



REPÚBLICA BOLIVARIANA DE
VENEZUELA
UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO



**ESPECIALIZACIÓN DE PROPIEDAD
INTELLECTUAL**

**PROTECCIÓN JURÍDICA DEL DATO Y
DE LAS BASES DE DATOS EN EL ORDENAMIENTO JURÍDICO VENEZOLANO**

Méndez Fuentes, Erika Marisela
Cédula de Identidad V-20.701.208

Asesor:
Olivero Pérez, William

Caracas, febrero de 2022

CARTA DE CONFIRMACIÓN DEL TUTOR

Quien suscribe, **WILLIAM ENRIQUE OLIVERO PÉREZ**, C.I. N° 10.823.302, actuando en mi carácter de Tutor, **APRUEBO EL TRABAJO ESPECIAL DE GRADO** presentado por la estudiante **ERIKA MARISELA MÉNDEZ FUENTES**, C.I.V-20.701.208, cursante de la **Especialización Propiedad Intelectual (EPROI)**, en la realización del Trabajo Especial de Grado titulado **PROTECCIÓN JURÍDICA DEL DATO Y DE LAS BASES DE DATOS EN EL ORDENAMIENTO JURÍDICO VENEZOLANO**, el cual orienté desde el punto de vista técnico y en reciprocidad el estudiante siguió los lineamientos y sugerencias que se le realizaron, de acuerdo con los requisitos exigidos por el Reglamento de Postgrado de la Universidad Monteávila.



Firma del Tutor

DATOS DEL ASESOR:

Nombre: William Enrique Olivero Pérez

Cédula: V.- 10.823.302

Teléfono: +58 (412) 3324106

E- mail: wolivero@profesor.uma.edu.ve

DEDICATORIA

La presente investigación está dedicada a cada persona ávida de interés sobre un tema cuyo auge apenas inicia.

AGRADECIMIENTOS

Quiero agradecer especialmente a mi madre Yuneida Fuentes, ¡una mujer ejemplar!, quien junto a mi padre me inculcaron grandes valores, entre ellos la importancia de la educación, de la preparación y el esfuerzo.

Gran admiración tengo por ella, por desempeñar un rol excepcional como madre y profesional, es mi ejemplo a seguir y sin duda le agradezco por apoyarme en mi nuevo rol de madre, gracias a su compañía he podido sobrellevar todas las nuevas responsabilidades, dedicación y esfuerzo que amerita ser una madre primeriza, trabajadora y estudiante, roles que no hubiese podido compaginar sin su apoyo incondicional.

De igual manera y no menos importante, agradezco al profesor William Olivero Pérez, por sus horas de orientación y guía.

Él indudablemente me condujo a buscar un tema de investigación innovador, incentivándome a expandir mis horizontes de conocimiento a un área nueva y tan relevante como lo es el manejo de datos.



REPÚBLICA BOLIVARIANA DE
VENEZUELA
UNIVERSIDAD MONTEÁVILA
COMITÉ DE ESTUDIOS DE POSTGRADO



ESPECIALIZACIÓN DE PROPIEDAD
INTELECTUAL

**PROTECCIÓN JURÍDICA DEL DATO Y
DE LAS BASES DE DATOS EN EL ORDENAMIENTO JURÍDICO VENEZOLANO**

Autor: Erika Marisela Méndez Fuentes
Asesor: William Olivero Pérez

Año 2022

RESUMEN

La era digital trajo consigo grandes cambios sociales, como el acceso al internet de manera viralizada y la transición a una economía digital basada en los datos, en su mayoría derivados del uso del internet, mediante plataformas sociales, compras en línea y/o cualquier otra herramienta o aplicación asociada a este medio. Dichos datos son almacenados y procesados en el Big Data, cuyo acceso y utilización en su mayoría es de entes públicos y privados con diversos fines.

La generación desmesurada de datos, trajo consigo un vacío legal en su manejo, por lo que ha surgido a nivel mundial, la necesidad de crear una regulación que atienda a la naturaleza jurídica del dato en consideración al valor económico, además de los intereses que confluyen en torno a los mismos, para garantizar los derechos de quienes crean, procesan o manejan las bases de datos.

De igual manera, es menester ponderar los derechos derivados del procesamiento y utilización, en consideración a los derechos que posee cada persona sobre el uso de sus datos

personales, los cuales pueden utilizarse con una índole comercial e incidir negativamente en la esfera de derechos personales, si son datos que se relacionan íntimamente con las personas y son utilizados con fines discriminatorios. Por lo tanto, es ineludible garantizar la esfera de los derechos personales de cada individuo, en consideración al derecho del honor y la privacidad.

Línea de Trabajo: Derecho de Propiedad Intelectual

Palabras Claves: Datos, Base de Datos no originales, Datos Personales, Derecho *sui generis*, economía digital, derecho al honor y la privacidad, habeas data, derecho a la información.

ABSTRACT

The digital age brought great social changes, such as vitalized internet access way and the transition to a digital economy based on data, mostly derived from the use of the internet, through social platforms, online purchases and / or any other tool or application associated with this medium. These data are stored and processed in Big Data, which access and use it is mostly from public and private entities for various purposes.

The excessive generation of data, brought with it a legal vacuum in the handling of data. It has arisen worldwide need of creating a regulation that attends the legal nature of data in consideration of the economic value, in addition to the interests that converge around them, to guarantee the rights of those who create, process or manage databases.

Similarly, it is necessary to weigh the rights derived from the processing and use, in consideration of the rights that each person has over the use of their personal data, which can be used for a commercial nature and negatively affect the sphere of personal rights, if it is data intimately related to people and are used for discriminatory purposes. Therefore, it is inescapable to guarantee the sphere of the personal rights of each individual, in consideration of the right of honor and privacy.

Line of Work: Intellectual Property

Law Keywords: Data, Non-original database, Personal data, *Sui generis* right, digital economy, right to honor and privacy, habeas data, right to information

ÍNDICE

DEDICATORIA	iii
AGRADECIMIENTOS	iv
RESUMEN	v
INTRODUCCIÓN	xi
CAPÍTULO I PLANTEAMIENTO DEL PROBLEMA	13
Objetivos de la Investigación	16
Objetivo General.....	16
Objetivos Específicos:.....	16
Justificación	17
Alcance de la Investigación.....	17
CAPÍTULO II MARCO TEÓRICO	19
Las Bases de Datos Originales.....	19
Datos de Prueba u Otros no Divulgados.....	20
Bases de Datos No Originales.....	22
Informes sobre la aplicación de la Directiva 96/9/CE	25
Los Datos	29
¿Qué es el Dato?	30
¿Qué es el Big Data?	31
I. Los Datos Personales y su Marco Regulatorio en Europa	35
¿Qué son los Datos Personales?	37

II. Tratamiento de Datos Personales	38
III. Tratamiento de Datos Personales relativos a Condenas e Infracciones Penales	41
IV. Autoridad de Control.....	42
V. Datos Personales y su Marco Regulatorio en España	43
VI. Tratamiento de Datos Personales relativos a Condenas e Infracciones Penales en España	46
El Dato como Base de la Economía Digital y la Propiedad Intelectual	48
Situación Jurídica en Venezuela en Relación a las Bases de Datos y el Dato.....	52
I. Protección de las Bases de Datos Originales.....	52
II. Protección de los Datos de Prueba u Otros No Divulgados	52
III. Protección del Dato.....	56
Derechos relacionados a los Datos Personales dentro del Ordenamiento Jurídico	56
Derecho al Honor, a la Privacidad, a la Informática y a la Intimidad	56
Derecho y acción del Habeas Data	60
Derecho a la información oportuna.....	64
Leyes relacionadas al Uso de Datos	66
CAPÍTULO III MARCO METODOLÓGICO.....	73
CAPÍTULO IV RESULTADOS.....	74
I. Identificar la protección jurídica de las bases de datos dentro del ordenamiento jurídico venezolano, mediante el estudio de la protección legal otorgada a las bases de datos riginales y no originales, con la finalidad de determinar si es necesario proponer consideraciones para su regulación.....	74

Con respecto a las bases de datos originales	74
Con respecto a las bases de datos no originales.....	75
II. Determinar la posible protección jurídica de los datos personales dentro del ordenamiento jurídico venezolano, mediante el análisis de la legislación existente sobre .la materia, en la Unión europea, España y Venezuela con la finalidad de evaluar sí es viable la trasposición del marco regulatorio español	77
a) El Derecho al honor, a la privacidad, a la informática y a la intimidad.....	78
c) El derecho a la información oportuna	80
III. Examinar la posible protección jurídica de los datos no personales dentro del ordenamiento jurídico venezolano, a través del estudio de la protección otorgada a nivel internacional en el Acuerdo Sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio (ADPIC) y la UE con el objetivo de recomendar cómo puede protegerse en Venezuela	81
CAPÍTULO V PROPUESTA	83
Consideraciones Generales sobre el Dato y las Bases de Datos	83
Consideraciones Generales sobre los Datos Personales	84
REFERENCIAS BIBLIOGRÁFICAS.....	88

INTRODUCCIÓN

En la presente investigación se pretende esbozar un posible marco legal para la regulación del dato y las bases de datos dentro del ordenamiento jurídico venezolano, a través del sistema de Propiedad Intelectual, haciendo necesariamente una distinción entre bases de datos originales y no originales, y la protección del dato en especial los datos personales, cuyo objeto de protección y naturaleza jurídica pueden considerarse disimiles y por ende, es menester determinar cuál es el régimen jurídico aplicable al momento de regular el manejo de dichos datos, si a través de un derecho *sui generis* como el aplicado en la Unión Europea (UE) o mediante el amparo de otro sistema de la Propiedad Intelectual.

Es por ello, que en el Capítulo I. Planteamiento del Problema, se realizó una investigación documental, cualitativa y según el abordaje de su objeto exploratoria, del Sistema de Propiedad Intelectual referente al manejo de bases de datos y el dato, en consideración al valor económico que representan los mismos y a la inversión que realizan los entes en su creación, y con mayor énfasis, con respecto al manejo de los datos personales, en concatenación con la protección de los derechos personales, protegidos en el régimen jurídico venezolano.

Como objetivo general de la investigación, se realizará un estudio del ordenamiento jurídico de la UE, en relación al tema planteado, con la finalidad de proponer de una manera armónica, el marco legal aplicable para el manejo de Bases de Datos, en el actual ordenamiento jurídico venezolano, y alcanzar los objetivos específicos para *i)* Identificar la protección jurídica de las bases de datos dentro del ordenamiento jurídico venezolano; *ii)* Determinar la posible protección jurídica de los datos personales dentro del ordenamiento jurídico venezolano, y *iii).* Examinar la posible protección jurídica de los datos no personales dentro del ordenamiento jurídico venezolano.

En el Capítulo II de la investigación, se desarrolla el Marco Teórico, donde se menciona como antecedente la protección de las bases de datos originales; posteriormente, dentro de las

bases teóricas se toman en cuenta la protección de las bases de datos no originales a través de un derecho *sui generis*, además se exponen las distintas posturas que existen en otras legislaciones para regular el actual manejo de datos, en especial la de la UE, por considerarse que encabeza a nivel mundial la regulación del dato, sucesivamente se hace mención de la situación jurídica en Venezuela, el posible marco legal aplicable para el tratamiento de datos, con fundamento a los de derechos constitucionales que permitirían la regulación del dato en Venezuela y mención a distintas leyes que lo regulan.

Posteriormente, se desarrolla el Capítulo III Marco Metodológico, donde se indica el método de la investigación; el Capítulo IV de los Resultados, donde la autora esboza algunas consideraciones que permitieron definir, si es posible trasladar las normativas analizadas, al ordenamiento jurídico de Venezuela, así como sus conclusiones.

Por último, en el Capítulo V se pretendió elaborar como objetivo final de la investigación las consideraciones que deben tomarse en cuenta para la protección del dato, de las bases de datos no originales, y las consideraciones pertinentes para la protección del dato personal dentro del ordenamiento jurídico venezolano.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

En el siglo pasado toda la información era recolectada de manera manual, organizada o esquematizada acorde al ingenio humano y fijada en un soporte material, lo que justificaba la necesidad de brindar una protección legal para resguardar las bases de datos, la cual se propició en muchos ordenamientos jurídicos, incluso en Venezuela, a través del Derecho de Autor. Sin embargo, a finales del siglo XX, se originaron grandes avances tecnológicos, como el internet y la inteligencia artificial que dieron apertura a lo que actualmente se denomina la era digital y el comercio digital.

La transición entre lo análogo a lo digital fue evidente y trajo consigo cambios sustancialmente radicales en el ámbito social, empresarial, comercial, abriendo paso a la creación de datos masivos y la globalización. Esta globalización permitió un comercio electrónico y un respaldo de la información en medios intangibles, asimismo, se originó el fenómeno viralizado de acceso a internet a la población mundial, permitiendo de esta manera romper las fronteras de la comunicación e información.

Desde niños hasta adultos de la tercera edad utilizan el internet, según datos estimados por la Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas, para el año 2018, alrededor de tres mil novecientos millones (3.900.000.000) de personas, que representaban el (51.2%) de la población mundial, hacían uso del internet, por su parte, según el Director General de la Organización Mundial de la Propiedad Intelectual (OMPI); Daren Tang (2021), en su Discurso de apertura del Diálogo de la OMPI Sobre Propiedad Intelectual (PI) y Tecnologías de Vanguardia en su Cuarta Sesión, para el año 2021 el sesenta (60%) de la población mundial, aproximadamente cuatro mil seiscientos millones (4.600.000.000) eran usuarios de internet y se procesaron alrededor de 2500 petra bytes de datos del internet, el cual es una red interconectada semejante a pequeñas conexiones neuronales, donde se almacenan

una infinita cantidad de datos de todo el mundo, respaldados en el Big Data de manera exponencial.

A principios del siglo XXI, era necesario una computadora para poder acceder a la red interconectada del internet, por lo tanto los datos que se generaban a nivel comercial, empresarial, financiero y social eran menores a los actuales, toda vez que, ya no es necesario estar conectado a la red a través de un computador, basta con contar con un televisor, un reloj, un teléfono celular, una tablet, o cualquier instrumento, aparato, que sea catalogado como inteligente, para que las actividades cotidianas, del día a día, de cada individuo, queden respaldadas en esta gran base de datos denominada Big Data, cuya información puede ser manejada por grandes empresas que hacen uso de dichos datos.

El crecimiento tecnológico es exponencialmente inimaginable para la población común, este cambio de paradigma ha roto los esquemas de las regulaciones jurídicas y económicas existentes que contemplan una regulación para la sociedad análoga, evidenciándose una brecha muy grande ante la falta de una normativa aparente que pueda regular el manejo de datos.

Los datos generados, pueden ser clasificados en bases de datos o se almacenan en el Big Data y estos datos pueden tener una índole comercial, pero si se relacionan íntimamente con las personas tienen una índole personal. Entonces, surgen una serie de interrogantes, ¿qué sucede con esos datos? ¿de quién son esos datos, de las personas que lo generan o de la entidad pública o privada que los utiliza para bases de datos?, ¿qué implicaciones tiene el uso de los datos.?

El manejo de información de este tipo, se ha vuelto necesaria en el mundo empresarial, ha permitido a las grandes empresas expandirse comercialmente, incluso en el sector público también se recolectan datos de la población, ejemplo de ello son las bases de datos que contienen cada país de sus nacionales y que, a su vez, es más común que las mismas, se cotejen e interconecten con más bases de datos de cada organismo público.

Por su parte en el sector privado, empresarial y comercial hay plataformas y páginas que crean perfiles de consumidores con base a los datos que cada persona ha generado de manera voluntaria o involuntariamente, haciendo uso del internet y muchos de ellos desconocen o no son conscientes de lo que consienten en cuanto al uso de esos datos, los cuales afectan a la esfera íntima de la personalidad de cada usuario, porque la información generada permite identificar o pueden asociarse de manera directa con la persona que los generó. Es por los hechos antes expuestos, que surge la necesidad de crear una protección legal, para salvaguardar los derechos de las personas que generan los datos, quienes tienen el derecho de tener control sobre dicha información, decidir con quién compartirla, el uso de la misma, e incluso de tener la potestad de decidir que se borren o modifiquen dichos datos.

Es necesario que países como Venezuela, en pleno desarrollo, creen regulaciones en pro de fomentar el comercio digital, como la de implementar una protección de las bases de datos no originales, a su vez garantizar la protección de los datos y regular el manejo de los mismos; pero se genera la disyuntiva para determinar cuál es el régimen jurídico aplicable al momento de regular el uso, almacenamiento y manejo de dichos datos, si a través de un derecho *sui generis* o bajo el amparo de la Propiedad Intelectual, bien por medio del Derecho de Autor o bajo otra figura legal.

En relación a la problemática expuesta, se considera necesario realizar una investigación documental, cualitativa y según su objeto explorativa, del Sistema de Propiedad Intelectual referente al manejo de bases de datos en general, haciendo necesariamente una distinción entre los datos según su naturaleza jurídica, en consideración al valor económico que representan las mismas y a la inversión que realizan los entes en su creación, y con mayor énfasis, con respecto al manejo de los datos personales, en concatenación con la protección de los derechos personales, protegidos en el régimen jurídico venezolano. De igual manera, se investigará el tratamiento de datos en ordenamientos jurídicos como el de la UE y en España, así como la protección que otorgan a bases de datos y el derecho *sui generis* aplicado en la UE, con la

finalidad de proponer consideraciones a tener en cuenta al momento de regular el marco legal aplicable en Venezuela, para el manejo de bases de datos, así como la regulación de los datos personales, en ponderación con los distintos derechos que convergen, más allá del ente público o privado que los maneje.

