ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Licitud de las Pruebas obtenidas en Redes Sociales ● Pág.: 232 – 262

LICITUD DE LAS PRUEBAS OBTENIDAS EN REDES SOCIALES

LEGALITY OF THE PROOFS OBTAINED IN SOCIAL MEDIA

Gloria Elizabeth La Paz Contreras Bez[1]

https://doi.org/10.53766/ESDER/2022.01.01.08

Fecha de Recepción: 04 de diciembre de 2021 **Fecha de Aprobación:** 20 de enero de 2022

RESUMEN

La información es poder. Los medios electrónicos utilizados contienen un cúmulo de información privada de las personas que interactuamos en redes sociales; recientemente se ha generado una discusión entre sí dejar de utilizar algunas redes, o migrar a otras, debido a los cambios en las políticas de privacidad. Políticas que no son más que contratos de adhesión que suscribimos virtualmente con las empresas al dar un clic de aceptación. El objetivo de este artículo es analizar, a través de la investigación documental, los problemas que se presentan por la obtención de pruebas ilícitas, violando la intimidad de las personas, a través de las redes sociales, con el simple hecho de suscribir el contrato de adhesión obligatorio y proponer el estudio a fondo de este tema, no sólo para futuras investigaciones y reformas legales que limiten, regulen y rijan en la materia, sino para identificar también todas las posibles soluciones.

Palabras Clave: Pruebas Ilícitas, Redes Sociales, Intimidad y Contratos de Adhesión.

ABSTRACT

Information is power. The electronic media that we use are an accumulation of private information those of us which we interact on social networks, recently there has been a discussion between whether to stop using some social networks, or to migrate for others, due to changes in policies. Policies that isn´t more than adhesion contracts, that we sign virtually with the social network company when you click the accept button. The objective of this short article is to analyze through documentary research, the problems that can arise from obtaining illegal evidence violating people's privacy, through social networks, by the simple fact of signing the contract of obligatory adherence and propose the in-depth study of this issue, not only for future research, laws or legal reforms that limit, regulate and govern the matter, but also to identify all possible solutions.

Key Word: Illegal Tests, Social Networks, privacy and Adhesion contracts.

[1] Abogada Egresada de la Universidad de Los Andes (ULA): Mención *Magna Cum Laude*. Profesora en Pre-Grado de Derecho Probatorio y Procesal Civil I. Profesora de Post-Grado en Derecho Probatorio (UBA). Especialista en Derecho Procesal (UCV). Coordinadora General de la Facultad de Ciencias Jurídicas y Políticas. Abogado en Ejercicio. **Correo Electrónico**: Prof.gloriacontreras@gmail.com.

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

INTRODUCCIÓN

La información es poder. El internet y los medios electrónicos que utilizamos hoy en día no sólo son un cúmulo de información masiva mundial, sino también un cúmulo de información privada de las personas que interactuamos diariamente con los medios de comunicación digitales y las redes sociales, aún más hoy en día debido a la crisis mundial por la pandemia del Covid-19 y al confinamiento prácticamente obligatorio en todo el mundo y a la necesidad que tenemos de estar conectados, informados y actualizados.

Recientemente se ha generado una discusión entre sí dejar de utilizar algunas redes sociales, o migrar otras, debido a los cambios en las condiciones de uso y políticas de privacidad, que no son más que contratos de adhesión que suscribimos virtualmente con la empresa al dar un clic de aceptación, entendiendo que, en la mayoría de los casos, si no damos ese clic, no podremos seguir utilizando dicha red social, tomando en cuenta que la mayoría de los usuarios de estas redes dan ese clic incluso sin leer, y que esto se traduce, en que toda la información que los usuarios manejan en redes sociales o aplicaciones conectadas descargadas en nuestros medios electrónicos, es recopilada, comparada, conectada y vendida a las empresas para ofertar publicidad, convirtiéndonos en productos, haciendo pública la recopilación de metadatos de los usuarios, y así nos estudian, nos exhiben y nos venden al mejor postor, sin que autoricemos realmente todo eso, hasta ahí, ya es grave, pero ¿Qué pasa si el postor no es un empresa de publicidad, sino es otra empresa con otras intenciones de control, o dominio? O es el estado que quiere manejar absolutamente todos estos datos con otros fines abusando de su autoridad.

Los términos de privacidad de las redes sociales, hasta hace algunos años, permitían la posibilidad de negar esta autorización, pero las últimas reformas nos impiden no estar de acuerdo, es decir, estamos obligados a aceptar, puesto que la no aceptación de los nuevos términos de privacidad, supone que el usuario no podrá usar de nuevo la red social.

De igual forma, hay problema cuando estas políticas violan la privacidad o intimidad de las personas y generan material, información, pruebas o medios que pueden convertirse en material usado para ir en contra a una persona en

cualquier ámbito, sobre todo tomando en cuenta, como señalamos anteriormente, que la mayoría de los usuarios de la *Web* o un alto porcentaje de ellos, no lee detenidamente las políticas o términos de uso, y no sólo eso, sino que aun leyéndolas, no tiene más opción que aceptarlas, puesto que en caso de no hacerlo, el usuario no la podrá seguir utilizando; como también hemos señalado antes, no se trata más que de un contrato de adhesión que, cada vez más, incluye cláusulas en las que autorizamos a las compañías el uso de nuestra información privada, dejando a su discreción compartir dicha información a través de inteligencia artificial a diferentes anunciantes y redes de empresas digitales asociadas o a cualquier otro.

La información que estamos dejando a criterio de las grandes empresas incluye nuestros nombres, profesión, edad, estado civil, número telefónico, los números de teléfonos de nuestros amigos, los nombres de nuestros amigos, las fotos de perfil, la última conexión o uso de la aplicación, si se encuentra "en línea," el tiempo que se dedica a las redes sociales, con que personas interactuamos más, la información del teléfono, que sistemas operativos y redes móviles usamos, la carga de batería que tiene el móvil, la información que otros comparten sobre ti y aún más grave nuestra ubicación geográfica exacta y con quien nos relacionamos y reunimos físicamente, en qué lugar y cuanto tiempo, cuánto tiempo pasamos en determinados lugares, información valiosa y delicada.

Esto ya es grave, pero aún más lo es el hecho que va abriendo la puerta para otras violaciones y para que cada vez se almacene y comparta más información, porque aunque todavía los mensajes de texto están cifrados o encriptados y las comunicaciones son en teoría, inviolables, salvo ciertos casos y en cumpliendo ciertas formalidades legales, es cuestión de tiempo para que se encuentre la forma de cifrarlos y venderlos o compartirlos, sólo con el hecho de cambiar de nuevo las políticas de privacidad.

En este orden de ideas, se han divulgado memes o chistes acerca del tema de la información que manejan las empresas digitales, mediante la interacción que se genera en ellas, a través de la inteligencia artificial, como la que vemos a continuación:

"Buenos días!
- Hola, ¿Pizza Hut?

