer informes crediticios estarán sujetos a la inspección y vigilancia de la Superintendencia de Bancos como órgano de control. De forma que, es la propia ley que manifiesta la parcialidad de la protección de datos, específicamente de créditos y aún más teniendo como órgano de control a la Superintendencia de Bancos, tal cual hemos indicado. En consecuencia, debemos de plantearnos, con respecto a la Ley No.172-13, lo siguiente: ¿Qué datos personales protege? ¿Solo estamos protegiendo datos crediticios? ¿Qué pasa con los demás datos? ¿Está siendo vulnerado el derecho de protección de datos personales?

Al respecto, nos encontramos ante una ley que en principio debe tener un carácter general para todos los datos de carácter personal, sin embargo, su aplicación está prácticamente restringida a la regulación de los servicios que prestan las Sociedades de Información Crediticia y muestra de eso es posible verlo en su artículo 29 que establece que el órgano de control para los archivos o bancos

[33] BERROA HICIANO, Román Arturo, Tesis doctoral: **Configuración jurídica del derecho fundamental a la protección de los datos personales en república dominicana. especial referencia a la tutela de los datos en el ámbito de las sociedades de información crediticia**, dirigido por Serrano Pérez, Maria Mercedes, Universidad de Castilla-La Mancha, Albacete, España, 2020, p. 215.

de datos destinados a proveer informes crediticios es la Superintendencia de Bancos y en los artículos 49 y siguientes de dicho texto legal. Esto representa una considerable debilidad debido a que, para el resto de los archivos, registros, bases de datos, listas, etc., no existe un órgano de control.

En ese sentido, se sometió ante el Tribunal Constitucional dominicano una acción directa de inconstitucionalidad, en relación a las atribuciones conferidas a la Superintendencia de Bancos en el artículo 29, a los fines de que dichas atribuciones les sean asignada a una institución independiente y vinculada a la protección de los derechos fundamentales.

Mediante la Sentencia TC/0484/16, el Tribunal Constitucional dominicano señaló que *"(…) a juicio de los accionantes, la Superintendencia de Bancos no es la institución idónea para garantizar la protección efectiva de los derechos fundamentales, en razón, según los accionantes, de que la labor que se le está asignando es ajena a las funciones que la Ley núm. 183-02, Monetaria y Financiera pone a su cargo".* Sin embargo, dicho Tribunal hace referencia a que *"la función de la institución que nos ocupa es esencialmente supervisar las actividades que realizan los bancos y, en sentido general, a los intermediarios financieros. Sin embargo, no podemos perder de vista, que, como derivación de sus funciones ordinarias, esta institución mantiene un registro respecto de las transacciones financieras que realizan las instituciones bancarias"*[34].

Por consiguiente, los aportantes de datos de mayor relevancia para las sociedades de información crediticia, son las instituciones financieras. De hecho, el objeto principal de la referida Ley No.172-13 lo constituye la protección de aquellos datos vinculados a la actividad financiera, así mismo lo expresa el Tribunal Constitucional dominicano[35].

Sin embargo, entendemos que con el fin de garantizar la efectividad de los derechos fundamentales de las personas afectadas por las bases de datos, se hace necesario que el órgano de control reúna los elementos de idoneidad y competencia funcional, más allá de la competencia atribuida mediante la ley para alcanzar así la coherencia con nuestro orden constitucional.

[34] TC/0484/16 del Tribunal Constitucional dominicano de fecha 18 de octubre del 2016, F.J.8.6.5.
[35] TC/0484/16 del Tribunal Constitucional dominicano de fecha 18 de octubre del 2016, F.J.8.6.9.

2. Normativa aplicada en Europa y España

Europa ha contado con importantes normativas en materia de protección de datos de carácter personal, del cual España ha formado parte, entre las que se encuentran: el Convenio Europeo de Derechos Humanos[36], el cual regula en su artículo 8 el derecho a la vida privada y familiar; la Carta de Derechos Fundamentales de la Unión Europea[37], en el que ya comienzan a garantizar el derecho que tiene toda persona a la protección de datos de carácter personal; además, del Tratado de Funcionamiento de la Unión Europea[38] en el que también se garantiza dicho derecho.

Por otro lado, existe el Convenio del Consejo de Europa[39] de fecha 28 de enero del 1981, el cual establece una serie de principios básicos para la protección de datos, indica criterios que regula su flujo y crea un Comité Consultivo, a quien se encomienda la formulación de propuestas para mejorar la aplicación del Convenio, siendo reconocida como la primera norma del Consejo de Europa relativa a la protección de datos. Con este convenio quedaba establecido un marco genérico de protección de la persona frente a las posibles intromisiones en su intimidad, o a la lesión de derechos de la personalidad de forma más genérica, por parte de la informática.

El citado Convenio fue actualizado por el denominado Convenio 108+, el cual reedita algunas medidas, recogiendo los principios de transparencia y proporcionalidad en el tratamiento de datos, incrementando las garantías que han de adoptarse junto a adecuadas medidas de salvaguarda. Las inclusiones más destacables son las siguientes: las bases legales bajo las cuales se pueden tratar los datos personales; amplía el catálogo de datos sensibles; obliga a notificar, al menos a las autoridades de supervisión, las brechas de seguridad que afecten a los individuos; garantizan y amplían los derechos de acceso y supresión; los responsables y encargados de tratamiento han de tomar las medidas necesarias para garantizar que se cumple con la normativa de protección de datos; se facilitan las transferencias de datos, ya sea entre miembros o terceros Estados.

Por otro lado, existe el Acuerdo Schengen[40] de fecha 14 de junio del 1985, el cual buscaba la coordinación entre Estados, con el fin de controlar y facilitar los datos que puedan ser de interés

[36] Aprobado en Roma el 4 de noviembre de 1950. Publicado en España en el BOE número 243, de 10 de octubre de 1979.
[37] Estrasburgo, 12/12/2007. Publicado en el Diario Oficial de la Unión Europea No. C.303, de 14/12/2007.
[38] DOUE núm.306, de 17 de diciembre del 2007.
[39] Ratificado por España el 27 de enero de 1984 (BOE No.274 de 15 de noviembre de 1985)
[40] Acuerdo Schengen de fecha 14 de junio del 1985, BOE No.181, de 30 de junio de 1991.

para las otras partes en la lucha contra la criminalidad. En definitiva, dicho acuerdo es un elemento de coordinación interestatal, que afecta el tratamiento y protección de datos, aunque no tenga un carácter concreto como lo tiene el Convenio de 1981, o el RGPD, al respecto del tratamiento de datos personales[41].

Además, la Unión Europea cuenta con el RGPD No.679/2016[42], el cual entró en vigor en mayo del 2018 y obliga a la realización de profundos cambios normativos a los Estados miembros de la Unión Europea. Además, añade la necesidad urgente de una nueva y más actualizada regulación de contenidos relativos a protección de datos que no habían sido contemplados en las regulaciones originarias. Los flujos transfronterizos de datos, la rápida evolución tecnológica y su generalización de uso social y de forma genérica la globalización, han constituido a los datos en un recurso esencial en la sociedad de la información. Este conjunto de circunstancias hacía necesaria una reformulación del mismo[43].

En ese sentido, el citado Reglamento regula lo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Este Reglamento tiene como finalidad *"...garantizar un nivel coherente de protección de las personas físicas en toda Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior..."*, además, busca ofrecer *"(...) a las personas físicas de todos los Estados miembros el nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados"*.

El RGPD No.679/2016, constituye una norma común aplicable a todo el territorio de la Unión, con lo que se produce la homogeneidad en las legislaciones sobre protección de datos de todos los Estados miembros, aunque dicha afirmación requiere de alguna matización que corrige ese efecto de aplicación directa en algunas de sus disposiciones. En efecto, pese al carácter de norma jurídica directamente aplicable que se predica del Reglamento, el mismo prevé en ciertos casos que los

[41] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.46
[42] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
[43] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.77.

criterios y reglas incorporados en algunos de sus preceptos sean especificados o restringidos por el Derecho de los Estados miembros, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinarios, puedan incorporar a su derecho nacional elementos del referido Reglamento. Junto a la necesidad de reglamentar de manera uniforme la libre circulación de los datos, no se puede ignorar que los avances tecnológicos demandaban también una nueva normativa que recogiera la respuesta a los retos que dichos avances y la globalización plantean[44].

Tal cual indicamos, el RGPD exhortaba la realización de profundos cambios normativos a los Estados miembros de la Unión Europea. Al respecto, la LOPDGDD surge como una forma de completar algunos contenidos relativos a la protección de datos que han sido regulados por el RGPD pero necesita la concreción de una norma nacional.

El objeto de la LOPDGDD No.3/2018 es complementar el ordenamiento jurídico español al RGPD, completar sus disposiciones y garantizar los derechos digitales de la ciudadanía conforme al mandato constitucional español en el artículo 18.4. Una de las características más importantes es su constante remisión al RGPD, la cual es reconocida como la norma troncal, siendo la citada ley una norma complementaria o de desarrollo del Reglamento General antes indicado.

Asimismo, la referida Ley trae consigo la transformación digital y los usos de internet, que se han producido en nuestra sociedad, y de manera destacable los derechos del ciudadano en internet, los que se identifican bajo el concepto de derechos digitales. En consecuencia, con la nueva regulación de datos de carácter personal, se identifica la clara evolución que ha tenido dicho derecho, así como las nuevas garantías jurídicas, y que está de forma permanente en evolución, tanto desde la perspectiva de las posibilidades técnicas, como desde las respuestas jurídicas.

En consecuencia, con la derogación de la Directiva 95/46/CE y la Ley Orgánica 15/1999 sustituidas por el RGPD y la LOPDGDD, estamos ante un nuevo derecho de protección de datos, esto es, ante un nuevo marco normativo multinivel en el que interaccionan normas europeas y

[44] SERRANO PÉREZ, Maria Mercedes, **Algunos aspectos del derecho fundamental a la protección de…**, ob. cit., pp.237 y 242.

nacionales, a lo que Rallo Lombarte indica que tal vez podría resultar exagerado interrogarse sobre si estamos ante un nuevo derecho de protección de datos[45].

D. Principios de protección de datos personales

Los principios generales de la protección de datos de carácter personal son reglas y criterios para orientar y regular el tratamiento de los datos. Conforme hemos indicado anteriormente, en el presente trabajo abordaremos la legislación dominicana y española, indicando los principios que ambos países tienen en común, además de los nuevos principios que introduce el RGPD, antes citado.

A partir del artículo 5 de la Ley No.172-13 se establecen los principios jurídicos sobre la protección de datos personales. Por su parte en Europa, el RGPD No.679/2016 en su artículo 5, que es aplicable a España presenta principios similares a los de la República Dominicana, aunque más precisos y actualizados. El cumplimiento de los principios incumbe al responsable del tratamiento, que además, como novedad del Reglamento, ha de poder demostrar que ha desarrollado una diligencia adecuada para su observancia, lo que obliga al responsable a dejar constancia de una actividad protectora, en relación al tratamiento que se le debe de dar a los datos de carácter personal.

La legislación dominicana establece el principio de licitud de los archivos de datos personales, señalando que, los archivos de datos personales no pueden tener finalidades contrarias a las leyes o al orden público, siendo debidamente registrados y apegados a los principios establecidos en esta ley. Este es muy parecido al que contiene el RGPD, denominado principio de licitud, lealtad y transparencia, el cual dispone que, los datos deben ser tratados de manera lícita, leal y transparente en relación con el interesado. En cuanto a la lealtad, la Ley No.172-13 establece el principio de lealtad como un principio individual, el cual impone la prohibición de recoger los datos por medios fraudulentos, desleales o ilícitos.

