RECORRIDO POR LA NORMATIVA SOBRE PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA Y LA SITUACIÓN EN VENEZUELA

Marianela Zubillaga*

Profesora Universidad Católica Andrés Bello

Resumen: *El entorno digital y tecnológico tiene su epicentro en los datos personales, como elemento fundamental de la "economía del dato", que se estructura sobre la capacidad de recopilar, tratar y vincular aquellos que se obtienen de los usuarios, a los fines de establecer, patrones de consumo, perfilamiento de gustos e incluso modelar opiniones, todo lo cual ha conllevado a crear modelos de negocio basados en la comercialización de dicha información.*

Frente a ello, paulatinamente se ha reconocido el derecho de las personas a la protección de sus datos personales, como derecho autónomo. La Unión Europea ha liderado el desarrollo de una normativa con el Reglamento General de Protección de Datos, en vigor desde mayo de 2018 que garantiza y protege los derechos de las personas físicas e impone obligaciones, deberes y cargas a las empresas tecnológicas. Se presenta un estudio de su normativa, ya que puede constituir una ley modelo para otras jurisdicciones, como la venezolana.

Finalmente, se brinda una panorámica de la normativa vigente en la materia en Venezuela, para poder marcar el camino hacia el cual deberán dirigirse las iniciativas legislativas en la materia.

Palabras Clave: *Derechos fundamentales, datos personales, protección de datos personales, Reglamento UE Protección de Datos*

Abstract: *The digital and technological environment has its epicenter in personal data, as a fundamental element of the "data economy", which is structured on the ability to collect, process and link those obtained from users, for the purpose of establishing, consumption patterns, profiling of tastes and even modeling opinions, all of which have led to the creation of business models based on the commercialization of that information.*

Faced with this, the right of people to the protection of their personal data has been gradually recognized as an autonomous right. The European Union has led the development of regulations with the "General Data Protection Regulation in force since May 2018 that guarantees and protects the rights of persons and imposes obligations, duties and charges on technology companies. A study of its regulations is review, since it can be a model law for other jurisdictions, such as Venezuela.

Finally, an overview of the current regulations on the matter in Venezuela is provided, to mark the path towards which the legislative initiatives on the matter should be directed.

Key words*: Fundamental rights, personal data, personal data protection, EU Data Protection Regulation.*

---

* Abogado Cum-laude Universidad Católica Andrés Bello (1988). Profesora Asistente Derecho Mercantil (Prácticas) y Fundamentos Derecho Mercantil (2011-2021). Abogado socia de Baumeister & Brewer, abogados consultores.

INTRODUCCIÓN

Las sociedades de todo el planeta, así como sus economías, se han visto profundamente afectadas ante el desarrollo acelerado del mundo tecnológico y digital. No hay actividad alguna del quehacer humano que no esté sujeta a la irrupción de la tecnología. El derecho se enfrenta a tal realidad y luce un tanto lento e inoperante, frente a los nuevos fenómenos. Pensamos que es un hecho indiscutible el rezago que existe entre, los avances tecnológicos y digitales, por una parte, y por la otra, la normativa que debe regular tales fenómenos, tanto en Venezuela como en otros países, por lo que urge ponernos al día y avanzar hacia regulaciones adaptadas a esta nueva realidad y que no se erijan como obstáculos para el crecimiento y desarrollo del entorno digital y tecnológico.

En este estado de cosas, observamos que el epicentro de este proceso de cambio es el dato personal. Tal como lo indica la comunicación de la Comisión de la Unión Europea (UE),

> "Los datos son el elemento vital del desarrollo económico: constituyen la base de muchos nuevos productos y servicios, lo que conduce a un aumento de la productividad y una mayor eficiencia en el uso de los recursos en todos los sectores de la economía, lo que permite, a su vez, que haya productos y servicios más personalizados y se mejore no solo la elaboración de políticas sino también los servicios públicos. Es un recurso esencial para las empresas emergentes y las pequeñas y medianas empresas (pymes) a la hora de desarrollar productos y servicios. La disponibilidad de datos es fundamental para entrenar a los sistemas de inteligencia artificial"[1].

De manera que se puede afirmar, que los datos personales tienen un valor económico, el cual recae, no tanto en el dato en sí mismo, sino en la posibilidad de su recopilación, tratamiento y vinculación con otros datos y la información que de allí se obtenga. El uso y la aplicación de tal información a la creación de patrones de consumo, perfilamiento de gustos, conduce a la obtención de lucro por parte de quienes recopilen y manejen tales datos, creando así un modelo de negocios soportado en la información que de allí se obtiene.

Por ello, es fundamental analizar cómo ha sido, en el derecho comparado, la regulación de los datos personales. A tales fines, observamos que los grandes bloques económicos de Occidente han asumido, de distinta manera, tal fenómeno: Por una parte, los Estados Unidos carece de una normativa general a nivel federal[2], a excepción de aquella dictada en protección de los menores[3] y ha dejado que sean los estados de la Unión[4], quienes dicten normas de carácter general o que dicha regulación se haya establecido por sectores de la economía[5].

---

1 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: "*Una estrategia europea para los datos*" (Bruselas, 19 de febrero de 2020) p., 4. Consultado en https://eur-lex.europa.eu/legal-content/EN/TXT/?qid =1593073685620&uri=CELEX%3ª52020DC0066

2 "La normativa norteamericana se caracteriza por una complicada pluralidad de instrumentos legales, institucionales y de organizaciones de estandarización. Podemos diferenciar entre leyes estatales, normativa sectorial de organizaciones de estandarización, otras regulaciones y directrices ("*self-regulatory guidelines and frameworks*") y actuaciones de vigilancia, control y supervisión llevadas a cabo por diferentes instituciones u organismos gubernamentales. Por tanto, no existe regulación federal genérica respecto a la protección de datos". Consultado en: https://www.lleytons.com/conocimiento/la-proteccion-de-datos-personales/.