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

- No, señor. Pizzería Google.
- Ah, discúlpeme... marqué mal
- No señor, marcó bien, Google compró la cadena Pizza Hut.
- Ah, bueno... entonces anote mi pedido, por favor...
- ¿Lo mismo de siempre?
- ¿Y usted cómo sabe lo que pido yo?
- Según su calle y su número de apartamento y las últimas 12 veces, usted ordenó una napolitana grande con jamón.
- Sí, esa quiero...
- ¿Me permite sugerirle una pizza sin sal, con ricota, brócoli y tomate seco?
- ¡No! Detesto las verduras.
- Su colesterol no es bueno, señor.
- ¿Y usted cómo sabe?
- Cruzamos datos con el IVSS y tenemos los resultados de sus últimos 7 análisis de sangre.
Acá me sale que sus triglicéridos tienen un valor de 180 mg/DL y su LDL es de...
- ¡Basta, basta! ¡Quiero la napolitana!
¡Yo tomo mi medicamento!
- Perdón, señor, pero según nuestra base de datos, usted no la toma regularmente. La última caja de Lipitor de 30 comprimidos que usted compró en la Farmatodo fue el pasado 2 de Diciembre a las 3:26 p.m.
- ¡Pero compré más en otra farmacia!
- Los datos de sus consumos con tarjeta de crédito y tarjeta de débito no lo demuestran.
- ¡Pagué en efectivo, tengo otra fuente de ingresos!
- Su última declaración de ingresos no lo demuestra. No queremos que tenga problemas con el SENIAT señor...
- ¡Ya no quiero nada!
- Perdón, señor, sólo queremos ayudarlo.
- ¿Ayudarme?
- ¡Estoy harto de Google, Facebook, Twitter, WhatsApp, Instagram!
¡Me voy a ir a una isla sin internet, cable, ni telefonía celular!
- Comprendo, señor, pero aquí me sale que su pasaporte está vencido desde hace 5 meses…" ☺

A pesar de lo gracioso que puede parecer, es una realidad que la inteligencia artificial conecta nuestra información, para muestra de eso, tenemos la increíble cantidad de publicidad que aparecen en nuestras redes, y no se trata de un mago que te muestra lo que piensas o quieres ver, simplemente se trata de la información que se genera por la interacción con el internet, específicamente

en redes sociales conectadas entre sí y conectadas con nuestros medios electrónicos.

Lamentablemente, el Derecho no va a la par de la tecnología. Las leyes y el Derecho siempre va pasos atrás de ella, en mayor medida en nuestro país, las preguntas que surgen para los abogados son: ¿Basta el clic de aceptación para dejar toda nuestra información y privacidad en manos de los dueños de las empresas digitales?, ¿La obligación que generan las redes sociales para la suscripción de las nuevas políticas, viola el derecho de privacidad?, ¿Cómo protegemos nuestra información?, ¿Existen mecanismos para protegerla jurídicamente? O ¿Es necesario dejar de utilizarlas y buscar otras alternativas?, ¿Qué sucede con las pruebas que se obtengan a través de la inteligencia artificial?, ¿Son válidas? y ¿Cómo se promueven legal y lícitamente?

Así las cosas, es importante analizar hasta qué punto, la obtención de toda esta información es lícita, aún más en el caso que pueda ser utilizada en juicio o por las autoridades judiciales, administrativas, de investigación; información que evidentemente se usa en la actualidad, pero, ¿Qué limitaciones debe tener?, ¿Es necesaria la orden de un juez para utilizarla o para que las compañías la proporcionen?, ¿Sólo con el hecho de aceptar las políticas de privacidad, dejamos en manos de la compañía esa información para que pueda ser utilizada por cualquiera o por el que pague por ella? Y en el caso de las instituciones del Estado que almacenan información de los usuarios ¿Cómo debe ser utilizada esa información?

1_. Licitud de las Pruebas Obtenidas en Redes Sociales.

Antes de analizar el problema, debemos tener claros algunos conceptos básicos. En primer lugar, a que se refiere cuando se habla de la prueba ilícita, aunque Cabrera (2010:5) la llama también “prueba ilegítima” Pág. 5. Las pruebas ilícitas son medios de prueba que se obtienen a través de la vulneración de derechos fundamentales, a diferencia de las pruebas irregulares, en las que se viola el procedimiento debido. Las pruebas ilícitas, son pruebas que pueden ser legales y pertinentes, pero no son válidas por la forma en la que se obtienen,

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

violentando derechos o libertades fundamentales, en el caso que se atañe, violando el derecho de privacidad e intimidad de las personas, bajo una dudosa suscripción de un contrato de adhesión, que no es más que, como dice el diccionario jurídico de Manuel Ossorio (1999):

> Una típica y cada vez más frecuente modalidad de contratación, que se caracteriza de que es una de las partes la que fija las cláusulas o condiciones, iguales para todos, del contrato, cuya celebración se propone, sin que quienes quieran participar en él tengan otra alternativa que aceptarlo o rechazarlo en su totalidad, es decir adherirse o no a los términos del contrato preestablecido, sin posibilidad de discutir su contenido. Pág. 234.

Teniendo todas estas características en cuenta, los contratos de políticas de privacidad son contratos de adhesión modernos, pero la dificultad principal es demostrar la voluntad, pues a pasar de existir las firmas electrónicas, la suscripción de estas políticas de privacidad no se firma, ni con una firma electrónica, sino basta el clic para que las redes tengan derecho a la información, vulnerando derechos fundamentales a la privacidad e intimidad, sin estar realmente claro, cuál es el verdadero consentimiento del usuario, por lo que es necesario crear vías, a través de las cuales se proteja al consumidor, mediante la prohibición de las cláusulas abusivas, que son nulas de pleno Derecho. Y a través de la vigilancia por parte de las instituciones públicas de la actuación de las empresas, pero para eso son necesarias leyes o políticas de Estado que regulen y controlen estos contratos, negociando y discutiendo previamente las cláusulas e incluso son necesarios organismos gubernamentales a los cuales acudir en caso de inobservancia o violación de cláusulas, y que pongan limitaciones a estos contratos.

Las redes sociales son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. A través de ellas, se crean relaciones entre individuos o empresas de forma rápida, sin jerarquía o límites físicos. Un gran número de personas de muy diversos grupos etarios pertenece a diferentes redes sociales, o utiliza internet de muchas maneras, para hacer amigos, relacionarse con personas, hacer negocios, comprar

y vender por internet, es decir, las redes sociales fueron creadas para reunir grupos de personas con intereses comunes, pero además son perfectas para hacer negocios o lo que llamamos comercio electrónico.

También existe en internet, según lo que cita Rico (2005) lo que se llama "*cookies:*"

> Estas son pequeños ficheros de datos generados en el computador del usuario en forma de archivos de texto, gracias a las instrucciones que los servidores Web envían a los programas de las computadoras, permitiendo el acceso a información del usuario sobre sus datos personales o sobre cualquier otra circunstancia (fecha, hora de visita del sitio Web, contenidos visitados, número de visitas) ya que pueden ser leídos desde el exterior, gracias al interfaz del servidor. Si un administrador de un servidor utiliza dicha información puede vulnerar la intimidad del usuario, de ahí la necesidad de establecer una regulación. En Venezuela el artículo 38 de la Ley de Protección al Consumidor y Usuario (2004) impone a los proveedores el deber de informar a los consumidores cuando el suministro de datos en operaciones de comercio electrónico sea parte integrante de su modelo de negocio. Pág. 273 y 274.