En relación al principio de calidad de los datos, la ley No.172-13 indica que, el tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando el principio de calidad, es decir, los datos personales deben ser: a) adecuados y pertinentes en relación al ámbito y

[45] RALLO LOMBARTE, A., "El nuevo derecho de protección de datos", **Revista Española de Derecho Constitucional**, núm. 116, 2019, p.48.

finalidad para los que se hubieren obtenido; b) exactos y actualizarse en el caso de que ello fuere necesario; c)suprimidos y sustituidos, o, en su caso, completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular de los datos establecidos en la presente ley; y, d) almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

Por su parte el RGPD, establece el principio exactitud y actualización, el cual va de la mano con el principio de calidad de los datos definido en la legislación dominicana. En ese sentido, los datos deben ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Por otro lado, la Ley No.172-13 dispone del principio de seguridad de los datos, en el que se establece que, el responsable del archivo de datos personales y en su caso, el encargado del tratamiento, deberán adoptar e implementar las medidas de índole técnica, organizativa y de seguridad necesarias para salvaguardar los datos de carácter personal y eviten su alteración, pérdida, tratamiento, consulta o acceso no autorizado. Asimismo, se establece el principio de deber de secreto, en el cual el responsable del archivo de datos personales y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del archivo de datos personales o, en su caso, con el responsable del mismo, salvo que sea relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Los principios indicados precedentemente se pueden verificar en el principio seguridad, integridad y confidencialidad dispuesto en el RGPD, en el cual se establece que, los datos son tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Además, la Ley No.172-13 contempla el principio de finalidad de los datos en el que dispone que los datos solo se recogerán para su tratamiento, cuando sean adecuados, pertinentes y no excesivos

en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido. El RGPD crea dos principios para hacer referencia, los cuales son: principio de limitación de la finalidad, en el cual los datos son recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. Por otro lado, se refiere a la minimización de datos, en el que los datos deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. La adecuación y pertinencia hacen alusión a la relación entre los datos que se recogen y la finalidad del tratamiento.

En relación al principio de derecho de información y el principio de consentimiento del afectado, la Ley No.172-13, aborda dichos principios como parte del tratamiento de datos, de la forma siguiente:

- Derecho de información. Cuando se recaben datos personales que requieran del consentimiento del titular de los datos, para que se les pueda dar el tratamiento de datos o ser cedidos después de obtener dicho consentimiento, se deberá informar previamente, a por lo menos uno de los titulares de los datos, en forma expresa y clara.

- Consentimiento del afectado. El tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, que deberá constar por escrito o por otro medio que permita que se le equipare, de acuerdo a las circunstancias. Al respecto de este principio, la ley indica que están exentos del requisito de consentimiento todos los organismos de investigación y de inteligencia del Estado encargados de la prevención, persecución y castigo de los crímenes y delitos, previa autorización de la autoridad judicial competente.

No obstante, la licitud de tratamiento y el consentimiento en el RGPD son tratados de manera más amplia, ya que ambos son ejes rectores del derecho de protección de datos de carácter personal. Cabe destacar que el derecho de información, la falta de la misma provoca un vicio insubsanable en el consentimiento y por tanto puede ocasionar una vulneración en el derecho fundamental a la protección de datos, ya que el derecho de información forma parte del contenido esencial del derecho[46]. El RGPD establece en su artículo 12.1 las características que debe poseer la información, en el que se destaca que debe ser: concisa, transparente, inteligible y de fácil acceso,

[46] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.120.

con un lenguaje claro y sencillo. En cuanto al consentimiento se le dedicará un acápite más adelante, por la importancia que recae en el mismo ante el citado derecho.

Por último, el RGPD, abarca el principio de limitación del plazo de conservación, en el cual los datos son mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el RGPD a fin de proteger los derechos y libertades del interesado.

E. Consentimiento del titular de los datos

El consentimiento es considerado como la piedra angular del sistema de protección de datos personales. Su importancia radica en que constituye el medio o la modalidad a través del cual el interesado tiene oportunidad de elegir el nivel de protección que le dará a la información sobre su persona, por eso de tratarse de una expresión de voluntad consciente e informada[47].

En la legislación española, a los fines de obtener los datos de una persona física de manera legítima, es preciso que ella los aporte y que, además, otorgue permiso para su tratamiento, cumpliéndose en ambos casos una serie de requisitos. No obstante, existirán supuestos tasados en que el consentimiento no sea necesario, y supuestos en que deba reunir algunas características adicionales que lo doten de validez. El artículo 6 de la LOPDGDD de conformidad con lo dispuesto en el artículo 4.11 del RGPD, define el consentimiento del afectado como toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Como regla general no podrá considerarse libre el consentimiento que se otorga en una clara relación de desequilibrio entre el interesado y el responsable del tratamiento, máxime si este es

[47] PEYRANO Guillermo F., citando a Alejandra M. Gils Carbó, **Régimen legal de los datos personales y habeas data**, Ediciones Depalma, Buenos Aires, 2002, p.71.

una autoridad pública y el consentimiento constituye el fundamento jurídico válido para ese tratamiento de datos de carácter personal[48].

Asimismo, señala el artículo 6.2 del citado Reglamento que cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. La licitud del tratamiento, se completa con la exigencia de un consentimiento para uno o varios fines específicos, lo que excluye el consentimiento en blanco, para fines genéricos o para fines indeterminados[49].

En el caso de los menores de edad, el artículo 7 de la LOPDGDD plantea que el tratamiento de los datos de los menores de 14 años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela. Por su parte, el RGPD no recoge una edad concreta para el tratamiento de datos de los menores de edad con carácter general. El artículo 8 del citado Reglamento se refiere al tratamiento de los datos del menor en el ámbito de la sociedad de la información, y en dicho ámbito tampoco establece una edad determinada, sino un límite mínimo fijado en los 16 años y una remisión a los estados miembros, a los que autoriza a rebajar la edad en estos casos hasta el umbral de los trece años.

De conformidad con el artículo 7.1 del RGPD obliga al responsable a poder demostrar que el interesado consintió el tratamiento de sus datos, lo que nos traslada al ámbito de la prueba y adoptar, por parte del responsable, las medidas necesarias para poder dar fe de la existencia del consentimiento por parte del sujeto. Asimismo, el artículo 7.2 del citado RGPD contempla la posibilidad del consentimiento en el contexto de una declaración escrita que se refiera también a otros asuntos, de manera que el consentimiento para el tratamiento de los datos sea uno más de ellos.

Como regla general de los tratamientos basados en el consentimiento, el artículo 7.3 del RGPD reconoce el derecho del interesado a retirar su consentimiento en cualquier momento del tratamiento, con la misma facilidad con la que la otorgó. Finalmente, el artículo 7.4 del RGPD

[48] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.112
[49] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p. 113

como el artículo 6.3 de la LOPDGDD se refieren a la posibilidad de vincular la ejecución de un contrato al consentimiento del tratamiento de datos personales que no son necesarios para su ejecución, siendo mucho más preciso el precepto interno. En concreto, el artículo 6.3 de la Ley Orgánica prohíbe ligar la ejecución de un contrato al consentimiento para el tratamiento de datos personales para fines que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual[50].

Al igual que en la legislación española, en la República Dominicana el consentimiento debe ser presentado por el afectado de forma libre, expreso y consciente. La Ley No.172-13 explica que las Sociedades de Información Crediticia, que es a lo que se refiere dicha ley, deberá contar con un permiso en el que el titular de los datos autoriza a que pueda ser consultado en las bases de datos de dicha sociedad, conforme al numeral 4 del artículo 5 de la citada ley. Cabe destacar, que no siempre se precisa el consentimiento del titular de los datos, al menos que exista una habilitación de la norma con rango legal para la cesión de información a favor de la administración, lo cual trataremos más adelante.

F. Derechos del titular de los datos ante el uso ilícito de los mismos

Los interesados, a la hora de proteger sus datos y frente a las agresiones que estos pudieran sufrir, cuentan con una serie de derechos reconocidos en el Título III de la LOPDGDD, tales como: acceso, rectificación, supresión, a la limitación del tratamiento de datos, a la portabilidad, oposición y a no ser objeto de decisiones automatizadas.

En la legislación dominicana se encuentran los derechos siguientes: acceso, rectificación, cancelación y oposición. Además, el titular de los datos cuenta con un derecho indemnizatorio, cuando sufran daños y perjuicios, como consecuencia del incumplimiento de lo dispuesto en la ley, pudiendo ser indemnizados conforme al derecho común. Por otro lado, sin perjuicio de lo establecido el titular de los datos podrá optar por una acción judicial de *hábeas data* de conformidad con la Constitución, a los fines de ejercer su derecho. El derecho indemnizatorio y el *hábeas data*, serán tratados de manera independiente en el presente capítulo.

[50] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.114.

Conforme a lo indicado precedentemente, la Ley No.172-13 a partir del artículo 7 y siguientes dispone de los derechos de las personas y su ejercicio, tal como se describen a continuación:

- **Derecho de acceso**

En República Dominicana, el derecho de acceso es el derecho del interesado a solicitar y obtener la información que precise acerca de sus datos en tratamiento, incluyendo el origen y las comunicaciones hechas o por hacer respecto de los mismos. El tratamiento de los datos e informaciones personales o de sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Solicitarán ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones que afecten ilegítimamente sus derechos, siendo muy parecido a la legislación española y europea.

Por su parte, en España el artículo 15 del RGPD, reconoce al interesado el derecho a obtener del responsable del tratamiento respuesta a la cuestión de si trata datos personales relativos a él, y en caso afirmativo acceder a ellos[51]. La LOPDGDD establece que el derecho de acceso se ejercitará según lo establecido en el artículo 15 del Reglamento, por lo que es necesario tener ambas normas en el caso de España, para diseñar el ejercicio completo de dicho derecho. De forma que, según el precepto europeo, el ejercicio del derecho de acceso comunica la siguiente información:

- La finalidad del tratamiento, la cual deberá ser determinada, explícita y legitima;
- Las categorías de datos de que se trata, es decir si se trata de categorías especiales de datos del artículo 9 del citado Reglamento;
- Los destinatarios a los que se comunican o comunicarán los datos;
- En caso de conocerse habrá que comunicar el pazo previsto para la conservación de los datos;
- El derecho a solicitar del responsable la rectificación o supresión de los datos, o la limitación del tratamiento, o a oponerse al mismo;
- El derecho a presentar una reclamación ante la autoridad de control;
- Si los datos no se han obtenido directamente del interesado, habrá que explicar cómo se ha obtenido;
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles.

[51] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.186.

En palabras de Preciado Doménech el "derecho de acceso constituye una condición previa a los demás derechos del interesado, pues sin acceso no son plausibles la rectificación, oposición, cancelación o reclamación judicial"[52]. La finalidad de obtener información acerca de dichas circunstancias persigue el mantenimiento del control de las informaciones personales, objeto último del derecho a la protección de datos personales y evitar un uso indiscriminado y exento de controles y garantías.

- **Derecho de rectificación**

La Ley No.172-13, señala que el derecho de rectificación es el derecho que tiene todo interesado a que se modifiquen aquellos datos de que es titular en el caso de que resulten ser inexactos o incompletos. Es decir, el derecho a corregir errores en los propios datos y así poder asegurar la certeza y garantizar la exactitud de la información que está siendo objeto de tratamiento. Por su parte, el RGPD, lo define en su artículo 16 como *"el derecho que tiene el interesado a obtener, sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive, mediante una declaración adicional"*.

En ese sentido, los datos intervienen en dos formas. En primer lugar, en caso de que el responsable mantenga un dato inexacto, el ejercicio del derecho de rectificación se ejercita para actualizar el dato, esto es, incorporar la información adecuada que el dato ha de transmitir. En segundo lugar, el precepto habla de completar los datos que sean incompletos, esto es, añadir información adicional a un dato que no contiene información inexacta, pero si incompleta[53].

- **Derecho de cancelación**

Se entiende por derecho de cancelación el derecho del interesado a que se suprima del fichero cualquiera de sus datos por ser inadecuado, excesivo, inexacto o incompleto. Para Velázquez

[52] PRECIADO DOMÉNECH, Carlos, **El derecho a la protección de los datos en el contrato de trabajo**, editorial Aranzadi, S.A.U., Madrid, 2017, p.61.
[53] SERRANO PÉREZ, Maria Mercedes, **Algunos aspectos del derecho fundamental a la protección de…**, ob. cit.,253.

Bautista la cancelación de los datos personales puede entenderse como anular, borrar, hacer ilegible, destruir o dejar irreconocible los datos[54].

Herrán Ortiz, indica que el derecho de cancelación procede cuando el tratamiento automatizado se realiza sin autorización, o el objeto del mismo lo son informaciones prohibidas, o a las que no alcanzan autorización del afectado, igualmente, cuando ha concluido legalmente el período de vida de los datos, cuando tiene lugar la revocación del consentimiento o se ha alcanzado el fin determinado, o se ha perdido la adecuación entre los datos registrados y el fin[55].

- **Derecho de oposición**

Se entiende por derecho de oposición, el derecho del afectado a que se cese o no se produzca el tratamiento de sus datos de carácter personal en tres situaciones. Podrá ejercitarse cuando: el consentimiento del afectado no fuere necesario para dicho tratamiento; el fichero tenga finalidad de actividades publicitarias o comerciales, o cuando el tratamiento tenga como fin la toma de una decisión referida al afectado y se base solo en el tratamiento automatizado de los datos, es decir, basada solo en un tratamiento destinado a evaluar determinados aspectos de su personalidad.