Objetivos de la Investigación

Objetivo General

- Determinar el posible marco legal aplicable para la protección del dato, dentro del ordenamiento jurídico venezolano, mediante el análisis de la legislación existente sobre la materia, específicamente en la Unión Europea (UE), España y Venezuela.

Objetivos Específicos:

- Identificar la protección jurídica de las bases de datos dentro del ordenamiento jurídico venezolano, mediante el estudio de la protección legal otorgada a las bases de datos originales y no originales, con la finalidad de determinar si es necesario proponer consideraciones para su regulación.

- Determinar la posible protección jurídica de los datos personales dentro del ordenamiento jurídico venezolano, mediante el análisis de la legislación existente sobre la materia, en la Unión Europea, España y Venezuela con la finalidad de evaluar si es viable la trasposición del marco regulatorio español.

- Examinar la posible protección jurídica de los datos no personales dentro del ordenamiento jurídico venezolano, a través del estudio de la protección otorgada a nivel internacional en el Acuerdo Sobre los Aspectos de los Derechos de Propiedad Intelectual

Relacionados con el Comercio (ADPIC) y la UE con el objetivo de recomendar cómo puede protegerse en Venezuela.

Justificación

El aumento de la generación de datos y su rol económico, los ha convertido en el motor de la economía digital, que utiliza tanto el procesamiento de datos personales como no personales. Esta realidad es relativamente reciente y por ende ha surgido la necesidad de actualizar el sistema normativo de los países a fin de regular el dato como un intangible de alto valor, que requiere de ciertas regulaciones, para evitar el abuso de dominio o la vulneración de las personas, en caso de que se realice un uso indebido de los datos personales.

En nuestro país, no existe una ley específica que proteja las bases de datos no originales o regule el tratamiento de datos, haciendo evidente un vacío jurídico, lo que conlleva a la necesidad de crear una legislación al respecto, en donde se ponderen los intereses empresariales y los derechos derivados de la esfera de la privacidad de cada individuo que genera datos personales.

Es por lo antes expuesto, que se considera pertinente realizar la presente investigación con el objetivo de comprender las normativas extranjeras analizadas y de esta forma delimitar un posible marco legal para la protección de las bases de datos y del dato distinguiendo su naturaleza jurídica, y con ello proponer algunas consideraciones al respecto para la protección de las bases de datos y tratamiento del dato dentro del ordenamiento jurídico de Venezuela.

Alcance de la Investigación

Con la presente investigación se pretende plantear las consideraciones a tomar en cuenta al momento de que el legislador, proceda a promulgar una ley de protección de los datos y de las bases de datos, determinar los derechos y principios que deben utilizarse para regular el uso, manejo y almacenamiento de datos, así como la protección a utilizarse para las bases de datos

no originales. Sin embargo, el presente trabajo tiene como limitante la investigación pormenorizada de las leyes dentro del ordenamiento jurídico para determinar cuáles han pretendido regular sobre las bases de datos y el tratamiento de datos, así como el poco desarrollo jurisprudencial o de la doctrina nacional al respecto.

CAPÍTULO II

MARCO TEÓRICO

En el presente capítulo, se procederá a desarrollar cuál ha sido la tendencia internacional para la protección del dato en atención a la naturaleza jurídica del mismo, lo cual ha conllevado a un tratamiento específico y distinto según sea la respectiva naturaleza, bien sea a través de bases de datos originales, de un derecho *sui generes*, del estándar mínimo de protección internacional de competencia desleal, establecido en el Acuerdo Sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio (ADPIC) o a través del régimen jurídico aplicado para el tratamiento de los datos personales. Posteriormente, se procurará desarrollar en el mismo orden secuencial, la protección del dato según su naturaleza jurídica, en el ordenamiento jurídico venezolano.

Las Bases de Batos Originales

A nivel internacional se encuentra, el estándar mínimo de protección que se brinda a las bases de datos originales, de conformidad con el ADPIC, en su anexo 1C, artículo 10, numeral 2, indica lo siguiente:

omissis

Las **compilaciones de datos** o de otros materiales, en forma legible por máquina o en otra forma, que por razones de **la selección o disposición de sus contenidos** constituyan creaciones de carácter intelectual, serán protegidas como tales. **Esa protección, que no abarcará los datos o materiales en sí mismos**, se entenderá sin perjuicio de cualquier Derecho de Autor que subsista respecto de los datos o materiales en sí mismos (Resaltado Nuestro)

La protección jurídica que puede otorgarse a las bases de datos en virtud del artículo antes mencionado, desarrolla como se indicó, el estándar mínimo de protección internacional para las bases de datos en consideración del esfuerzo intelectual para su elaboración, es decir por la originalidad que emplea el autor, bien en sea por la selección o disposición de su contenido. Esta protección no abarca el contenido de las bases de datos como bien indica el artículo, por lo tanto, el dato en sí mismo carece bajo estas normativas de una regulación o resguardo jurídico al igual que las bases de datos carentes de originalidad, denominadas bases de datos no originales.

Datos de Prueba u Otros no Divulgados

Incera, K. (2009) señala como antecedente legislativo de la protección de datos de prueba para la comercialización de productos farmacéuticos y agroquímicos que contienen nuevas entidades químicas, el Acuerdo del Acta Final de la Ronda Uruguay de 1990, artículo 42, párrafo 4-A y explica:

la información aportada para las autorizaciones de productos farmacéuticos no podría ser utilizada para la comercialización de productos competidores por un período razonable de tiempo (no menos de 5 años), salvo que el titular diera su consentimiento para el uso, la cual fue tomada a su vez de los ordenamientos internos de los Estados Unidos y la Unión Europea. (p. 3).

Dicha autora además indica, que esta regulación es actualmente de obligatorio cumplimiento para todos los Estados Miembros de la Organización Mundial de Comercio (OMC) de conformidad con el artículo 39.3 del ADPIC, el cual establece como estándar mínimo lo siguiente:

Protección de la Información No Divulgada

Artículo 39 1. Al garantizar una protección eficaz contra la competencia desleal, de conformidad con lo establecido en el artículo 10 bis del Convenio de París (1967), los Miembros protegerán la información no divulgada de conformidad con el párrafo 2, y los ***datos que se hayan sometido a los gobiernos o a organismos oficiales, de conformidad con el párrafo 3.***

(omissis)

3. Los Miembros, cuando exijan, como condición para aprobar la comercialización de productos farmacéuticos o de productos químicos agrícolas que utilizan nuevas entidades químicas, la presentación *de datos de pruebas u otros no divulgados* cuya elaboración suponga un esfuerzo considerable, **protegerán esos datos contra todo uso comercial desleal.** Además, ***los Miembros protegerán esos datos contra toda divulgación, excepto cuando sea necesario para proteger al público,*** o salvo que se adopten medidas para garantizar la protección de los datos contra todo uso comercial desleal. ***(Resaltado Nuestro).***

Nótese que la protección otorgada por el ADPIC, no se encuentra limitada por un periodo de tiempo como sí lo indica el antecedente legislativo antes mencionado, sin embargo, ha unificado entre todos los Estados miembros un estándar mínimo de protección internacional, de los datos cuya naturaleza jurídica radica en estudios preclínicos y clínicos que no constituyen un proceso inventivo, de usos contrarios a la competencia leal por parte de terceros.

Según Incera, K. (2009) la protección es otorgada a estos datos de pruebas, “por cuanto la obtención de los mismos ha supuesto para sus generadores o poseedores legítimos, esfuerzos considerables en tiempo y en dinero, y por consiguiente son valiosos” (p. 2). En el mismo orden de ideas, la precitada autora, explica en referencia las implicaciones de la protección de protección de los datos de prueba, “no constituye un derecho de propiedad, sino una garantía

para el generador o poseedor de la confidencialidad de la información valiosa y secreta, con lo cual no se constituyen derechos exclusivos” (p. 13).

Bases de Datos No Originales

Para mediados de noviembre del año 2002, ante el Comité Permanente de Derecho de Autor y Derechos Conexos, de la OMPI, en su octava sesión Ginebra, del 4 al 8 de noviembre de 2002, la UE y sus Estados Miembros, presentaron un documento sobre la Protección Jurídica de las Bases de Datos, en el cual realzaron la importancia económica de estas en el comercio, precisamente con la aparición de los servicios digitales, donde afirmaron que “Las bases de datos son la fuente del comercio electrónico y constituyen su núcleo” (p. 2), siendo esta la razón por la cual consideran que es necesario que estas bases de datos cuenten con una protección a través de la Propiedad Intelectual a fin de “proporcionar la suficiente seguridad jurídica **a los inversores y usuarios y el acceso de acuerdo con términos apropiados.**” (ob. Cit., p. 3) **(Resaltado Nuestro)**

En el mismo orden de ideas, expusieron la necesidad de brindar la protección jurídica de estas bases de datos, a través de un derecho *sui generis* y no mediante el Derecho de Autor, con justificación a la inversión económica que implica la elaboración de las mismas. El autor Sherif El-Kassas, (2002), explica que los partidarios de la protección por ese régimen legal, sostienen que hay un vacío jurídico en los sistemas de Propiedad Intelectual, porque la protección de las bases de datos a través de Derecho de Autor no protege las bases **de datos no originales** e indica, que

De aquí surgen las propuestas de proteger *las bases de datos no susceptibles de protección por Derecho de Autor en virtud de sistemas especiales o sui generis de Propiedad Intelectual* que se apartan de los modelos clásicos de protección por patente y Derecho de Autor subyacentes a los Convenios de París y de Berna (p. 6).

En la misma sintonía, en la Directiva 96/9/EC sobre Bases de Datos de la Comunidad Europea, aprobada el 11 de marzo de 1996, se distingue la protección que se otorga a las bases de datos **originales y creativas** las cuales “*gozan de protección mediante el Derecho de Autor en tanto que son obras literarias,*” Sherif El-Kassas, (2002), (p. 3) cuya protección no es extensiva al contenido de las bases de datos, lo cual se indica en el artículo 3, apartado 2 “sin perjuicio de los derechos que pudieran subsistir sobre dicho contenido”; *de las “**otras bases de datos** pueden gozar, bajo ciertas condiciones, de **protección de la Propiedad Intelectual en forma de un derecho sui generis, en particular si se crearon gracias a una inversión considerable,**”(Resaltado Nuestro) en la aplicación de medios financieros y/o en el empleo de tiempo, esfuerzo y energía, con independencia de los derechos existentes sobre su contenido¹ y según el considerando número 42 de la mencionada Directiva, el objetivo en sí es:*

facilitar al fabricante de una base de datos la posibilidad de impedir la extracción y/o reutilización no autorizadas de la totalidad o de una parte sustancial del contenido de la base de datos; que el fabricante de una base de datos es la persona que toma la iniciativa y asume el riesgo de efectuar las inversiones; que esto excluye, en particular, de la definición de «fabricante» a los subcontratistas.

Otros de los aspectos relevantes de la Directiva 96/9 CE, es que plantea como objeto del derecho *sui generis*, proteger y garantizar por un tiempo determinado de 15 años², la inversión en la obtención, verificación o presentación del contenido de una base de datos, la cual se define como “recopilaciones de obras, de datos o de otros elementos independientes dispuestos de

¹ Artículo 7, numeral 4 ídem

² Según el Artículo 10 , apartado 3, este periodo es extensivo “Cualquier modificación sustancial, evaluada de forma cuantitativa o cualitativa, del contenido de una base de datos y, en particular, cualquier modificación sustancial que resulte de la acumulación de adiciones, supresiones o cambios sucesivos que conduzcan a considerar que se trata de una nueva inversión sustancial, evaluada desde el punto de vista cuantitativo o cualitativo, **permitirá atribuir a la base resultante de dicha inversión un plazo de protección propio.**” (Resaltado Nuestro)

manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma.”³

En la Directiva se reconoce que la extracción y/o reutilización no autorizada del contenido de las bases de datos, son actos que pueden tener una consecuencia grave desde el punto de vista económico, por lo que se procura proteger a los fabricantes de bases de datos, contra la apropiación de los resultados por su inversión, esfuerzo, trabajo por recopilar el contenido, protegiendo el conjunto o las partes sustanciales de las bases de datos, de aquellos usuarios o competidores. Aunado a ello, se establece que el agotamiento del derecho de distribución no se plantea en el caso de las bases de datos en línea, que entran en el marco de la prestación de servicio, en consideración que para la época no había el auge del uso del internet y por ende las bases de datos electrónicas o en línea eran poco frecuente.

Con el objeto de incorporar el marco regulatorio de la Directiva sobre las bases de datos, en España, dictaron la Ley 5/1998, de 6 de marzo, de trasposición, en la que se reconoce que el Derecho *sui generis* es una novedad en el ordenamiento jurídico español, por lo que consideraron necesario crear un nuevo Título VIII en el Libro II del texto refundido de la Ley de Propiedad Intelectual dedicado a esta materia, aunado de otros artículos que incorporaron en el resto del texto de esa ley, con pequeños retoques para delinear mejor el alcance de dicha regulación.

Ejemplo de ello, es lo establecido como salvaguardia de aplicación de otras disposiciones, donde expresamente se establece o reconoce que lo establecido como derecho *sui generis* se debe entender:

Artículo 137. Salvaguardia de aplicación de otras disposiciones.

Lo dispuesto en el presente Titulo se entenderá sin perjuicio de otras disposiciones legales que afecten a la estructura o contenido de una base de datos tales como las relativas al Derecho de Autor u otros derechos de Propiedad Intelectual, al derecho de

³ Artículo 1. Ámbito de aplicación, apartado 2.

propiedad industrial, derecho de la competencia, derecho contractual, secretos, protección de los datos de carácter personal, protección de los tesoros nacionales o sobre el acceso a los documentos públicos.⁴

Informes sobre la aplicación de la Directiva 96/9/CE

En las disposiciones finales, artículo 16 apartado 3, de la Directiva 96/9/ CE, se establece que la Comisión presentará al Parlamento Europeo, al Consejo y al Comité Económico y Social un informe sobre la aplicación de la Directiva cada tres años, a partir de la entrada en vigencia de dicha normativa, evaluando la aplicación del derecho *sui generis*. Esta disposición no se cumplió de manera cabal, a la fecha tan solo se han presentado dos informes, uno en diciembre del año 2005 y otro en abril del año 2018.

El primer informe del año 2005, tuvo como finalidad evaluar el impacto de la directiva, su transposición en los ordenamientos jurídicos internos de los países miembros de la UE, así como el impacto en el mercado de las bases de datos; las posturas de los afectados y no menos importante, analiza los aspectos que pudiesen ser conflictivos sobre el derecho *sui generis* como: a) es difícil de interpretar, b) en ocasiones puede que proteja los datos en sí mismos, y c) el impacto económico del derecho *sui generis* no se ha cuantificado, (García. C, s.f.) y además se discutieron cuatro aspectos sobre la Directiva, *i) la posibilidad de eliminar la Directiva; ii) Suprimir la incorporación del derecho sui generis, lo que tendría como objetivo retomar la situación legal que existía; iii) mantener la normativa tal cual y como está, iv) o modificar la Directiva.*

El informe de 2005, concluyó que la directiva había logrado armonizar el derecho entre los países miembros de la UE, al implementar el estándar de originalidad, para la protección a través del Derecho de Autor, a pesar de existir deficiencias o ambigüedades conceptuales y que el derecho *sui generis* no tuvo efectos positivos o negativos que impactaran en la industria de las bases de datos. Además, salió a relucir el impacto de las interpretaciones restrictivas del derecho

⁴ Dicho texto quedó inserto en la Ley de Propiedad Intelectual de España, como el artículo 137.

sui generis por parte del Tribunal de Justicia de la Unión Europea⁵ (TJUE), que a la luz del informe de 2018, se consideraron como una limitación acertada del alcance para salvaguardar el equilibrio porque “garantizó de manera eficiente que no fuera necesario el consentimiento del creador de la base de datos en relación con el derecho *sui generis* para acceder a dichos datos, aliviando así los temores de monopolios de la información” (p. 25).

Por su parte el informe del año 2018, se basó en un estudio enfocado en la evaluación de la directiva de bases de datos, en el cual se incorporaron entrevistas, reuniones *ad hoc*, taller de partes interesadas, encuestas en línea. En este estudio se determinó, que aparentemente el derecho *sui generis* no estimula la inversión para la creación de bases de datos, pero sí es importante para la protección frente a terceros, ya que se usa como instrumento legal *ex post*.

Otro aspecto relevante es el cambio desde el 2005 al 2018 sobre el uso, valor económico y tecnológico de los datos, es decir sobre la economía de datos, cuyo aspecto no se protege por este derecho *sui generis*, debido a las interpretaciones del TJUE, pero dio lugar a la necesidad de evaluar si la protección podría extenderse a tal situación, como es el caso del sector deportivo, que considera necesario extender la protección a los datos, según lo indicado en dicho informe, incluso “algunos expertos destacan que no está claro qué papel jugará la Directiva de bases de datos, dada la creciente importancia de los datos generados por máquinas y sensores en el futuro⁶” (p. 26).