Tenemos en juego, como hemos comentado anteriormente la violación de derechos fundamentales, específicamente el derecho a la intimidad o privacidad como personas, Mejan (1994) define la intimidad como:

> El conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que el ser humano desea mantener reservado para sí mismo, con libertad de decidir a quién le da acceso, imponiéndose a todos los demás la obligación de respetar y que sólo puede ser obligado a develar, en casos justificados cuando la finalidad perseguida por la develación sea lícita. Pág. 87.

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

La Declaración Universal de los Derechos Humanos (1948), en su artículo 12, establece que:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra esas injerencias y ataques.

Y la Convención Americana sobre Derechos Humanos (1969) -Pacto de San José-, en el artículo 11, se refiere a que:

> Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto no deberá ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, domicilio, correspondencia, ni deberá sufrir ataques ilegales a su honra o reputación; también, establece el derecho de la persona a ser protegida por la ley contra esas injerencias o ataques.

El derecho fundamental a intimidad o privacidad, a pesar que es muy difícil de definirlo con precisión, pues depende de múltiples factores de tiempo y lugar, sin embargo, dentro de esta esfera de vida privada podemos considerar a las relaciones personales y familiares, afectivas y de filiación, las creencias y preferencias religiosas, convicciones personales, inclinaciones políticas, condiciones personales de salud, identidad y personalidad psicológica, inclinaciones sexuales, comunicaciones personales privadas por cualquier medio, incluso algunos llegan a incluir la situación financiera, económica, personal y familiar, por lo tanto, incluye el derecho a la inviolabilidad del domicilio, el derecho a la inviolabilidad de correspondencia, el derecho a la inviolabilidad de las comunicaciones privadas, el derecho a la propia imagen, el derecho al honor, el derecho a no participar en la vida colectiva y a aislarse voluntariamente, el derecho a no ser molestado y por supuesto, en nuestro caso, el derecho a la privacidad informática.

En este particular, señala Rico (2005) que:

> Los datos que son compartidos en la red relativos a identificación, sexo, edad, profesión, domicilio, números de tarjetas, gustos, preferencias, formas de pago, comportamiento ante determinado producto o servicio, estos datos transmitidos que pueden ser usados con fines distintos para los que fueron enviados, por ejemplo, cuando hacemos una compra por internet en las diferentes páginas que existen, en ocasiones, deben llenarse algunos formularios de pedido, incluso encuestas del servicio y preferencias, información que permite la creación de perfiles y estándares automatizados, mediante la categorización de sujetos para luego utilizarlos con fines comerciales de publicidad y mercadeo, causando graves perjuicios a la esfera íntima del individuo. Pág. 259.

En la Constitución nacional (1999) el artículo 28 consagra:

> Toda persona tiene 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 a 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.

Este procedimiento se conoce como *Hábeas Data* y no es más que como lo señala Rico (2005):

> La facultad de cualquier persona de solicitar ante el tribunal competente la actualización, rectificación o destrucción de los datos e información sobre sí mismos o sobre sus bienes, en caso que fueren erróneos o afecten ilegítimamente sus derechos fundamentales, comprende dos aspectos: 1. El derecho de las personas a acceder a la información registrada en las distintas bases de datos con la finalidad de ejercer un control y 2. El derecho a interponer una acción dirigida a exigir la actualización, rectificación o destrucción de aquella información que le afecte directamente. Pág. 262.

La acción de *Hábeas Data* está prevista en la Ley Orgánica del Tribunal Supremo de Justicia, específicamente en el Capítulo IV, denominado "*Del Habeas Data,*" que forma parte del Título X denominado Disposiciones Transitorias de dicha Ley publicada en Gaceta Oficial de la República Bolivariana de Venezuela N° 39.552 del 1 de Octubre de 2010. Así el artículo 169 establece, que: "*la acción de hábeas data se presentará por escrito ante el tribunal de municipio con competencia en lo Contencioso Administrativo y con competencia territorial en el domicilio del o de la solicitante*."

Pese a ello, es el caso que en Venezuela hasta la fecha no han sido creados dichos tribunales, por lo que debe remitirse a la Ley Orgánica de la Jurisdicción Contencioso Administrativa publicada el 16 de Junio de 2010, cuya disposición Transitoria Sexta dispone: *"…hasta tanto entren en funcionamiento los Juzgados de Municipios de la jurisdicción contencioso administrativa, conocerán de las competencias atribuidas por esta Ley a dichos tribunales, los Juzgados de Municipio (…)."* Por lo tanto, hoy en día los tribunales competentes para interponerlo son los Juzgados de Municipio Civiles.

La Ley Orgánica del Tribunal Supremo de Justicia, también precisa en su artículo 167 que "*los ciudadanos tienen derecho a conocer la información que sobre ellos se refiera y esté contenida en los archivos de los bancos públicos y privados, además podrá solicitar la confidencialidad*."

Los derechos que tutelan el *Hábeas Data* son el derecho a la información, el derecho a la intimidad, el derecho a la identidad o el derecho a la

autodeterminación informática. En este sentido, parte de la doctrina sostiene que, debido el nacimiento de la informática y con ella el procesamiento de datos, existe la posibilidad de registrar una gran cantidad de datos sobre las personas que permiten reconstruir sus detalles íntimos y con ello afectar su vida privada o intimidad.

Dentro de este contexto, consideran al *Hábeas Data* como un mecanismo tendiente a proteger ese espacio íntimo de la persona, es decir, como lo dice Ávila Hernández y otros (2008:319) *"una herramienta para defenderse de las intromisiones, tanto por parte del Estado como de los particulares."*

Así mimo, el artículo 48 de la Constitución de la República Bolivariana de Venezuela (1999) señala:

> Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.

Y por último, el artículo 60 también de nuestra carta magna reza que:

> 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.

Así las cosas, la acción de *Habeas Data* debe interponerse alegando estos artículos, específicamente el artículo 60 constitucional en concordancia con el artículo 28, antes citado. Estos artículos consagran nacionalmente los que las legislaciones extranjeras llaman derecho al olvido o derecho de supresión, que es un concepto relacionado con el *habeas data* y la protección de los datos personales,

así como el derecho al secreto, para así poder solicitar a los tribunales competentes la suspensión, bloqueo, destrucción, eliminación de la información que se considera cierta, pero obsoleta por el transcurso de tiempo, porque es errónea, está alterada, o fue obtenida de manera ilícita, o causa daño, o cuando se haya retirado el consentimiento para utilizarla. No obstante, en Venezuela no existen leyes de carácter especial o procedimental, tampoco muchos precedentes acerca de este tema, solamente unos primeros intentos.

Por ejemplo, en nuestro país existe algunos antecedentes de esta acción, específicamente la sentencia N° 10 de la Sala Constitucional del Tribunal Supremo Justicia de Venezuela de fecha 01 de Marzo 2016, en la que Tomás Mariano Adrián Hernández solicito el recurso de *Habeas Data* para anular, corregir, eliminar y sustituir de los datos, tanto públicos como privados la vinculación de su nombre, sobre los cuales la parte actora alega un desfase, pues no corresponden a la realidad y condición de ser humano actual, ya que se transformaron por el transcurso de los años debido a nuevos actos, por lo que pide se elimine ese nombre y vinculación con su persona, puesto que se trata de una mujer transgénero, con una nueva identidad, en este caso, el tribunal admitió la medida innominada.