En España la LOPDGDD y el RGPD, parte de los derechos antes citados, sin embargo, prevén otros derechos. En ese sentido, el RGPD ha completado los derechos instrumentales que tradicionalmente se incluían en el derecho de protección de datos (acceso, rectificación, supresión, oposición) con nuevos perfiles que lo adecúan al ámbito digital. Por ejemplo, el derecho al olvido comporta la obligación de informar a terceros de la petición de supresión de "cualquier enlace, copia o replica" y el derecho a la portabilidad de los datos ampara transmitir datos conservados en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado[56]. Sin embargo, vamos a mencionarlo de una forma más amplia a continuación:

[54] VELÁZQUEZ BAUTISTA, Rafael, **Protección jurídica de datos personales automatizados**, Colex, Madrid, 1993, p. 68.
[55] HERRÁN ORTIZ, Ana Isabel, **La violación de la intimidad en la protección de datos personales**, Editorial Dykinson, S.L. Madrid, 1998, p. 290.
[56] RALLO LOMBARTE, A., "El nuevo derecho de protección de datos…", ob. cit., p.49.

- **Derecho a la supresión. El derecho al olvido**

El RGPD define el derecho al olvido como '*el derecho a obtener, de nuevo sin dilación indebida por parte del responsable del tratamiento, la supresión de los datos a él se refiera y este a efectuarla en las circunstancias que recoge el precepto*[57].' Por su parte, el Tribunal Constitucional español ha señalado que el derecho al olvido consiste en el derecho a la supresión de los datos personales de una determinada base que los contuviera. Eso, y no otra cosa, es el derecho al olvido[58]. El derecho al olvido en relación a la protección de datos personales recoge los matices que ese conflicto presenta cuando en la exposición de la intimidad de la persona y la protección de sus datos personales interfiere la tecnología, en particular el internet[59].

- **Derecho a la limitación del tratamiento de datos**

El artículo 18 del RGPD recoge el derecho a la limitación del tratamiento y otorga al interesado el derecho a ver limitadas las operaciones en que consiste el tratamiento de los datos personales en las circunstancias que señala el precepto. Por su parte, la LOPDGDD añade en su apartado segundo del precepto una garantía para el interesado, pues obliga a hacer constar en los sistemas de información del responsable el ejercicio del derecho de limitación, con el fin de permitir el tratamiento de los datos solamente en las circunstancias que recoge el artículo 18.2 de dicho Reglamento. En efecto, el ejercicio del derecho de limitación respecto de los datos del interesado en un tratamiento acarrea unas consecuencias determinadas que impiden la utilización de los datos en las mismas condiciones que antes del ejercicio del derecho de limitación. Por tanto, tras el ejercicio del derecho a la limitación se impide el tratamiento de los datos, lo que supone una restricción a su utilización, salvo que el interesado consienta nuevamente el tratamiento de los datos, o bien para proteger los derechos de otra persona al margen del consentimiento del interesado, en cuyo caso el derecho a la limitación del interesado cedería ante la necesidad de proteger estos últimos. El derecho a la limitación del tratamiento es un derecho con una duración temporal, mientras se mantienen las circunstancias que justifican su ejercicio[60].

[57] ÁLVAREZ CARO, M., **El derecho a la supresión o al olvido**, en Piñar Mañas, J. L., Reglamento europeo de protección de datos. Hacia un nuevo modelo europeo de privacidad, Editorial Reus, Madrid, 2016, pp.241.
[58] STC 58/2018 del Tribunal Constitucional español de fecha 4 de junio, F.J.5.
[59] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.172.
[60] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., pp.175-176.

- **Derecho a la portabilidad**

El derecho a la portabilidad de datos se encuentra establecido en el artículo 20 del RGPD y en el artículo 17 de la LOPDGDD, en el cual ambas legislaciones refieren a que es posible un traspaso de datos fácil y ordenado, el cual permite mantener el control de los datos personales del individuo, por lo que forma parte del contenido esencial del derecho fundamental a la protección de datos. El artículo 20.1 del Reglamento describe el derecho a la portabilidad como el derecho a *'recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado de uso común y de lectura mecánica y a transmitirlos a otro responsable del tratamiento'*.

El derecho a la portabilidad reconoce dos derechos. Por su parte, *'el derecho del interesado a recibir un subconjunto de datos personales que le conciernan, procesado por un responsable del tratamiento, y a almacenar dichos datos para un uso personal posterior'*, con lo que la portabilidad de los datos complementa el derecho de acceso, y, por otra parte, *'derecho a transmitir los datos de un responsable del tratamiento a otro responsable del tratamiento, sin impedimentos'*. Esto cuando sea técnicamente posible hacerlo. Ahora bien, los responsables deben establecer mecanismos que aseguren que los datos que se transmiten son efectivamente los que el interesado desea transportar, por ejemplo, mediante confirmación de este último antes de la transmisión. Después de la portabilidad, el responsable se convierte en responsable del nuevo tratamiento a todos los efectos, por lo que ha de respetar todos los principios del RGPD y asumir la responsabilidad derivada del tratamiento de los datos[61].

- **Derecho a no ser objeto de decisiones automatizadas**

El artículo 22.1 del Reglamento atribuye al interesado *'el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar[62]'*. El precepto no reconoce el derecho a no ser objeto de una decisión o a la elaboración de un perfil, sino a basar ambos en un tratamiento automatizado de datos con efectos jurídicos, o por el que el interesado se vea afectado significativamente. En cualquier caso, además del respeto a los principios del

[61] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p. 179
[62]Modelo de ejercicio del derecho a no ser objeto de decisiones automatizadas de la AEPD. Disponible en: www.aepd.es/media/formularios/formulario-derecho-de-oposicion-decisiones-automatizadas.pdf

Reglamento, se debe informar de forma específica al interesado y preverse el derecho a obtener una intervención humana, a que el interesado exprese su opinión, a recibir una explicación de la decisión tomada tras evaluación y a impugnar la decisión[63].

II. UTILIZACIÓN DE DATOS PERSONALES POR PARTE DE LA ADMINISTRACIÓN

El uso de los datos de carácter personal debe ser debidamente autorizado, aunque existen circunstancias en que la administración pública puede utilizar dichos datos. En efecto, el derecho a la protección de datos atribuye al afectado el derecho de información, oposición a la recogida de la información que le afecta, derecho de acceso, rectificación y cancelación de sus datos, al igual que se exige como principio general, la necesidad del consentimiento para el tratamiento de los mismos, configurándose medios legales de tutela para el ejercicio de dichos derechos. No obstante, su alcance puede ser objeto de limitaciones cuando se adopte una medida que sea necesaria y proporcionada en una sociedad democrática para salvaguardar una serie de objetivos, entre los que se encuentra algún interés económico y financiero importante u otro tema de interés por parte de la administración pública.

En consecuencia, la doctrina constitucional ha establecido que los derechos fundamentales no son absolutos y pueden ceder ante otros bienes constitucionalmente relevantes, siempre que la restricción que experimenten sea necesaria y proporcionada para lograr el fin legítimo previsto, y se respete el contenido esencial, es decir, el derecho a la autodeterminación informativa[64].

A. Las actuaciones de la administración pública frente al derecho de protección de datos

El Estado se hace representar por las diversas administraciones públicas y se constituye como la mayor fuente de información en relación a los individuos, siendo el mismo considerado como un órgano susceptible de lesionar derechos fundamentales, así como de poder garantizarlos. En definitiva, sea como sujeto actuante, o para cumplir las obligaciones propias del Estado Social y Democrático de Derecho, el Estado es el elemento principal de análisis en el ámbito de la protección de datos[65].

[63] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.181.
[64] STC 292/2000 del Tribunal Constitucional español de fecha 30 de noviembre, F.J.11.
[65] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.81.

A grandes rasgos abordaremos, las actuaciones de la administración pública ante el uso de la información de los individuos frente a la protección de datos de carácter personal, específicamente en los ámbitos tributario, sanitario y estadísticos, desde el ámbito español como de la dominicana.

1. Administración tributaria

En España, en relación al tratamiento de la información con trascendencia tributaria, pueden encontrarse sentencias en las que se reconoce como bienes dignos de protección constitucional, aptos para establecer restricciones, entre otros, de los derechos del artículo 18, el deber de contribuir del artículo 31.1 (en razón de una gestión tributaria eficaz, la lucha contra el fraude fiscal o una justa distribución de la carga fiscal)[66]. El Tribunal Constitucional español ha considerado que *'el deber de comunicación de datos se convierte… en un instrumento necesario, no solo para una contribución justa a los gastos generales (artículo 31.1 de la CE), sino también para una gestión tributaria eficaz, modulando el contenido del derecho fundamental a la intimidad personal y familiar'*.[67]

El RGPD, así como la LOPDGDD contienen un régimen común a todo tratamiento de datos, sin referencias especiales a su cesión, más que en los casos de transferencias internacionales. En ese sentido, solo se considera lícito el tratamiento basado en determinados escenarios, de modo que, además del realizado con el consentimiento del afectado, se legitiman, entre otros, los llevados a cabo en cumplimiento de una obligación legal, o de una misión realizada en interés público o en el ejercicio de los poderes públicos del responsable[68].

La LOPDGDD en su artículo 8 indica que *"1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable…cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento… 2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una*

[66] GONZÁLEZ MÉNDEZ, Amelia, **Cesión y publicación de datos tributarios versus protección de datos personales,** UGARTEMENDIA ECEIZABARRENA, Juan Ignacio, (Coord), Derechos fundamentales y ordenamiento tributario, España, 2018, p.484.
[67] Autos del TC 197/2003 de fecha 16 junio y 212/2003 de fecha 30 de junio.
[68] Reglamento General de la Unión Europea 679/2016, artículo 6.1, a). c) y e)

misión realizada en interés público o en el ejercicio de poderes públicos… cuando derive de una competencia atribuida por una norma con rango de ley".

El apartado i) del artículo 34 de la Ley General Tributaria[69] establece que los obligados tributarios tienen el *"derecho, en los términos legalmente previstos, al carácter reservado de los datos, informes o antecedentes obtenidos por la administración tributaria, que sólo podrán ser utilizados para la aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de sanciones, sin que puedan ser cedidos o comunicados a terceros, salvo en los supuestos previstos en las leyes".*

Asimismo, la citada Ley en su artículo 95 contiene algunas reglas garantistas que deben guiar las decisiones administrativas sobre cesión de información con trascendencia tributaria, cuyo carácter reservado se proclama: a) se aplica el principio de finalidad, en el sentido de que los datos tributarios solo pueden ser utilizados para la gestión de los tributos y la imposición de sanciones (artículo 95.1); b) la administración tributaria tiene la obligación de adoptar medidas que garanticen su confidencialidad (artículo 95.3); se establece el deber de sigilo respecto de dicha información por parte de las autoridades y funcionarios, y de retenedores y obligados a realizar pagos a cuenta (artículos 95.3 y 95.5); d) se especifican los supuestos, destinatarios y finalidades en que se permite su cesión, con o sin consentimiento del afectado[70].

Serrano Pérez, expresa que si bien es cierta la necesidad de tener en cuenta la distribución equitativa de la carga fiscal, acorde con la capacidad económica de cada ciudadano (artículo 31.1 CE) y la sumisión de toda riqueza del país al interés general (artículo 128 CE), no lo es menos que la prevalencia de unos derechos sobre otros los configura la sociedad en su devenir histórico. El Estado tiene recursos suficientes para salvaguardar las obligaciones que contienen los referidos artículos sin tener que lesionar el derecho a la protección de datos de carácter personal.

Cabe destacar que, materia colateral con la información tributaria es la regulada por el artículo 20[71] de la LOPDGDD, en relación a los sistemas de información crediticia, en el cual se establece

[69] Ley 58/2003, de fecha 17 de diciembre, General Tributaria, BOE-A-2003-23186.
[70] La Agencia Española de Protección de Datos ha señalado insistentemente que no es posible la cesión de datos tributarios fuera de los supuestos contemplados expresamente en el artículo 95.1 de la Ley general Tributaria, no cabiendo la aplicación de una interpretación extensiva de los mismos (Ver informes 0469/2005,0172/2008, 0290/2009 o 0301/2009) y sin otra habilitación legal.
[71] Art.20 de la Ley Orgánica 3/2018, de 5 de diciembre de 2018, sobre Protección de Datos y Garantías de los Derechos Digitales: (…) Que los datos hayan sido facilitados por el acreedor; Que se refieran a deudas ciertas,

que se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito, por sistemas comunes de información crediticia cuando se cumplan los requisitos establecido en el citado artículo.