3 En EEUU se ha dictado la "Ley de protección de la privacidad en línea de los niños (*Children's Online Privacy Protection Act COPPA*)", la cual regula todo lo relativo a la recopilación en línea de información sobre niños menores de 13 años.

4 El estado de California ha sido el primero en dictar una normativa que regula el manejo de datos de manera general, la cual entró en vigor en el año 2020. Ver https://www.lavanguardia.com/

Por la otra, el derecho de la Unión Europea ha ido creando paulatinamente un marco jurídico más integral, regulando en áreas como la protección de datos personales, derechos fundamentales, competencia[6] y ciberseguridad, así como en diversos sectores de la economía[7], dictando un conjunto de normas, de diverso ámbito, que pretende erigirse como un marco jurídico de referencia a nivel internacional, a los fines de cumplir con uno de sus objetivos, como es la creación de un "espacio europeo único de datos"[8].

Por lo tanto, pensamos que es el Derecho Europeo el que tiene hoy en día el liderazgo en la regulación de esta nueva realidad, por lo que, ante la posibilidad de que las normas dictadas en Europa se erijan como leyes modelos, dada la velocidad con la que avanza el mundo tecnológico, hemos considerado relevante, hacer un estudio de la normativa dictada y el horizonte hacia el cual se dirige el Derecho Europeo en la protección de los datos de sus ciudadanos y su seguridad, para comparar con la normativa venezolana actual y poder establecer paralelismos, para marcar el camino hacia el cual deberán dirigirse las iniciativas legislativas en esta área, en nuestro país.

A los fines de este artículo, nos centraremos en el estudio de la normativa de aplicación directa y de carácter general dictada por la UE, contenida en el REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la pro-

---

vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio -electronico.html

5 En materia sectorial, se han regulado y establecido requisitos de privacidad específicos en el sector financiero, con relación a las comunicaciones electrónicas privadas existe la *Electronic Communications Privacy Act (ECPA*); en materia de salud, la *Health Insurance Portability and Accountability Act* (HIPAA), así como ciertas reglas vinculadas con el uso de información crediticia, *The Fair Credit Reporting Act* (FCRA).

6 Ley de Servicios Digitales (Digital Services Act o DSA) y la Ley de Mercados Digitales (Digital Markets Act o DMA), fueron aprobadas durante el pleno del 5 de julio, por el Parlamento Europeo, faltando su publicación en el Diario Oficial de la Unión Europea, y su entrada en vigencia se prevé para otoño de 2022.

7 En este sentido, han dictado legislación sectorial específica, sobre el acceso a los datos en el sector de la automoción, los proveedores de servicios de pago, la información en materia de medición inteligente, sobre los datos de la red eléctrica o sobre los sistemas de transporte inteligente. También promulgaron una directiva sobre contenidos digitales, destinada a capacitar a las personas, estableciendo en sus derechos contractuales, cuando se prestan servicios digitales a consumidores que facilitan el acceso a sus datos.

8 En la Comunicación de la Comisión, "*Una estrategia europea para los datos*" se afirma que: "La UE debe crear un entorno político atractivo a fin de que, de aquí a 2030, la cuota de la UE en la economía de los datos -datos almacenados, tratados y valiosos para su uso en Europa- al menos se corresponda con su peso económico, y ello no por imposición, sino por libre elección. El objetivo es crear un espacio único europeo de datos, un verdadero mercado único de datos, abierto a datos procedentes de todo el mundo, en el que los datos personales y no personales, incluidos los datos sensibles de empresas, estén seguros y las empresas también tengan fácil acceso a una cantidad casi infinita de datos industriales de alta calidad, de manera que se impulse el crecimiento y se cree valor, minimizando al mismo tiempo la huella humana medioambiental y de carbono. Debe ser un espacio en el que la legislación de la UE pueda aplicarse con eficacia y en el que todos los productos y servicios basados en los datos cumplan las normas pertinentes del mercado único de la UE. Al efecto, Europa ha de combinar una legislación y una gobernanza adaptadas al fin perseguido para garantizar la disponibilidad de datos, con inversiones en normas, herramientas e infraestructuras, así como en competencias para el manejo de los datos. Este contexto favorable, en el que se promuevan los incentivos y la posibilidad de elegir, dará lugar a que se almacenen y traten más datos en la UE". Consultado en: -https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

tección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD o el Reglamento).[9]

I. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES

El Reglamento fue promulgado el 27 de abril de 2016, no obstante, tuvo una *vacatio legis* de más de dos años ya que, no fue sino hasta el 25 de mayo de 2018, que empezó a tener pleno vigor en todos los Estados miembros y con una prelación sobre la normativa nacional.

a. Bien jurídico protegido:

La norma parte de considerar a la protección de datos personales[10] de las personas físicas[11], como un derecho fundamental del ciudadano[12] y ha sido dictada con el objetivo de que éstos tengan un mejor control sobre sus datos, a los fines de que exista mayor confianza por parte de los consumidores europeos, lo cual conducirá a la creación y fortalecimiento de un mercado único digital.

Frente a ello, y dado lo sensible que es cierta información sobre los ciudadanos y con el objetivo de su protección integral, el Reglamento prohíbe expresamente, tratar aquellos datos personales que "… revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física"[13] (datos sensibles). De manera que, en principio, ninguna aplicación, plataforma, o página web, puede requerir a sus usuarios o consumidores, información sobre los citados datos[14].

---

9 El texto del reglamento se consultó en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri =CELEX%3A32016R0679

10 Según el artículo 4, se entiende por "dato personal" "toda información sobre una persona física identificada o identificable". Así, se consideran datos, el nombre, apellidos, dirección postal o electrónica, edad, fecha de nacimiento, número de documento de identidad/pasaporte, ingresos, perfil cultural, dirección de protocolo internet (IP), fotografías, voz, datos de geolocalización, datos en poder de hospitales o médicos (que identifican únicamente a una persona con fines sanitarios).