⁵ Ejemplo de estas interpretaciones, es el de la sentencia de 2004 donde el TJUE señaló que 'los recursos utilizados para elaborar una lista de caballos en una carrera y para realizar controles al respecto no constituyen una inversión **en la obtención y verificación del contenido de la base de datos** en la que aparece dicha lista. Por tanto, las bases de datos que son subproductos de las actividades principales de una empresa económica (bases de datos derivadas) no están, en principio, protegidas por el derecho *sui generis*, ya que no alcanzarían el umbral de «inversión sustancial». Esto podría aplicarse, por ejemplo, en muchas situaciones que impliquen la creación automatizada de datos generados por máquinas (por ejemplo, datos de Internet de las cosas). Sin embargo, en el contexto de la recopilación automatizada de datos por parte de objetos de la 'Internet de las cosas' conectados y equipados con sensores, se vuelve cada vez más difícil distinguir entre la creación y la obtención de datos cuando ya existe una categorización sistemática de los datos por parte del objeto de recopilación de datos (por ejemplo, robots industriales). p16 del informe de 2018. **(Resaltado Nuestro)**

⁶ Esto se relaciona por ejemplo con parte de los resultados que arrojaron las encuestas en línea, según los participantes, “la recopilación de datos requiere mayores esfuerzos de inversión que la creación de bases de datos. El 39,6 % de los propietarios que respondieron a la consulta pública dijeron que habían invertido

En el informe de 2018, de manera similar al del 2005, se concluyó que, la Directiva no ha hecho una contribución considerable en la competitividad del mercado de las bases de datos. Con respecto al análisis de los aspectos jurídicos, se hizo alusión a la duración de la protección, criticando que puede considerarse perpetua; con respecto al concepto de fabricante, critican que la definición se rige por quien asume el riesgo y esta interpretación puede conllevar a considerar que hay más de un fabricante, por la variedad de riesgos que existen (financieros, organizacionales o profesionales); con respecto al término de inversión sustancial, sigue siendo objeto de crítica⁷, sin embargo, algunos tribunales de los países miembros en especial Alemania, Francia, Italia y Grecia utilizan la regla de *exclusión de minimis* (mínimo de inversión), considerando como mínimo de inversión 4.000 euros.

De igual manera, se discutió sobre los derechos exclusivos con respecto a la extracción y reutilización de la parte sustancial⁸ de la base de datos, porque los derechos exclusivos no se aplican a la parte insustancial, mientras no sea un uso repetido y sistemático. No obstante, este criterio puede afectar de manera negativa a las bases de datos dinámicas.

Es importante la evaluación ejecutada por la Comisión de la UE, a fines realizar un seguimiento y estudiar el impacto de la Directiva 96/9/CE, porque a criterio de quien realiza la presente investigación, puede servir como herramienta para constatar la efectividad de la Directiva o para determinar los aspectos que son menester actualizar de la normativa, cuya necesidad se acentúa por el cambio económico-cultural exponencial, que se da a consecuencia de la Revolución de Datos, la cuarta revolución y la economía digital basada en los datos,

sustancialmente más en el contenido de las bases de datos que en la producción de las propias bases de datos. La mayoría de los creadores de bases de datos también consideran que la verificación del contenido de la base de datos es una actividad costosa". (p. 37.) del informe de 2018

⁷ Este aspecto fue evaluado con un resultado similar en el informe de 2005.

⁸ En el informe de 2018, explica que "Sustancial siempre se compara con la totalidad de una base de datos y debe medirse en comparación con el tamaño de los datos incluidos en la base de datos. En este punto el TJUE se pronunció a favor de un entendimiento amplio al permitir medir la sustancialidad a una parte subordinada de la base de datos, siempre que equivaliera, en sí misma, a una base de datos, aunque formara parte de una mayor base de datos p30

(aspecto que se mencionará más adelante), los cuales carecen de una protección a través de los sistemas jurídicos antes analizados.

Es importante traer a colación, que uno de los objetivos de crear la Directiva 96/9/CE, era cerrar la brecha existente entre la UE y los Estados Unidos en términos de producción de bases de datos. En este último país, no existe un derecho *sui generis* para proteger las bases de datos no originales, pero es el principal creador de bases de datos, como se reconoce en la sección 5.2.2.3 Producción de bases de datos de la UE en comparación con EE. UU, del informe de 2018, donde se indica que el número total de bases de datos publicadas en Europa en 2013 y registradas por la Gale Directory of Databases (GDD) fue de 4 684, mientras que en EE. UU, la cifra fue de 14 604. EE. UU, posicionándose estos como los mayores creadores de bases de datos del mundo.

Aunque se escapa del objeto de la presente investigación, se hará una somera mención a indicar que en Estados Unidos, la protección de las bases de datos se puede realizar a través del Secreto Comercial, con fundamento en la Ley de Defensa de los Secretos Comerciales (Public Law 114–153—May 11, 2016 Defend Trade Secrets Act Of 201) que define el término de apropiación indebida y mediante la Ley de Espionaje económico (Economic Espionage Act of 1996, 18 U.S.C 1831 et seq), que define el Secreto Comercial como:

“Artículo (3)

Significa todas las formas y tipos de información financiera, comercial, científica, técnica, económica o de ingeniería, incluidas las pautas, los planes, las compilaciones, los dispositivos de programa, las fórmulas, los diseños, los tipos, los métodos, las técnicas, los procesos, las proposiciones, los programas o los códigos, ya sean tangibles o intangibles, y si se almacenan o se almacenan en forma física, electrónica, fotográfica, fotográfica o por escrito si

- A) El titular de la misma haya optado medidas razonables para mantenerlo en secreto; y
- B) La información derivada de un valor económico independiente, real o potencial, de no

ser generalmente conocido, y no ser fácilmente averiguable por medios adecuados, por el público.⁹

Los Datos

Consideramos que fue futurista la comunidad europea a principios de este siglo al vislumbrar la emergente necesidad de regular el uso de información o bases de datos, a pesar de que no había un manejo masivo de macros datos como se ha venido generando en la última década, incluso de manera más reciente, se ha llegado a afirmar que nos encontramos ante una demanda creciente del uso de los datos, que han dado lugar a una verdadera revolución de datos, según el reporte preparado a solicitud del Secretario General de las Naciones Unidas por el Grupo Asesor de Expertos Independientes sobre la **Revolución de los Datos** para el Desarrollo Sostenible (2014), definen a esta revolución como:

Una explosión en el volumen de datos, en la velocidad con que se producen los datos, el número de productores de datos, la diseminación de datos, y la gama de asuntos sobre los que existen datos, ya sea que se produzcan a partir de nuevas tecnologías, como la telefonía celular y la “Internet de las cosas”, como de otras fuentes, como **los datos cualitativos, los datos generados por los ciudadanos y los datos acerca de las percepciones subjetivas.** (p. 6) **(Resaltado Nuestro).**

⁹ La anterior cita es una traducción libre del artículo (3) cuyo contenido es: the term “trade secret” means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if⁹

(A) the owner thereof has taken reasonable measures to keep such information secret; and
(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public

Recuperado de: <https://wipolex.wipo.int/es/text/500490>

¿Qué es el Dato?

Para El dato es un registro, es un hecho, que se puede clasificar según distintos factores como su origen, tipo de lenguaje, estructura, representación, entre otras. Para algunos, la clasificación más práctica es:

- **Datos estructurados** “son un esquema determinado que define cómo son las tablas en las que se almacenan los datos, qué tipo de campos tienen y cómo se relacionan entre ellas” (LUCA AI Powered Decision. Unidad de Datos de Telefónica. s.f p.s/n);
- **Datos semiestructurados** “no tienen un esquema definido. No encajan en un formato de tablas/filas/columnas, sino que se organizan mediante etiquetas o “tags” que permiten agruparlos y crear jerarquías. También se les conoce como no relacionales o NoSQL” (LUCA AI Powered Decision. Unidad de Datos de Telefónica. s.f p.s/n).
- **Datos no estructurados:** “pueden tener una estructura interna, pero no siguen ningún esquema o modelo de datos predefinido.” Pueden ser datos de texto, o no textuales; haber sido generados por una máquina o por una persona; y almacenarse en una base de datos” (LUCA AI Powered Decision. Unidad de Datos de Telefónica. s.f p.s/n).

En el mismo orden de ideas, el manejo masivo de datos se debe a la gran cantidad de información que se genera cada día, como se indicó, por el uso de internet “internet de las cosas” o dispositivos asociados a este e interconectados en una red, cuyo volumen es inmanejable por la mente humana o mecanismos análogos, la variedad es infinita debido a las fuentes de las que emanan, generando datos que, según Becerra, *et. al.* (2018), “pueden estar estructurados, no estructurados o parcialmente estructurados; no obstante, más allá de la cantidad o estructura, se destaca con el término Big Data elementos como la V del gran valor potencial presente y futuro.” (p. 40.) al espacio intangible en el cual se van almacenando los datos.

¿Qué es el Big Data?

Según la Real Academia Española (RAE) (2020) el Big Data es el “Conjunto de técnicas que permiten analizar, procesar y gestionar conjuntos de datos extremadamente grandes que pueden ser analizados informáticamente para revelar patrones, tendencias y asociaciones, especialmente en relación con la conducta humana y las interacciones de los usuarios”. (p.s/n).

Entendemos que la base de macros datos o el Big Data, es un término que se comenzó a implementar a mediados de este siglo, para identificar la mayor base de datos del mundo, donde queda almacenada toda la información “datos” que se genera dentro de la red, estos datos pueden ser de distintas naturaleza o índole, y **se pueden segregar en dos tipos de datos, personales o no personales.**

Uno de los aspectos jurídicos fundamentales al momento de analizar el proyecto del Big Data, es la privacidad, es por ello que Pérez, C (2016), comenta que se debe garantizar una finalidad legítima de los datos. Por su parte, Becerra, *et. al.* (2018), plantean la necesidad de regular el manejo de datos masivos, con un enfoque que no se limita a justificar la necesidad de un cambio de paradigma por la inversión económica que representa el manejo de estos datos, **sino por los derechos e interés que confluyen** entorno al Big Data:

Para ello, una de las premisas jurídicas es determinar y diferenciar el tratamiento jurídico de la actividad de Big Data cuando se realiza ya sea por poderes públicos o por el sector privado. El marco jurídico puede ser diferente a partir de la responsabilidad del Estado, el principio de legalidad y el interés público, frente a la libertad de empresa y los derechos en juego por el sector empresarial. Trátase del sector público o del privado que realicen acciones de Big Data, hay que plantearse la discrecionalidad o potestad para usar y tratar los datos masivos, la protección jurídica que tienen respecto a los métodos, las tecnologías y los resultados del Big Data; en especial debe tenerse en cuenta la

propiedad industrial y la concurrencia de posibles obligaciones de transparencia y puesta a disposición de los datos abiertos para su reutilización (ob. cit., p 47).

Además, resaltan la necesidad de identificar si el Big Data versa sobre datos personales o no, para poder determinar cuál es el régimen jurídico aplicable y esbozan la posibilidad de regular la utilización del Big Data, en consideración al daño masivo que puede ocasionar el manejo indiscriminado de estos datos al colectivo en un sector o sociedad, por lo que parten de la premisa de que “se requiere abordar jurídicamente el Big Data **desde la privacidad** y, en concreto, **desde el derecho de protección de datos personales**, a modo de una vis atractiva” (ob. cit., p 53). (Resaltado Nuestro)

Se trae a colación el artículo de González Fuster, Gloria (2012)¹⁰, en el cual, realizó un análisis jurisprudencial del Tribunal de Justicia de la Comunidad Europea, a fin de desarrollar el tema del equilibrio entre la Propiedad Intelectual y la protección de datos como un derecho emergente. La autora indica que en el caso de *Société belge des auteurs, compositeurs et éditeurs (SABAM) vs el proveedor de servicio de internet Scarlet Extended SA, (Scarlet)* año 2011, se basa en la negativa de Scarlet a instalar un sistema de filtrado de comunicaciones electrónicas generadas por el uso de software de intercambio de archivos “peer to peer” donde se procesaría de manera sistemática las direcciones IP en aras de garantizar el derecho a la Propiedad Intelectual, en el cual, la autora indica lo siguiente:

El Tribunal de Justicia, tras reconocer que el derecho a **la Propiedad Intelectual debe ser protegido, apuntó que no se trata de un derecho absoluto y que, por consiguiente, debe ser equilibrado con otros derechos fundamentales cuando sea necesario**. En línea con su sentencia de 2008 en el caso *Promusicae contra Telefónica (Promusicae)*, el Tribunal declaró que en el contexto de las medidas adoptadas para

¹⁰ González Fuster, Gloria (2012). «Equilibrio entre propiedad intelectual y protección de datos: el peso oscilante de un nuevo derecho» [artículo en línea]. IDP. Revista de Internet, Derecho y Política. N.º 14, págs. 47-60. UOC.

proteger a **los propietarios de los derechos de autor las autoridades nacionales y los tribunales tienen que encontrar un equilibrio justo entre la protección de los derechos de autor y la protección de los derechos fundamentales** de los individuos afectados por estas medidas. **Estos derechos incluyen, según especificó el Tribunal, la libertad de empresa, la libertad de recibir o comunicar informaciones y el derecho a la protección de datos de carácter personal (p. 3). (Resaltado Nuestro)**

Con un enfoque similar, en el informe del año 2014 de Un mundo que cuenta Movilización de la Revolución de los Datos Para el Desarrollo Sostenible, indican que la revolución de datos, trae consigo una serie de riesgos como el aumento a la desigualdad en el acceso y el uso de la información y a su vez determinan la necesidad de *“salvaguardar los elementos fundamentales de los derechos humanos: la privacidad, el respeto a las minorías o la soberanía de los datos nos obligan a establecer un equilibrio entre los derechos de las personas y los beneficios de la colectividad”*, en vista a la manera en que se recolectan los datos, a través de las denominadas *“huellas digitales que dejan las personas, a partir de objetos habilitados con sensores, o se infiere a través de algoritmos”*. p 6

Evidencia de estos riesgos de desigualdad en el acceso y uso de la información, fue el caso de Cambridge Analytica y Facebook, el cual se hizo público a mediados de marzo del año 2018, por publicaciones de los periódicos The Guardian y The New York Times, donde informaron que la base de datos creada por Aleksandre Kogan y su empresa Global Science Research con fines académicos, había sido utilizada por una empresa de investigación política y ciencia de datos llamada Cambridge Analytica quienes recopilaron de manera inapropiada, datos de más de 50 millones de perfiles de personas usuarias de Facebook, donde la gran mayoría de estos usuarios no habían proporcionado su consentimiento para que sus datos se utilizaran para elaborar perfiles políticos y psicológicos y hacer anuncios con esta índole, para manipular a la población; (Fruchter, N. *et. al.*, 2018).

Otro ejemplo de la vinculación de los datos con la propiedad industrial, es la patente que otorgó la Superintendencia de Industria y Comercio de Colombia en el año 2018, que consiste en un método y un sistema de seguridad que a través de datos biométricos gestiona y controla a las personas que acceden, adquieren y cumplen con actividades cargadas a su cuenta personal en un recinto, por lo que se comparte la opinión de Hernández, Pamela s.f, al indicar que “**no hay una relación directa sino específica entre datos personales y Propiedad Industrial**”, quien además resalta el hecho de que “*relación que habría entre la propiedad industrial y los datos personales estaría intrínseca en el manejo y las finalidades que se le da a la invención*”.(p s/n).

Por su parte y en contraposición al enfoque de protección de los datos, según el enfoque del derecho a la privacidad, Glazer, D, Sonsini, W, *et al*, (2017) Data As IP and Data License Agreements, indican que, en Estados Unidos, las empresas reconocen el valor de los datos como un activo empresarial que debe ser protegido y puede explotarse mediante la venta a terceros o concesión de licencias cuya protección puede depender de: i) La naturaleza de los datos recopilados y el motivo de su recopilación y ii) su forma de agregación. Asimismo, indican que: “los datos pueden protegerse por una o más categorías de Propiedad Intelectual, bien como secreto comercial¹¹, por Derecho de Autor, como una categoría de propiedad intangible y por una patente.” (p 3), pero cada una de estas opciones, pueden no ser las más efectivas.

A nuestro criterio, los casos antes mencionados, son tan solo algunos de los muchos indicios que vislumbran la inminente necesidad de diferenciar si los datos son personales o no, para salvaguardar la esfera de derechos fundamentales de las personas y ponderarlos con la esfera de derechos económicos que pueden existir entorno al uso de datos.

En el mismo orden de ideas, consideramos que estos casos permiten resaltar el rol de la Propiedad Intelectual como un derecho que se puede utilizar de manera efectiva para esbozar y

¹¹ Esta protección es una de las más usuales en Estados Unidos y su fundamento se encuentra en Ley de Espionaje económico (Economic Espionage Act of 1996, 18 U.S.C 1831 et seq)

delimitar el manejo de los datos, además de incentivar el modelo económico que ha venido implementándose con fundamento en el uso de los mismos y que ha buscado regular la UE a través del derecho comunitario, no solo a través de la Directiva 96/9/CE antes analizada, sino también ante la regulaciones que ha implementado para el manejo, uso y almacenamiento de los datos personales, que a continuación se mencionarán.

I. Los Datos Personales y su Marco Regulatorio en Europa

La UE, así como encabezó la regulación de un derecho *sui generis* para el resguardo de las bases de datos no originales, también encabezó la regulación de los datos personales, e implementó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de Estos Datos, posteriormente derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD) del 27 de abril de 2016 actualmente vigente, en conjunto con la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 Relativa a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales por Parte de las Autoridades Competentes Para Fines de Prevención, Investigación, Detección o Enjuiciamiento de Infracciones Penales o de Ejecución de Sanciones Penales, y a la libre Circulación de Dichos Datos, conforman el marco regulatorio en dicha materia.

Dentro de las consideraciones previas del RGPD, se encuentra resaltado la protección de las personas físicas en relación con el tratamiento de datos personales como un derecho fundamental, por lo tanto, el tratamiento de estos datos, debe estar concebido para servir a la humanidad. El derecho que envuelve la protección de datos personales no es un derecho

absoluto, sino que debe considerarse en relación con su función en la sociedad, y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad¹².