En cuanto al ámbito tributario en República Dominicana, el Código Tributario[72] en su artículo 44 otorga a los órganos de la administración tributaria amplias facultades de inspección, fiscalización e investigación a través de sus funcionarios competentes, con el objeto de que sean cumplidas las disposiciones de dicho Código, y de otras leyes, reglamentos y normas tributarias puestas a su cargo. El literal j) del referido artículo dispone la facultad de requerir informaciones a los bancos o instituciones de crédito, públicas o privadas, las cuales estarán obligadas a proporcionarlas.

No obstante, el citado Código en el párrafo IV del artículo 56 hace referencia a que *"Los datos de carácter personal de los contribuyentes o responsables registrados para acceder y realizar declaraciones y pagos de tributos, a través de la Oficina Virtual, serán almacenados en una base de datos propiedad de la DGII. La información contenida en la citada base de datos será usada para la correcta identificación del contribuyente o responsable que solicita los servicios que se ofrecen electrónicamente"*. Además, *"la Dirección General de Impuestos Internos protegerá la confidencialidad de la información suministrada electrónicamente por los contribuyentes o responsables, a menos que deba ser divulgada en cumplimiento de una obligación legal o fundamentada en una orden de la autoridad administrativa o judicial competente"*.

Por su parte, la Ley No.172-13 en su artículo 5 numeral 4 dispone que el tratamiento y la cesión de datos personales es ilícito cuando el titular de los datos no hubiere prestado su consentimiento libre, expreso y consciente, el cual deberá constar por escrito. Sin embargo, la propia ley indica que están exentos del requisito del consentimiento, todos los organismos de investigación y de inteligencia del Estado encargados de la prevención, persecución y castigo de los crímenes y delitos, previa autorización de la autoridad judicial.

---

vencidas y exigibles; Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquellos en los que participe; Que los datos solo se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de 5 años; Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación; En el caso de que se denegase la solicitud de celebración del contrato, o este no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

[72] Ley núm. 11-92, de 16 de mayo de 1992, que aprueba el Código tributario de la República Dominicana.

Además, el numeral 6 del citado artículo nos destaca el deber de secreto, en el que el responsable del archivo de datos personales y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional, respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del archivo de datos personales del mismo, salvo que sea relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

De igual modo, la citada ley indica que en el artículo 5, numeral 6 literal b) que: *"Todas las personas físicas o jurídicas, las entidades públicas o privadas, debidamente reconocidas como usuarios o suscriptores de una Sociedad de Información Crediticia (SIC), que tengan acceso a cualquier información relacionada con el historial de un titular de los datos, de conformidad con esta ley, deberán guardar la debida reserva sobre dicha información y, en consecuencia, no revelará a terceras personas, salvo que se trate de una autoridad competente".* También, hace la salvedad de que *"Los funcionarios públicos o empleados privados que con motivo de los cargos que desempeñen tengan acceso a la información de que trata esta ley, están obligados a guardar la debida reserva, aun cuando cesen en sus funciones"*.

Sin embargo, en relación a la comunicación de datos entre instituciones de la administración pública, el artículo 39 de la Ley No.172-13 se refiere a que *"los datos de carácter personal recogidos o elaborados por la administración pública para el desempeño de sus atribuciones pueden ser comunicados a otras instituciones de la administración pública. La cesión de datos de carácter personal, objeto de tratamiento, que debe efectuar la administración tributaria en el ejercicio de sus competencias, conforme a lo dispuesto en su normativa reguladora, no requerirá el consentimiento del afectado de conformidad con lo establecido en la presente ley"*.

En ese sentido, la administración pública podrá intercambiar información con otra institución del Estado, siempre y cuando sea para fines de colaboración interinstitucional, y acorde a las competencias de ambas instituciones. Cabe destacar que, la administración tributaria, antes de ser aprobada la actual Ley No.172-13, venía estableciendo conceptos propios de la materia como el de base de datos, para el caso público, y establecía la obligación de resguardo y protección a cargo de los sujetos responsables y encargados de dichos bancos. Sin embargo, las previsiones del Código Tributario no suplían las carencias en cuanto al resguardo de información.

2. Administración sanitaria

La administración sanitaria también se puede constituir en fuente de conflictos respecto de los derechos fundamentales, y más con el derecho de protección de datos de carácter personal. En España, la Ley General de Sanidad[73] establece que los usuarios de la sanidad pública tienen derecho al respeto de su personalidad, dignidad humana e intimidad, así como a la confidencialidad de toda información relacionada con sus estancias o sus procesos, ya sea en instituciones sanitarias públicas, como privada. Además, de la obligación de los profesionales del área de la salud de guardar secreto sobre la actividad en relación con sus pacientes.[74]

Rebollo Delgado indica que, en relación a la protección de datos del individuo es uno de los que con más radicalidad se defiende y del cual el ordenamiento jurídico español toma una mayor conciencia. La gestión médica y hospitalaria en España tiende al estudio en conjunto de historiales médicos y dolencias de los pacientes, lo que supone una diversificación de datos y por tanto un mayor riesgo de lesión de los mismos, y en la misma medida, el paciente no controla de forma concreta quien tiene acceso a su historial clínico. Asimismo, hace referencia a que se constata hoy en España la inexistencia, tanto de la sanidad pública como en la privada, de un plan genérico de salvaguarda de protección de datos. Si bien, rige en todos los centros médicos las obligaciones establecidas por la LOPDGDD, pero esta se muestra en exceso genérica para el control y no acceso de la información médica relativa a los pacientes.[75]

La Ley de Derechos y Deberes de los Pacientes señala en su artículo 2.1 que *"La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica"*. A su vez, el artículo 2.2 de la citada Ley indica que: *"Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios. El consentimiento, que debe obtenerse después de que el paciente reciba una información adecuada, se hará por escrito en los supuestos previstos en la Ley".* Asimismo, el artículo 2.7 establece que *"La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida"*.

[73] Ley 14/1986, de 25 de abril, General de Sanidad, BOE-A-1986-10499.
[74] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p. 96.
[75] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p. 96.

La referida ley debe ser interpretada a la luz del Convenio 108 del Consejo de Europa, tal cual explica Rebollo Delgado, en cuyo apartado 45 se definen los datos relativos a la salud como *"las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo"*. Asimismo, explica que el concepto de datos relativos a la salud, son todos aquellos *"que tienen que ver con el cuerpo humano, como la sexualidad, la raza, el código genético, pero además, los antecedentes familiares, los hábitos de vida, de alimentación y consumo, así como las enfermedades actuales, pasadas o futuras previsibles, bien sean de tipo físico o psíquico; y las informaciones relativas al abuso de alcohol o al consumo de drogas"*.[76]

Además, los artículos 16 al 18, señalan quién, y de qué forma, tienen acceso a la historia clínica, así como el artículo 19 que se refiere a que el paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. De esta forma, Rebollo manifiesta que la Ley 41/2002 viene a paliar las deficiencias existentes en el ámbito de la protección de datos de carácter personal relativos a los pacientes, teniendo como elemento vertebrador de la protección de estos datos, la liberalidad del sujeto, en este caso concreto, la intimidad como pretensión genérica y la dignidad humana como fundamento.

La LOPDGDD viene a modificar el apartado 3 del artículo 16, por el cual se delimita el acceso a la historia clínica, estableciendo de forma concreta, que el acceso a la historia clínica con fines judiciales epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986 General de Sanidad y demás normas de aplicación. De forma que, el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, queda asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos[77].

El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso. También se autoriza a las administraciones sanitarias, cuando sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, para

[76] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p. 100.
[77] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…,** ob. cit., p. 101

acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. Dicho acceso deberá realizarse, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la administración que solicitase el acceso a los datos[78].

Finalmente, la disposición adicional decimoséptima de la LOPDGDD establece que el tratamiento de los datos de salud se encuentra amparado en el contenido del artículo 9.2 del RGPD, es decir como categorías especiales de datos, lo que supone una protección reforzada de los mismos. El artículo 9.1 del citado Reglamento dispone que *"Quedan prohibidos el tratamiento de datos personales que revelen (...) el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física".* Sin embargo, el citado Reglamento, establece algunas excepciones en cuanto a la recogida de los datos, indicados en los literales c) g) h) e i) del artículo 9.2 del citado RGPD, conforme se indican a continuación:

- El interés público en el ámbito de la salud pública (art. 9.2.i), que en este caso se configura como interés público esencial (art. 9.2.g);
- Cuando sea necesario para la realización de un diagnóstico médico (art. 9.2.h);
- Cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otras personas, cuando el interesado no esté capacitado para prestar su consentimiento. (art. 9.2.c)

Un ejemplo en la actualidad, son los datos relativos a la salud como consecuencia de la pandemia del COVID 19, pues estos tipos de datos son considerados sensibles, no obstante, los mismos pueden ser utilizados con el fin de proteger intereses vitales o por razones de interés público siempre y cuando sea proporcional al objetivo que se persigue con dichos datos. Al respecto, la Agencia Española de Protección de Datos ha publicado un informe en el que analiza el tratamiento de los datos personales, en relación con la situación derivada de la pandemia. Dicho Organismo señala que, el RGPD contiene las reglas necesarias para permitir legítimamente tratamientos de datos personales en situaciones en la que existe una emergencia sanitaria de alcance general. En consecuencia, según se recoge en el informe, la protección de datos de carácter personal no debería

[78] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p. 102.

utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, en especial las sanitarias en la lucha de la pandemia[79].

Ortega Giménez explica que, el COVID-19 está permitiendo la adopción de todo tipo de medidas excepcionales que no serían justificadas en una situación de estado normal, sin embargo siempre que se mantenga un correcto equilibrio entre la prevención de contagios y la recogida, tratamiento y cesión de datos de carácter personal que puedan promover la identificación de personas concretas. La protección de datos de carácter personal ni es ni puede ni debe ser un obstáculo para la más efectiva de las luchas contra el Coronavirus, sino que, en este escenario, las medidas que se adopten en materia de protección de datos de carácter personal deben adoptarse desde la "normalidad jurídica"[80].

Además, el referido informe recoge que el RGPD reconoce explícitamente en su Considerando 46 como base jurídica para el tratamiento lícito de datos personales en casos excepcionales, como el control de epidemias y su propagación, la misión realizada en interés público (art.6.I.e) o los intereses vitales del interesado u otras personas físicas (art.6.I.d), sin perjuicio de que puedan existir otras bases como, por ejemplo, el cumplimiento de una obligación legal. Finalmente, el informe destaca que los tratamientos de datos personales, aun en estas situaciones de emergencia sanitaria, deben seguir siendo tratados de conformidad con la normativa de protección de datos (RGPD y LOPDGDD), ya que dichas normas han previstos esta eventualidad.

En República Dominicana, la Ley General de Salud No.42-01 en su artículo 28 enlista una serie de derechos que tienen todas las personas, en relación a la salud, en la que se destaca el literal e), haciendo referencia a que las personas tienen derecho a: *"e) A la confidencialidad de toda la información relacionada con su expediente y con su estancia en instituciones prestadoras de servicios de salud pública o privada. Esta confidencialidad podrá ser obviada en los casos siguientes: cuando sea autorizado por el paciente; en los casos en que el interés colectivo así lo reclame y de forma tal que se garantice la dignidad y demás derechos del paciente; por orden judicial y por disposición de una ley especial*[81]*."*

[79] ORTEGA GIMENEZ, Alfonso, "COVID 19: Un desafío para la protección de datos de carácter personal", **Revista Actualidad Jurídica Iberoamericana**, núm.12, 2020, p.865.
[80] ORTEGA GIMENEZ, Alfonso, "COVID 19: Un desafío para la protección…", ob. cit., p.861.
[81] Ley No.42-01, de fecha 8 de marzo, General de Salud de la República Dominicana.