De igual forma, se intentó el *Habeas Data* para invocar el derecho al olvido, ante la Sala Constitucional interpuesta por Elías Pernía, contra el entonces diputado Luis Tascón, por la presunta divulgación a través del sitio electrónico www.luistascon.com de información violatoria de su derecho al honor y a la reputación constituida por un archivo de datos de personas que participaron en la recolección de firmas para solicitar el referendo revocatorio en contra del entonces Presidente de la República, el cual se llevó a cabo en el mes de agosto de 2004, la Sala del Tribunal Supremo de Justicia ordenó acumular la presente causa con otras seguidas en términos similares y en mayo de 2005 se dictó sentencia indicando que fue violado el derecho a la protección de su honor y reputación, por lo que Luis Tascón retiró la lista de su sitio web, aunque algunos consideran que ya el daño estaba hecho, por lo que entonces procedía era la indemnización de daños y perjuicios.

El 13 de Mayo de 2014 el Tribunal de Justicia de la Unión Europea dictó una famosa sentencia en contra de la compañía Google Inc. para la protección de

datos a través del derecho al olvido, en un juicio contencioso entre la Agencia Española de Protección de Datos y Google Inc., solicitando que se eliminara el nombre de una persona en el buscador, porque se vinculaba con una subasta de un inmueble embargado, que ya estaba superada. Dicha sentencia hace responsable a Google Inc. del tratamiento de los datos personales y condeno a la compañía a eliminar de la lista de búsqueda la vinculación del nombre con la subasta, así la publicación sea lícita, sólo por el hecho de ser obsoleta. La compañía ha señalado que está tratando de aplicar la sentencia y se trata de un proceso complicado ya que debe ser analizado cada caso separadamente, por lo que, tal como explica Tudares (2005):

> Para realizar la solicitud de eliminación hay que rellenar un formulario web, advirtiéndonos que puede que el trámite tarde un tiempo, pues ya han recibido muchas solicitudes. Hay fuentes que hablan de que han recibido en torno a 150.000 solicitudes desde la publicación de la Sentencia. Así que en teoría, una vez recibida la solicitud por Google, evaluará si efectivamente se trata de información obsoleta de la persona del solicitante y si es lesiva a sus intereses, ponderando si existe un interés público en lo que respecta a la información que permanece en los resultados de búsqueda, decidiendo de forma unilateral si deja de indexar esa información.

Cabe destacar que estas sentencias sólo rigen para los estados miembros de la Unión Europea, es decir, la compañía ha aclarado que solamente será eliminada la búsqueda en las versiones europeas, pero consideramos que debería eliminarse en todos los buscadores y ser mundial para que realmente sea efectiva, tal como lo había planteado el Regulador de Datos Francés, en la sentencia previa a la del Tribunal de Justicia Europea.

Entonces, el punto es que todos pueden entender que existen violaciones a la intimidad y privacidad de las personas, pero ¿Qué mecanismos existen o pueden existir para proteger a la información?, pues realmente muy pocos y menos en Venezuela, porque a pesar que la constitución nacional establece la

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

protección a la privacidad, no existen mecanismos o procedimientos para que se haga efectiva esta protección y tampoco leyes que regulen los límites del manejo de la información que contiene el internet, ni leyes o reglamentos que limiten estos contratos.

En Venezuela encontramos algunos pequeños avances, primero con el Decreto con Rango y fuerza de Ley de Mensajes de Datos y Firma Electrónica (2001), en el que en su artículo 4, se le otorga a los mensajes de datos o documentos electrónicos el mismo valor probatorio que la Ley le otorga a los documentos escritos. Y en su artículo 5 consagra, que la ley Mensajes de Datos estarán sujetos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y el acceso a la información personal.

Esta Ley también crea la Superintendencia de Servicios de Certificación Electrónica, que es un organismo de Estado adscrito al Ministerio del Poder Popular para la Ciencia y Tecnología, que funciona como un ente regulador entre los proveedores de servicios de certificación públicos o privados y el Estado, organismo que creemos, puede controlar también las diferentes políticas respectos a la privacidad de las personas en redes sociales, bien porque se amplíen sus facultades y competencias, o dicho Ministerio debe crear un organismo especial para esto, pero esto sólo resolvería el problema a nivel nacional, y evidentemente en la mayoría de los casos, no se trata de compañías nacionales, sino que se trata de compañías internacionales, son las normas de derecho internacional las que deben regular estos contratos, acuerdos y faltas.

Otra de las leyes venezolanas que encontramos, es la Ley Especial contra los Delitos Informáticos (2001), que le corresponde a la materia penal, específicamente su artículo 20 señala:

> 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.

De igual forma, el 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.

Y el 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 obtenida 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.

Entonces esta Ley sí tipifica como delito la revelación, el abuso o aprovechamiento de los datos electrónicos que pueden atentar contra la privacidad de las personas, y en este caso se tendrá que aplicar la responsabilidad penal empresarial.

La Ley de Protección a la Privacidad de las Comunicaciones (1991) en el artículo 5 señala que "*el que perturbe la tranquilidad de otra persona mediante el uso de información obtenida por procedimientos condenados por esta Ley, y creare estados de angustia, incertidumbre, temor o terror, será castigado con prisión de seis a treinta*

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

meses" y además en el artículo 6 autoriza a los organismos de seguridad del Estado a:

> *…impedir, interrumpir, interceptar o gravar comunicaciones, pero únicamente a los fines de la investigación de los siguientes hechos punibles: a) Delitos contra la seguridad o independencia del estado; b) Delitos previstos en la Ley Orgánica de Salvaguarda del Patrimonio Público; c) Delitos contemplados en la Ley Orgánica sobre Sustancias Estupefacientes y Psicotrópicas; y, e) Delitos de secuestro y extorsión.*

El artículo 7 señala, que sólo se hará mediante autorización de un Juez de Control penal competente, "*y la inobservancia de esta norma o autorización producirá que la intervención, grabación interceptación sea ilícita y no surtirá efecto probatorio alguno, y los responsables serán castigados con prisión de tres a cinco años"*. También, el artículo 8 de esta Ley consagra que:

> Toda grabación autorizada, será de uso exclusivo de las autoridades policiales y judiciales encargadas de su investigación y procesamiento, quedando en consecuencia prohibido a tales funcionarios divulgar la información obtenida. Y sanciona a los funcionarios que infrinjan esto con pena hasta de hasta 8 años.

Así mismo, Rico (2005) señala que:

> La única ley destinada a la protección de la intimidad de las personas es la Ley de Protección a la Privacidad de las Comunicaciones del 16 de diciembre de 1991, que tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas, pero se refiere solamente a la intercepción u obstrucción de las comunicaciones telefónicas quedando excluidas las comunicaciones escritas privadas. Pág. 263.