Adicionalmente, es oportuno señalar que de conformidad con el RGPD cuando los datos sean anonimizados, pierden la protección. Según el considerando 26, "… los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación". Ahora bien, es importante tener en cuenta que Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible.

11 De conformidad con el considerando 14 del Reglamento, éste "… no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto".

12 El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

13 Artículo 9.1 del RGPD.

14 Es de advertir que el Reglamento prevé ciertas excepciones en las que puede ser autorizada la recopilación de dichos datos sensibles, como es en el supuesto que, (i) cuando la persona haya hecho manifiestamente públicos sus datos sensibles, (ii) cuando se haya dado el consentimiento explícito, (iii) cuando una ley rija un tipo específico de tratamiento de datos para un fin específico relacionado con el interés público o la salud,(iv) cuando una ley que incluya las garantías adecuadas de protección prevea el tratamiento de datos personales sensibles en ámbitos como la sanidad pública, el empleo y la protección social. Un típico ejemplo, son las encuestas desarrolladas por la

Por lo que respecta a las "*cookies*"[15], en la medida en que requieran datos personales de los usuarios, éstas también caen bajo la lupa del RGPD, de ser el caso[16].

Ahora bien, se debe destacar que la UE había dictado una normativa anterior en materia de *cookies* y privacidad por lo que respecta concretamente a las comunicaciones electrónicas, contenida en la "Directiva 2002/58/CE de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)"[17]. No obstante, al ser una directiva [18] -y no una norma de carácter general, directamente aplicable en los Estados miembros- la aplicación de su contenido no fue, ni simultanea ni la misma, en todos los estados europeos, por lo que no vino a ser sino con la entrada en vigor del RGPD, que se observó -a nivel mundial- un cambio importante en los sitios web, los cuales incluyeron una declaración, que aparece cada vez que se va a acceder a ellos, con la que se debe dejar constancia de la autorización o el rechazo, que da el usuario, para que dichas *cookies* accedan a tal información, así como los demás permisos e información requeridos con la nueva norma, tal como se verá a lo largo de este artículo.

---

agencia gubernamental responsable de realizar un censo público, que por lo general contienen preguntas vinculadas con el sexo, la raza o el origen étnico. En este supuesto, dicha encuesta tiene fundamento en una ley y tiene una finalidad de interés público.

15 Las cookies son archivos de texto que una página o sitio web envía a cada visitante o usuario, que quedan almacenados en los navegadores de éste y que pueden o no recoger y tratar ciertos datos personales. Por lo general, los datos que se incluyen en las cookies pueden versar sobre las preferencias de idioma del usuario o el tamaño de su pantalla, por ejemplo, en cuyo caso no se necesitará del consentimiento del usuario. Ahora bien, también pueden pedir la dirección de IP, el navegador que se utiliza o sobre el comportamiento cuando se navega por Internet. En este sentido, se señala, por ejemplo, que "las *cookies de marketing* registran el comportamiento del usuario a lo largo de todo Internet (y no solo del concreto sitio web que esté visitando) para elaborar un perfil que después permita mostrarle publicidad personalizada" https://cookieinformation.com/es/que-es-el-rgpd/.

16 Según sus características y necesidades, las cookies son de cuatro tipos: (i) *Cookies necesarias* (cookies propias), son indispensables, para que un dominio funcione correctamente y por lo general sólo duran mientras el usuario visita tu sitio (cookies de sesión). Esta es la única categoría que puede quedar exentas del consentimiento de cookies del RGPD. (ii) *Cookies de preferencia,* recuerdan las elecciones que hizo el usuario la primera vez que accedió al sitio web, como por ej., como la configuración del idioma o la moneda en tu sitio web. (iii) *Cookies estadísticas,* la mayoría de las veces son de servicios de terceros, como software analítico que se incluyen en un sitio web. (iv) *Cookies de marketing*, casi siempre proceden de empresas tecnológicas o publicitarias de terceros, con el fin de ofrecer publicidad a los usuarios, o para recopilar algunos datos personales, para futuros fines de marketing. Conforme al RGPD, con excepción de las primeras, las cookies solo podrán activarse luego de que el usuario haya manifestado su consentimiento libre, firme y explícito, para el propósito específico de su funcionamiento y a la recopilación de datos personales.

17 La directiva en comento contiene normas destinadas a que los Estados miembros regularan el mercadeo directo que hacen las empresas, por correo electrónico; el uso de cookies, y buscaba minimizar la utilización de datos de manera la minimización de datos y otros aspectos de la privacidad de datos. Se llama coloquialmente como la Directiva *ePrivacy.*

18 Es decir, sus disposiciones tienen que ser objeto de transposición por parte de los Estados Miembros. Por ejemplo, en España sus normas hicieron parte del derecho interno a través de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones. Ver https://www.boe.es/buscar/doc.php?id=BOE-A-2022-10757.

La directiva fue objeto de modificación por la "Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores". https://www.boe.es/buscar/doc.php?id=DOUE-L-2009-82479

Por los motivos antes indicados, la UE ha venido trabajando en el texto de un reglamento que unifique la normativa de los estados miembros particularmente en materia de comunicaciones electrónicas, y ha preparado el "*Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas*)"[19], el cual aún no ha sido aprobado.

El proyecto de dicha normativa señala que tiene por finalidad "… garantizar un elevado nivel de protección de la intimidad a los usuarios de servicios de comunicaciones electrónicas y condiciones de competencia equitativas para todos los agentes del mercado", ya que, "El contenido de las comunicaciones electrónicas puede desvelar información muy delicada sobre las personas físicas que participan en ellas, tales como experiencias personales y emociones, problemas de salud, preferencias sexuales y opiniones políticas, cuya divulgación podría causar daños personales y sociales, pérdidas económicas o situaciones embarazosas. Del mismo modo, los metadatos derivados de las comunicaciones electrónicas también pueden desvelar información muy delicada y de carácter personal. Entre esos metadatos figuran los números a los que se ha llamado, los sitios web visitados, la localización geográfica o la hora, la fecha y la duración de una llamada, información que permite extraer conclusiones precisas sobre la vida privada de las personas participantes en la comunicación electrónica tales como sus relaciones sociales, sus costumbres y actividades de la vida cotidiana, sus intereses, sus preferencias, etc.…". Por lo que respecta a personas jurídicas pauta que, "… los datos de las comunicaciones electrónicas también pueden revelar información relativa a las personas jurídicas, como secretos comerciales u otro tipo de información confidencial que tiene valor económico".