Asimismo, el artículo 34 de la Ley General de Salud señala que *"se creará un sistema de información general de salud automatizado, a través de la SESPAS[82], que garantizará el análisis, diseño e implementación de Base de Datos distribuidas y descentralizadas para la investigación y gestión del sector salud".*

Además, el artículo 35 de la citada Ley, señala que *"el Sistema de Información General de Salud garantizará, además, la calidad de la información independientemente de su origen institucional. (...) PÁRRAFO III.- La SESPAS en colaboración con las instituciones competentes elaborará la reglamentación necesaria para la puesta en funcionamiento del Sistema de Información Gerencial y para regular el acceso a la información".*

Sin embargo, la Ley No.172-13 en su artículo 78 hace referencia a datos relativos a la salud, indicando que sin perjuicio de lo establecido en dicha ley *"respecto de la cesión de datos, las instituciones y los centros sanitarios, públicos y privados, y los profesionales correspondientes pueden proceder al tratamiento de los datos de carácter personal relativos a la salud física o mental de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación dominicana sobre salud".*

Asimismo, el citado artículo destaca que *"(...) pueden ser objeto de tratamiento los datos de carácter personal que se refieren al origen racial, a la salud y a la vida sexual, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. Los establecimientos sanitarios, públicos o privados, y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos 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 los principios del secreto profesional".*

Conforme a lo indicado precedentemente, la realidad es que la Ley General de Salud no tiene un tratamiento para los datos, sin embargo, hace mención a que se requiere de un consentimiento previo por parte de la persona que recibe el servicio de salud para poder hacer uso de los mismos.

[82] Hoy día Ministerio de Salud Pública.

Además, la Ley No.172-13 no aborda como se manejan los datos relativos a la salud, sino más bien de forma general establece un artículo en relación a dicho tema y manda a la Ley General de Salud a encargarse de dicho aspecto.

3. Estadísticas

La Ley No.12/1989 de fecha 9 de mayo de la Función Estadística Pública[83] española, establece limitaciones con el objeto de salvaguardar los derechos fundamentales. Dicha ley nacional establece la posibilidad de que los servicios estadísticos soliciten datos tanto a personas físicas como jurídicas, nacionales y extranjeros, siempre que residan en España. El artículo 11.2 de la citada Ley, refiere a que los datos relativos al origen étnico, opiniones políticas, convicciones religiosas o ideológicas, y cuyas circunstancias puedan afectar a la intimidad personal o familiar, serán de aportación estrictamente voluntaria y solo podrá recogerse previo consentimiento expreso del interesado.

En ese sentido, el artículo 4 de la Ley No.12/1989 indica que para que el interesado forme su voluntad, la ley obliga a poner en conocimiento de este, la naturaleza, fin, obligatoriedad o no con la colaboración y la protección que se dispensa a los datos, así como las sanciones en que puede incurrir el sujeto ante la negativa de no colaborar. También regula el secreto estadístico destinado a los datos personales, los cuales son aquellos que guardan relación con las personas físicas o jurídicas que permiten su identificación directa o indirecta. La obligación del secreto recae sobre la administración que posee los datos.

En cuanto al acceso de terceros, se establece el requisito del consentimiento expreso de los afectados, o el transcurso de 25 años desde su muerte, si consta esta, en caso contrario, el plazo se amplía a 50 años, salvo que exista un interés legítimo. Para la correcta protección de los derechos fundamentales frente a la acumulación de datos estadísticos, opera otro factor substancial, como es el de la seguridad de los mismos, siendo la aplicación en esta materia la normativa sobre la protección de datos.

De este modo, se puede evidenciar que en el ordenamiento jurídico español opta en la regulación estadística por un sistema de protección activa, lo cual supone una restricción del derecho a la

[83] Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, BOE-A-1989-10767.

información de todo ciudadano, pero se realiza en aras de una mayor confidencialidad, y por tanto, de un mayor respeto al ámbito de los derechos fundamentales. Otro aspecto, es la facilidad en la disociación, de tal forma que a la estadística lo que le interesa para obtener resultados es cuantificar, no identificar[84].

La LOPDGDD en su artículo 25 obliga a que los datos contemplados en los artículos 9 y 10 del Reglamento solo pueden recogerse previo consentimiento expreso de los afectados. La administración estadística puede denegar el ejercicio de los derechos ARCO, cuando los datos se encuentren amparados por las garantías de secreto estadístico previsto en la legislación estatal y autonómica.

De manera general, la función estadística pública tiene por objeto la descripción de los fenómenos colectivos y de la realidad social mediante la recopilación, elaboración y ordenación sistemática de datos así como la presentación, publicación y difusión de los resultados que se obtengan a partir del tratamiento de aquéllos siendo todas estas tareas llevadas a cabo por una serie de servicios públicos especializados que se integran en la organización de las respectivas administraciones públicas. En el caso de España, las diferentes leyes estadísticas, reguladoras de la función estadística pública desarrollada en el correspondiente ámbito administrativo (estatal o autonómico) dedican parte de su articulado a la protección de los datos que son objeto de recogida y tratamiento por sus respectivos servicios estadísticos[85].

Los datos estadísticos los cuales son de diversa índole, contribuyen a obtener números certeros de alguna situación concreta, estos datos son más para los fines de cuantificar y no de identificar a la persona. A medida que los datos no se atribuyan a una persona en específico no existirá riesgo al momento de utilizar los mismos.

En República Dominicana, la Ley No.172-13 en su artículo 72 establece que *"Las disposiciones de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable"*.

[84] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p. 89.
[85] FUENTE MIGUÉLEZ, Alberto, "Aplicabilidad de la normativa sobre protección de datos de carácter personal en el ámbito de la función estadística pública", **Revista Vasca de Administración Pública**. **Herri-Arduralaritzako Euskal Aldizkaria**, núm. 107, 2017.

Por su parte, la Ley No.5096 sobre Estadísticas y Censos Nacionales, establece en su artículo 12 *"Los datos o informes estadísticos que provengan de particulares serán considerados como confidenciales y utilizados únicamente, en la preparación de la estadística nacional."*

En ese sentido, la Ley No.172-13 determina que siempre que no se identifiquen a las personas que proporcionen los datos para fines estadísticos, no se necesita de un debido tratamiento de datos, ya que los mismos son utilizados para poder completar una estadística y no para identificar a la persona que suministró los datos. Por su parte, la Ley sobre estadísticas y censo si dispone de forma expresa que los datos recolectados que provengan de particulares deben ser tratados de manera confidencial y deben ser utilizados con carácter estadísticos. En consecuencia, en ciertos aspectos se puede interpretar que las estadísticas es una actividad que pudiera lesionar derechos fundamentales como es la protección de datos, pero no en todos sus ámbitos, sino más bien cuando posibles estudios estadísticos pudieran incidir en hechos morales o físicos de una persona y más cuando hacen que la persona sea identificable.

B. Otras bases legítimas de la obtención de datos personales. Excepción al requerimiento del consentimiento

En el desarrollo del presente trabajo se ha establecido que el consentimiento es necesario para el tratamiento lícito de los datos. Sin embargo, el RGPD, destaca en su artículo 6, las bases que legitiman un tratamiento de datos son: el consentimiento, una relación contractual, los intereses vitales del interesado o un tercero, la existencia de una obligación legal para el responsable, la consecución del interés público o el ejercicio de poderes públicos e intereses legítimos prevalentes o de terceros a quienes se comunican los datos.

En cuanto a la relación contractual, el contrato es la pieza principal y el tratamiento de los datos es accesorio a este, pero a su vez necesario para la ejecución o para adoptar medidas precontractuales. En relación a la obligación legal, se justifica el tratamiento de datos al margen del consentimiento, ya que es la ley la que prevé la existencia de un tratamiento de datos y lo legitima. El artículo 8.1 de la LOPDGDD indica que dicha obligación legal deberá estar prevista en una norma de Derecho de la Unión Europea o una norma con rango de ley, *"que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento"*.

Además, se prevé la necesidad de proteger intereses vitales del sujeto o de otra persona física, en cuyo caso la exigencia del consentimiento para el tratamiento de datos personales cede para proteger otros bienes o intereses vitales que prevalecen frente a la exigencia del consentimiento. Algunos tipos de tratamiento pueden responder tanto a motivos de interés público como a intereses vitales del sujeto, como tratamientos con fines humanitarios, como el control de epidemias y su propagación, o situaciones de emergencia humanitaria, como catástrofes naturales o humanas.

En relación al interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento es necesario para el cumplimiento de una misión. En este caso, conforme al artículo 8.2 de la LOPDGDD, ha de tratarse de una competencia atribuida por una norma con rango de ley, precisión interna que responde a la facultad reconocida en el artículo 6.2 del RGPD. Por su parte, el artículo 6.3, último párrafo del RGPD, precisa más dicho tratamiento, pues obliga a determinar la finalidad del tratamiento en la base jurídica que lo justifica.

Finalmente, el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. En cuanto a este aspecto, no se aplicará si el tratamiento lo realiza una autoridad pública en el ejercicio de sus funciones. La existencia de un interés legítimo requerirá una evaluación minuciosa que pueda establecer la prevalencia de los intereses del responsable del tratamiento.

En República Dominicana, la Ley No.172-13 es muy específica en las situaciones que existen excepciones al consentimiento. El artículo 27 hace referencia a que no será necesario el consentimiento para el tratamiento y la cesión de datos, en los casos siguientes:

1. Se obtengan de fuentes de acceso público;

   Esto es por la propia naturaleza de la información, que en principio puede ser considerada personal, por lo que no necesita de un tratamiento de datos. Un ejemplo es la guía telefónica, donde se ponen los nombres y números telefónicos, en este aspecto al ser información de público acceso, el responsable de tratarlos queda liberado.

2. Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

   La administración pública recaba, almacena, procesa y transfiere diariamente una cantidad considerable de información personal, siendo un gran fichero de datos personales, sin necesidad de requerir con anticipación el consentimiento del titular de la información. Sin embargo, conforme a sus propias competencias, la administración puede prescindir del consentimiento del titular de los datos.

   Esta concesión de la ley con la administración pública pudiera estar justificada por el interés público. Rodríguez Arana[86] señala que "el concepto de interés general se refiere al interés social, al interés de todos y cada uno de los ciudadanos como miembros de la comunidad". En consecuencia, si bien la administración pública está autorizada por la ley al tratamiento de los datos personales sin el consentimiento del titular, lo que supone para este último algún nivel de riesgo, lo contrario implicaría también colocar en situación de riesgo la estabilidad del Estado y su normal desenvolvimiento, por tanto, el interés general[87].

3. Se trate de listas para fines mercadológicos, cuyos datos se limiten a nombre, cédula de identidad y electoral, pasaporte, identificación tributaria y demás informaciones biográficas;

   La propia excepción lo describe y es que, si dichos datos son utilizados solo para fines de mercadeo, los mismos podrán ser utilizados, siempre y cuando se limite a lo planteado en dicha excepción y más si el titular de datos no es identificable.

4. Se deriven de una relación comercial, laboral o contractual, científica o profesional con la persona física, y resulten necesarios para su desarrollo o cumplimiento;

   En ese sentido, la base jurídica que justifica el tratamiento de la información lo constituye la propia norma, que exime al responsable de requerir del titular su consentimiento.

5. Se trate de datos personales que reciban de sus clientes en relación a las operaciones que realicen las entidades de intermediación financiera reguladas por la Ley Monetaria y

[86] RODRIGUEZ ARANA, Jaime, **Interés General, Derecho Administrativo y Estado de Bienestar**, Iustel, Madrid, 2012, p. 11.
[87] BERROA HICIANO, Román Arturo, Tesis doctoral: **Configuración jurídica del derecho…,** ob. cit., p. 117.

Financiera y de agentes económicos, de las Sociedades de Información Crediticia (SIC), y de las entidades que desarrollan herramientas de puntajes de crédito para la evaluación del riesgo de los deudores del sistema financiero y comercial nacional, de acuerdo a las condiciones establecidas en el artículo 5, numeral 4;

Al respecto, existe una contradicción con esta excepción, ya que el artículo 5.4 de la Ley No.172-13 indica que se requiere del consentimiento del titular de los datos. En ese sentido, Berroa Hiciano en su tesis doctoral indica que "No es posible, de una parte, excluir el consentimiento en el supuesto concreto objeto de análisis, y de otra parte, que esa exclusión se haga de conformidad con el art. 5.4 de la Ley No.172-13 que precisamente condiciona la licitud del tratamiento a la procuración previa del consentimiento. Por lo cual señala que, ambas situaciones sencillamente no coexisten".[88]

6. Así lo disponga una ley;

   Este artículo no tiene razón de ser, porque deja una reserva de ley de manera ilimitada. También, no existe una concordancia con respecto a las excepciones enlistadas en la Ley No.172-13 con respecto a las excepciones y que dentro de una lista se establezca "así lo disponga la ley", no tiene ningún sentido.

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

   En este caso, siempre y cuando exista una obligación legal de la administración de obtener datos bajo sus respectivas competencias y que lo mismos deban ser suministrados debido a que existe una colaboración interinstitucional, por lo cual la Ley No.172-13 prevé dicha excepción. Cabe destacar, que las administraciones públicas deben de conservar una debida confidencialidad de los datos que utilizan.