Asimismo, entre otra de las consideraciones del RGPD, destaca como objetivo la libre circulación de datos dentro de la comunidad europea, la cual no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales, además se toma en cuenta, el derecho que tienen las personas de mantener control sobre sus propios datos¹³.

Resulta interesante hacer mención, que en el RGPD consideración 38, se toma expone, la necesidad de brindar una protección específica de los datos de los niños toda vez que los mismos *“pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales.”* Los niños son el consumidor de relevo, por eso, esta consideración está contemplada, en ocasión a los estudios de mercadotecnia y además por la elaboración de perfiles de personalidad o de usuario que hacen de ellos.

De igual manera, el RGPD resalta que la protección sobre los datos personales debe aplicarse a las personas físicas con independencia de su nacionalidad o de su lugar de residencia¹⁴¹⁵, esto se relaciona con el objetivo de la libre circulación de datos dentro de la UE, o con terceros que deben cumplir con los estándares de garantías del tratamiento de datos o adecuar su ordenamiento para garantiza a los interesados derechos efectivos y exigibles, así como un derecho a la tutela administrativa y judicial efectiva. aspectos que son tomados en consideración dentro de la Directiva (UE) 2016/680¹⁶ e influye en la cooperación entre las autoridades de control de los Estados miembros.

¹² Consideración 4 del referido Reglamento

¹³ Consideración 7

¹⁴ Considerando 14 concatenado con el art. 3 Ámbito territorial

¹⁵ El mismo precepto se establece en el considerando 17 de la Directiva (UE) 2016/680

¹⁶ Considerando 7 de Directiva (2016/680) establece: “Para garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial, es esencial asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros. A tal efecto, el nivel de protección de los

¿Qué son los Datos Personales?

El RGPD en su artículo 4, define a los **datos personales**, como:

Artículo 4 Definiciones A efectos del presente Reglamento se entenderá por:

1) «datos personales»: Toda información sobre una persona física identificada o identificable¹⁷ («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Dentro de la clasificación de datos personales, también puede haber una subclasificación o categoría de datos sensibles, denominados por el Reglamento como **categoría especial** de datos personales, que ameritan un tratamiento especial, según el considerando 51 del RGPD, debido a que *“podría entrañar importantes riesgos para los derechos y las libertades fundamentales”*, toda vez, que estos datos pueden revelar el origen racial o étnico, por lo que se prohíbe elaborar perfiles que den lugar a la discriminación de personas físicas por razones basadas en datos personales de dicha naturaleza, con sus excepciones como por ejemplo fines de salud pública. Ahora bien, los datos que revelen opiniones políticas, convicciones religiosas o

derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, debe ser equivalente en todos los Estados miembros”

¹⁷ En cuanto a ese aspecto, el considerando 26 del Reglamento indica lo siguiente: “Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.”

filosóficas, biométricos, genéticos, relativos a la orientación sexual o vida sexual, también pueden clasificarse en dicha categoría y ameritan un tratamiento especial.

Como se desprende de la definición de datos personales, estos se pueden clasificar según el aspecto que traten o contenido en datos genéticos, biométricos o de salud, cuyas normativas los definen como¹⁸:

- **datos genéticos**¹⁹: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;
- **datos biométricos**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;
- **datos relativos a la salud**: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

II. Tratamiento de Datos Personales

Hay un criterio unificado dentro de ambas normativas analizadas en cuanto el alcance del tratamiento, que implica una serie de operaciones como lo son la organización, estructuración, comunicación por transmisión, difusión, acceso, cotejo, supresión y limitación de datos. De igual

¹⁸ Art. 4 de El Reglamento y art.3 de la Directiva (UE) 2016/680,

¹⁹ En el considerando 23 de la Directiva (UE) 2016/680, los datos genéticos contienen una definición más amplia que indica; "Debe entenderse por datos genéticos todos los datos personales relacionados con las características genéticas de una persona física que se hayan heredado o adquirido y que aporten información única sobre la fisiología o la salud de esa persona física, y que resultan de análisis de una muestra biológica de la persona física de que se trate, en particular cromosómicos, del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o de análisis de cualquier otro elemento que permita obtener información equivalente."

manera, se establece una serie de principios que determinan la manera en que deben ser tratados los datos, es decir rigen el tratamiento como lo son: i) licitud, lealtad y transparencia, ii) limitación de la finalidad; iii) Adecuados y pertinentes, iv) Minimización de datos, v) Exactitud; vi) limitación del plazo de conservación y vii) Responsabilidad proactiva.

Estos principios implican una delimitación del tratamiento, por ejemplo, el responsable del tratamiento de datos (*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*),²⁰ o en su defecto el encargado del tratamiento (*persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*),²¹ deben procurar recoger los datos para una finalidad específica, por un tiempo determinado y la persona que genera los datos debe saber para qué se usarán los mismos (transparencia), además los datos deben ser pertinentes, es decir tener una relación, ser adecuados al objetivo por el cual han sido recogidos o almacenados.

Ahora bien, dentro de toda esta delimitación, juega un rol importante en el tratamiento de datos personales desarrollado por el RGPD, el consentimiento²² de quien genera los datos, porque esta persona debe aceptar o permitir el uso de los mismos y para ello debe ser informada de una manera clara y sencilla el motivo y finalidad del uso de sus datos.

Por su parte, también se exige que el tratamiento cumpla con una serie de condiciones para ser considerado lícito, esto se interrelaciona con los principios antes mencionados y algunas de esas condiciones son la exigencia del consentimiento informado para utilizar los datos con fines específicos; que el tratamiento persiga intereses legítimos por parte del responsable o tercero en ponderación con los derechos y libertades del interesado, particularmente cuando el

²⁰ Artículo 4 de El Reglamento.

²¹ Artículo 4 ídem.

²² En el Reglamento se define el consentimiento en el artículo 4.1 como: “*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*”.

interesado sea un niño; otra condición, en el supuesto en cual el interesado es parte, es la exigencia de necesidad del tratamiento para la ejecución de un contrato, todas estas condiciones son establecidas en el artículo 6 y siguientes del RGPD.

Aunado a lo anterior, el RGPD indica siete derechos que tiene el interesado (persona que genera los datos) como lo son: **i) Transparencia de la información, comunicación y modalidades** de ejercicio de los derechos del interesado, **ii) Información y acceso**, **iii) de rectificación**, es decir podría el interesado solicitar que se modifiquen los datos existentes, **iv) de supresión - Derecho al olvido** por ejemplo cuando ya no son necesarios los datos o el interesado desea retirar el consentimiento de uso de los datos personales, o estos últimos hayan sido tratados ilícitamente, **v) limitación del tratamiento**, **vi) de portabilidad de los datos**, y **vii) oposición y decisiones individuales automatizadas**: por ejemplo el interesado podría oponerse al tratamiento de datos cuando tenga por objeto la mercadotecnia, fines de investigación científica, investigación histórica y/o estadísticos, además tiene derecho a no ser objeto de una decisión basada en el tratamiento automatizado de sus datos.

El incumplimiento de estos derechos y principios, da derecho a que el interesado afectado solicite la indemnización de daños y perjuicios y adicionalmente acarrea una sanción administrativa dependiendo de la naturaleza, gravedad y duración de la infracción, la intencionalidad, el grado de responsabilidad²³, así como otros elementos regulados por el RGPD y según el caso en concreto las multas pueden oscilar entre 20.000.000 a 10.000.000 Euros o porcentajes como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

A criterio del investigador, todos estos derechos son una extensión y efectiva manifestación del ejercicio que se deriva en gran medida de la autonomía que tiene la persona

²³ Artículo 83 de El Reglamento Condiciones generales para la imposición de multas administrativas

física de otorgar su consentimiento, relacionado con una serie de derechos personales como son el derecho de información, la personalidad y privacidad.

Como mecanismo de protección o garantía del tratamiento de datos, el RGPD prevé la figura *del delegado de protección de datos*, que es designado²⁴ por el responsable y el encargado del tratamiento. Es una figura que debe mantener cierta dependencia de quienes lo designan, porque su rol es asesorar, supervisar sobre el cumplimiento del RGPD en cuanto al tratamiento de los datos personales, además también tiene una función de cooperador entre la autoridad de control y canal de contacto con ella, así como con los interesados, en lo que respecta al tratamiento de sus datos, es por ello y debido a la responsabilidad del cargo, es necesario que, quien desempeñe este rol respete la confidencialidad del tratamiento.

III. Tratamiento de Datos Personales Relativos a Condenas e Infracciones Penales

En este supuesto, el responsable es el Estado o la autoridad competente que cada Estado miembro designe con el objetivo de que hagan un tratamiento de los datos personales relativos a condenas e infracciones penales o medidas de seguridad, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, salvo que exista autorización por parte del Derecho de la Unión o del Estado Miembro, esto es una diferencia importante con respecto a las condiciones el tratamiento, porque en este supuesto no depende del consentimiento de la persona cuyos datos se tratan.

En el manejo de esta categoría de datos, igual existen una serie de derechos como lo son: el derecho de información del interesado, el cual impone la obligación a la autoridad que maneja los datos de informar al interesado quién es el responsable de los datos, los fines para los cuales se usarán sus datos e incluso tiene derecho de acceso a sus datos, que puede ser

²⁴ Su designación y supuestos están establecidos en el Artículo 37 de El Reglamento.

limitado por cada Estado miembro según el artículo 6 apartado 4: “*siempre que constituya una medida necesaria y proporcional en una sociedad democrática*” y en igual sentido el interesado tiene el derecho de solicitar la rectificación, supresión o a la limitación de su tratamiento, los cuales pueden verse limitados por el Estado Miembro.

IV. Autoridad de Control

El RGPD, tiene el mandato de que cada Estado Miembro cree una autoridad de control²⁵, que tendrá la responsabilidad de supervisar la aplicación del reglamento y la Directiva 2016/680,²⁶ para garantizar los derechos y obligaciones, además dicha autoridad será independiente en el desempeño de sus funciones, esto implica incluso independencia de recursos humanos, técnicos y financieros. Sus miembros deben ser nombrados por un procedimiento transparente, bien por su gobierno, jefe de Estado, parlamento o un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros²⁷.

Es el organismo competente a fin de reconocer algún reclamo referente a una infracción de RGPD, tiene poderes para iniciar investigaciones, auditorías de protección de datos, notificar de las infracciones de RGPD, ejercer poderes correctivos, por lo que podrá sancionar , ordenar al responsable o encargado de datos que atiendan las solicitudes de ejercicio de los derechos

²⁵ Artículo 51 de El Reglamento

²⁶ Entre sus considerandos indica: “(148) A fin de reforzar la aplicación de las normas del presente Reglamento, **cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento**, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

²⁷ Artículo 53 de El Reglamento y artículo 43 de la Directiva (UE) 2016/680

del interesado o que se ajusten a las disposiciones del RGPD; imponer limitaciones temporales o definitivas del tratamiento, incluso su prohibición; ordenar la rectificación o supresión de datos, limitación del tratamiento, imponer multas administrativas, ordenar la suspensión de los flujos de datos, tendrá asimismo facultades consultivas, podrá hacer dictámenes, aprobar cláusulas contractuales, administrativas o corporativas siempre sujeto a las garantías adecuadas, a la tutela judicial efectiva y garantías procesales establecidas en la Unión²⁸.

V. Datos Personales y su Marco Regulatorio en España

Con la finalidad de adaptar dentro del ordenamiento jurídico de España y hacer la debida transposición del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD) del 27 de abril de 2016, dictaron la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la cual reconoce en su preámbulo que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental y de rango constitucional, que se desprende del artículo 18.4 de la Constitución Española²⁹, que versa sobre el Derecho a la intimidad, el cual establece lo siguiente:

Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

...

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.

En sintonía con el RGPD, busca fomentar la libre circulación de datos y su ámbito de aplicación es el tratamiento total o parcialmente automatizado de datos personales, así como al

²⁸ Artículo 57 de El Reglamento y artículo 46 de la Directiva (UE) 2016/680

²⁹ Constitución Española Aprobada por Las Cortes en sesiones plenarias del Congreso de los Diputados y del Senado celebradas el 31 de octubre de 1978 Ratificada por el pueblo español en referéndum de 6 de diciembre de 1978 Sancionada por S. M. el Rey ante Las Cortes el 27 de diciembre de 1978

tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.³⁰el cual se rige por los mismos principios y derechos establecidos en El RGPD.

Como novedad y a diferencia del RGPD, la Ley Orgánica 3/2018 regula el tratamiento de los datos de las personas fallecidas³¹ a solicitud de los familiares o herederos del fallecido, quienes podrán solicitar el acceso de los datos, rectificación o supresión a menos que la persona fallecida lo hubiese prohibido expresamente. Otro aspecto diferente es el consentimiento de los menores de edad, el cual es lícito cuando sean mayores de 14 años y si son menores, 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 tutela³²

Aunado a lo anterior, la Ley en su Título IV, disposiciones aplicables a tratamientos concretos como el de empresarios individuales y profesionales libres, de sistemas de información crediticia, cuya información debe estar limitada a un tiempo determinado máximo 5 años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito. Tratamiento con fines de video vigilancia, en el cual sólo se permite videos de vías públicas y el almacenamiento de los datos por un mes;³³ datos con ámbito de función estadística publicitaria, archivo de interés público por parte de las autoridades administrativas entre otros.

Con respecto al ejercicio de las funciones de la autoridad de control de datos, las desempeña la Agencia Española de Protección de Datos,³⁴ la cual es una autoridad independiente, que ejerce las facultades y poderes antes indicados en la sección de la autoridad de control de conformidad con el RGPD, los cargos como el presidente de la agencia y su adjunto, deben ser nombrados por un mecanismo particular y su duración en el cargo es de 5 años,

³⁰ Artículo 2 Ley Orgánica 3/2018.

³¹ Artículo 3 ídem.

³² Artículo 7 ídem.

³³ Artículo 22 ídem.

³⁴ Es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

renovados por otro periodo de igual duración, un aspecto que blinda de independencia a sus cargos, es el hecho de que no son de libre remoción, sino por petición propia o por separación acordada por el Consejo de Ministros con supuestos particulares.³⁵

En cuanto al aspecto de las infracciones, esta ley en armonía con las cuantías previstas en el apartado de las sanciones del RGPD, hace distinción entre:

- **Infracciones muy graves:** (prescriben a los 3 años) cuando se vulnere de manera sustancial los principios y garantías, no se cumplan con las condiciones de licitud del tratamiento, el incumplimiento de los requisitos de validez del consentimiento, así como la utilización de los datos con una finalidad distinta para la cual fueron recogidos sin contar con el consentimiento, manejo de datos sensibles o relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos, la omisión de informar al afectado acerca del tratamiento de sus datos, violación del deber de confidencialidad entre otros supuestos regulados en el artículo 72 de la Ley.
- **Infracciones graves:** (prescriben a los 2 años) suponen una vulneración sustancial por ejemplo del tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el titular de su patria potestad o tutela, no acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por quien ejerza la titularidad de la patria potestad o tutela, entre otras infracciones enunciadas en el artículo 73 de la Ley;
- **Infracciones leves:** (prescriben al año) de aspectos meramente formales, por ejemplo: No cumplir con los derechos de acceso, rectificación, supresión,

³⁵Los supuestos particulares son: a) Incumplimiento grave de sus obligaciones, b) incapacidad sobrevenida para el ejercicio de su función, c) incompatibilidad, o d) condena firme por delito doloso, según el Artículo 48 de la Ley Orgánica 3/2018.

limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado; el incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento; entre otras infracciones enunciadas en el artículo 74 de la Ley.

VI. Tratamiento de Datos Personales Relativos a Condenas e Infracciones Penales en España

Con la finalidad de adaptar dentro del ordenamiento jurídico de España y hacer la debida transposición de la Directiva (UE) 2016/680, se promulgó la novísima Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, cuyos aspectos más relevantes para la presente investigación se procederán a mencionar.

En el preámbulo de dicha Ley, se resalta la necesidad de promulgar una ley con el objetivo ineludible de promover la *cooperación internacional y la transmisión de información de carácter personal entre los servicios policiales y judiciales de los países implicados* siempre garantizando la seguridad de las personas a lo largo de las fases del tratamiento

Con respecto a la categoría especial de datos mantiene lo desarrollado en el RGPD, e indica que, se pueden incluir los datos biométricos (como las huellas dactilares o la imagen facial) sólo cuando su tratamiento está dirigido a identificar de manera unívoca a una persona física. Además de esto, en línea general se reconocen los derechos de acceso, rectificación, supresión y limitación del tratamiento; el interesado también tiene facultad para conocer si se están tratando o no sus datos y en dado caso, solicitar la rectificación de los mismos, si fuesen inexactos o en cumplimiento de una obligación legal.

Ahora bien, la Ley en su artículo 24, contempla restricciones a los derechos de información, acceso, rectificación, supresión de datos personales (el tiempo máximo para

mantener los datos será de 20 años, luego deben suprimirse) y la limitación de su tratamiento, por fines específicos como la seguridad pública, nacional, por la seguridad de otras personas; para impedir que obstaculicen indagaciones, investigaciones o procedimientos judiciales y/o evitar que se cause un perjuicio a la prevención detección, investigación y enjuiciamiento de infracciones penales o a la ejecución de sanciones penales.

En el supuesto de personas o menores de edad fallecidos y/o personas con discapacidad, el ejercicio de los derechos antes mencionados, serán ejercidos por sus familiares, herederos o quien ejerza la patria potestad o tutela y en el caso de menores de edad fallecidos, podrá actuar el Ministerio Fiscal.