De igual modo, la Ley de Protección al Consumidor y Usuario (2004), una norma importante para el tema que tratamos, en el artículo 37 al establecer, la obligación de garantizar la privacidad y confidencialidad de los datos de los usuarios, imponiendo al proveedor el deber de utilizar medios adecuados que permitan la privacidad de los consumidores o usuarios, así como la confidencialidad de las transacciones realizadas de forma tal que la información intercambiada no sea inteligible para terceros no autorizados que tengan acceso a ella voluntaria o accidentalmente. En la misma disposición se establece como dice Rico (2005) la obligación de señalar: "*de manera suficiente los fines para los cuales el proveedor utilizará está información a terceros no relacionados con el negocio, y bajo qué circunstancias pudiera darse este supuesto.*" Pág. 277

En Venezuela existe el Centro de Digitalización del Consejo Nacional Electoral (CNE), que es la autoridad nacional de Trámites y Permisos en Venezuela, y también el Servicio Autónomo de Registros y Notarías (SAREN) que son instituciones del Estado venezolano, que manejan la información de los nacionales, y además están interconectadas, ésta información actualmente puede ser básica, pero de todos modos se trata de datos privados de las personas del país que si se van interconectando con todas las instituciones del Estado, podrían igualmente crear perfiles, por lo que es importante tener las herramientas para proteger a los ciudadanos de los abusos que puedan existir por parte del Estado al trasmitir y utilizar esta información.

En el ámbito del derecho comparado, el país que cuenta con más leyes y regulaciones en la materia son los Estados Unidos, que posee leyes desde el año 1970, pero es en 1986, como señala Rico (2005):

> Como consecuencia del auge alcanzado por las comunicaciones electrónica, donde fue promulgada la Electronic Communications Privacy Act, destinada a regular la privacidad de las comunicaciones electrónicas prohibiendo las intervenciones no autorizadas, el acceso no autorizado a mensajes almacenados en los sistemas computarizados, así como la intercepción de mensajes durante su transmisión. Pág. 265.

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

Modernamente se encuentra la Ley de intercambio de información sobre la ciberseguridad, que es una Ley Federal de USA, trazada para perfeccionar la ciberseguridad en los Estados Unidos mediante un mayor intercambio de información sobre amenazas de ciberseguridad y para otros fines. Esta Ley permite el intercambio de información sobre el tráfico de internet entre el Gobierno y las empresas de tecnología y fabricación.

El Proyecto de Ley se presentó en el Senado el 10 de Julio de 2014 y se aprobó en el Senado el 27 de Octubre de 2015. Pero los opositores cuestionan el valor de esta Ley, porque consideran que pasará la responsabilidad de las empresas privadas al gobierno, lo que aumentará la vulnerabilidad de la información personal privada, así como la dispersión de información personal privada en siete agencias gubernamentales, incluida la Agencia de Seguridad Nacional y la policía local de ese país.

El texto del proyecto de ley se incorporó mediante una enmienda en un proyecto de ley de gasto consolidado en la Cámara de los Estados Unidos el 15 de Diciembre de 2015, que fue promulgado por el Presidente Barack Obama el 18 de Diciembre de 2015.

En la Unión Europea, existe el Reglamento General de Protección de Datos (RGPD) que impide que algunas redes sociales compartir los datos para su propio interés, con ninguna persona natural o jurídica. De hecho, las grandes empresas se vieron en la obligación de crear una especie de sub-empresa para los usuarios europeos, por lo que se ha logrado, a través de estos mecanismos, frenar los abusos de las grandes empresas digitales.

Éste reglamento también ha obligado a que las estas compañías que manejan datos de información personal, reestructuren las condiciones o políticas para los 27 países que conforman la Unión Europea y han estado obligados a negociar las cláusulas con la Comisión Europea, incluso esta comisión ha tenido que sancionar con multas de millones de dólares a algunas personas jurídicas por la violación de estos acuerdos.

De igual modo, específicamente en España, existe la Ley Orgánica de Protección de Datos de Carácter Personal del 13 de Diciembre de 1999. Ésta es una norma jurídica española cuyo objetivo es *"garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos*

fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar."

La norma entró en vigor el 14 de Enero del año 2000 para regular el tratamiento de los datos personales. Cualquier empresa que maneje datos de carácter personal de sus clientes debe cumplir esta ley que, a grandes rasgos, establece lo siguiente: 1. Obligación de dar de alta los ficheros de datos en la Agencia Española de Protección de datos; 2. Obligación de elaborar y mantener actualizado el Documento de Seguridad. El documento de seguridad recoge las medidas que aplica la empresa para cumplir con la LOPDC y 3. Obligación de Obtener la legitimidad de los afectados.

En cuanto a la exigencia del consentimiento del interesado, es de advertir que la propia LOPDC establece ciertas excepciones basadas en razones de interés público que permiten el tratamiento de datos independientemente del cumplimiento de estos requisitos, el régimen de excepciones está consagrado en el artículo 6.2. El artículo 6 consagra:

> Tratamiento basado en el consentimiento del afectado. 1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. 2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas. 3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

La Corte Europea de Derechos Humanos con sede en Estrasburgo ha sido desde siempre uno de los tribunales más atentos al desarrollo del nuevo modelo interpretativo relativo a la privacidad, acogiendo la idea de un derecho relacionado a la identidad personal y a la autodeterminación del individuo, sobre

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

en el caso específico de todos con el derecho a la protección de los datos personales que se relacionan con la vida privada.

El artículo 8.1 de la Convención Europea para la Salvaguarda de los Derechos Humanos y de las Libertades Fundamentales, tal como lo cita Ávila y Otros (2008) dice que:

> ´cada persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia´ determinando, y progresivamente ampliando el significado a asignar a los conceptos de ´vida privada´ y ´correspondencia´ (CEDU, Sentencia Malone c. Reino Unido, 2 Agosto 1984 (corte plenaria) serie A n.82; Sentencia Gaskin c. Reino Unido, 7 Julio 1989, corte plenaria, serie A n.160; Sentencia Z. c. Finlandia, 25 Febrero 1997.), sentando así las bases de la positivización de un derecho al control consciente sobre cada forma de circulación de las propias informaciones personales.” Pág. 327.

La Unión Europea también ha publicado el Reglamento 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 (Reglamento general de protección de datos) creado por la Directiva Europea sobre Protección de Datos, en el que se establece que es obligatorio tener dentro de todas las empresas europeas un delegado especializado de protección de datos que asesore a las compañías en estos temas, y además crea en el artículo 51 una o varias autoridades públicas independientes, autoridad de control, que se encarga de supervisar la aplicación del reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

Ahora bien, el principal problema que se presenta en las negociaciones celebradas, a través de internet en el momento de prestar el consentimiento para el tratamiento de datos personales, se relaciona directamente con la inclusión en los contratos de condiciones generales donde se inserta una cláusula tipo,

autorizando al proveedor a incluir los datos personales de los clientes en una base de datos y utilizarlos después de efectuada la transacción.