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

[88] BERROA HICIANO, Román Arturo, Tesis doctoral: **Configuración jurídica del derecho…,** ob. cit., p. 120.

Si bien es cierto que, el tratamiento de estos datos requiere como regla general recabar con anticipación el consentimiento de su titular, la normativa de protección de datos excluye la formalidad del consentimiento a partir de tres situaciones puntuales: 1. el tratamiento de datos personales es necesario por razones de salud pública; 2. es necesario debido a una emergencia; y 3. es necesario para la realización de estudios epidemiológicos. En ese sentido, tal como establece el magistrado Berroa Hiciano ante la confrontación de derechos o intereses dignos por igual de tutela (el derecho del titular de los datos vs el interés general, en los casos de salud pública; el derecho del titular de los datos vs el interés general derivado de la necesidad de realizarse estudios epidemiológicos) decantarse por aquellos que considera más importantes. En todo caso, la ley obliga al responsable del tratamiento y a los encargados por igual, a garantizar la confidencialidad de la información tratada[89].

9. Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables.

   Esto se debe a que, como no existe una conexión del titular de los datos con la información recabada, pues el consentimiento no es necesario, ya que el titular de dichos datos no puede ser considerado identificable.

C. Carácter reservado a los datos obtenidos por parte de la Administración

El derecho de acceso a la información ante la administración pública es una vía para los ciudadanos para conocer los procedimientos, toma de decisiones y actividades que realizan las administraciones. Sin embargo, existen informaciones que posee la administración que ostentan un carácter reservado. La información reservada tiene su sustento en el "secreto de la defensa nacional o de la policía exterior, en el secreto en materia comercial o industrial, en la seguridad nacional, en la seguridad pública, en los procedimientos jurisdiccionales y en las operaciones de policía judicial en materia fiscal y aduanera, y la información confidencial se sustenta en el "secreto de la vida privada" y en la protección de datos personales"[90].

[89] BERROA HICIANO, Román Arturo, Tesis doctoral: **Configuración jurídica del derecho…,** ob. cit., p. 121.
[90]SALGADO REMIGIO, Sofía, "El Secreto en la Administración Pública: información reservada y confidencial como excepción al derecho a la información", Universidad Nacional Autónoma de México Ponencia para el III Congreso GIGAPP, 2012, Madrid España, Disponible en: http://www.gigapp.org/administrator/components/com_jresearch/files/publications/100%20SALGADO.pdf

Leonor Rams Ramos, explica que debe de existir un replanteamiento entre las relaciones, entre las exigencias de transparencia que las leyes vigentes establecen para la actuación de la administración pública y la garantía del derecho fundamental a la protección de datos. Asimismo, enfatiza que no hay duda de que el exponencial crecimiento de la actuación administrativa y de su incidencia en la esfera jurídica de los ciudadanos hace que sea cada vez más necesario conciliar la protección de dos bienes jurídicos que en muchos casos se nos presentan como antagónicos. Sin embargo, la necesidad de poner a disposición de los ciudadanos la información pública, es susceptible de lesionar el derecho fundamental a la protección de datos, pues la mayor parte de la información que obra en poder de las instituciones públicas, bien porque la reciben de los ciudadanos o porque sean autoras de la misma, está plagada de datos de carácter personal tanto de las personas que se insertan en estas, como de los destinatarios de su acción.[91]

En España, la Ley 19/2013[92] de Transparencia, Acceso a la Información y Buen Gobierno en su artículo 13 define información pública como: *"los contenidos o documento, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones."*

Asimismo, hace referencia a que existe una amplia conciencia social sobre la necesidad de proteger un bien jurídico que la revolución tecnológica imparable que vivimos puede hacer peligrar; pero, como es bien evidente, no puede tratarse de un derecho de protección absoluta que impida la realización o satisfacción de otros derechos que reconoce el ordenamiento jurídico[93]. En ese sentido, como afirma Ricard Martínez, una aproximación literal al derecho fundamental a la protección de datos personales, no puede erigirse en condición de prevalencia del derecho si no se quiere vaciar por completo de contenido el deber de transparencia. Si en caso de conflicto no se produce una interpretación de naturaleza cualitativa, el uso instrumental de la privacidad al servicio de la opacidad estar garantizado. Si se apuesta por una consideración del derecho fundamental a la protección de datos personales como barrera insalvable, la garantía de este

[91] RAMS RAMOS, Leonor, "El derecho fundamental a la protección de datos de carácter personal como límite ¿infranqueable? Para la transparencia administrativa", **Estudios de Deusto**, Vol. 66/2, julio-diciembre 2018, pp. 119-152.
[92] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, Referencia: BOE-A-2013-12887.
[93] RAMS RAMOS, Leonor, "El derecho fundamental a la protección…", ob. cit., p.122.

derecho fundamental constituiría sin duda la excusa perfecta para la denegación sistemática de acceso a la información[94].

En virtud del principio de transparencia, las leyes, en general y la Ley de Transparencia española, regulan los instrumentos jurídicos que hacen posible que la información pública pueda ser conocida por los ciudadanos, no obstante, dicho derecho se ve limitado en muchos casos por la gran cantidad de datos personales que, lógicamente, aparecen en esa información sobre la gestión de lo público, y que goza de una especial y justificada protección.

En República Dominicana, la Ley General de Libre Acceso a la Información Pública[95] establece en su artículo 2 que *"(…) derecho de información comprende el derecho de acceder a las informaciones contenidas en actas y expedientes de la administración pública, así como a estar informado periódicamente, cuando lo requiera, de las actividades que desarrollan entidades y personas que cumplen funciones públicas, siempre y cuando este acceso no afecte la seguridad nacional, el orden público, la salud o la moral públicas o el derecho a la privacidad e intimidad de un tercero o el derecho a la reputación de los demás. (…) con las únicas limitaciones, restricciones y condiciones establecidas en la presente ley."*.

En ese sentido, la citada ley en el artículo 18 indica la limitación al acceso cuando existen razón de interés privado preponderantes, conforme se indica a continuación: *"Cuando se trate de datos personales cuya publicidad pudiera significar una invasión de la privacidad personal. No obstante, la administración podría entregar estos datos e informaciones si en la petitoria el solicitante logra demostrar que esta información es de interés público y que coadyuvará a la dilucidación de una investigación en curso en manos de algún otro órgano de la administración pública. (…) Cuando se trate de datos personales, los mismos deben entregarse sólo cuando haya constancia expresa, inequívoca, de que el afectado consiente en la entrega de dichos datos o cuando una ley obliga a su publicación."*

Sin embargo, el artículo 19 de la referida ley destaca que: *"Cuando el acceso a la información dependa de la autorización o consentimiento de un tercero protegido por derechos de reservas o de autodeterminación informativa en los términos de los artículos 2 y 17 de esta ley, podrá*

[94] MARTÍNEZ MARTINEZ, Ricard, "De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia. Régimen jurídico de la transparencia del sector público", **Revista Aranzadi**, 2014, pp.244 y 245.
[95] Ley No.200-04, de fecha 28 de julio, General de Libre Acceso a la Información Pública.

entregarse la información cuando haya sido dado el consentimiento expreso por parte del afectado. Este consentimiento también podrá ser solicitado al afectado por la administración cuando así lo solicite el peticionario o requeriente (…)"

En cuanto a la entrega de información entre órganos de la administración pública, el artículo 20 se refiere a que *"Cuando no se trate de datos personales, especialmente protegidos por el derecho a la autodeterminación informativa del ciudadano, las administraciones (…), podrán permitir el acceso directo a las informaciones reservadas, recopiladas en sus acervos, siempre y cuando sean utilizadas dentro de sus competencias de los entes y órganos solicitantes y se respete, en consecuencia, el principio de adecuación al fin público que dio sentido a la entrega de la información".*

Conforme a lo indicado precedentemente, se especifica que en todo caso, los órganos de las administraciones solicitantes deberán de respetar la finalidad, el principio de reserva de las informaciones y documentos que reciban. El carácter de reservado sólo podrá ser admitido cuando la solicitud se base en las argumentaciones derivadas del principio de necesidad, adecuación y necesidad en sentido estricto que rigen en materia de lesión justificada de derechos fundamentales.

Un ejemplo, es el caso de la administración tributaria dominicana, que establece un deber de reserva por parte de la administración, señalando en el artículo 47 del Código Tributario lo siguiente: *"Las declaraciones e informaciones que la administración tributaria obtenga de los contribuyentes, responsables y terceros por cualquier medio, en principio tendrán carácter reservado y podrán ser utilizadas para los fines propios de dicha administración y en los casos que autorice la ley. Párrafo I. No rige dicho deber de reserva en los casos en que el mismo se convierta en un obstáculo para promover la transparencia del sistema tributario, así como cuando lo establezcan las leyes, o lo ordenen órganos jurisdiccionales en procedimientos sobre tributos, cobro compulsivo de éstos, juicios penales, juicio sobre pensiones alimenticias, de familia o disolución de régimen matrimonial."*

III. MECANISMOS Y GARANTÍAS POR PARTE DEL TITULAR DE LOS DATOS PERSONALES

La protección de datos de carácter personal es esencial para el respeto de la vida privada. En dicho contexto se debe de garantizar y proveer mecanismos con el cual el titular de los datos pueda

salvaguardar su derecho fundamental a posibles intromisiones por parte de terceros sin una debida autorización, al menos que exista una provisión legal en el cual se pueda acceder a datos personales.

De forma general, abordaremos el tema del hábeas data, que, si bien en España no existe dicha figura, en República Dominicana sí. Además, verificaremos el Derecho de Indemnización que tienen los titulares de datos cuando los usos de los mismos no sean adquiridos de una forma legítima. Finalmente, el procedimiento de tutela de los derechos que la legislación española contempla en su normativa.

A. Acción de hábeas data

La CD busca garantizar los derechos fundamentales a través de los mecanismos de tutela y protección, que ofrecen a la persona la posibilidad de obtener la satisfacción de sus derechos, frente a los sujetos obligados o deudores de ellos mismos. Los derechos fundamentales vinculan a todos los poderes públicos, los cuales deben de garantizar su efectividad en los términos establecidos por la CD y la ley, conforme lo establecido en el artículo 68 de la citada Constitución.

Es así como el derecho de protección de datos, se encuentra protegido mediante el hábeas data, establecido en el artículo 70 de la CD, el cual establece que *'Toda persona tiene derecho a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística*[96]*.'* A dicho texto, el artículo 64 de la Ley No.137-11 le agrega que *"la acción de hábeas data se rige por el régimen procesal común del amparo*[97]*".*

En principio, toda persona tiene derecho a tener acceso, rectificación, cancelación y oposición, en relación a los datos personales de los que sea titular y estén incluidos en un fichero, sea público o privado. En caso de que exista algún incumplimiento de esta obligación dentro del término acordado, conforme al artículo 8 de la Ley No.172-13 se habilitará al interesado a promover sin

[96] Constitución de la República Dominica, artículo 70.
[97] Ley 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales de fecha 15 de junio del 2011, artículo 64.

más requisitos la acción de protección de los datos personales o de hábeas data prevista en esta ley.

En virtud de lo antes expuesto, una vez el titular de los datos haga su solicitud dependiendo del caso en concreto, el responsable del registro deberá dar respuesta al reclamo en un plazo no mayor a diez (10) días hábiles. Puesto de lo contrario, la persona afectada estará habilitada para interponer la acción de hábeas data.

De lo anterior se desprende, que toda persona tiene derecho a interponer la acción de hábeas data para acceder a la información y a los datos que sobre ella reposen en los registros públicos o privados. Igualmente, puede introducirse para solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones inexactas, falsas, discriminatorias o que afecten ilegítimamente el derecho del titular de los datos.

Al respecto el Tribunal Constitucional dominicano en la Sentencia No. TC/0404/16 dispone que *"la acción constitucional de hábeas data supone la acción idónea para la protección efectiva del derecho fundamental a la autodeterminación informativa contenido en el artículo 44.2 de nuestra Carta Magna"*[98].

Es importante señalar, que la acción de hábeas data es extensiva a las personas jurídicas, en virtud de la Sentencia No.TC/0404/16 del Tribunal Constitucional. Esto debido a que también son titulares de derechos y obligaciones. Es decir, que pueden beneficiarse de ésta y otras garantías constitucionales para tutelar sus derechos fundamentales. Esta aclaración se hizo a causa de que la Ley No.172-13 sobre Protección de Datos de Carácter Personal, en sus artículos 4.4 y 6.1 excluía o limitaba a las personas jurídicas al uso de este mecanismo de protección de derechos.