Ley Orgánica 7/2021, en desarrollo de la Directiva 2016/680, impone un deber de colaboración, el cual implica el deber de la administración pública o cualquier persona física o jurídica proporcione a las autoridades judiciales, al Ministerio Fiscal o a la Policía Judicial los datos, informes y antecedentes a la autoridad competente que lo soliciten, y aunado a ello, con el fin de garantizar la actividad de investigación, el interesado no será informado de la transmisión de sus datos a las autoridades competentes, ni de haber facilitado el acceso a los mismos por dichas autoridades de cualquier otra forma.³⁶ A criterio del autor, esto es un ejemplo de ponderación entre los derechos individuales y los derechos del colectivo, la seguridad pública o nacional, por lo que se limitan pero sin menoscabar los derechos individuales

En cuanto a las autoridades de control de datos se dispone que serán la Agencia Española de Protección de Datos y las Agencias Autonómicas de Protección de Datos, en sus respectivos ámbitos competenciales.

Aunque en las demás leyes mencionadas contemplan El Registro de operaciones, en esta lo clasifican como “pieza angular de este sistema e instrumento básico para acreditar el cumplimiento de varios de los principios de tratamiento, que comprenderá la recogida, la

³⁶ Artículo 7 Ley Orgánica 7/2021.

alteración, las consultas y las transferencias de los datos personales entre otras operaciones³⁷”
Es decir, es una garantía que permite corroborar el tratamiento de datos es lícito y cumple con las medidas y políticas de protección de datos con el fin de salvaguardar la integridad y seguridad de datos en el ámbito penal.

En desarrollo al derecho de indemnización del interesado, la ley distingue la responsabilidad del sector público, la administración pública, la responsabilidad que provenga de un órgano judicial en su artículo 53 y el Derecho a indemnización por encargados del tratamiento del sector privado en su artículo 55. Con respecto al régimen de sanciones, mantiene la distinción entre la gravedad y con multa de la siguiente cuantía: a) Las infracciones muy graves, con multa de 360.001 a 1.000.000 euros. b) Las infracciones graves, con multa de 60.001 a 360.000 euros. c) Las leves, con multa de 6.000 a 60.000 euros.³⁸ Las cuales prescribirán a los seis meses, a los dos o a los tres años de haberse cometido, según sean leves, graves o muy graves, respectivamente.³⁹

El Dato como Base de la Economía Digital y la Propiedad Intelectual

Hemos expuesto hasta los momentos cómo se ha desarrollado la protección de las bases de datos no originales, posteriormente se dio apertura al tema de los datos, su relación con la Propiedad Intelectual, la distinción de la naturaleza del dato, la estructura legal que ha creado la UE para el tratamiento de datos personales, para proteger aspectos neurálgicos como lo es el desarrollo a derechos personales como la intimidad o la privacidad. Todo eso fue necesario para

³⁷ Consideraciones del preámbulo de la Ley Orgánica 7/2021.

³⁸ Artículo 62 de la Ley Orgánica 7/2021.

³⁹ Artículo 63 de la Ley Orgánica 7/2021.

poder entender, que en la actualidad el dato esta interconectado con la cotidianidad y ha pasado a convertirse en la base de la economía, aspecto que desarrollaremos a continuación.

Muestra de tal afirmación, fue prevista en el informe de 2018, contentivo de la Evaluación de la Directiva 96/9/CE sobre la protección jurídica de las bases de datos, en el cual, publicaron la implicación de diversos sectores en la creación de datos:

Prácticamente todos los sectores económicos están profundamente implicados en la creación de datos, con tasas de crecimiento variable. El valor del mercado de datos para la UE-27 se estimó en 238 000 millones EUR en 2016, lo que representa más del 1,92 % del PIB de la UE- 27193. Según la Herramienta europea de seguimiento del mercado de datos, la tasa de crecimiento del valor de los datos entre 2015 y 2016 fue del 9,5 % en los 28 EM, siendo la minería y la fabricación (21,5 %) y el sector financiero (19,8 %) la cuota de mercado más alta. (p. 38)

Compartimos el criterio del ex director general de la OMPI, Francis Gurry (2019), de afirmar que los datos “son catalogados como el motor que impulsa la tecnología digital”, quien además explicó que, “las tecnologías digitales avanzadas, incluida la IA, son capaces de desarrollar nuevos productos y servicios beneficiosos mediante la manipulación de datos” (p. s/n)

Francis Gurry (2019), no prevé un nuevo derecho de propiedad susceptible de registro para los datos, pero sí resalta la necesidad de “**definir prácticas adecuadas y legítimas con respecto a la recopilación, el almacenamiento y el uso de los datos**”(p s/n) (**Resaltado Nuestro**), en la actualidad hay factores que se usan como eventuales restricciones del uso de los datos, como **la privacidad**, es uno de los factores con mayor atención, regulado en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Sin embargo, él considera que hay una falta de claridad en su regulación, que se presta para que algunas empresas lo utilicen como herramienta competitiva; otro factor es **la seguridad**, la cual debe definirse en cuanto su aplicación en la economía digital, porque los datos son un factor

fundamental para la producción y distribución en este tipo de economía. **La fiscalidad en la economía digital**, el derecho de imposición en el mundo físico se basa en la nacionalidad y residencia, pero no en la economía digital, la plataforma puede estar en un país y el consumidor en otro, pero de los factores que expone, el que consideramos más revelador es el de **la Propiedad Intelectual**

En el sistema clásico de PI, cualquier dato no público respecto al cual un agente económico haya adoptado medidas razonables para mantenerlo confidencial y que se considera tiene valor económico puede constituir un secreto comercial. **En la economía digital, los secretos comerciales se han convertido en el principal medio para proteger datos de importancia económica que no estén publicados, pero ¿los protegen adecuadamente? Los secretos comerciales no son un derecho de propiedad en el sentido clásico, sino que son derechos que surgen de una relación, en el sentido de que las personas no tienen derecho a entrometerse en el secreto comercial de otros ni utilizarlo de manera abusiva.** Por ejemplo, si una empresa cede datos a una subcontratista para un determinado fin, el subcontratista no puede utilizarlos para ningún otro fin. (Gurry, F. 2019 par 17.) **(Resaltado Nuestro)**.

Diane Coyle (2021), ponente del *Diálogo de la OMPI Sobre Propiedad Intelectual (PI) y Tecnologías de Vanguardia en su Cuarta Sesión*, considera que los datos son intangibles, y es clave evaluarlos desde el punto de vista económico, porque los datos no se desgastan, lo que implica su empleo en múltiples ocasiones. Consideración similar se encuentra en el informe de 2018 sobre las bases de datos, en el cual se afirma lo siguiente:

Los datos en sí mismos tienen un valor competitivo solo cuando se procesan, analizan y convierten en conocimiento comunicado. La naturaleza no rival de los datos digitales significa que los datos pueden ser utilizados varias veces y por múltiples usuarios sin que disminuya su valor. El óptimo social con respecto a los conjuntos de datos digitales se alcanza cuando se maximiza el análisis de datos, en la medida en que esta

apertura no conduzca a un suministro insuficiente de datos y, por lo tanto, a una falla del mercado. Con las tecnologías en línea, estas características se intensifican. (p. 39)

(Resaltado nuestro)

Por su parte, Jiro Kokuryo (2021), también ponente del *Diálogo de la OMPI Sobre Propiedad Intelectual (PI) y Tecnologías de Vanguardia en su Cuarta Sesión*, indicó, en cuanto al uso y restricciones de los datos, el punto que se plantea es si los datos pertenecen a los individuos o la sociedad y cómo podemos beneficiarnos de los metadatos y el Big Data al mismo tiempo que se protege la dignidad de los individuos. A su vez indicó que, en Asia se enfatiza más la benevolencia hacia con los otros, por encima de los derechos individuales y tal vez esta concepción podría resultar más válida para el tipo de economía en ecosistemas de los datos.

Dicho ponente ha categorizado la regulación del dato en tres opciones **i) privacidad y derechos individuales**, que según su criterio no es una opción realmente eficaz; **ii) enfoque antimonopolio**, su centro se encuentra en la competencia, beneficia a los grandes actores y no a los medianos actores y, **iii) los deberes de lealtad**, con quien primero facilitó los datos iniciales, esta es la vía que el propone para la gobernanza de los datos.

Creemos que continuará la revolución del sistema económico debido al dato lo que conllevará a un cambio de las instituciones de Derecho existente a nivel mundial. El debate indubitablemente es incipiente, aún falta mucho para poder terminar de comprender el verdadero alcance del dato y sus implicaciones a nivel económico, pero será este el motivo por el cual, el sistema de Propiedad Intelectual debe considerarse como una herramienta idónea para acompañar la transición del cambio, además de hacer un balance entre los distintos derechos que convergen ante el uso de datos y de este modo, continuar impulsando las inversiones económicas.

Situación Jurídica en Venezuela en Relación a las Bases de Datos y el Dato

I. Protección de las Bases de Datos Originales

Dentro de nuestro ordenamiento jurídico, se promovió en el año 1993, la Ley Sobre Derecho de Autor⁴⁰, dentro de la cual, se hace mención expresa de la protección a las bases de datos a través del Derecho de Autor en su artículo 3, que indica lo siguiente:

Son obras del ingenio distintas de la obra original, las traducciones, adaptaciones, transformaciones o arreglos de otras obras, así como también las antologías o compilaciones de obras diversas **y las bases de datos, que por la selección o disposición de las materias constituyen creaciones personales (Resaltado Nuestro)**

Con una línea uniforme al derecho internacional desarrollado en el ADPIC su artículo 10 Apartado 3, se brinda una protección a las bases de datos que cuentan con el elemento de originalidad por la selección o disposición de su contenido. Ahora bien, este artículo responde a la realidad social de la época analógica y que en la actualidad su aplicación puede surtir efectos, pero que de igual manera dejan un vacío jurídico para regular las bases de datos no originales, porque carecemos dentro de nuestro ordenamiento una regulación al respecto.

II. Protección de los Datos de Prueba u Otros No Divulgados

Venezuela, es un país miembro de la Organización Mundial de Comercio, que suscribió el ADPIC, por lo que tiene la obligación de otorgar el estándar mínimo contemplado en el artículo 39.3, referente a la información no divulgada sobre los datos de pruebas u otros no divulgados, a los ciudadanos de esos países miembros. Sin embargo, esta protección debe ser aprobada por

⁴⁰ Promulgada el 14 de agosto de 1993, Gaceta Oficial N Oficial N° 4.638 Extraordinaria, del 1 de octubre de 1993.

una ley dentro de nuestro ordenamiento jurídico, para ser incorporada y aplicada de manera directa a los connacionales.

No obstante, es necesario hacer mención del desarrollo jurisprudencial que se dio sobre la protección de estos datos de pruebas u otros no divulgados en la Sentencia N° 151, de la Sala Político Administrativo, el 13 de febrero de 2008, la cual indicó:

Lo anterior se justifica si tomamos en cuenta que siendo la salud un derecho humano que debe ser garantizado por el Estado, regulaciones como las descritas en las líneas que anteceden y las cuales se dirigen a establecer limitaciones para el expendio de medicamentos, deben orientarse a la satisfacción de los intereses colectivos, lo cual como se explicará más adelante, **puede incluso ameritar el sacrificio de intereses económicos concretos en aras de hacer prevalecer una necesidad colectiva primordial**, esto es, la dotación a la población de medicamentos genéricos a unos precios más accesibles.

.... omissis

Por lo tanto, tratándose de una norma programática que otorgaba a cada Estado miembro un cierto margen de discrecionalidad para fijar plazos de protección en la materia y cuya única limitante consistía en entender que “normalmente” la expresión “plazo razonable” aludía a un período no menor de cinco años y visto igualmente, que la República Bolivariana de Venezuela, nunca procedió a regular dicha materia, debe concluirse que **en nuestro país no existía un plazo preestablecido que debiese respetarse para la aprobación de sustancias cuyo principio activo es el mismo de aquellas consideradas novedosas**

....

Por lo tanto, estima la Sala que aun **cuando deba admitirse la existencia de un régimen de protección de la información que suministran tales laboratorios** y el cual es concebido en aras a estimular y proteger las inversiones que éstos realizan para

descubrir nuevas sustancias farmacológicas, ello no obsta para que el Estado cuando la tutela del interés colectivo así lo aconseje y siempre que se emplee la debida proporcionalidad, adopte medidas limitadoras de dicha protección.

No obstante, se reitera una vez más, que deberán analizarse en cada caso concreto si tales medidas atienden o no a la señalada proporcionalidad, así como la posible afectación de intereses particulares. (p s/n) **(Resaltado Nuestro)**

Como se desprende de las consideraciones para decidir de la sentencia citada, se reconoció un régimen de protección a la información, entendida como datos en el área farmacéutica, que debe ser protegida por la información no divulgada, a pesar de ser informada como requisito indispensable durante el procedimiento de solicitud de un medicamento con un producto nuevo e innovador.

Además, se indica que los derechos económicos que derivan de esta protección se ven ponderados y restringidos en cada caso concreto, en beneficio de un bien mayor, como lo es el acceso a la salud pública y a medicamentos genéricos que son de menor costo, lo cual se justifica por la proporcionalidad en relación al daño vs beneficio, por ello, se trae a colación la definición de proporcionalidad que se utiliza en dicha sentencia al citar a Pietro, L. 2002:

en sentido estricto que "...supone ponderar entre daños y beneficios, es decir acreditar que existe un cierto equilibrio entre los beneficios que se obtienen con la medida limitadora en orden a la protección de un bien constitucional o a la consecución de un fin legítimo y los daños o lesiones que de la misma se derivan para el ejercicio del derecho..." (p s/n).

Posteriormente y en desarrollo de la sentencia N° 151 antes cita, la Corte Segunda de lo Contencioso Administrativo, Sentencia N° 1543 a los doce (12) días del mes de agosto del año dos mil ocho (2008) sobre el caso lipitor, en el cual se señala el alcance de la interpretación del artículo 39,3 del ADPIC:

En efecto, y en consonancia con lo anterior, debe tenerse en cuenta, tal como lo señala la citada decisión del Tribunal de Justicia de la Comunidad Andina, que en la Declaración Ministerial de la OMC de Doha sobre los ADPIC y la Salud Pública, de la cual Venezuela formó parte, adoptada el 14 de noviembre de 2001, se decidió en su punto 4, lo siguiente:

“4. Convenimos en que el Acuerdo sobre **los ADPIC no impide ni deberá impedir que los Miembros adopten medidas para proteger la salud pública**. En consecuencia, al tiempo **que reiteramos nuestro compromiso con el Acuerdo sobre los ADPIC, afirmamos que dicho Acuerdo puede y deberá ser interpretado y aplicado de una manera que apoye el derecho de los Miembros de la OMC de proteger la salud pública y, en particular, de promover el acceso a los medicamentos para todos (...).**”

Omissis...

En consecuencia, y con fundamento en lo antes expuesto, considera la Corte que, como ocurrió en el presente caso, la realización de procedimientos sumarios para la aprobación de **la solicitud del registro sanitario de un producto conocido, con apoyo de los datos de prueba originalmente presentados por otro con ocasión del registro de un producto nuevo, en modo alguno constituye un supuesto de uso comercial desleal, sino una situación normalmente generada en los campos donde la actividad económica es de alguna manera regulada por el Estado, sin que pueda calificarse como ilegal su actuación, ni afirmarse que desconoce, divulga o incurre en infracción de la protección del secreto de la información, con el otorgamiento de la autorización para la comercialización de los productos farmacéuticos conocidos**, pues se hace en aras de tutelar un derecho superior fundamental, como lo es el derecho a la salud y, por ende, garantizar a todos sus ciudadanos la disponibilidad de medicamentos eficaces, seguros, de calidad, y de precios accesibles. Así se decide. (p s/n) **(Resaltado nuestro)**.

III. Protección del Dato

En Venezuela no existe una ley específica para la regulación del uso, manejo o almacenamiento de datos, a pesar de ello, hay normas de rango constitucional que se relacionan a los datos personales y distintas leyes que hacen mención a los datos, por lo que iniciaremos por los derechos de rango constitucional que se relacionan con el dato personal y luego las leyes que se relacionan con la materia de datos.

Derechos relacionados a los Datos Personales dentro del Ordenamiento Jurídico

En la Constitución de la República Bolivariana de Venezuela (CRBV)⁴¹, hay diversos derechos y acciones como la de habeas data, que podrían servir como base legal para delimitar el uso de datos personales, que iremos desarrollando en orden preferente para la presente línea de este trabajo, posteriormente se hará mención a diversas leyes que tienen relación a los derechos personales mencionados o a los datos.

Es menester mencionar que el Estado dentro de sus fines esenciales, contempla el respeto a la dignidad en el artículo 3 de la C RBV⁴², debido a ello, el Estado tiene el deber de promover la garantía del cumplimiento de los principios, derechos y deberes reconocidos y consagrados en esta Constitución en especial los que a continuación indicaremos, en vista de su importancia en el manejo de datos personales.