De acuerdo con lo señalado en el texto del borrador del Reglamento, el motivo que conlleva a dictar esta normativa adicional, en materia de comunicaciones electrónicas es porque, cada vez con mayor frecuencia, los servicios de comunicación tradicional han venido siendo desplazados, tanto por los consumidores, como por los oferentes de bienes y servicios, por "…los nuevos servicios basados en Internet que hacen posibles comunicaciones interpersonales tales como servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico basados en la web…" es decir servicios de transmisión libre (denominados en inglés «*Over-the-Top*» y conocidos por su sigla en inglés «OTT») los cuales no están regulados por la normativa de telecomunicaciones.

Por lo que respecta a la vinculación entre este reglamento y el RGPD, su propio texto señala que, "La presente propuesta constituye una *lex specialis* en relación con el RGPD, precisándolo y completándolo en lo que respecta a los datos de comunicaciones electrónicas que se consideran datos personales. Todas las cuestiones relacionadas con el tratamiento de datos personales que no se contemplan específicamente en la propuesta quedan amparadas por el RGPD"[20].

b. Ámbito de aplicación:

De conformidad con lo establecido en el artículo 3 del RGPD, dicha normativa se aplicará en los siguientes supuestos:

i. Organizaciones o empresas de cualquier tipo, ya sea públicas o privadas, que estén ubicadas en la UE, independientemente de que el tratamiento de dichos datos tenga o no lugar en la UE.

ii. Organizaciones o empresas de cualquier tipo (públicas o privadas), que estén fuera de la UE, cuando traten datos personales de interesados que se encuentren en la UE, vinculadas con la oferta de bienes o servicios a dichos interesados en la Unión, (así sean pagos o gratuitos) u observan el comportamiento de éstos en la UE.

---

19 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010. También llamado Ley ePrivacy o Ley Cookies.

20 Citas tomadas del texto del reglamento en https://eur-lex.europa.eu/legal-content/ES/TXT/ HTML/?uri=CELEX:52017PC0010&from=ES

iii. Organizaciones o empresas de cualquier tipo (públicas o privadas) que estén fuera de la UE, pero que, por aplicación de las normas de Derecho Internacional Público, le es aplicable el derecho de los Estados miembros.

Así, por ejemplo, las redes sociales más importantes como Facebook, Twitter, Instagram y WhatsApp, todas ubicadas fuera de la UE, actualizaron sus políticas de privacidad, para adaptarla a la entrada en vigor del reglamento[21].

c. Consentimiento e información sobre el responsable de la recogida de datos, sus fines y su compartición:

Uno de los cambios más relevantes introducidos por el RGPD, fue el relativo a la exigencia de que cada usuario manifieste -de manera inequívoca- su aceptación al tratamiento de los datos, para el fin que se indica. Dada la envergadura de los cambios que esta norma conllevó en la práctica, citamos el texto del Nº 32 del RGPD que establece que,

> "El consentimiento debe 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, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

Tal exigencia es la que conllevó -al igual que la política sobre las *cookies*- a profundos cambios en páginas webs, aplicaciones y redes sociales a nivel mundial, en las cuales se acostumbraba a usar el llamado consentimiento tácito o el presunto[22] para soportar o justificar la recogida de datos. Con la entrada en vigor del RGPD se hizo necesario obtener el consentimiento "claro, expreso e inequívoco" del usuario para cada intercambio de datos[23]. Por otra parte, esta nueva exigencia puso también sobre la mesa una gran discusión, vinculada con la necesidad o no de obtener un nuevo consentimiento por parte de los usuarios que ya estaban registrados o que eran clientes, con anterioridad a la entrada en vigencia del RGPD. Dada la redacción de la norma, se concluyó que, si el consentimiento no había sido manifestado de

---

21 De los cambios más relevantes introducidos por estas empresas fue el vinculado al consentimiento expreso del usuario, para la recogida de datos, así como para el caso en que compartan éstos con otras RRSS. Para mayor información sobre los cambios implementados por las tecnológicas, https://resolving.es/como-afecta-rgpd-redes-sociales/

22 Conforme a la doctrina, el consentimiento tácito consiste en considerar que el silencio o la inacción del usuario, implica una aceptación; y el presunto, es aquel que se extrae del comportamiento del interesado, de manera que es necesario (a diferencia del tácito) que haya habido algún acto o acción por parte del usuario, a partir del cual se deduce que ha manifestado su consentimiento; así por ejemplo, se entendía que había consentimiento presunto cuando el usuario ingresaba a la página y sin aceptar las condiciones, revisaba la página navegando en ella o deslizando su cursor hacia arriba o hacia abajo (*scroll*).

23 En el caso concreto de Facebook, esta empresa revisó tres configuraciones concretas y solicitó a los usuarios europeos que la reevaluaran, es decir, aquellos datos vinculados con el reconocimiento facial; cierta información de perfil relativa a la afiliación política u opiniones religiosas; y los datos compartidos con terceras empresas, para que Facebook pudiera publicar anuncios. Ver https://www.washingtonpost.com/news/the-switch/wp/2018/04/20/facebooks-privacy-changes-look-different-for-europeans-and-americans/

manera clara, debía volverse a solicitar, lo que motivó a que -por ejemplo- Facebook e Instagram enviaran un correo electrónico a sus usuarios en territorio europeo, solicitando la manifestación de consentimiento de la manera indicada.

El segundo cambio es la necesidad de ampliar la información sobre las personas responsables del tratamiento de datos y demás datos[24]. Si bien con anterioridad a la entrada en vigencia del RGPD ya la mayoría de la normativa europea exigía que se identificara a la persona responsable del tratamiento de datos, de la finalidad de la recogida de éstos y de las vías a través de las cuáles se pueden ejercer los derechos denominados ARCO[25], la entrada en vigencia del RGPD impuso la obligación de informar sobre aspectos adicionales, como son: (i) la base legal para el tratamiento de los datos; (ii) el período en que se conservarán y mantendrán los datos almacenados y (iii) el derecho a retirar el consentimiento y a la posibilidad de hacer reclamaciones.

Otras innovaciones que resaltar fueron, por una parte, el relativo a la obligación de exigir que el usuario manifieste, también de manera clara e inequívoca, su autorización para que los datos que recopile una empresa sean compartidos con terceros, y por la otra, la necesidad de informar cuando se pretenda usar los datos recabados, para un fin distinto a aquel para el que inicialmente se recogieron, con anterioridad a tal tratamiento posterior[26].

También es oportuno destacar que el RGPD consagró lo que se denomina la "Protección de datos desde el diseño y por defecto[27]" conforme al cual se exige al responsable del tratamiento, que en el momento de configurar los datos que serán recogidos, se haga de manera que, por defecto, se recoja la menor cantidad de datos personales, en mínima extensión del tratamiento, así como en el plazo de conservación. Para ampliar tal recogida se deberá contar con la aprobación expresa del usuario. Es por esta exigencia que, contrariamente a lo que antes sucedía, al acceder a la política de privacidad y cookies de una página, tendrá marcado por defecto, el "rechazar todo" o términos similares. De manera que, para cambiar tales opciones, el usuario deberá acceder directamente a las políticas de la aplicación o la página o plataforma del producto o servicio a los fines de cambiar dicha configuración y manifestar su consentimiento de manera clara e inequívoca, en cuanto a dicho cambio solicitado.

d. Derechos consagrados:

La Directiva 95/46/CE, de fecha 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 (que fue derogada por el RGPD), dio nacimiento a cuatro derechos fundamentales reconocidos a las personas físicas, relacionados con sus datos personales. Tales derechos se denominaron de Acceso, Rectificación, Cancelación (ahora supresión) y Oposición y fueron denominados -por sus siglas- como derechos ARCO. El RGPD ratifica todos ellos y ha consagrado otros dos más, llamados, de Limitación y Portabilidad, por lo que ahora se denominan derechos ARSULIPO. Se describirá brevemente el contenido de cada uno de ellos:

i. *Derecho de Acceso*: Consagra el derecho que tienen los usuarios de acceder gratuitamente a sus datos personales y en contrapartida, la obligación que tienen los responsables del tratamiento de dichos datos de informar sobre éstos[28].

---

24 Ver artículo 13 del RGPD, relativo a la "Información que deberá facilitarse cuando los datos personales se obtengan del interesado".

25 Son los derechos de acceso, rectificación, supresión (antes cancelación) y oposición, que se verán en el literal siguiente.

26 Artículo 13.b del RGPD.

27 Artículo 25 del RGPD.

28 El RGPD regula claramente toda la información que hay que suministrar a los usuarios, tanto cuando la información y los datos personales se han obtenido del interesado (artículo 13) como cuando no (artículo 14).

ii. *Derecho de Rectificación:* Se refiere al "…derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan"[29] o que se completen los existentes.

iii. *Derecho de Supresión* (antes de Cancelación) (*Derecho al Olvido*): Este derecho no estaba expresamente recogido en la Directiva 95/46/CE y fue inicialmente reconocido como tal, en la Sentencia del Tribunal de Justicia de la Unión Europea de 2014, (asunto C-131/12)[30] y consiste -en los términos de la Agencia Española de Protección de Datos (AEPD)-, en "… el derecho a impedir la difusión de información personal a través de internet, cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa"[31]. Tal derecho abarca el de limitar la difusión de datos personales en los buscadores, cuando la información es obsoleta o ya no tiene relevancia ni interés público, o el usuario retiró su consentimiento o los datos fueron tratados ilícitamente, aunque la publicación original sea legítima y siempre que, quien posea esos datos, no tenga razones legítimas para retenerlos. Con el RGPD ese derecho adquiere rango legal al consagrarlo en su artículo 17, como un derecho de los usuarios.

   Adicionalmente, este derecho impone la obligación a los responsables del tratamiento que han difundido la información a terceros, a comunicarles a estos la obligación de suprimir cualquier enlace a los datos publicados, así como a eliminar cualquier copia o réplica de dichos datos.

   Es interesante citar lo que señala la AEPD al distinguir que tal derecho se puede ejercer con relación al motor de búsqueda o el editor que primero publicó la noticia y que el tratamiento en ambos casos puede ser diferente.[32]

iv. *Derecho la limitación del tratamiento:* Consagrado en el artículo 18 del Reglamento, consiste en el derecho que le asiste a toda persona para solicitar que sus datos solo se utilicen de manera limitada, cuando se presenten alguna de las condiciones establecidas en la norma citada[33].

---

29 Artículo 16 del RGPD.

30 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CA0131&from=FR

31 https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido#:~:text=El%20derecho%20de%20supresi%C3%B3n%20('pertinencia%20previstos%20en%20la%20normativa.

32 En una publicación sobre el Derecho al Olvido, contenida en la página de la AEPD, se pregunta "¿Puedo ejercerlo frente al buscador sin acudir previamente a la fuente original? Sí. Los motores de búsqueda y los editores originales realizan dos tratamientos de datos diferenciados, con legitimaciones diferentes y también con un impacto diferente sobre la privacidad de las personas. Por eso puede suceder, y de hecho sucede con frecuencia, que no proceda conceder el derecho frente al editor y sí frente al motor de búsqueda, ya que la difusión universal que realiza el buscador, sumado a la información adicional que facilita sobre el mismo individuo cuando se busca por su nombre, puede tener un impacto desproporcionado sobre su privacidad. (…)

   Si lo ejerzo frente a un buscador, ¿la información desaparecerá de internet? No. La sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014 determina que sólo afecta a los resultados obtenidos en las búsquedas hechas mediante el nombre de la persona y no implica que la página deba ser suprimida de los índices del buscador ni de la fuente original. El enlace que se muestra en el buscador sólo dejará de ser visible cuando la búsqueda se realice a través del nombre de la persona que ejerció su derecho. Las fuentes permanecen inalteradas y el resultado se seguirá mostrando cuando la búsqueda se realice por cualquier otra palabra o término distinta al nombre del afectado". Tomado de https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido#:~:text=El%20derecho%20de%20supresi%C3%B3n%20(',pertinencia%20previstos%20en %20la%20normativa.

33 "a) el interesado impugne la exactitud de los datos personales en un plazo que permita al responsable verificar la exactitud de los mismos;

   b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

   c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el intere-

v. *Derecho a la Portabilidad*[34]*:* Consiste en el derecho que tienen las personas a solicitar que, los datos personales que han transmitido a una empresa o responsable sean transferidos a otra persona. Para dicha devolución, el RGPD exige que sea hecha en un formato utilizado habitualmente y de lectura automática.

vi. *Derecho de Oposición:*[35] De conformidad con este derecho, el usuario tiene el derecho a oponerse al tratamiento de sus datos, por motivos personales. Ante tal solicitud, el responsable del tratamiento deberá dejar de dejar de tratarlos, a menos que evidencie "… motivos legítimos imperiosos para el tratamiento, que prevalezcan sobre los intereses, los derechos y las libertades del interesado…".

Señala textualmente el RGPD que "…el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia". Puede oponerse también cuando el tratamiento tenga fines históricos o estadísticos, pero no surgirá efecto si tiene como misión el interés público.

Este derecho se debe ejercer de manera directa, por parte del usuario o interesado, mediante el envío de una solicitud por escrito de oposición al tratamiento de datos personales, al responsable del tratamiento, indicando los motivos y la base legal del RGPD para ejercer tal oposición.

e. Delegado de Protección de Datos

El RGPD creó la figura del "delegado de protección de datos", quien tiene la responsabilidad de verificar y supervisar el cumplimiento de la normativa por parte del responsable; en este sentido, tiene competencias para coordinar y controlar las acciones de éste en el tratamiento de los datos personales; así como incluso cooperar con la autoridad responsable en materia de protección de datos del país o ser el enlace entre el responsable y ésta.

El nombramiento de un delegado no es obligatorio para todo aquél que tenga una página o plataforma o presencia en internet, sino que el artículo 37 lo exige en tres supuestos[36]. El delegado puede ser alguien de la organización con conocimiento en la materia o muchas veces son designados terceros, especialistas en el área, mediante la suscripción de un contrato de servicios.

f. Notificación adecuada en caso de violación de datos

El RGPD exige que toda violación de datos, divulgación ilegal o incluso accidental a otras personas no autorizadas, o su indisponibilidad temporal[37], es preciso notificarlo a la autoridad

---

sado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado".

34 Artículo 20 del RGPD

35 Consagrado en el artículo 21 del RGPD.

36 De acuerdo con la norma citada, se exige en los siguientes supuestos:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

37 El considerando 85 enumera los posibles daños que puede causar tal filtración, incluyendo los siguientes eventos: "pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudo-

de protección de datos competente en un plazo de 72 horas, contados a partir del momento en que se conozca la infracción, así como a los interesados en caso de que represente un riesgo para sus derechos y libertades individuales.

g. Infracciones

El incumplimiento de la normativa impone sanciones muy altas, ya que éstas pueden ascender hasta los 20 millones de euros o hasta el 4 % del volumen de ventas mundial del ejercicio fiscal anterior.

II. SITUACIÓN EN VENEZUELA

En nuestro país, al día de hoy carecemos de una normativa general que regule, como lo hace el RGPD, el uso y garantice la protección de datos personales. Sin embargo, tenemos diversas normas en varios instrumentos legislativos, que nos permiten afirmar que la protección de datos personales en nuestro país está garantizada como derecho autónomo.

1. *La Constitución*

La Constitución, en su artículo 28 consagra -como un derecho fundamental del individuo- a la protección de datos personales, con un carácter distinto e independiente al de la privacidad y la intimidad, mediante el ejercicio de la acción constitucional de *habeas data*[38]. De manera que, se puede afirmar que nuestra carta magna, por una parte, consagra al derecho en estudio como un derecho autónomo[39], y por la otra, reconoce a los derechos ARCO, como garantías vinculadas con su ejercicio. Siendo así, podemos señalar que contamos con el soporte constitucional necesario, a los fines de avanzar en todo el desarrollo legislativo que se requiere, para entrar en los estándares de la normativa existente en el derecho comparado en esta materia, como es la europea antes analizada.

Por su parte, el artículo 60, si bien no incluye expresamente en la enumeración de los derechos allí consagrados -concretamente, el honor y la intimidad personal y familiar- a la protección de datos personales, sí establece que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos…". Por lo que permite establecer limitaciones legales al acceso de datos, a los fines de salvaguardar las garantías antes enumeradas.

2. *La Ley Orgánica del Tribunal Supremo de Justicia*

También están reconocidos dichos derechos y consagrados a nivel legislativo, concretamente en el artículo 167 de la Ley Orgánica del Tribunal Supremo de Justicia,[40] el cual establece el derecho que tiene toda persona a "… a conocer los datos que a ella se refieran,

---

nimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional".

38 La norma citada se refiere al *Habeas Data* y pauta que: "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".

39 Al referirse a "autónomo" se quiere resaltar que se erige como un derecho independiente de otros, como son el derecho a la intimidad, a la propia imagen, a la confidencialidad, y a la reputación, consagrados en el artículo 60, a los fines de brindarle entidad propia, hacia donde están avanzando el derecho comparado.

40 Gaceta Oficial N° 6.684 Extraordinario del 19 de enero de 2022.

así como su finalidad, que consten en registros o bancos de datos públicos o privados; y, en su caso, exigir la supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de los datos cuando resulten inexactos o agraviantes".

Sin embargo, el artículo impone, como paso previo para interponer el recurso, la obligación de acudir al administrador de la base de datos en cuestión para formular la petición de corrección, supresión o modificación, y solo ante su negativa o inacción, luego del transcurso de 20 días hábiles, el agraviado podrá acudir a los tribunales e interponer el recurso en cuestión.

3. *Ley de Delitos Informáticos*

El artículo 20 de la Ley de Delitos Informáticos[41] tipifica como "violación de la privacidad de la data o información de carácter personal" el acto de apoderarse, utilizar, modificar o eliminar 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.

Por otra parte, el artículo 22 también castiga la revelación, difusión o cesión de hechos, imágenes, audio, data o información obtenida por violación de la privacidad de la data, imponiéndole a tal conducta punitiva, pena de prisión y multa[42].

4. *La Ley de Infogobierno*

Por último, la Ley de Infogobierno[43]que regula el uso de las tecnologías de información por parte de todos los órganos del Poder Público en la gestión pública y en los servicios que brinda y en sus relaciones con los administrados y ciudadanos, consagra que el uso de dicha tecnología está limitado por "…la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas…" [44]e impone a todos los órganos la obligación de notificar a los ciudadanos, sobre diversos aspectos vinculados con la protección de datos personales, como son:

> "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"[45].

De manera que, los derechos ARCO también están reconocidos en este cuerpo normativo, y en consecuencia se erigen como unos derechos exigibles, por parte de los ciudadanos, frente a la administración y las relaciones surgidas entre ellos, a través de las tecnologías de la información.

---

41 Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.

42 El artículo 22 señala, a la letra: "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 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".

43 Gaceta Oficial N° 40.274 del 17 de octubre de 2013.

44 Artículo 25 de la Ley.

45 Artículo 75.

5. *Sentencia de la Sala Constitucional del Tribunal Supremo de Justicia del 4 de agosto de 2011, que fija interpretación vinculante respecto del derecho a la protección de datos personales*

Por último, debemos hacer referencia a la sentencia de la Sala Constitucional, dictada con ocasión del recurso de nulidad por inconstitucionalidad incoado por el ciudadano Germán José Mundaraín Hernández y otros, contra "el artículo 192 del Decreto N° 1.526 con Fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras, publicado en la Gaceta Oficial N° 5.555 del 13 de noviembre de 2001 y, por vía de consecuencia, '*los artículos 1, 6 y 8 de la Resolución N° 001-06-98, publicada en la Gaceta Oficial N° 36.484, de fecha 26 de junio de 1998, emitida por la Junta de Emergencia Financiera'* - artículo 90 del vigente Decreto con Rango, Valor y Fuerza de Ley de Reforma Parcial de la Ley de Instituciones del Sector Bancario[46] (Caso SICRI[47]) en la cual la Sala Constitucional fijó -con carácter vinculante- los principios que deben cumplir, ".. toda normativa o sistema sobre datos personales que contenga información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables", las cuales deberán garantizar nueve principios[48]:

i. *"El principio de la autonomía de la voluntad*. Lo cual comporta la necesaria existencia de un consentimiento previo, libre, informado, inequívoco y revocable para el uso o recopilación de datos personales".

ii. *"El principio de legalidad*. La recopilación de datos personales comporta que la limitación a la autodeterminación informativa sea el resultado de normas de rango legal".

iii. *"El principio de finalidad y calidad*. La recopilación de datos personales debe responder a finalidades, motivos o causas predeterminadas, que no sean contrarias al ordenamiento jurídico constitucional y sectorial, lo cual se constituye además en un requisito necesario para obtener un consentimiento válido".

iv. *"El principio de la temporalidad o conservación*. La conservación de los datos se extiende hasta el logro de los objetivos para las cuales han sido elaborados, vale decir, que justificaron su obtención y tratamiento".

v. "*El principio de exactitud y de autodeterminación*. Los datos deben mantenerse exactos, completos y actualizados, respondiendo a la verdadera situación de la persona a la que se refieran".

vi. *"El principio previsión e integralidad*. La tutela de los derechos fundamentales vinculados con la recopilación de datos personales debe plantearse inicialmente en relación con la protección del individuo contra la recopilación, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona".

vii. *"Principio de seguridad y confidencialidad*. Corolario de los anteriores principios, es la necesaria garantía -según los casos- de confidencialidad, de no alteración de datos por terceros y del acceso a tales datos por parte de las autoridades competentes de conformidad con la ley".

viii. *"Principio de tutela*. Al respecto, cabe reiterar que "en sentido amplio el derecho a acceder a la información y al conocimiento del fin (…) se trata de derechos que han de ser ejercidos previamente (incluso extrajudicialmente y tal vez hasta por vía administrativa en algunos casos) ante el recopilador real o supuesto, por lo que la lesión al titular de los derechos nace de ese ejercicio extrajudicial fallido".

---

46 Expediente Nº AA50-T-2004-2395. Consultada el 18 de noviembre de 2022 en: https://ve.microjuris.com/getContent?page=fullContent.jsp&reference=MJ-S-127616-VE&links=%5b042395%5d

47 Sistema de Información Central de Riesgos

48 Por ser muy extenso el desarrollo de la sentencia de estos principios, se incluye solo su enunciación.

ix. *"Principio de Responsabilidad*. La violación del derecho a la protección de datos personales debe generar de conformidad con el ordenamiento jurídico aplicable, sanciones de tipo civil, penal y administrativas, según sea el caso".

De su lectura, se observa que la Sala Constitucional desarrolló ampliamente el ámbito de esos principios, incorporando por esta vía los derechos ARCO, e incluso, ciertas exigencias consagradas posteriormente en el RGPD, como, por ejemplo, la de contar con un "consentimiento previo, libre, informado, inequívoco y revocable[49]". Cabe señalar que, a tenor de tal exigencia, pareciera que todas las plataformas, aplicaciones y demás instrumentos digitales, a las cuales se tenga acceso en el país, deben requerir -al igual que ocurrió en la UE- la aceptación afirmativa y previa, antes de navegar, siendo insuficiente, las pestañas marcadas por defecto, ya que en ese caso, el consentimiento dado no cumpliría con tales requisitos.

También llama la atención que, conforme la Principio de la Tutela, la obligación de acudir en primer término, al recopilador de datos y solo, si tal reclamo ha sido infructuoso, es que nacerá la lesión y, en consecuencia, el derecho a reclamar tal violación y su resarcimiento.

CONCLUSIÓN

Como se observa, si bien contamos con algunas normas diseminadas en diversos instrumentos legales que consagran la protección de los datos personales como un derecho en sí mismo, se requiere de una ley que integre y regule tal protección, en sus diversos aspectos, tanto frente al uso y tratamiento por parte de particulares, como por los órganos de los poderes públicos y que brinde garantías suficientes a los fines de salvaguardar dicha protección como un derecho fundamental y autónomo.

Por otra parte, las limitaciones y violaciones de las que muchos venezolanos han sido víctimas a lo largo de los últimos años por razones políticas, en materia de protección de datos personales, los cuales han sido obtenidos de manera ilegal e inconstitucional, impone también la necesidad de que se dicte dicha normativa y más importante aún, que se cuente con órganos jurisdiccionales independientes que pueden velar por esa protección y de ser el caso, castigar a los responsables.

BIBLIOGRAFÍA

AZNAR, Javier, "*ePrivacy, para asegurar la privacidad en las comunicaciones electrónicas*", consultado en https://www.tendencias.kpmg.es/2018/07/normativa-eprivacy-privacidad-comunicaciones-electronicas/

"Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: "*Una estrategia europea para los datos*" (Bruselas, 19 de febrero de 2020) Pag., 4. Consultado en https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

"*Derecho de supresión ('al olvido'): buscadores de internet*", 14 de Junio de 2022, Agencia Española de Protección de Datos, consultado en https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido#:~:text=El%20derecho%20de%20supresi%C3%B3n%20(',pertinencia%20previstos%20en%20la%20normativa

GARCÍA, Carilym: "*Habeas Data como mecanismo de protección del derecho al acceso a la información personal en el derecho constitucional venezolano*", Revista Electrónica Multidisciplinaria, Vol.1 Nº1. Septiembre-Diciembre 2018, p., 67-83, consultado en https://produccioncientificaluz.org/index.php/dataciencia/article/view/29747

[49] Ver principio de la autonomía de la voluntad.

"*Informe Privacidad y datos personales en Venezuela: Una aproximación a la legislación y práctica vigentes*", Informe Enero 2022, realizado por Espacio Público. Consultado en https://espaciopublico.ong/wp-content/uploads/2022/01/Informe-Privacidad-y-datos-personales-en-Venezuela-Enero-2022.pdf

"La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del Comité Europeo de Protección de Datos", Agencia Española de Protección de Datos, 28 de julio de 2020, consultado en https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-actualiza-guia-cookies

"La aplicación de la ley de cookies europea en España", Digital Guide Ionos, 16 de febrero de 2022, consultado en https://www.ionos.es/digitalguide/paginas-web/derecho-digital /la-ley-de-cookies-y-su-aplicacion-en-espana/

"*La ley de cookies de la UE (Directiva ePrivacy*)", consultado en https://www. cookiebot.com/es/ley-de-cookies/

"*La normativa sobre protección de datos en la Unión Europea*" Consultado en: https://www.lleytons.com/conocimiento/la-proteccion-de-datos-personales/.

"*La Unión Europea trata de poner orden al caos de las cookies*" La Vanguardia, Barcelona, 8 de mayo de 2020. Consultado en https://www.lavanguardia.com/vida/20200105 /472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html

"*Ley de cookies de la UE y aplicación en España*", consultado en https://protecciondatos-lopd.com/empresas/ley-cookies/

MOLINS RENTER, Albert, "*La primera ley de privacidad en línea de EE.UU. entra en vigor en California*", Barcelona, 5 de enero de 2020, consultado en https:// www. lavanguardia.com/vida/20200105/472713380363/california-estados-unidos-privacidad-consumidor-e-commerce-comercio-electronico.html

"*Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas*" consultado en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010.

"¿Qué es la Directiva sobre la privacidad electrónica?" Consultado en: https://www.cloudflare.com/es-es/learning/privacy/what-is-eprivacy-directive/

"*Reglamento ePrivacy: ¿qué hay que saber?*" Digital Guide Ionos, 9 de febrero de 2022, consultado en https://www.ionos.es/digitalguide/paginas-web/derecho-digital/eprivacy-reglamento-sobre-privacidad-electronica-en-la-eu/

"*Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* (Texto pertinente a efectos del EEE)" consultado en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

TSUKAYAMA, Hayley "Facebook's privacy changes look different for Europeans and Americans", 20 de abril de 2018, consultado en: https://www.washingtonpost.com/news/the-switch/wp/2018/04/20/facebooks-privacy-changes-look-different-for-europeans-and-americans/

"*Vulneración del derecho a la privacidad y protección de datos en Venezuela*" La Voz de América, 31 de enero de 2022.https://www.vozdeamerica.com/a/venezuela-vulneracion-derecho-privacidad-proteccion-datos/6419822.html