Por su parte, en España la protección del derecho de protección de datos, no se hace a través del hábeas data, sino que se busca garantizar a través de la acción de amparo, conforme se dispone en el artículo 53.2 de la Constitución española *"Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección 1.ª del Capítulo Segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional."*

[98] Sentencia No. TC/0404/16 del Tribunal Constitucional dominicano de fecha 9 de septiembre del 2016.

B. Derecho de indemnización

En Europa el RGPD en su artículo 82.1 establece que **"***Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del Responsable o el Encargado del tratamiento una indemnización por los daños y perjuicios sufridos*"**.** En ese sentido, el Responsable o el Encargado del tratamiento deben indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento, habiendo incumplido sus obligaciones. Esto debe realizarse teniendo en cuenta las posibles vulneraciones a las disposiciones del citado Reglamento en los Estados Miembros y en el caso de España, la LOPDGDD.

Cabe destacar que dicha indemnización es independiente de los recursos administrativos o extrajudiciales disponibles, reclamaciones ante la Agencia Española de Protección de Datos. Por su parte, el Reglamento General de Protección de Datos reconoce el Derecho a los interesados a una tutela judicial efectiva para reclamar tales daños y perjuicios, pues el artículo 79.2 señala que estas *acciones contra un Responsable o Encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que tengan un establecimiento.* Conforme al artículo 80, dichas acciones, podrán ser promovidas por el mismo interesado o por entidades, organizaciones o asociaciones sin ánimo de lucro**,** debidamente establecida con arreglo al Derecho y cuyos objetivos sean el interés público en el ámbito de protección de los derechos y libertades en materia de protección de datos.

En República Dominicana, la Ley No.172-13 dentro de los Derechos de las personas y su ejercicio establece la indemnización como un derecho, cuando en el artículo 16 de la mencionada ley señala que: *"Derecho a indemnización. Los interesados que como consecuencia del incumplimiento de lo dispuesto en la presente ley, sufran daños y perjuicios, tienen el merecimiento a ser indemnizados conforme al derecho común"*.

C. Procedimiento de tutela del derecho de protección de datos en España

La LOPDGDD desde el artículo 63 hasta el 69 regula el procedimiento que debe de seguir el interesado ante la Agencia Española de Protección de Datos, en caso de posible vulneración de dicha normativa en los casos previstos en el artículo 63. La Agencia Española de Protección de

Datos es la autoridad de control ante la que se pueden presentar reclamaciones, según el artículo 77 del RGPD.

En ese sentido, el artículo 63 de la LOPDGDD indica que las normas contenidas en dicho título *"serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 al 22 del Reglamento 2016/679, así como en los que ella investigue la existencia de una posible infracción de los dispuesto en el mencionado Reglamento y la Ley Orgánica."*

Los procedimientos que se realicen por la Agencia Española de Protección de Datos se regirán por la norma europea, por la LOPDGDD y por normas reglamentarias que se creen y por las normas comunes sobre procedimiento administrativo. En el caso de que no se haya atendido la solicitud de ejercicio de los derechos se pudiera entender que: 1) denegación de lo pretendido en la solicitud; y, 2) como una falta de respuesta expresa en el plazo de un mes desde la recepción de la solicitud, en dichos casos existe la posibilidad de interponer una reclamación ante la autoridad de control[99]. En definitiva, la norma española distingue entre los procedimientos de denegación del ejercicio de los derechos por parte del responsable del tratamiento y los procedimientos de posible infracción de lo previsto en el RGPD y en la LOPDGDD, en el que ambos procedimientos inician con una fase de admisión a trámite.

Sin embargo, con carácter previo a la admisión a trámite de reclamación la Agencia Española de Protección de Datos tras la presentación de una reclamación se dirige a examinar su competencia. Para determinar si la Agencia Española de Protección de Datos es la autoridad de control competente, se debe tener en cuenta el artículo 4.22 del Reglamento, que indica que la autoridad de control interesada en base a tres circunstancias: a) si el responsable o el encargado están establecidos en el territorio del Estado miembro de esa autoridad de control; b) si los interesados que residen en el Estado miembro de la autoridad de control están afectados por el tratamiento; o c) si se ha presentado una reclamación ante esa autoridad de control[100].

[99] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.149.
[100] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.149.

Asimismo, el artículo 56 del Reglamento indica que cada autoridad de control tendrá competencia para *"tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en un Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro."*

La actuación de la Agencia Española de Protección de Datos se refiere a la posibilidad de enviar la reclamación presentada a otras instancias con el fin de intentar, sin la intervención de la Agencia, la solución del conflicto. En ese sentido, el artículo 65 de la LOPDGDD prevé: 1) que la Agencia Española de Protección de Datos podrá dirigir la reclamación ante la Delegación de Protección de Datos que hubiera sido designado por el responsable o encargado del tratamiento; 2) la Agencia Española de Protección de Datos podrá dirigir la reclamación al organismo extrajudicial de resolución de conflictos incluido en el código de conducta, en caso de haberse elaborado uno para el sector en el que se plantea la reclamación, de acuerdo con los artículos 37 y 38.2 de la citada ley[101].

La Agencia Española de Protección de Datos podrá remitir la reclamación al responsable o encargado de tratamiento, a falta de Delegado de Protección de Datos y de mecanismo de supervisión extrajudicial de conflictos, quien tiene la obligación de resolver en el plazo de un mes. En este caso, el Delegado de Protección de Datos dispone del plazo de dos meses como máximo para responder al interesado. Por su parte el artículo 37.2 de la LOPDGDD recoge la posibilidad de que la Agencia Española de Protección de Datos, tras recibir una reclamación y con carácter previo a su resolución, pueda devolverla al Delegado de Protección de Datos de la entidad ante la que denuncia el interesado, para que aquel resuelva en el plazo de un mes. Si finalizado dicho plazo, el Delegado de Protección de Datos no hubiera comunicado a la Agencia Española de Protección de Datos el resultado de la reclamación, el procedimiento podrá ya continuar ante la propia Agencia, que iniciará las actuaciones dirigidas a pronunciarse sobre la admisión a trámite de la petición.

Al respecto, la intervención del Delegado de Protección de Datos parece consolidarse como una vía previa que hay que agotar antes de la admisión a trámite de la reclamación por la Agencia Española de Protección de Datos, lo que puede justificarse para descargar de trabajo a la Agencia Española de Protección de Datos y para dar una respuesta más ágil y rápida a reclamaciones de

[101] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.150.

fácil solución, que pueden ser satisfechas en esta instancia, sin necesidad de continuar el trámite ante la Agencia Española de Protección de Datos[102].

Luego procede el inicio de las actuaciones, en el cual el artículo 64 de la Ley Orgánica recoge dos tipos de procedimientos. El primero cuando exista *"falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 al 22 del Reglamento de la Unión"*. En este caso, el procedimiento iniciará por un acuerdo de admisión a trámite adoptado según lo previsto en el artículo 65 de la Ley Orgánica. El plazo de la Agencia Española de Protección de Datos para resolver la reclamación presentada por denegación del ejercicio de los derechos será de 6 meses desde que se notifica al interesado el acuerdo de admisión a trámite de la reclamación. Transcurrido dicho plazo, el interesado podrá considerar estimada su petición.

El segundo procedimiento tiene como objeto *"la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento de la Unión Europea y en la Ley Orgánica, artículo 63.2"*. En este contexto, las actuaciones iniciarán de oficio o a instancia de parte, pues la norma habla de comenzar la tramitación mediante un acuerdo de inicio acordado por iniciativa de la propia Agencia o como consecuencia de la reclamación. El plazo máximo para resolver sobre una reclamación por infracción del Reglamento o de la Ley Orgánica es de 9 meses desde la fecha del acuerdo de inicio, o del proyecto de acuerdo de inicio. El plazo es de caducidad por lo que, tras los 9 meses sin respuesta, se entienden archivadas las actuaciones y abierta la reclamación en vía jurisdiccional.

Tras la admisión a trámite de la reclamación, o bien iniciado el procedimiento a iniciativa de la Agencia Española de Protección de Datos por infracción del Reglamento Europeo o de la Ley Orgánica, con carácter previo al acuerdo de inicio, se puede incoar una fase previa de investigación. El objeto de las actuaciones de investigación es *"lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento"*. [103]

El inicio de las actuaciones de investigación queda a criterio de la Agencia Española de Protección de Datos, salvo cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales. Dicha investigación se encomienda a los funcionarios de la Agencia Española

[102] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.151.
[103] REBOLLO DELGADO, Lucrecio, SERRANO PÉREZ, Maria Mercedes, **Manual de…**, ob. cit., p.155.

de Protección de Datos, aunque también la puede desempeñar funcionarios ajenos habilitados específicamente por la Presidencia, que tendrán consideración de agentes de la autoridad y están sometidos al deber de secreto. Toda administración pública está obligada a colaborar con la Agencia Española de Protección de Datos, así como los particulares y a proporcionar a la Agencia toda la documentación en su poder necesaria para el desarrollo de la actividad investigadora. Dicha Agencia podrá, en el marco de la actividad investigadora, solicitar las informaciones imprescindibles para poder identificar a los responsables de las conductas que pueden ser constitutivas de infracción del Reglamento y de la Ley Orgánica.

Dada la amenaza que esta posibilidad puede traer para el derecho de protección de datos y el derecho a la intimidad del sujeto, el precepto prevé un requerimiento motivado de la Agencia Española de Protección de Datos y su cesión, solamente en el caso de una investigación iniciada tras la presentación de una denuncia por un afectado como consecuencia de la conducta de una persona jurídica o respecto de la utilización de sistemas que permitan divulgar datos personales sin ningún tipo de limitación. En el resto de los casos, el artículo 53.1 de la Ley Orgánica exige para la cesión de datos la previa autorización judicial. Finalizadas las actuaciones de investigación, corresponde a la Agencia Española de Protección de Datos, según el artículo 68 de la Ley Orgánica, dictar acuerdo de inicio del procedimiento de la actividad sancionador de la Agencia.

IV. CREACIÓN DE UNA AUTORIDAD ÚNICA PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA REPÚBLICA DOMINICANA

Como bien explicamos en España existe la Agencia Española de Protección de Datos, en ese caso funciona como una autoridad de control ante la que se pueden presentar reclamaciones. Dicha autoridad de control principal cooperara con las demás autoridades de control interesadas, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente. En ese sentido, cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y respetando los plazos.

En el caso de la República Dominicana, no existe una autoridad de control, pues la Ley No.172-13 al ser muy específica para un sector, el único organismo regulador es la Superintendencia de Bancos, dejando desamparado otros sectores. La importancia de una autoridad única para la

protección de los datos personales es que se busque garantizar los derechos de la protección de datos a favor de los interesados, así como poder sancionar posibles infracciones, y teniendo un único regulador para dichos temas pudiendo ser más efectivo la tutela de los derechos, pues se estaría bajo el velo de un regulador especializado en temas de protección de datos personales.

La Red Iberoamericana de Protección de Datos, en su documento sobre Estándares de Protección de Datos Personales indica que *"la imperiosa necesidad de que cada Estado Iberoamericano cuente con una autoridad de control independiente e imparcial en sus potestades cuyas decisiones únicamente puedan ser recurribles por el control judicial, ajena a toda influencia externa, con facultades de supervisión e investigación en materia de protección de datos personales y encargada de vigilar el cumplimiento de la legislación nacional en la materia, la cual esté dotada de recursos humanos y materiales suficientes para garantizar el ejercicio de sus poderes y el desempeño efectivo de sus funciones"*.[104] En efecto, estos órganos no deben de recibir instrucciones de otras instituciones del Estado, estando libre de influencias externas.

En ese sentido, una autoridad de control deberá de contar con una cualificación técnica, competencias suficientes, infraestructura, recursos adecuados y un presupuesto propio, para poder conocer las denuncias de los interesados e intervenir en los casos necesarios, correctivas y/o sancionadoras. La Unión Europea enfatiza la necesidad de que los órganos de control de protección de datos tengan la capacidad de cooperar con sus homólogos a nivel regional e internacional, lo que facilitaría el intercambio de información en actividades de investigación.