Derecho al Honor, a la Privacidad, a la Informática y a la Intimidad

Con rango constitucional se encuentra el derecho al honor, a la privacidad, a la informática y a la intimidad plasmados en el art. 60 C RBV que predica lo siguiente:

⁴¹ Gaceta Oficial N° 5.908, Extraordinaria del 19/2/1999

⁴² Artículo 3 C RBV. El Estado tiene como fines esenciales la defensa y el desarrollo de la persona y el respeto a su dignidad, el ejercicio democrático de la voluntad popular, la construcción de una sociedad justa y amante de la paz, la promoción de la prosperidad y bienestar del pueblo y la garantía del cumplimiento de los principios, derechos y deberes reconocidos y consagrados en esta Constitución

Toda persona tiene derecho a **la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.**

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

El autor Brewer-Carias, Allan (1994), explica que en el ámbito internacional, el derecho a la vida privada, fue proclamando por la Organización de Naciones Unidas (ONU) la Organización de Estados Americanos (OEA) en 1948, mediante la Declaración Universal de Derechos Humanos⁴³, en el mismo año, también se desarrolló en la Declaración Americana de los Derechos y Deberes del Hombre⁴⁴, luego en el Pacto Internacional de Derechos Civiles y Políticos, aprobado por la Asamblea General de la ONU el 16 de diciembre de 1966, y por Ley en Venezuela⁴⁵, mediante el cual se establece:

Artículo 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

De igual manera, este derecho también fue desarrollado en el Pacto de San José o la Convención Americana sobre Derechos Humanos⁴⁶, y aprobada por Ley en nuestro país⁴⁷, que instauro lo siguiente:⁴⁸

⁴³ En su artículo 12 establece: - "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques en su honra o a su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques".

⁴⁴ En su artículo V establece. - "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar"

⁴⁵ A través de la Gaceta Oficial N° 2146 Extraordinario de 28 de enero de 1978.

⁴⁶ Adoptada por la Conferencia Especializada Interamericana sobre Derechos Humanos el 22 de noviembre de 1969.

⁴⁷ Mediante Gaceta Oficial N° 31.256 de 14 de junio de 1977.

⁴⁸ Es importante resaltar, que de conformidad con el artículo 23 de la CRBV, los tratados sobre derechos humanos suscritos y ratificados por Venezuela tienen jerarquía constitucional y tendrán preferencia sobre la misma, en tanto y en cuanto, sus normas sobre su goce o ejercicio sean más favorable a las de la Constitución.

Artículo 11.-

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques.

El mencionado autor Brewer-Carias, Allan (1994), indica que “la intimidad de la vida privada ha adquirido cada vez más importancia debido a los avances de la tecnología y de la informática, que han venido permitiendo una mayor posibilidad **de penetración en la vida privada**, sin consentimiento de las personas” (p. 54) (**Resaltado Nuestro**), esta situación incluso ha abierto el debate entre ponderar el derecho a la información y el derecho a la privacidad, que según a nuestro criterio amerita ser objeto de análisis en cada caso en concreto, porque pueden haber individuos más vulnerables que otros o el derecho a la privacidad deberá interpretarse de manera más estricta o laxa según el caso, por ejemplo, no se debe ponderar el derecho a la privacidad de un niño, de la misma manera que la privacidad de un artista.

El derecho a la intimidad de la vida privada, tiene dos connotaciones, explica el referido autor una negativa para impedir penetraciones o injerencias arbitrarias o abusivas en la vida privada y una connotación positiva, que implica el derecho de controlar los datos referidos a la propia persona y todo esto no es más que una extensión del derecho al libre desenvolvimiento de la personalidad que tiene cada persona, al respecto Brewer-Carias, Allan (1994) indica:

al considerarse el derecho a la intimidad como una condición, necesaria para el libre desenvolvimiento de la personalidad, y en sí mismo, uno de los derechos de la personalidad, toda limitación al mismo, como a la libertad en general, no sólo debe ser expresa sino además razonable, lógica y adecuada en relación al fin constitucional perseguido, **respetando la proporcionalidad y concordancia práctica, asegurando la**

confidencialidad respecto de quienes acceden a la información obtenida, y no invadiendo el contenido esencial del derecho (p. 12) (*Resaltado Nuestro*).

El derecho al libre desenvolvimiento de la personalidad, tiene rango constitucional y se encuentra contemplado en el artículo 20 que predica lo siguiente: “*Toda persona tiene derecho al libre desenvolvimiento de su personalidad, sin más limitaciones que las que derivan del derecho de las demás y del orden público y social.*” Este derecho respalda o permite desarrollar la premisa antes expuesta, en cuanto a la ponderación de los derechos de cada individuo que giran en torno a la información y la privacidad, sobre todo ante niños que son sujetos más vulnerables y que se encuentran en pleno desarrollo de su personalidad, por lo que justifica que el derecho a su privacidad, tenga un mayor alcance. En el mismo orden, la Ley Orgánica de Protección de Niños Niñas y Adolescentes (LOPNNA) en su artículo 65 desarrolla precisamente el alcance de este derecho e incluso limita el uso de la información sobre niños o adolescentes que hayan sido sujetos de hechos punibles.

Artículo 65 LOPNNA. Derecho al honor, reputación, propia imagen, vida privada e intimidad familiar

Todos los niños, niñas y adolescentes tienen derecho al honor, reputación y propia imagen. Asimismo, tienen derecho a la vida privada e intimidad de la vida familiar. Estos derechos no pueden ser objeto de injerencias arbitrarias o ilegales.

Parágrafo Primero. **Se prohíbe exponer o divulgar**, a través de cualquier medio, la imagen de los niños, niñas y adolescentes contra su voluntad o la de su padre, madre, representantes o responsables. Asimismo, se prohíbe exponer o divulgar datos, imágenes o informaciones, a través de cualquier medio, que lesionen el honor o la reputación de los niños, niñas y adolescentes o que constituyan injerencias arbitrarias o ilegales en su vida privada o intimidad familiar.

Parágrafo Segundo. Está prohibido exponer o divulgar, por cualquier medio, datos, informaciones o imágenes que permitan identificar, directa o indirectamente, a los niños,

niñas y adolescentes que hayan sido sujetos activos o pasivos de hechos punibles, salvo autorización judicial fundada en razones de seguridad u orden público. **(Resaltado Nuestro)**

Un ejemplo del uso de este artículo, se da en la prohibición de colocar los datos como nombre o la cédula de los niños o adolescentes en sentencias emanadas de cualquier órgano judicial y que son publicadas en la página oficial del Tribunal Supremo de Justicia (TSJ), a fin de no divulgar datos que puedan lesionar su privacidad o exponerlos.

A criterio del autor de la presente investigación, el artículo 60 de la CRBV, es crucial y vital para crear una regulación entorno al uso de datos personales, porque en su segundo párrafo, contiene un precepto expreso al indicar que **La ley limitará el uso de la informática para garantizar el honor y la intimidad**, precepto que también tiene la Constitución Española en el citado artículo 18.4 que se utilizó como fundamento legal para desarrollar la protección del dato personal y en concordancia con el derecho comunitario, hacer la debida transposición de El Reglamento al ordenamiento jurídico español, además desarrollar la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Derecho y acción del Habeas Data

El Derecho a la acción de Habeas Data que se estipula en el artículo 28 de la CRBV, no había sido contemplado de manera previa en ninguna de las anteriores constituciones del país, así lo establece el preámbulo de la misma y el mencionado artículo predica lo siguiente:

Toda persona tiene el derecho de **acceder a la información** y a **los datos que sobre sí misma o sobre sus bienes** consten en registros oficiales o privados, con las excepciones que establezca la ley, así **como de conocer el uso que se haga de los mismos y su finalidad**, y de solicitar ante el tribunal **competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen**

ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley. **(Resaltado Nuestro)**

Este artículo contempla varios derechos, en relación a ello, la Sala Constitucional del TSJ Sentencia N° 1050, del 23 de agosto de 2000, del Magistrado Ponente Jesús Eduardo Cabrera, en la cual se desarrolla los siguientes aspectos de la acción de habeas data e indica los derechos que contiene el precitado artículo:

- 1) El derecho de conocer sobre la existencia de tales registros.
- 2) El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas.
- 3) El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él.
- 4) El derecho de conocer el uso y finalidad que hace de la información quien la registra.
- 5) El derecho de actualización, a fin que se corrija lo que resulta inexacto o se transformó por el transcurso del tiempo.
- 6) El derecho a la rectificación del dato falso o incompleto.
- 7) El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas.

Se trata de derechos que giran alrededor de los datos recopilados sobre las personas o sobre sus bienes, por **lo que se requiere un interés, personal, legítimo y directo en quien ejerza estos derechos**, ya que es la información sobre su persona y bienes el que lo origina

Omissis

Lo personal de la información, restringe para aquellos que no piden sus datos o informaciones, el derecho que otorga el aludido artículo 28, ya que de no ser así, se estaría ante una vía para interferir en la intimidad o en la vida privada de las personas, en la obtención de secretos industriales o comerciales, en asuntos atinentes a la defensa y seguridad nacional, etc., los cuales son valores constitucionales igualmente protegidos y por ello la remisión que hace la norma a documentos de cualquier naturaleza que contengan información de interés para comunidades o grupos de personas, no puede ser entendida sino como aquellas informaciones que corresponden al peticionario, como parte de una comunidad o un grupo de personas. (p s/n) **(Resaltado Nuestro)**

También la Sala Constitucional del TSJ ha indicado que la acción de Habeas Data, funciona con sistemas informáticos, por compilación de datos, que, a criterio del autor, podría ser aplicado por analogía al concepto de Big Data o a bases de datos con macrodatos, por ello se cita a continuación lo determinado por la Sala Constitucional en la Sentencia N° 1281, del veintiséis (26) de junio de 2006, Expediente 05-1964; Magistrada ponente Carmen Zuleta:

funciona con sistemas -no solo informáticos- de cualquier clase de ordenación de información y datos sobre las personas o sus bienes, con fines de utilizarlos en beneficio propio o de otros, y que real o potencialmente pueden serlo en forma perjudicial contra aquellos a que se refiere la recopilación, se trata, por lo tanto, **de bancos de datos**, no referidos a alguien en particular, con independencia de que estén destinados a producir informaciones al público. Los registros objeto del *habeas data*, como todo registro, son **compilaciones generales de datos sobre las personas o sus bienes ordenados de forma tal que se puede hacer un perfil de ellas, de sus actividades, o de sus bienes; los registros oficiales y los privados**, objeto de la norma, tienen un sentido general, ellos están destinados a inscribir documentos, operaciones, actividades -entre otros- de las personas en determinados campos o temas, por lo que se trata de codificaciones de

series de asuntos que forman patrones, matrices y asientos temáticos. (Vid. Fallo N.º 332, del 14 de marzo de 2001. Caso: *INSACA*). (p s/n). **(Resaltado Nuestro)**

En la sentencia citada, se parte de la premisa que la acción se puede ejercer en vista a que el uso de datos podría “real o potencialmente” perjudicar a la persona sobre cual versan los datos, sin embargo, Según Belandria, José (2017) el derecho de habeas data:

no está sujeto a una eventual lesión a los referidos derechos, y más bien se articula sobre la noción de autodeterminación informativa.

Para la doctrina venezolana la autodeterminación informativa constituye un auténtico derecho que tiene fundamento en el citado artículo 28 de la Constitución, y **supone no sólo el tomar conocimiento de la existencia de información o datos inherentes a la persona en archivos automatizados o manuales, públicos o privados, sino también el derecho de acceder a ella, y consecuentemente la posibilidad de hacer oposición, modificación o supresión de esa información.** (p 7) **(Resaltado Nuestro)**

El ejercicio de esta acción, es un derecho personalísimo y tan sólo tienen legitimación de intentar la acción la persona a quien pertenezcan los datos, no en el sentido de propiedad, sino en el sentido que los datos versan sobre la persona, como se señala en la sentencia N° 1050 de la Sala Constitucional previamente citada, pero también tiene facultad para interponer una acción por Habeas Data el Defensor del pueblo en ejercicio de sus atribuciones de conformidad con el artículo 281.3 CRBV, y al deber que tiene de velar por el efectivo respeto y garantía de los derechos humanos reconocidos artículo. 281.2 CRBV, como es el caso del derecho al honor y privacidad.

Derecho a la información oportuna

Es un derecho sin precedente en las anteriores constituciones de Venezuela, y se encuentra contemplado en el artículo 58 de la CRBV, el cual establece lo siguiente:

Artículo 58. La comunicación es libre y plural y comporta los deberes y responsabilidades que indique la ley. Toda persona tiene derecho a la información oportuna, veraz, imparcial, sin censura, de acuerdo con los principios de esta Constitución, así como a la **réplica y rectificación cuando se vea afectada directamente por informaciones inexactas o agraviantes.** Los niños, niñas y adolescentes tienen derecho a recibir información adecuada para su desarrollo integral” **(Resaltado Nuestro)**

Para clarificar, el contenido del precedente artículo 58, traemos a colación lo desarrollado por el abogado Ortiz Ortiz, Rafael, (2000) sobre los términos réplica y la rectificación de la información:

La réplica y la rectificación aluden a la "información" y no meramente a las "opiniones" por cuanto son fenómenos diversos. Se pretende con ello que la persona *cuente con un mecanismo de defensa* frente a las agresiones que puede sufrir con respecto de las informaciones que sobre sí misma se comuniquen, en cualquier medio de comunicación y no sólo en los medios de comunicación social;

Desde luego que se trata de una consecuencia del derecho fundamental de la información por desprenderse directamente de ello, para garantizarle a la persona el acceso al mismo medio de comunicación donde su difundió el hecho informativo;

2) El derecho a rectificación, en los términos constitucionales, procede frente a la información inexacta, errónea, incompleta, pues lo que se pretende tutelar es la posibilidad que tiene toda persona de corregir los datos informativos que le incumban directamente;

Omissis

De esto puede concluirse que, si bien la rectificación opera frente a informaciones inexactas o erróneas, el derecho a réplica procede cuando la información ha sido transmitida acompañada de ideas, opiniones y criterios del informador, o la conexión con otras informaciones que pudieran manipular la información en un sentido contrario a la realidad (pp. 45-46) **(Resaltado Nuestro)**.

Resulta importante traer a colación el artículo 143 de la CRBV referente al Derecho a la información administrativa y acceso a los documentos oficiales que indica lo siguiente:

Artículo 143. Los ciudadanos y ciudadanas tienen ***derecho a ser informados e informadas*** oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados e interesadas, y a conocer las resoluciones definitivas que se adopten sobre el particular. Asimismo, ***tienen acceso a los archivos y registros administrativos***, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto. No se permitirá censura alguna a los funcionarios públicos o funcionarias públicas que informen sobre asuntos bajo su responsabilidad **(Resaltado Nuestro)**.

Pues bien, la importancia de dicho artículo radica en que, debe interpretarse en concordancia con los artículo 58 y el 28 antes mencionados, a fin de esbozar el alcance del derecho al acceso a la información desarrollados por estos dos artículos y el derecho a rectificación de la información, indistintamente si la misma es manejada por un ente privado, incluso por una interpretación extensiva del artículo 28, cualquier persona natural o jurídica que maneje una base de datos con información o datos personales o por un ente público de conformidad el precepto del artículo 143 CRBV, que a criterio de Belandria, José (2017) “El ejercicio del derecho de acceso a la información pública se debe compaginar con el principio de transparencia administrativa, en virtud de la conexión evidente que existe entre ambos”. (p 11)

Leyes relacionadas al Uso de Datos

A continuación, procederemos de manera meramente enunciativa a mencionar artículos de diversas leyes que se relacionan con el uso de los datos, tratando en la medida de lo posible llevar una secuencia lógica, a pesar de que dichos artículos se encuentran en diversas leyes, no necesariamente relacionadas en cuanto su ámbito de aplicación.

- ***Ley de Infogobierno:***⁴⁹

Aplicable a los entes de la administración pública⁵⁰, así como a las personas jurídicas creadas con fondos de la administración y tiene como objeto⁵¹ 1) establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, y 2) promover el desarrollo de las tecnologías de información libres en el Estado.

Por su parte, hay dos artículos relevantes para la presente investigación, en esta ley los cuales son el artículo 74 que en desarrollo del artículo 60 de la CRBV y protección del derecho al honor y la privacidad, reconoce la confidencialidad de la información personal y las referentes a la seguridad y defensa de la nación

Naturaleza de la información

Artículo 74. La información que conste en los archivos y registros en el Poder Público y en el Poder Popular es de carácter público, salvo que se trate de información sobre el honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas, la seguridad y defensa de la Nación, de conformidad con lo establecido en la Constitución de la República, la ley que regule la materia sobre protección de datos personales y demás leyes que rigen la materia.

⁴⁹ Gaceta Oficial de la República núm. 40.274, de fecha 17 de octubre de 2013.

⁵⁰ Artículo 2 de la mencionada ley

⁵¹ Artículo 1 de la ley

El Segundo artículo es el 75, el cual reconoce el derecho a notificar a las personas sobre la recolección de datos, regula algunos aspectos del tratamiento, transferencia de datos (sin aparente consentimiento de la persona de la cual se desprenden los datos, derecho a la supresión o rectificación, derecho a la oponibilidad al uso.

Suministro de información

Artículo 75. El Poder Público y el Poder Popular, a través de las tecnologías de información, están obligados a notificar a las personas:

1. Que la información será recolectada de forma automatizada;
2. Su propósito, uso y con quién será compartida;
3. Las opciones que tienen para ejercer su derecho de acceso, ratificación, supresión y oposición al uso de la referida información y;
4. Las medidas de seguridad empleadas para proteger dicha información, el registro y archivo, en las bases de datos de los organismos respectivos.

Con respecto a este artículo concretamente en su numeral 2, Belandria, José (2017) opina:

El artículo 75 de la LI, concretamente en su numeral 2, y de la relación de este precepto con la Ley de Interoperabilidad, es necesario señalar que dicha normativa prevé la posibilidad efectiva de intercambiar información y datos de carácter personal. Ello con el propósito de potenciar la interoperabilidad como uno de los objetivos del Estado venezolano para prestar mejores servicios a los ciudadanos. Sin embargo, la norma parte del hecho de que es posible compartir la información personal y nada dice con relación a una eventual autorización o consentimiento del titular para compartir la misma. (p 15)

Nótese que muchos de estos derechos son desarrollados por el Reglamento de la UE y la Ley española que hace su transposición, sin embargo, no se desarrolla el aspecto del consentimiento informado para aceptar el tratamiento de datos y transferencia de datos, tal vez, esto se deba a una restricción del consentimiento por tratarse de bases de datos creadas por la

administración pública, pero esto debiese ser justificado, desarrollado e informado de tal forma, considerando que pudiese ser sujeto al principio de legalidad y justificable por ejemplo en caso de seguridad Nacional, sin embargo este análisis va más allá de los objetivos de la presente investigación.

A fines de ejemplificar, vale resaltar que el consentimiento y el derecho a la información en materia de protección de datos personales relativos a condenas e infracciones penales dentro España, se ve restringido al principio de una investigación, donde se recolectan datos sin notificar al interesado de manera previa, pero posteriormente tienen acceso a la información, igual se garantizan los derechos en cuanto al tratamiento de datos personales.

En el caso que nos concierne, creemos necesario la transferencia de datos dentro de los organismos de la administración pública, esto permitiría crear un sistema integrado, siempre que se regule expresamente, acorde al principio de legalidad, a los derechos y principios que convergen en la materia.

- **Ley Especial Contra los Delitos Informáticos**⁵²

El objeto de esta ley se encuentra en su artículo 1, el cual indica que es *“la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías”*

Además, en su artículo 2 trae una serie de definiciones, que son importante mencionar:

a) Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el

⁵² Gaceta Oficial N.º 37.313 del 30 de octubre de 2001

desarrollo y uso del “hardware”, “firmware”, “software”, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

b) Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c) Data (datos): hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado.

d) Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

n) Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

La presente ley, contiene una serie de delitos tipificados dentro el título II, como lo son: Acceso indebido, el sabotaje o daño a sistemas, favorecimiento culposo del sabotaje o daño, Acceso indebido o Sabotaje a sistemas protegidos, posesión de equipos o prestación de servicios de sabotaje, espionaje informático, falsificación de documentos. Luego en su Capítulo II. Desarrolla los Delitos Contra la Propiedad, y contempla el Hurto⁵³ tanto de bienes tangibles como

⁵³ Artículo 13. Hurto. Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse

intangibles, por lo que consideramos que este delito puede aplicarse a quienes hurten una base de datos, también desarrolla el delito de fraude, obtención indebida de bienes o servicios, Manejo fraudulento de tarjetas inteligentes o instrumentos análogo. Por su parte en el Capítulo III. **Desarrolla los delitos contra la privacidad de las personas** y de las comunicaciones, nuevamente con fines ejemplificativos citamos el artículo 20, 21 y 22, que indican lo siguiente:

Artículo 20. **Violación de la privacidad de la data o información de carácter personal.** Toda persona que intencionalmente ***se apodere, utilice, modifique o elimine*** por cualquier medio, sin el consentimiento de su dueño, ***la data o información personales de otro*** o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21. **Violación de la privacidad de las comunicaciones.** Toda persona que mediante **el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena,** será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22. **Revelación indebida de data o información de carácter personal.** Quien **revele, difunda o ceda, en todo o en parte, los hechos descubiertos,** las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión

un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad. **(Resaltado Nuestro)**.

Por su parte en el Capítulo V. De los Delitos Contra el Orden Económico hace alusión a un delito contra la Propiedad Intelectual, el cual podría aplicarse por ejemplo para proteger bases de datos originales cuando se encuentre en internet o de invenciones que hagan uso de datos.

Artículo 25. Apropiación de Propiedad Intelectual. Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias. **(Resaltado Nuestro)**.

Esta ley tiene definiciones que pueden servir para referirse a ciertos aspectos básicos, sin embargo, la realidad tecnológica para el año 2001, cuando fue promulgada no se asemeja a la era digital en la que nos encontramos, por ese motivo debe ser actualizada dicha ley. Ahora con respecto a los delitos tipificados, también deberían ser objeto de revisión porque son muy amplios, algunos pudiesen no contener la terminología adecuada, por último, la tendencia europea es la de estipular sanciones e infracciones, mientras que esta ley aplica penas y sanciones que por la inflación se han vuelto irrisorias, sin embargo, un análisis más detallado de la misma, amerita una completa investigación y sobrepasa el objeto de esta.

- **Decreto Con Rango y Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas**⁵⁴

Reconoce ya el avance de las tecnologías y de la importancia del comercio electrónico, por lo que en su preámbulo prevé la necesidad inminente de crear un marco jurídico mínimo “la regulación de las modalidades básicas de intercambio de información por medios electrónicos, a

⁵⁴ Gaceta Oficial N° 37.076m 13 de diciembre de 2000.

partir de las cuales han de desarrollarse las nuevas modalidades de transmisión y recepción de información, conocidas y por conocerse” (p. 1.)

Dentro del mismo orden de ideas, el referido Decreto Ley en su artículo 1, indica que su objeto de aplicación es “otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas”. Esta regulación recae sobre los correos electrónicos, que son hechos, registros, abarcados dentro de la definición de datos, que previamente mencionamos.

Se evidencia por las leyes mencionadas, que en Venezuela a mediados del 2000 al 2005 se trató de actualizar la legislación en consideración a las nuevas tecnologías, Incluso y en relación con la presente ley, el Código Penal de Venezuela con reforma parcial del año 2005, estableció como tipo penal el delito por difundir información falsa “datos” a través de correos electrónicos, en su artículo 296-A que predica:

Todo individuo que por medio de informaciones falsas difundidas por cualquier medio impreso, radial, televisivo, telefónico, *correos electrónicos o escritos* panfletarios, cause pánico en la colectividad o la mantenga en zozobra, será castigado con prisión de dos a cinco años.

Si los hechos descritos en el aparte anterior fueren cometidos por un funcionario público, valiéndose del anonimato o usando para tal fin el nombre ajeno, la pena se incrementará en una tercera parte. Este Artículo será aplicado sin perjuicio a lo establecido en la legislación especial sobre los delitos informáticos, telecomunicaciones, impresos y transmisión de mensajes de datos.

CAPÍTULO III

MARCO METODOLÓGICO

Descripción del Marco Metodológico

La presente investigación se realizó bajo un diseño de investigación documental y cualitativa, según el abordaje de su objeto, se determinó que es exploratoria, en vista de la novedad del tema, cuyo debate es incipiente y se encuentra en plena discusión a nivel internacional, como así lo ha indicado el ex director general de la OMPI Francis Gurry (2019) Por ello, la investigación se basó en recopilar información de normativas legales de otros países, investigación de artículos de revistas, artículos de opinión, trabajos referentes al tema de investigación, sentencias, jurisprudencia, artículos de revistas y publicaciones relacionadas al tema.

Con miras a esbozar el marco legal utilizado hasta los momentos para la protección de las bases de datos desde la óptica de su importancia económica, protegido como un derecho *sui generis* en la Comunidad Europea se investigó sobre la Directiva 96/9/CE y la Ley 5/1998 transposición dentro del ordenamiento jurídico de España de la mencionada Directiva. En igual sentido, se investigó sobre el marco de regulación con respecto al dato personal en la UE, con las leyes de transposición dentro del ordenamiento jurídico de España, con la finalidad de desarrollar el objetivo general y determinar si es posible la trasposición del marco legal de las normativas evaluadas y aplicable para la Protección del Dato, dentro del ordenamiento jurídico venezolano.

CAPÍTULO IV

RESULTADOS

En relación a los objetivos planteados en este trabajo y en concordancia al hilo investigativo, procederemos a exponer las consideraciones que se creen pertinentes a fin de poder determinar los objetivos específicos planteados al inicio de la investigación y por consiguiente el objetivo general de la misma.

- **Identificar la protección jurídica de las bases de datos dentro del ordenamiento jurídico venezolano, mediante el estudio de la protección legal otorgada a las bases de datos originales y no originales, con la finalidad de determinar si es necesario proponer consideraciones para su regulación.**

Para abordar la respuesta a este objetivo es necesario realizar la distinción entre bases de datos originales y bases de datos que carecen de originalidad, en la sintonía del desarrollo de la investigación.

Con respecto a las bases de datos originales

Sin duda alguna y como se afirmó anteriormente, dentro de nuestro ordenamiento jurídico existe una protección a las bases de datos originales, bajo el amparo del artículo 3 de la LSDA, por lo tanto, se protegen las mismas toda vez que, por la disposición de los materiales que la constituyen sea considerada una creación personal. En caso que se lesione este derecho de propiedad, el autor puede ejercer acciones judiciales para que se le restituya el derecho lesionado y se le indemnice por los daños y perjuicios causados.

Si la base de datos se encuentra en un medio electrónico, por ejemplo, en una página web, podría ejercerse la vía penal con fundamento a la Ley Especial Contra los Delitos Informáticos de conformidad con el artículo 25 anteriormente citado, cuando se hayan apropiado, obtenido

derecho económico sin autorización del autor, se afecte la integridad de la obra, se lesione el derecho a la paternidad por ejemplo se desconozca la paternidad con el propósito de aprovecharse económicamente.

Conclusión:

Por lo antes expuesto, podemos concluir que no hay discusión con respecto a la protección de las bases de datos Originales. Distinta situación nos enfrentamos en cuanto a la protección que pueda otorgarse a las bases de datos no originales, porque no hay dentro de nuestro ordenamiento jurídico una protección *sui generis* como en el derecho comunitario europeo.

Con respecto a las bases de datos no originales

Partimos de la premisa de que no hay una normativa que se asemeje al derecho *sui generis* otorgada a las bases de datos en UE, pero consideramos que sí se puede proteger las bases de datos a través de la autonomía de la voluntad de las partes, siempre que no se estipule algo contrario a la ley y no se vaya en detrimento de los derechos personales u otro derecho, será lícito que pacten una cláusula de confidencialidad.

Incluso, podría protegerse bajo la figura del secreto comercial como se hace en Estados Unidos de América. Uno de los aspectos que pudiesen avalar esta postura, es el hecho que, en la Ley Especial Contra los Delitos Informáticos, tipifica el delito de revelación indebida de data o información de carácter personal en su artículo 22, en concordancia con el artículo 20 de la mencionada ley, que tipifica la violación de la data. También es importante mencionar, que podría protegerse las bases de datos a través de otros sistemas de la Propiedad Intelectual, por ejemplo, si la data forma parte de una invención.

La protección a través de secreto comercial, o una cláusula de confidencialidad pueden ser eficientes para algunos casos, pero tal vez, no proporcionen la protección más adecuada en

los supuestos en los cuales las bases de datos forman parte de la prestación de un servicio. Ante estos supuestos la protección de un derecho *sui generis*, puede ser el más adecuado y valdría la pena tener en consideración legislar para crear una protección por esta vía; es imperante resaltar que, si se considera crear un derecho *sui generis* para la protección a las Bases de datos no originales, sería necesario tener en cuenta el informe de 2018 y las **siguientes**

Conclusiones:

- La Directiva 96/9/CE es una normativa contemplada para proteger la inversión en términos de recursos humanos, técnicos y económicos, cuyos parámetros era menester valorar para el momento en que se consideró y creó. Esto se ve reflejado a su vez, cuando determina que considera creador de las bases de datos a las personas físicas o jurídicas. Ahora bien, en la actualidad en la creación de bases de datos, interviene muchos más factores que el esfuerzo humano, porque las bases de datos se crean, procesan y analizan en su mayoría por la inteligencia artificial, pero aún no se considera autor a la IA y tampoco creador.
- Según el informe de 2018, muchos empresarios alegaron que era mayor la inversión realizada en el procesamiento de datos, que la propia inversión para la creación de las bases de datos. Son estas las razones que justifican crear una protección entorno a la inversión sustancial
- Es necesario prever la intervención de la inteligencia artificial para el procesamiento, generación y/o creación de datos y del hecho de que la IA se alimenta y optimiza su funcionamiento por el procesamiento de datos, lo que conlleva a la necesidad de fomentar la libre circulación de datos, bajo los parámetros de protección de datos personales o respetando los derechos de autor que intervengan, es decir que se mantenga sin perjuicio de los derechos existentes sobre su contenido.

- La protección a través de un esquema de derecho *sui generis*, puede fomentar el rendimiento empresarial y estatal, y sería esencial en la economía digital la disponibilidad del dato, para regular la comercialización y la extracción del dato.
- El manejo de los datos se encuentra totalmente automatizado, ellos son la base del comercio digital, por lo que surge la necesidad de actualizar dicha normativa y considerar si es necesario extender una protección al dato, en cuyo caso debería protegerse en consideración, si el mismo ha sido procesado, siendo esto uno de los aspectos por los cuales se le da valor. Consideramos que proteger un dato sin procesamiento, iría contra la tendencia de la libre circulación de datos, por lo que podría perjudicar a la economía y entorpecería el desarrollo o mejoramiento de la IA.

II. Determinar la posible protección jurídica de los datos personales dentro del ordenamiento jurídico venezolano, mediante el análisis de la legislación existente sobre .la materia, en la Unión europea, España y Venezuela con la finalidad de evaluar sí es viable la trasposición del marco regulatorio español

Como previamente se detalló dentro del apartado *Derechos relacionados a los Datos Personales dentro del Ordenamiento Jurídico*, y con la finalidad de no ser repetitivos nos limitaremos a indicar que sí es posible determinar bajo el actual ordenamiento jurídico la protección jurídica de los datos personales, incluso es un deber del Estado garantizar el desarrollo de las personas y el respeto a su dignidad. No obstante, consideramos que debe tenerse en cuenta los siguientes aspectos:

1. Dentro de la constitución se prevé un pool de derechos y garantías que se interrelacionan entre sí, como lo son el deber de garantizar el desarrollo a la personalidad y su libre desenvolvimiento, las condiciones jurídicas para que la igualdad ante la ley sea real y efectiva,

por ende, la no discriminación y principalmente expresa tres artículos que sirven como base legal para el desarrollo de la protección de los datos personales, los cuales son:

a) El Derecho al honor, a la privacidad, a la informática y a la intimidad artículo 60 CRBV. Estos derechos delimitan el alcance y restringen el uso de los datos, a fines de garantizar el libre desenvolvimiento a la personalidad, debido al alcance de las connotaciones negativas y positivas que implican estos derechos. Es indispensable que ante cualquier situación de conflicto que menoscabe esta garantía constitucional o ante situaciones en las que se dude sobre el alcance de otro derecho relacionado al tratamiento de datos personales, se resuelva a través de la ponderación, siguiendo la línea del RGPD entendiendo que el derecho que envuelve la protección de datos personales “no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad, y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad” considerando 4 del RGPD.

El aspecto medular de los datos personales, se encuentra precisamente en la recogida, el uso y almacenamiento, que no es más que otra cosa, que el tratamiento, y una inadecuada recolección, uso, almacenamiento o disposición de los mismos, iría en detrimento de los derechos personales, por ello es indispensable establecer los principios necesarios para delimitarlo y por supuesto desarrollarlos de una manera similar a la UE.

b) Derechos implicados en el habeas data: el artículo 28 CRBV que contiene el derecho a la Acción del Habeas Data, desarrollado además por vía jurisprudencial, contiene 7 principios: (1) El derecho de conocer sobre la existencia de tales registros. 2) El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas. 3) El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él. 4) El derecho de conocer el uso y finalidad que hace de la información quien la registra. 5) El derecho de actualización, a fin que se corrija lo que resulta inexacto o se transformó por el transcurso del

tiempo. 6) El derecho a la rectificación del dato falso o incompleto. 7) El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas.⁵⁵

Estos principios deben ser utilizados para regular el tratamiento de los datos, los cuales son contemplados como derechos del usuario dentro del Reglamento de la UE, que adicionalmente prevé el **derecho a la portabilidad**, el cual implica: (El interesado tendrá 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 lectura mecánica), derecho que no está desarrollado en el mencionado artículo y es necesario preverlo.

La Ley de Infogobierno, anteriormente mencionada, a través del artículo 75 pretendió regular el uso de datos personales a nuestro criterio de manera inconstitucional, porque viola el derecho a la privacidad y el libre desenvolvimiento de la personalidad, al obviar el requisito del consentimiento para la transferencia de datos. Consideramos que esto sucede debido a la carente estipulación de los principios utilizados para delimitar el tratamiento.

Los principios a los cuales nos referimos son los contemplados dentro de EL RGPD: i) licitud, lealtad y transparencia, ii) limitación de la finalidad; iii) Adecuados y pertinentes, iv) Minimización de datos, v) Exactitud; vi) limitación del plazo de conservación y vii) Responsabilidad proactiva.

Creemos que se pueden restringir los derechos personales, siempre que constituya una medida necesaria y proporcional en una sociedad democrática, por ello debe hacerse una restricción acorde al principio de legalidad y se respete un mínimo de garantías como el consentimiento informado y no mediante un consentimiento tácito porque vulneraría los siete derechos antes mencionados.

⁵⁵ El RGPD contempla los mismos derechos, tal vez con algunas denominaciones distintas Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado, 2 Información y acceso; de rectificación; de supresión - Derecho al olvido, limitación del tratamiento, de portabilidad de los datos, de oposición y decisiones individuales automatizadas.

c) El derecho a la información oportuna, contemplado en el artículo 58 CRBV, contempla expresamente el derecho al acceso a la información sin necesidad de ejercer una acción como la de habeas data y además el derecho a la rectificación de los datos personales cuando sean inexactos o generen un perjuicio

2.- Con referencia al régimen sancionador para restablecer el orden en cuanto el tratamiento de datos personales, consideramos que sería más conveniente utilizar un régimen sancionador administrativo como el de España, mediante infracciones y multas dependiendo de la naturaleza, gravedad y duración de la infracción, la intencionalidad, el grado de responsabilidad y no mediante un régimen punitivo como el de la Ley Especial Contra los Delitos informáticos, la cual tiene una técnica legislativa que deja mucho que desear y además esta desactualizada.

En conclusión:

Se puede y necesariamente se debe promulgar una ley en la materia de datos personales antes de que sea tarde, de conformidad con la base legal que se encuentra en la CRBV, en especial con el artículo 60 de la CRBV. Esta ley necesariamente debe regular todos los aspectos del uso, almacenamiento y disposición de los datos personales, además de contemplar los derechos de los usuarios, los principios rectores del tratamiento de datos, sus implicaciones y unificar en un solo cuerpo legislativo, sus correspondientes sanciones derogando las leyes antes mencionadas para evitar la colisión normativa. Además, siguiendo los pasos y estructuras creados en el RGDP, como de la ley española que hace su debida trasposición, será necesario contemplar la figura de un ente de control, que se encargue de garantizar y supervisar el cumplimiento de la ley, con las consideraciones señaladas en el próximo capítulo.

I. Examinar la posible protección jurídica de los datos no personales dentro del ordenamiento jurídico venezolano, a través del estudio de la protección otorgada a nivel internacional en el Acuerdo Sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio (ADPIC) y la UE con el objetivo de recomendar cómo puede protegerse en Venezuela

A nivel internacional, se encuentra en pleno debate, si debe o no otorgarse una protección jurídica al dato, pudiésemos indicar que hay dos posturas al respecto, quienes promueven la libre circulación del dato, en justificación al mejoramiento del estado de la técnica gracias que, a mayor cantidad de datos para procesar por la IA, mejor resultado tiene su procesamiento y análisis, aunado del crecimiento económico.

No obstante, la otra postura, indica que es necesario concebir la protección del dato en función al valor competitivo que adquiere solo cuando se procesan, analizan y convierten en conocimiento, porque es este conocimiento el que es explotado como derecho patrimonial, para maximizar el alcance u objetivo por el cual se crean las bases de datos. Creemos que ambas posturas tienen aspectos válidos, pero para poder decidir cuál es la más idónea, habría que realizar necesariamente una ponderación de derechos económicos y evaluar cuál es el fin que se busca tutelar, los cuales podrían ser el interés público, frente a la libertad de empresa y los derechos en juego por el sector empresarial.

En conclusión:

Concebimos como una relación sine qua non, el procesamiento y análisis de datos con el Big Data, por lo que la solución a este objetivo puede brindarse mediante la tutela de las bases de datos no originales otorgada por el derecho *sui generis*, con justificación a la inversión sustancial para la creación, adquisición y procesamiento de datos en concatenación con los

principios de lealtad y licitud para delimitar el tratamiento de datos, precisamente porque el aspecto medular se encuentra en el uso del derecho de explotación de dichas bases.

CAPÍTULO V

PROPUESTA

Es apremiante actualizar el marco regulatorio en materia de bases de datos y protección de datos, por ello se procederá a precisar un compendio de consideraciones pertinentes para desarrollar la protección jurídica del dato y de las Bases de datos en el ordenamiento jurídico de Venezuela, que se desprenden de los resultados de la presente investigación.

Consideraciones Generales sobre el Dato y las Bases de Datos

- El Estado debe promover la iniciativa privada, la producción de bienes y servicios para satisfacer las necesidades de la población, garantizar el derecho a la propiedad, así como el uso, goce y disfrute de los bienes, lo que incluye a los intangibles, como las bases de datos digitales, en desarrollo de los artículos 112 y 115 de la CRBV, es necesario promulgar una ley en la materia.
- En la elaboración y procesamiento de las bases de datos, hay una inversión económica, esfuerzo y tiempo, que se debe proteger indistintamente que las mismas sean protegidas por prácticas comerciales de confidencialidad o secreto empresarial. En este sentido, la regulación que se implemente no debe ser excluyente de los derechos que puedan concederse por los demás sistemas de Propiedad Intelectual a las bases de datos o manejo de datos.
- El tratamiento de datos esta intrínseco dentro de las finalidades de la creación de una base de dato, por ello y en consideración a la experiencia de la UE, recomendamos se protejan las bases de datos no originales a través de un derecho *sui generis*.
- Es preciso aprender de la experiencia de la UE, su avance en cuanto a la regulación la materia es indiscutible, por ello creemos necesario considerar las observaciones

realizadas a la Directiva 96/9/CE en el informe del año 2018, como lo es el tiempo de protección, el cual es excesivo por la posibilidad de renovar de manera perpetua la duración de la protección de las bases de datos no originales, en ponderación al beneficio social que pueda generar pasar esa información al estado de la técnica. Esto a su vez, evita abusos en cuanto al uso y limita las posiciones de dominio.

- En la actualidad se ha convertido en un elemento sine qua non la intervención de la IA para la creación y procesamiento de datos que a su vez se interconecta con la creación de las bases de datos, por consiguiente, esto debe preverse y modificarse antes de realizar una trasposición de la protección *sui generis* contenida en la Directiva 96/9/CE en Venezuela.
- El dato es un intangible cuyo valor no perece al ser utilizado. No obstante, su valor comercial, proviene de su debido procesamiento y análisis, esta actividad es lo que debe protegerse a través de la Propiedad Intelectual, preferiblemente a través de un derecho *sui generis*.
- El Estado debe intervenir para evitar los monopolios o el abuso de las posiciones de dominio, consecuencias estas, que se pueden propiciar por la falta o excesiva regulación en el uso de datos y/o bases de datos, se hace necesario que se adopten medidas para prevenir tales consecuencias de conformidad con el artículo 113 de la CRBV, por estas razones, consideramos que el modelo adecuado de protección es a través de un *derecho sui generis*.

Consideraciones Generales

sobre los Datos Personales

Como se indicó en el capítulo anterior, en la CRBV están previstos los derechos individuales necesarios para ser utilizados como base legal al momento de legislar sobre la

materia. Los derechos y deberes previstos en la CRBV que deben fungir como base legal son: el respeto a la dignidad, el libre desenvolvimiento de la personalidad, el derecho al honor, a la privacidad, a la informática y a la intimidad, el derecho a la información, a la igualdad y no discriminación, el derecho de acceso a la información y a los datos que sobre sí mismos o sobre sus bienes consten en registros oficiales o privados, así de conocer el uso de que se hagan los mismos, en pro de los derechos de protección de la seguridad personal.

El Estado está en deuda con los ciudadanos y debe dictar una ley para la protección del dato personal, por lo que proponemos realizar una transposición de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y Garantía de los Derechos Digitales promulgada en España, al considerarse una de las legislaciones más avanzadas en cuanto al tratamiento de datos o en su defecto utilizarse como ley modelo.

Al momento de legislar la materia debe tenerse como norte, el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Es necesario que el cuerpo normativo que se promulgue, contenga una serie de definiciones que permitan su entendimiento, además de unificar criterios a fines de evitar colisión de normas, por la falta de consenso en las definiciones.

Debe entenderse como requisito fundamental del tratamiento de datos, el consentimiento, el cual debería darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen.

Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de

personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño como los video juegos.

Los derechos que limitan el tratamiento de datos ya se encuentran previstas en el artículo 28 de la CRBV, ahora sugerimos hacer una transposición del ordenamiento español en la materia, a fin de incluir en nuestro ordenamiento el derecho a la portabilidad y los principios que giran en torno al tratamiento de datos personales como su estándar de la licitud sobre el tratamiento de datos.

Es innovadora la Ley española en regular el uso de datos de personas fallecidas, traslada el derecho del olvido o supresión a cabeza de sus familiares o herederos, según el caso en concreto, este alcance no se encuentra previsto en el artículo 28 de la CRBV, por ser una acción personalísima, sin embargo, sería prudente trasladar este derecho a nuestro ordenamiento jurídico.

Es necesario crear en un mismo cuerpo normativo con todo lo antes expuesto en este apartado, aunado de un sistema de responsabilidad por el uso indebido del dato con sus respectivas consecuencias, las cuales se sugiere sean sanciones pecuniarias y no penas, por lo que implicaría derogar las normativas que coliden con la nueva ley.

Con respecto a las responsabilidades de quien haga el uso de los datos, debe contemplarse la obligación de informar sobre la recolección de los datos, solicitar además autorización para el uso de los datos personales que les conciernen a cada persona, así como informar la medida en que dichos datos son o serán tratados.

Otro aspecto indispensable que debe implementarse del modelo español es la estructura administrativa de control denominada como Autoridad de Control, que es creada para hacer cumplir los lineamientos previstos en la Orgánica 3/2018, de 5/12, por ello tiene poderes correctivos, que le permiten ejercer una función sancionadora, hacer auditorías de protección de datos y supervisar el correcto funcionamiento.

Para poder lograr el funcionamiento de la institución dentro de nuestro ordenamiento, se considera también necesario que se procure garantizar que la institución sea independiente y entre los aspectos que consideramos que sirve para colaborar con el correcto funcionamiento de un organismo de tal índole, es que el presidente y el adjunto de la autoridad de control (así es previsto en la Ley española), ejercerán las funciones de su cargos por una duración de cinco años y puede ser renovado para otro período de igual duración, este tipo de provisiones otorgan seguridad y perdurabilidad de las políticas a desempeñar y periódicamente debiese rendir cuentas de su gestión incluyendo una evaluación de la efectividad de la normativa, así como de sus consecuencias.

REFERENCIAS BIBLIOGRÁFICAS

- *¿Qué son los datos estructurados?* (s.f) <https://luca-d3.com/es/data-speaks/diccionario-tecnologico/datos-estructurados>
- Artículo de la página “El Milenio” sobre los Datos de población con acceso a internet, del 7/12/2018. <https://www.milenio.com/tecnologia/la-mayoria-del-mundo-tiene-acceso-a-internet-onu>
- Becerra, J., Cotino Hueso, L., León, I. P., Sánchez-Acevedo, M. E., Torres Ávila, J. y Velandia Vega, J. (2018). *Derecho y Big Data*. Editorial Universidad Católica de Colombia.
- Belandria García, José (2017). *La recolección e intercambio de datos de carácter personal por medios telemáticos en Venezuela, de acuerdo con la Ley de Infogobierno*. BEDA Boletín Electrónico de Derecho Administrativo de la Universidad Católica Andrés Bello N° 2.
[http://w2.ucab.edu.ve/tl_files/POSTGRADO/BEDA/Numero%202%20\(2017\)/Art%204.pdf](http://w2.ucab.edu.ve/tl_files/POSTGRADO/BEDA/Numero%202%20(2017)/Art%204.pdf)
- Brewer-Carias, Allan (1994). *Consideraciones sobre el derecho a la vida privada y la intimidad económica y a su protección*. Separata del libro “La Corte y el Sistema Interamericanos de Derechos Humanos” Nieto Navia, R. Editor.
- Comisión Europea (2018). *Evaluación de la Directiva 96/9/CE sobre la protección jurídica de las bases de datos*. Documento de Trabajo de los Servicios de la Comisión.
- Comité Permanente de Derecho de Autor y Derechos Conexos, de la Organización Mundial de la Propiedad Intelectual, (2002). *La protección jurídica de las bases de datos*. Documento presentado por la comunidad europea y sus Estados Miembros. Octava sesión Ginebra, 4 al 8 de noviembre de 2002.
- Constitución de la República Bolivariana de Venezuela (1999). Gaceta Oficial N° 5.908, Extraordinaria del 19/2/1999.

- Constitución Española (1978). Aprobada por las Cortes en sesiones plenarios del Congreso de los Diputados y del Senado celebradas el 31 de octubre de 1978 Ratificada por el pueblo español en referéndum de 6 de diciembre de 1978 Sancionada por S. M. el Rey ante Las Cortes el 27 de diciembre de 1978.
- Diálogo de la OMPI Sobre Propiedad Intelectual (PI) y Tecnologías de Vanguardia en su Cuarta Sesión.(2021) <https://webcast.wipo.int/> min
- Diccionario Panhispánico del español jurídico de la Real Academia Española. (2020) Big Data. <https://dpej.rae.es/lema/big-data> A1
- Diccionario Tecnológico, LUCA AI Powered Decision. Unidad de Datos de Telefónica .(s.f p.s/n. *definición de dato no estructurado* <https://luca-d3.com/es/data-speaks/diccionario-tecnologico/datos-no-estructurados>
- Diccionario Tecnológico LUCA AI Powered Decision. Unidad de Datos de Telefónica .(s.f p.s/n) <https://luca-d3.com/es/data-speaks/diccionario-tecnologico>
- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo del 27 de abril de 2016 Relativa a la Protección de las Personas Físicas en lo Que Respecta al Tratamiento de Datos Personales Por Parte de las Autoridades Competentes Para Fines de Prevención, Investigación, Detección o Enjuiciamiento de Infracciones Penales o de Ejecución de Sanciones Penales, y a la libre Circulación de Dichos Datos.
- Directiva 96/9/EC sobre Bases de Datos de la Comunidad Europea.
- El Decreto Con Rango y Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas Gaceta Oficial N° 37.076m 13 de diciembre de 2000. https://www.oas.org/juridico/spanish/mesicic3_ven_anexo19.pdf
- Economic Espionage Act of 1996, 18 U.S.C 1831 et seq https://members.wto.org/crnattachments/2016/IP/USA/16_4983_00_e.pdf

- Fruchter, N., Specter, M. y Yuan, B. (2018). *Facebook / Cambridge analytica: privacy lessons and a way forward*. Internet Policy Research Initiative Massachusetts Institute of Technology <https://internetpolicy.mit.edu/blog-2018-fb-cambridgeanalytica/>
- Gallo Sallent, Juan Antonio, “*El Big Data. Implicaciones jurídicas para un cambio de paradigma: El derecho al olvido y el consentimiento*”, (2020), Universidad Internacional de Cataluña
- García, C. (s.f). *El futuro incierto de la Directiva 96/9 CE Sobre la Protección jurídica de las bases de datos*
- Glazer, D, Sonsini, W, et al, (s.f) *Data As Ip And Data License Agreements*. [https://www.friedfrank.com/siteFiles/Publications/Data%20as%20IP%20and%20Data%20License%20Agreements%20\(1\).pdf](https://www.friedfrank.com/siteFiles/Publications/Data%20as%20IP%20and%20Data%20License%20Agreements%20(1).pdf)
- González Fuster, Gloria (2012). *Equilibrio entre Propiedad Intelectual y protección de datos: el peso oscilante de un nuevo derecho*. IDP. *Revista de Internet, Derecho y Política*. Nº 14, pp. 47-60. UOC.
- Hernández, Pamela (s.f.). *Los datos personales y la propiedad industrial*. <https://www.sic.gov.co/ruta-pi/junio27/los-datos-personales-y-la-propiedad-industrial>
- Incera, Karen (2009). *Protección de datos de prueba protegidos: viabilidad del resarcimiento de daños y perjuicios por aprovechamiento del esfuerzo ajeno (Especial referencia al caso venezolano)*. https://www.revistajuridicaonline.com/wp-content/uploads/2010/10/39a88_proteccion.pdf
- Organización Mundial de la Propiedad Intelectual (2019). *La Propiedad Intelectual en un mundo impulsado por los datos*. *Revista de la OMPI*, https://www.wipo.int/wipo_magazine/es/2019/05/article_0001.html
- Ley de Infogobierno Gaceta Oficial de la República núm. 40.274, de fecha 17 de octubre de 2013.
- Ley de Propiedad Intelectual de España Real Decreto Legislativo 1/1996, de 12 de abril.

- Ley Especial Contra los Delitos Informáticos Gaceta Oficial N.º 37.313 del 30 de octubre de 2001.
- Ley Orgánica 3/2018, de 5/12, de Protección de datos personales y garantía de los derechos digitales.
- Ley Sobre el Derecho de Autor, Gaceta Oficial N.º 4.638 Extraordinaria del 1 de octubre de 1993.
- Ortiz-Ortiz, Rafael (s.f.). *Las implicaciones jurídico positivas del derecho a la información y la libertad de expresión en el nuevo orden constitucional*, <http://servicio.bc.uc.edu.ve/derecho/revista/1-2000/1-2000-6.pdf>
- Pérez Sanz, Carlos (2016). *Aspectos legales del big data*. Tema de Portada. pp. 18-22.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD) del 27 de abril de 2016.
- Secretaría del Grupo Asesor de Expertos Independientes Sobre la Revolución de los Datos para el Desarrollo Sostenible (2014.) *Un mundo que cuenta movilización de la revolución de los datos para el desarrollo sostenible*.
- Sentencia N.º 1050, del 23 de agosto de 2000 <http://historico.tsj.gob.ve/decisiones/scon/agosto/1050-230800-00-2378%20.HTM>
- Sentencia N.º 1281, del veintiséis (26) de junio de 2006, Expediente 05-1964. <http://historico.tsj.gob.ve/decisiones/scon/junio/1281-260606-05-1964.HTM>
- Sentencia N.º 151, de la Sala Político Administrativo, del trece (13) de febrero de 2008.
- Sentencia N.º 1543 a los doce (12) días del mes de agosto del año (2008) sobre el caso lipitor <http://jca.tsj.gob.ve/DECISIONES/2008/AGOSTO/1478-12-AP42-N-2004-001149-2008-1543.HTML>
- Sherif El-Kassas, (2002). *Estudio sobre la protección de las bases de datos no originales*. OMPI, Comité Permanente de Derecho de Autor y Derechos Conexos.
- Westreicher, Guillermo s.f *Dato*. Par. 10 <https://economipedia.com/definiciones/dato.html>