Rico (2005: 270) dice que en estos casos, es importante que "*la redacción de la cláusula sea clara, de manera que no deje lugar a dudas que el titular de estos datos ha manifestado su consentimiento en forma inequívoca para el tratamiento posterior, tal como lo establece la ley*." Pero no sólo es importante tener clausulas claras, sino también leyes que regulen estos contratos, normas generales que limiten los abusos y procedimientos que protejan las futuras violaciones a estas leyes, limitaciones y contratos.

La prueba electrónica o digital se define, como toda aquella información con valor probatorio, que se encuentra incluida en un medio electrónico o que es transmitida por dicho medio. Por ello cabe distinguir dos modalidades básicas de prueba electrónica: 1. Los datos almacenados en sistemas o aparatos informáticos; 2. La información transmitida electrónicamente a través de redes de comunicación.

En cualquier orden jurisdiccional, la identificación y uso de la prueba electrónica recorre las siguientes fases: 1. Obtención de la información: Las partes han de acceder a la información de forma lícita, sin violar los derechos fundamentales. 2. Incorporación de los datos al proceso: Para que los datos sean incorporados al proceso deben cumplir unos requisitos: pertinencia, necesidad, licitud y admisibilidad procesal. 3. Valoración de los datos incorporados: Por último, y si cumplen los requisitos anteriores sobre obtención e incorporación, la prueba electrónica será objeto de valoración por parte del juez o tribunal. Por lo tanto, el primer requisito fundamental para la prueba digital sea incorporada válidamente a un proceso judicial es la licitud, es decir, haber sido obtenida de manera lícita, sin violentar ningún derecho fundamental.

De la Torre (2009) señala:

> A diferencia de los medios de prueba tradicionales, la prueba digital tiene las siguientes características: 1. **Intangible**: La prueba digital es intangible, no pudiendo apreciarse

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

> directamente a través de los sentidos, sino mediante complejos procesos informáticos. 2. **Replicable**: La prueba digital se encuentra en formato digital, pudiéndose copiar o replicar tantas veces como se desee. Con ello se plantea el problema de distinción de la originalidad, el cual se declara como trivial para su adquisición de fuerza probatoria si se puede acreditar indubitadamente que original y copia son exactos, bit a bit. 3. **Volátil**: La prueba digital es mudable, inconstante por su propia naturaleza intangible, y especialmente sujeta a la posibilidad de modificación o alteración, lo que añade especial complejidad para que una prueba digital adquiera capacidad probatoria. 4. **Deleble**: La prueba digital puede ser fácilmente destruida, no siendo necesaria la destrucción del soporte digital que la contiene. 5. **Parcial**: En ocasiones, la prueba digital está formada por múltiples ficheros informáticos, repartidos en distintos soportes digitales y localizaciones, como por ejemplo un sistema de información en la nube, lo que añade todavía más complejidad en su aprehensión y preservación.

Puede hablarse indistinto de pruebas electrónicas, digitales o tecnológicas, y como se trata de mensajes de datos, el Decreto con Rango y Fuerza de Ley sobre Mensaje de Datos y Firma Electrónica (2001) señala en su artículo 4, que la promoción de estas pruebas debe hacerse como medio de prueba libre, tomando en cuenta el *principio de libertad probatoria*, pero la admisión y evacuación de estas pruebas *sí representa un desafío para los jueces modernos*, y llegamos específicamente al punto que nos interesa en esta investigación, porque en Venezuela la admisión de las pruebas está supeditada a la legalidad, licitud y pertinencia de la prueba, por lo que es necesario determinar si las pruebas electrónicas que compartimos en un red social son lícitas o no.

La admisión y práctica de la prueba digital, como dice De la Torre (2009):

> No constituye un algo mágico ni arbitrario, sino que responde a un régimen jurídico que requiere, en ausencia de normativa legal adecuada, de un esfuerzo de aproximación de los conceptos procesales a la realidad tecnológica habitual en la

sociedad de la información, en muchos aspectos, aún en proceso de construcción.

En primer lugar, y más importante, se debe conversar acerca de la forma en que aceptamos los términos de privacidad, puesto que basta con un clic para poner en manos de las compañías digitales el uso, tratamiento y divulgación de nuestra información, poniendo muy en duda la forma en que el usuario expresa su consentimiento, porque como abogados se entiende que basta el consentimiento para que el contrato exista, pero en estos casos no hay opción de rechazarlo, sólo se tiene la opción de dejar de utilizar la red social, cosa que sucede con cualquier contrato de adhesión, y es aceptado así, pues la mayoría de los contratos públicos o privados de suministros de bienes y servicios modernamente, son contratos de adhesión, y decir que estos no son válidos, paralizaría casi todo el mercado y sería imposible el tráfico económico.

Por lo tanto, lo que debe existir son normas que los regulen y organismos que los fiscalicen, es decir, vías a través de las cuales se dé protección al consumidor mediante la prohibición de las cláusulas abusivas, que son nulas de pleno Derecho, y a través de la vigilancia por las instituciones públicas de la actuación de las empresas, en algunos casos, la comercialización de productos esenciales se regulan directamente por el Estado mediante normas imperativas, de forma que el estado suplanta el consentimiento de las partes y lo sustituye por una relación jurídica regulada previamente de forma equilibrada. El intervencionismo puede tener distintos grados, y puede abarcar la casi totalidad de la relación contractual.

El otro punto importante, es la suscripción del contrato de adhesión, puesto a diferencia de los otros contratos de adhesión que conocemos, como por ejemplo, el de la energía eléctrica o el de la empresa que nos suministra internet en nuestros hogares, la suscripción, firma o aceptación es a través de darle clic al botón de aceptar; no existe un traslado físico a la empresa y tampoco firmamos manuscritamente un contrato y tampoco se realiza a través de los que modernamente se utiliza para verificar la voluntad digitalmente con una firma electrónica, puesto que si hay una firma no hay duda de la inequívoca voluntad de suscribirlo, sino con un simple clic, que la mayoría de los usuarios no entiende

ISSN 2739-0330 (en línea)
REVISTA RECHTSSTAAT: ESTADO DE DERECHO ● Número 1 Especial ● noviembre 2022
Gloria Elizabeth La Paz Contreras Bez ● Pág.: 232 – 262

que alcance puede tener. Pareciera que es la forma moderna de estar de acuerdo y suscribir contratos, y entendemos que es legal, pero inevitablemente se vuelve entonces a la necesidad de la regulación.

Aun así, siendo que el contrato sea válido, es importante analizar en segundo lugar si, viéndose el Juez en la obligación de admitir las pruebas, por considerarlas legales, licitas y procedentes, bien reservándose el derecho a inadmitirlas en sentencia definitiva o admitiendo por el principio de *favor probationen,*[2] ¿Cuál sería la forma de aportarla válidamente al proceso?

Para la evacuación de estas pruebas el Decreto con Rango y Fuerza de Ley sobre Mensaje de Datos y Firma Electrónica en su artículo 4 remite a lo previsto para las pruebas libres, y esto no es más que la analogía a otros medios de prueba ya existentes, o la forma que determine el juez; creemos que será necesario, debido a las características de las pruebas digitales, la celebración de una audiencia especial probatoria, en la que a través del mismo medio electrónico el juez verifique la prueba, y será necesaria la intervención de un perito informático forense público o privado, que se encargue de acreditar la validez de la prueba, no sólo por la licitud y legalidad de la prueba y determinar que se obtuvo de manera adecuada, porque no se violó la intimidad de la persona; sino también determinar que no se alteró, modificó o eliminó información necesaria para que la prueba sea considerada válida.

Es de vital importancia, para De la Torre (2009):

> Que el dictamen pericial informático recoja las circunstancias de la obtención de la prueba digital de la forma más detallada posible. La obtención de una prueba digital que pueda desplegar valor probatorio en un proceso judicial consiste en: 1. **Acreditación del origen y existencia de los datos**. Ésta se puede hacer mediante fotografías, grabación de vídeo, participación de testigos y/o el concurso de un fedatario público o tercero de confianza que den fe sobre el particular. 2. **La licitud de la**

[2] Cuando el Juez tiene dudas de la admisibilidad de la prueba, es preferible admitirla, ya que se causa menos daño admitiendo y desechándola en sentencia definitiva, que no admitiéndola siendo relevante para el caso.

> **obtención de los datos**, es decir, su obtención sin vulnerar derechos fundamentales ni normativa de aplicación sobre el particular. 3. **La no alteración de los datos**, y pérdida de información relevante, en el momento de acceder el perito informático a su origen o continente, por su propia naturaleza o por descuido negligente de éste. 4. **El acceso a datos en poder de la otra parte** en el litigio, si fuera el caso.

Por lo tanto, el Juez deberá analizar todas estas consideraciones y en caso de no cumplirse todos estos requisitos necesariamente deberá considerar que las pruebas no son válidas.

Ahora bien, ¿Se puede establecer diferencia entre las pruebas obtenidas de perfil privado o público?, es decir, si el perfil de una cuenta es público y voluntariamente el usuario aporta información, documentos, fotos, grabaciones, quiere decir, que se trata necesariamente de pruebas lícitas, evidentemente si seguimos el mismo criterio que se tiene hasta ahora con las demás pruebas, todo lo que es público o lo que ocurre en lugares públicos, es entiende obtenido de manera lícita y entendemos entonces que no viola necesariamente la intimidad o privacidad, puesto que el usuario voluntariamente lo hace público, y las redes sociales son espacios públicos, aún más si el perfil no tiene limitaciones de acceso y permite que cualquier persona lo vea.

Es importante aclarar que el hecho que sea lícito, o que la obtención no viole la intimidad, no quiere decir que sea legal o pertinente, o que no viole el orden público y las buenas costumbres, por ejemplo, si se publican fotos o videos en un perfil público, se deben tener como lícitas, pues su obtención así lo fue, pero si se trata de desnudos, pues no pueden ser legales y van contra las buenas costumbres, por lo tanto, no podrán ser aportadas válidamente en juicio y aún aportadas no serán válidas.

Pero también es útil aclarar que en el supuesto, que la cuenta esa hackeada, entonces si encontraríamos un supuesto de prueba ilícita y el responsable de la violación será el hacker, que debe tener la sanción penal del artículo 20 de la Ley Especial contra los Delitos Informáticos, si logra descubrirse su identidad, cosa que también requiere de especialistas peritos en la materia. Pero ¿Qué sucede si

la red social, sí posee limitaciones de acceso, solamente para los usuarios que se acepten previamente? A pesar que la red social este programada en forma privada, el contenido que se comparte es público para los usuarios aceptados, así que de igual forma existe cierta publicidad, a pesar de ser limitada, por lo que estas pruebas igualmente se consideran obtenidas de manera lícita porque no violan la privacidad.

En relación a la información que no publicamos, sino a la información o datos que manejan las empresas digitales a través de la inteligencia artificial o intercambio de datos o a través de la llamadas "*cookies*", como lo son la ubicación geográfica de los dispositivos, o la conexión con personas, o la lista de contactos, entre otras, de las que ya hemos comentado; esta información si puede violar nuestra privacidad e intimidad, por lo que las normas o medidas de regulaciones deben ser mayores y consideramos además que deben cumplir los mismos requisitos que la intervención de comunicaciones, es decir, únicamente por que existe una investigación pendiente, por necesidad de los órganos de investigación y únicamente en determinados casos que ameritan por proporcionalidad de principios la violación de la intimidad o privacidad.

CONCLUSIONES

Son realmente muy pocos los mecanismos que hay en Venezuela para la protección de la información y datos personales íntimos que están contenidos en los espacios digitales, porque a pesar que la Constitución Nacional establece la protección a la privacidad, y existe para nosotros la acción de *Habeas Data* como un mecanismo tendiente a proteger ese espacio privado de las personas, es decir, como una herramienta para defenderse de las intromisiones, tanto por parte del Estado como de los particulares; no existen los mecanismos para que se haga efectiva esta protección, ni leyes especiales o reglamentos que limiten estos contratos de adhesión con las instituciones públicas o privadas.

En Venezuela tenemos algunos pequeños avances, primero con la Ley de Mensajes de Datos y Firma Electrónica, que consagra que estos mensajes de datos

estarán sujetos a las disposiciones constitucionales y legales y que garantizan los derechos a la privacidad de las comunicaciones y el acceso a la información personal.

El Ministerio correspondiente debe crear un organismo especial que se encargue de este tema, puede tratarse de un organismo que regule, asesore, fiscalice y controle los contratos digitales y el uso de la información que almacenan estas compañías en forma amplia.

También tenemos la Ley Especial contra los Delitos Informáticos en materia penal, que consagran penas para las personas que revelen información y tipifica como delito la revelación, el abuso o aprovechamiento de los datos electrónicos que pueden atentar contra la privacidad de las personas.

La única ley destinada a la protección de la intimidad de las personas es la Ley de Protección a la Privacidad de las Comunicaciones del que tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas, pero se refiere solamente a la intercepción u obstrucción de las comunicaciones telefónicas quedando excluidas las comunicaciones escritas privadas, determinando los motivos y formalidades legales para intervenir comunicaciones privadas.

Y por último está la Ley de Protección al Consumidor y Usuario, una norma importante para el tema que tratamos, al establecer la obligación de garantizar la privacidad y confidencialidad de los datos de los usuarios, imponiendo al proveedor el deber de utilizar medios adecuados que permitan la privacidad de los consumidores o usuarios, así como la confidencialidad de las transacciones realizadas, de forma tal, que la información intercambiada no sea inteligible para terceros no autorizados que tengan acceso a ella voluntaria o accidentalmente. En la misma disposición se establece la obligación de señalar de manera suficiente los fines para los cuales el proveedor utilizará está información a terceros no relacionados con el negocio, y bajo qué circunstancias pudiera darse este supuesto.

En relación a la información que no publicamos, sino a la información o datos que manejan las empresas digitales a través de la inteligencia artificial o intercambio de datos, su divulgación, venta y uso sí puede violar nuestra privacidad e intimidad, por lo que las normas o medidas de regulaciones deben

ser mayores y creemos que además, debe darse únicamente por que existe una inequívoca autorización sin derivar necesariamente de un contrato de adhesión, sino indicar, tal como se autoriza en algunas páginas *web* especificando cada rubro por separado, y así poder estar de acuerdo o no en cada punto de manera independiente y con el derecho del usuario a no aceptar las políticas y no por eso prohibir el acceso o uso de la misma.

Además se cree, que es posible que el Estado acceda a esta información cumpliendo los mismos requisitos que la intervención de comunicaciones de igual forma puede investigación pendiente, por necesidad de los órganos de investigación y únicamente en determinados casos que ameritan por proporcionalidad de principios la violación de la intimidad o privacidad, suponiendo que existen motivos suficientes y que hay una orden de un juez competente.

Es necesario crear órganos, vías y leyes a través de las cuales se proteja al consumidor, mediante la prohibición de las cláusulas abusivas, que son nulas de pleno Derecho, y a través de la vigilancia por parte de las instituciones públicas de la actuación de las empresas, pero para eso son necesarias leyes o políticas de estado que regulen y controlen estos contratos, como lo que sucede en la Unión Europea con normativa internacional, por ellos es importante que haya leyes y mecanismos internacionales para resolver el problema internacionalmente, consideramos que por ahora la forma adecuada para esto es a través de la organización de países, como en el caso europeo para negociar los términos con estas grandes compañías y mientras tanto, le corresponde a cada Estado dirimir los conflictos en sede jurisdiccional, apoyándose en las normas de derecho internacional privado, en contra de las grandes compañías por la defensa del derecho a la privacidad, alegando la violación de la intimidad o por violación de algunas cláusulas contractuales, así como lo hizo el Consejo Francés en 2016 que multo a Google con 100.000 mil Euros por no eliminar los datos a nivel mundial, aunque posteriormente el Tribunal de Justicia de la Unión Europea señalara que solamente se aplicará en los estados miembros; pues no existe un tribunal universal para ningún caso, evidentemente menos para estos temas.

Creemos, que para próximas reformas debe estudiarse como referencia y tomarse en cuanta el REGLAMENTO 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 (Reglamento general de protección de datos) creado por la Directiva Europea sobre Protección de Datos, en el que se establece que es obligatorio tener dentro de todas las empresas europeas un delegado especializado de protección de datos que asesore a las compañías en estos temas y establece las creación de entes reguladores de estos derechos.

Se propone, que las pruebas electrónicas, digitales o tecnológicas se promuevan como medio de prueba libre, y deben admitirse si son legales y pertinentes, así se trate de pruebas obtenidas en redes sociales o mediante la orden judicial, ya que el contrato de adhesión que se suscribe, a través de un clic por los momentos es válido, hasta que exista una ley que regule otra cosa. La forma en la que se puede evacuar la prueba digital es celebración de una audiencia especial probatoria, en la que a través del mismo medio electrónico el juez verifique la prueba. Y será necesaria la intervención de un perito informático forense público o privado, que se encargue de acreditar la validez de la prueba, no sólo por la licitud y legalidad de la prueba y determinar que se obtuvo de manera adecuada, porque no se violó la intimidad de la persona, sino también determinar que no se alteró, modificó o eliminó información necesaria para que la prueba sea considerada válida. La publicidad de las redes sociales opera así la cuenta sea pública, o reservada para un grupo de personas.

REFERENCIAS BIBLIOGRÁFICAS

Ávila, F. M.-Castaldo, K.-Urdaneta, A. (2008) Los Derechos a la Intimidad y a la Privacidad en Venezuela y en el Derecho Comparado En "*Revista Telemática de Filosofía del Derecho.*" Nº 11. Págs. 313-333 http://www.rtfd.es/numero11/18-11.pdf

Cabrera, J. E. (2010) "*La Prueba Ilegítima por Inconstitucional*." Ediciones Homero. Caracas D.F., Venezuela. Págs. 1010.

De La Torre, P. (2009) "*Prueba Digital en el Proceso Judicial*." https://indalics.com/blogperitajeinformatico/pruebadigital#:~:text=Se%20refiere

%20a%20cualquier%20clase,una%20categor%C3%ADa%20de%20prueba%20tecnol%C3%B3gica

Mejan, L. M. (1994) "*El Derecho a la Intimidad y a la Informática*." Editorial Porrúa. México D.F., México. Págs. 318.

Meréndez, U. (2014) *"Sentencia Google Spain Y Derecho al Olvido."* Revista Actualidad Jurídica. Madrid, España. Págs. 9. https://www.uria.com/documentos/publicaciones/4370/documento/fe04.pdf?id=5584#:~:text=derecho%20al%20olvido,La%20sentencia%20del%20Tribunal%20de%20Justicia%20de%20la%20Uni%C3%B3n%20Europea,y%20sin%20que%20se%20eliminen

Ossorio, M. (1999) "*Diccionario de Ciencias Jurídicas, Políticas y Sociales*." Editorial Heliasta. Buenos Aires, Argentina. Págs. 1038.

Rico, M. (2005) "*Comercio Electrónico, Internet y Derecho*." Editorial Legis. Bogotá, Colombia. Págs. 346.

Rojas, M. E. (2011) "*Eficacia de la Prueba Obtenida Mediante Irrupción de la Intimidad*." Universidad Externado de Colombia. Bogotá, Colombia. https://books.openedition.org/uec/159?lang=es

Tudares, C. (2015) *"El Derecho al Olvido y Google."* Red Venezolana de Derecho Informático. Caracas, Venezuela. http://revederin.blogspot.com/2015/06/el-derecho-al-olvido.html

Gaceta Oficial Nº 5.453 Extraordinaria del 24 de Marzo de 2000. Constitución de la República Bolivariana de Venezuela.

Resolución 217 A (III) del 10 de Diciembre de 1948. Declaración Universal de los Derechos Humanos.

Gaceta Oficial N° 34.863 del 16 de Diciembre de 1991. Ley de Protección a la Privacidad de las Comunicaciones.

Gaceta Oficial N° 37.148 del 28 de Febrero de 2001. Decreto con Rango y Fuerza de Ley sobre Mensaje de Datos y Firma Electrónica. Venezuela.

Gaceta Oficial N° 37.313 del 30 de Octubre de 2001. Ley Especial contra los Delitos Informáticos.

Gaceta Oficial N° 39.930 del 04 de Mayo de 2004. Ley de Protección al Consumidor y Usuario.

Ley Orgánica de Protección de Datos Personales y Garantías de Derechos Personales. España (2000).

Resolución de la Agencia Española de Protección de Datos, de 30 de Julio de 2010, núm. R/01680/2010, Procedimiento núm. TD/00650/2010, fundamento de derecho duodécimo.

Reglamento 2016/679 del Parlamento Europeo y Del Consejo. Fecha: 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 (Reglamento general de protección de datos) creado por la Directiva Europea sobre Protección de Datos.

Sentencia Tribunal de Justicia de la Unión Europea. **Asunto C-131/12**. Caso: Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos Personales, Mario Costeja González. Fecha: 13 de Mayo 2014.

Sentencia N° 10 de la Sala Constitucional. Tribunal Supremo Justicia de Venezuela. Expediente N° 04-1310. Habeas Data: Caso Tomás Mariano Adrián Hernández. Fecha 01 de Marzo 2016. Magistrada Ponente: Lourdes Benicia Suárez Anderson.