En nuestro país, no contamos con un órgano de control de protección de datos personales. Actualmente, existe una Comisión que está trabajando en una posible modificación a la Ley No.172-13 con el fin de obtener una ley acorde a nuestros tiempos. Tendremos que esperar que nuestras autoridades contemplen la necesidad de crear una autoridad de control para poder tutelar y garantizar el derecho de protección de datos de una forma más amplia y precisa, con el fin de garantizar los datos personales y garantizar de forma fehaciente el derecho de protección de datos, con una verdadera garantía y tutela del mismo.

[104]Red Iberomericana de Protección de Datos. Disponible en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

CONCLUSIÓN

El derecho a la protección de datos de carácter personal es el derecho a decidir y controlar las informaciones personales que sobre nosotros conocen los demás, con independencia del carácter de íntimo o no del dato. En ese sentido, en el diario vivir los datos personales son utilizados muchas veces por la administración pública, siendo esta gran fichero de datos personales. De ahí radica su importancia, siendo los datos caracterizados como un activo de la persona hoy día.

Debemos estar conscientes de que los datos tanto conocidos o desconocidos deben ser protegidos, razón por el cual nació el derecho de protección de datos personales para cubrir dicha necesidad y así impedir su uso, destino y tráfico ilícito de la información personal, lesivo a la dignidad humana y a los derechos del afectado.

En el caso de la Unión Europea, la protección de datos de carácter personal es un derecho fundamental, y el Reglamento General de Protección de Datos (RGPD) es el nuevo marco regulatorio para este derecho, el cual permite a los europeos recuperar el control sobre su información personal. Otros países toman de referencia las normativas vigentes en la Unión Europea para el desarrollo e implementación de sus propias leyes de protección de datos.

Partiendo de que la administración pública es una gran creadora de ficheros que almacena datos de carácter personal y que resultan necesarios para cumplir con eficacia sus funciones, hoy día existe la necesidad de poner a disposición de los ciudadanos la información pública, la cual pudiera ser susceptible de lesionar el derecho fundamental a la protección de datos, pues la mayor parte de la información que obra en poder de las instituciones públicas, bien porque la reciben de los ciudadanos o porque sean autoras de la misma, está plagada de datos de carácter personal tanto de las personas que se insertan en estas, como de los destinatarios de su acción.[105]

Sin embargo, ningún derecho es absoluto, tal es el caso del derecho de protección de datos, el cual debe de ceder ante otros derechos fundamentales que deben ser protegidos. Tal como abordamos en el presente trabajo, la administración pública de por si debe de utilizar ciertos datos a los fines de poder ejercer sus funciones, no obstante debe existir una obligación legal

[105]RAMS RAMOS, Leonor, "El derecho fundamental a la protección…", ob. cit.,p.121.

para que la administración pueda otorgar los datos para fines procedentes, ya que existen límites y excepciones para el uso de los mismos. En consecuencia, el apoderamiento por parte de los poderes públicos de recoger, almacenar, tratar, usar y en algunos casos ceder datos personales, solo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos, como muchas veces pasa en el ámbito tributario.

No obstante, es necesario que realmente exista una protección a dicho derecho y más en un ambiente en el que se desenvuelve la sociedad hoy día. Los datos son informaciones sensibles, por tal razón deben ser protegidos para que no sean utilizados para fines no contemplados y en perjuicio del titular de los mismos.

En República Dominicana falta una mayor protección a este derecho, que si bien está constitucionalmente protegido como un verdadero derecho fundamental, la realidad es que actualmente en este país la evolución del mismo ha sido por la Constitución y la jurisprudencia dominicana, ya que la ley general existente es muy deficiente, pues solo se concentra en un sector determinado que es el de intermediación financiera. En consecuencia, sería necesario hacer una modificación integral de la ley No.172-13 vigente, ya que dicho derecho solo puede ser protegido en sede judicial a través de hábeas data, y no en sede administrativa.

Por su parte, en Europa, específicamente en España dicho derecho ha evolucionado con el paso del tiempo, en el que la jurisprudencia y los tratados le han dado un verdadero significado. Y más aún, ahora que España contempla un RGPD que es aplicable a todos los países pertenecientes a la Unión Europea, así como una LOPDGDD que busca completar el citado reglamento.

BIBLIOGRAFÍA

Doctrina

ÁLVAREZ CARO, M., **El derecho a la supresión o al olvido**, en Piñar Mañas, J. L., Reglamento europeo de protección de datos. Hacia un nuevo modelo europeo de privacidad, Editorial Reus, Madrid, 2016.

BERROA HICIANO, Román Arturo, Tesis doctoral: **Configuración jurídica del derecho fundamental a la protección de los datos personales en república dominicana. especial referencia a la tutela de los datos en el ámbito de las sociedades de información crediticia**, dirigido por Serrano Pérez, Maria Mercedes, Universidad de Castilla-La Mancha, Albacete, España, 2020.

FUENTE MIGUÉLEZ, Alberto, "Aplicabilidad de la normativa sobre protección de datos de carácter personal en el ámbito de la función estadística pública", **Revista Vasca de Administración Pública**. **Herri-Arduralaritzako Euskal Aldizkaria**, núm. 107, 2017.

GILS CARBÓ, Alejandra M., **Régimen legal de los datos personales y habeas data**, Ediciones Depalma, Buenos Aires, 2002.

GONZÁLEZ MÉNDEZ, Amelia, **Cesión y publicación de datos tributarios versus protección de datos personales,** UGARTEMENDIA ECEIZABARRENA, Juan Ignacio, (Coord), Derechos fundamentales y ordenamiento tributario, España, 2018.

HERRÁN ORTIZ, Ana Isabel, **La violación de la intimidad en la protección de datos personales**, Editorial Dykinson, S.L. Madrid, 1998.

MARTINEZ MARTINEZ, Ricard, "El derecho fundamental a la protección de datos: perspectivas", **Revista de los Estudios de Derecho y Ciencia Política de la UOC**, núm. 5, 2007,

MARTÍNEZ MARTINEZ, Ricard, "De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia. Régimen jurídico de la transparencia del sector público", **Revista Aranzadi**, 2014.

MURILLO DE LA CUEVA, Pablo Lucas, "Informática y protección de datos personales", **Cuadernos y Debates Centro de Estudios Políticos y Constitucionales**, núm. 43, Madrid, 1993.

MURILLO DE LA CUEVA, Pablo Lucas, "La Construcción del derecho a la autodeterminación informativa", **Revista de Estudios Políticos**, núm. 104, abril-junio 1999.

MURILLO DE LA CUEVA, Pablo Lucas, "El derecho a la autodeterminación informativa y la protección de datos personales", **Revista Azpilcueta**, núm.20, 2008.

ORTEGA GIMENEZ, Alfonso, "COVID 19: Un desafío para la protección de datos de carácter personal", **Revista Actualidad Jurídica Iberoamericana**, núm.12, 2020.

PEYRANO, G. F., **Régimen legal de los datos personales y habeas data, Comentarios a la Ley 25.326 y a la Reglamentación aprobada por el Decreto 1558/2001**, Lexis Nexis Depalma editorial, Buenos Aires, 2002.

PRECIADO DOMÉNECH, Carlos, **El derecho a la protección de los datos en el contrato de trabajo**, editorial Aranzadi, S.A.U., Madrid, 2017.

RALLO LOMBARTE, A., "El nuevo derecho de protección de datos", **Revista Española de Derecho Constitucional**, núm. 116, 2019,.

RAMS RAMOS, Leonor, "El derecho fundamental a la protección de datos de carácter personal como límite ¿infranqueable? Para la transparencia administrativa", **Estudios de Deusto**, Vol. 66/2, julio-diciembre 2018.

REBOLLO DELGADO, Lucrecio y SERRANO PÉREZ, María Mercedes, **Manual de Protección de Datos**, Tercera Edición, Editorial Dykinson, S.L, Madrid, 2019.

RODRIGUEZ ARANA, Jaime, **Interés General, Derecho Administrativo y Estado de Bienestar**, Iustel, Madrid, 2012.

SERRANO PÉREZ, María Mercedes, **El derecho fundamental a la protección de datos**, Derecho español y comparado, Thomson Civitas ediciones, SL, Madrid, 2003.

SERRANO PÉREZ, María Mercedes, **Los Derechos al Honor, a la intimidad personal y familiar y a la propia imagen. La inviolabilidad del domicilio. La protección de datos,** GARCÍA GUERRERO, José Luis, (Coord), Los Derechos Fundamentales: La vida, la igualdad y los derechos de libertad, Tirant lo Blanch, Valencia, 2013.

SERRANO PÉREZ, Maria Mercedes, **Algunos aspectos del derecho fundamental a la protección de los datos personales a la luz del reglamento general de protección de datos de la UE: Los principios de la protección de datos y los derechos de los sujetos**, Anuario 2018 del Tribunal Constitucional dominicano, impresión Búho, S.R.L., República Dominicana, 2019.

VELÁZQUEZ BAUTISTA, Rafael, **Protección jurídica de datos personales automatizados**, Colex, Madrid, 1993.

España

Normativa

Constitución de España de fecha 29 de diciembre del 1978.

Ley 14/1986, de 25 de abril, General de Sanidad, BOE-A-1986-10499.

Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, BOE-A-1989-10767.

Ley Orgánica 15/1999, de 13 de diciembre, orgánica de protección de datos de carácter personal (LOPD).

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Ley 58/2003, de fecha 17 de diciembre, General Tributaria, BOE-A-2003-23186.

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, BOE-A-2013-12887.

Ley Orgánica 3/2018, de 5 de diciembre de 2018, sobre Protección de Datos y Garantías de los Derechos Digitales.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Jurisprudencia

STC 254/93 del Tribunal Constitucional español de fecha 20 de julio, F.J.6.

STC 292/2000 del Tribunal Constitucional español de fecha 30 de noviembre, F.J.9.

Autos del TC 197/2003 de fecha 16 junio y 212/2003 de fecha 30 de junio.

Tribunal de Justicia, Sala Segunda de fecha 20 de diciembre del 2017, Peter Nowak c. Data Protection Commissioner (Asunto C-434/16).

STC 58/2018 del Tribunal Constitucional español de fecha 4 de junio, F.J.5.

República Dominicana

Normativa

Constitución de la República Dominicana de fecha 10 de julio del 2015.

Ley núm. 11-92, de 16 de mayo de 1992, que aprueba el Código tributario de la República Dominicana.

Ley No.42-01, de fecha 8 de marzo, General de Salud de la República Dominicana.

Ley No.200-04, de fecha 28 de julio, General de Libre Acceso a la Información Pública.

Ley 137-11 Orgánica del Tribunal Constitucional y de los procedimientos constitucionales de fecha 15 de junio del 2011.

Ley No.172-13, de fecha 15 de diciembre del 2013, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.

Jurisprudencia

Sentencia TC/0240/2017 del Tribunal Constitucional dominicano de fecha 19 de mayo, F.J.1.

TC/0484/16 del Tribunal Constitucional dominicano de fecha 18 de octubre del 2016, F.J.8.6.5.

Sentencia No. TC/0404/16 del Tribunal Constitucional dominicano de fecha 9 de septiembre del 2016.

Convenios y Tratados

Acuerdo Schengen de fecha 14 de junio del 1985, BOE No.181, de 30 de junio de 1991.
Carta de Derechos Fundamentales de la Unión Europea, aprobado en Estrasburgo, 12/12/2007. Publicado en el Diario Oficial de la Unión Europea No. C.303, de 14/12/2007.

Convenio Europeo de Derechos Humanos, aprobado en Roma el 4 de noviembre de 1950. Publicado en España en el BOE número 243, de 10 de octubre de 1979.

Convenio del Consejo de Europa, Ratificado por España el 27 de enero de 1984 (BOE No.274 de 15 de noviembre de 1985.

Declaración Universal de los Derechos Humanos adoptada por la Asamblea General de Naciones Unidas.
Pacto Internacional de Derecho Civiles y Políticos adoptado por la Asamblea General de Naciones Unidas.

Tratado de Funcionamiento de la Unión Europea DOUE núm.306, de 17 de diciembre del 2007.

Documentos en línea.

Modelo de ejercicio del derecho a no ser objeto de decisiones automatizadas de la AEPD. Disponible en: www.aepd.es/media/formularios/formulario-derecho-de-oposicion-decisiones-automatizadas.pdf

Salgado Remigio, Sofía, *El Secreto en la Administración Pública: información reservada y confidencial como excepción al derecho a la información*, Universidad Nacional Autónoma de México Ponencia para el III Congreso GIGAPP, 2012, Madrid España, Disponible en: http://www.gigapp.org/administrator/components/com_jresearch/files/publications/100%20SALGADO.pdf

Red Iberoamericana de Protección de Datos. Disponible en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf