EL HABEAS DATA EN LAS REDES SOCIALES ONLINE: RESPONSABILIDAD Y VIGILANCIA

"Habeas Data in online social networks: liability and surveillance"

Para referencias: SOTELO VARGAS, Diego Andrés (2012) "*EL HABEAS DATA EN LAS REDES SOCIALES ONLINE:*

RESPONSABILIDAD Y VIGILANCIA", En Revista Iter Ad Veritatem 10. Universidad Santo Tomás. Tunja.

Diego Andrés Sotelo Vargas*

"P*ara saber quiénes somos tenemos que comprender cómo estamos conectados.***"***
James Fowler

Fecha de Recepción: 14-09-2012
Fecha de Aprobación:06-11-2012

RESUMEN**

Este artículo es el resultado parcial de la investigación sobre protección de datos personales en el internet, específicamente en las redes sociales. Se pretende establecer, si el ámbito de protección nacional de los datos personales es lo suficientemente efectivo cuando se presentan fenómenos de carácter global como el flujo transfronterizo de información.

Al ser la protección de datos personales un derecho fundamental se debe crear un escenario adecuado para la protección de los mismos, lo cual garantiza no sólo este derecho sino muchos otros de los titulares de la información

PALABRAS CLAVE

Protección de Datos personales, Dato personal de carácter sensible, modelos de regulación de la protección de datos personales, Habeas data, flujo transfronterizo de información.

* *Estudiante investigador, del módulo privado, adscrito al centro de investigaciones socio - jurídicas en la Universidad Santo Tomás, Seccional Tunja diegosotelo.abogado@gmail.com.***AI**

***Artículo de investigación, resultado del proyecto "El Habeas data en las Redes Sociales online: Responsabilidad y Vigilancia", vinculado a la línea de investigación de Derecho Privado y Nuevas Tecnologías del Centro de Investigaciones Socio-Jurídicas de la Universidad Santo Tomás de Tunja.*

Método: el método utilizado en esta investigación es el analítico basado en el hermenéutico-jurídico y tomando como fuentes la Constitución Política de Colombia, jurisprudencia y doctrina respecto del derecho a la información y el derecho informático.

ABSTRACT

This article is the partial result of research on protection of personal data in the Internet, specifically social networking. It seeks to establish, if the scope of protection of personal data is sufficiently effective when there are global phenomena such as cross-border flow of information.

When personal data protection is a fundamental right must create an appropriate setting for their protection which guarantees no west sun right but many of the owners of the information

KEY WORDS

Protection of Personal Data, personal information of a sensitive nature, patterns of regulation of personal data protection, habeas data, cross-border flow of information.

RESUME

Cet article est lerésultat partiel derecherche sur la protectiondes données personnellessur l'Internet, les réseaux sociauxen particulier. Elle vise à établirsi la portéede la protection nationaledes données personnellesest suffisamment efficacelorsqu'ils sont présentsphénomènes mondiaux tels quela circulation transfrontalièrede l'information. Commela protectiondes données personnelles estun droit fondamental doitcréerun cadre approprié pourleur protectionqui garantitnon seulement le droit, mais la plupart despropriétaires de l'information Mots-clés: protection des données personnelles, les données personnelles à caractèresensible, des modèles de réglementationde la protection desdonnées à caractère personnel, l'habeas data, la circulation transfrontalièrede l'information.

MOTS CLES

Protection des données personnelles, les données personnelles à caractèresensible, des modèles de réglementationde la protection desdonnées à caractère personnel, l'habeas data, la circulation transfrontalièrede l'information.

SUMARIO

1. INTRODUCCIÓN

El concepto de la cibernética, se refleja en dos partes, por un lado se encuentra el hombre y por el otro la máquina, y su resultado es el dominio y uso del hombre frente a éstas, por tal razón las medidas tecnológicas tienden a un fin primordial y es aumentar la productividad, es aquí donde se presenta la relación de que la evolución del individuo que es análoga a la de la humanidad, y donde la tecnología desempeña un papel importante cuando se une con otras ciencias, ya que se podrían esperarse los mejores resultados.

El ser humano desde siempre ha sido fuente de información, y a través de la historia se vio la necesidad de recopilar los datos de cada integrante de la sociedad, desde el censo en su forma más rústica, hasta la utilización de tecnologías y la condensación de forma virtual o electrónica, esta recolección de información permite determinar qué clase de sociedad y las necesidades de ésta, para así tomar las decisiones más acertadas dando como resultado cambios tanto en la sociedad como en la economía.

Este fenómeno es conocido como la informática a lo que el doctor Téllez, J. (1987) define:

> *La palabra "informática" es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en el año de 1962. En sentido general, la informática es un conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones desde el punto de vista de un sistema integrado. (Téllez, 1987).*

El uso de la tecnología, en específico de la computadora y el internet, se ha vuelto cada vez más indispensable y presente desde las organizaciones de diferentes tamaños hasta los hogares, lo que constituye una de las fuerzas sociales más poderosas, generando aspectos positivos como negativos.

En cuanto a los aspectos positivos solo tienen como límite el ingenio humano, ya que son aplicables a todos los campos sociales mejorando los resultados y la productividad, por mencionar en el derecho, la tecnología tiene implicaciones ya que puede mejorar la preservación y recolección de documentos jurídicos, hacer más ágil la administración de justicia; por otro lado están las implicaciones negativas que pueden verse en problemas psicológicos y hasta físicos, a esto se añaden los problemas de carácter jurídico como lo son la confidencialidad de la información, la seguridad y los demás delitos informáticos.

Adviértase que frente a lo anteriormente dicho, está presente un administrador responsable, que garantiza el buen uso de la información, ya sea el estado o un privado que da las medidas necesarias de seguridad para la recolección y utilización de dicha información; ahora se comprende que existe un ente determinable que realiza la función y se le puede endilgar la responsabilidad en caso de perjuicio, pero cuando estamos frente a fenómenos de las redes sociales, se dificulta la tarea de determinar quién es el infractor y ante quien recae la responsabilidad por la utilización de los datos personales.

No obstante el derecho no puede permitirse dejar este nuevo fenómeno social por fuera de sus alcances, ya que con el uso de la

computadora y el internet, se han generado nuevas situaciones de riesgo, que si bien son de interacción virtual, estas tienen consecuencias materiales.

Por tal razón, la exigencia de una reglamentación imperativa o coercitiva que busque proteger los intereses del individuo y las relaciones que se den con el internet en específico con las redes sociales y el fenómeno de la recolección universal de datos personales, es decir, el fin es crear un espacio jurídico para que un tercero que acceda a esos datos personales no genere un perjuicio en la forma de recolección y de uso.

2. METODOLOGÍA

Se trata de una investigación descriptiva y documental, básicamente tendiente a determinar la formulación de un problema jurídico específico y que implica establecer cuál es el ámbito de protección jurídico para los datos personales que fluyen las páginas web especialmente en las redes sociales.

Inicialmente se realizó el análisis de la declaración de derechos y responsabilidades de la red social Facebook entre otras redes sociales y en segundo lugar se realiza un cotejo con la ley 1266 de 2008 y ley 1581 de 2012 junto con el artículo 15 de la Constitución política de 1991 entre otras disposiciones legales de carácter nacional e internacional, en tercer lugar, se analiza la perspectiva de la protección de datos personales en el internet, su uso y recolección tanto por páginas web y redes sociales como por terceros no determinados y finalmente se compara la situación planteada con las tendencias de protección de datos personales Europeas con el fin de dilucidar el problema jurídico central de la investigación.

De la misma forma se realizó una revisión de la doctrina nacional y comparada sobre el tema, tendiente a verificar la existencia de tensión frente a la problemática planteada.

3. EL HABEAS DATA COMO DERECHO FUNDAMENTAL

A finales de los sesenta la ONU advertía sobre las posibles amenazas del uso inadecuado de las computadoras a través de beneficios propios o ajenos en detrimento de intereses de terceras personas y diez años más adelante con la primera ley de datos de 1970, empiezan a surgir las primeras inquietudes respecto a las eventuales repercusiones del uso de las computadoras y el fenómeno informático. No obstante era necesario que se le diera un tratamiento constitucional a los datos personales, ya que con dicho tratamiento, se les brindaba protección a otros derechos (el buen nombre, el debido proceso, a la intimidad, entre otros) y libertades siendo necesario un trato decente a los datos de las personas como titulares de la información.

No obstante la declaración universal de los derechos humanos de 1948 en su artículo 12.

> *Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

Ratifica la trascendencia de la esfera íntima de la persona y la protección de la información y datos que de ésta puedan emanar, igualmente la declaración de santa cruz de la sierra de los jefes de estado y de gobierno de los países iberoamericanos (2003) dice:

> *45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad.*

Otro claro ejemplo es la carta de derechos humanos de la unión Europea en su artículo 8.

> *Artículo 8. Protección de datos de carácter personal: Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente*

En las constituciones latinoamericanas, es una constante la mención de temas sobre datos personales, es decir hay disposiciones referentes a aspectos relacionados con la protección de datos personales, República Dominicana introduce en el 2010 el listado de principios constitucionales por los cuales se regirá el tratamiento de datos personales

> Artículo 44.- Derecho a la intimidad y el honor personal. Toda persona tiene derecho a la intimidad. Se garantiza el respeto y la no injerencia en la vida privada, familiar, el domicilio y la correspondencia del individuo. Se reconoce el derecho al honor, al buen nombre y a la propia imagen. Toda autoridad o particular que los viole está obligado a resarcirlos o repararlos conforme a la ley. Por tanto:
> 1. El hogar, el domicilio y todo recinto privado de la persona son inviolables, salvo en los casos que sean ordenados, de conformidad con la ley, por autoridad judicial competente o en caso de flagrante delito;
> 2. Toda persona tiene el derecho a acceder a la información y a los datos que sobre ella o sus bienes reposen en los registros oficiales o privados, así como conocer el destino y el uso que se haga de los mismos, con las limitaciones fijadas por la ley. El tratamiento de los datos e informaciones personales o sus bienes deberá hacerse respetando los principios de calidad, licitud, lealtad, seguridad y finalidad. Podrá solicitar ante la autoridad judicial competente la actualización, oposición al tratamiento, rectificación o destrucción de aquellas informaciones

que afecten ilegítimamente sus derechos;
3. Se reconoce la inviolabilidad de la correspondencia, documentos o mensajes privados en formatos físico, digital, electrónico o de todo otro tipo. Sólo podrán ser ocupados, interceptados o registrados, por orden de una autoridad judicial competente, mediante procedimientos legales en la sustanciación de asuntos que se ventilen en la justicia y preservando el secreto de lo privado, que no guarde relación con el correspondiente proceso. Es inviolable el secreto de la comunicación telegráfica, telefónica, cablegráfica, electrónica, telemática o la establecida en otro medio, salvo las autorizaciones otorgadas por juez o autoridad competente, de conformidad con la ley;
4. El manejo, uso o tratamiento de datos e informaciones de carácter oficial que recaben las autoridades encargadas de la prevención, persecución y castigo del crimen, sólo podrán ser tratados o comunicados a los registros públicos, a partir de que haya intervenido una apertura a juicio, de conformidad con la ley.

Por otro lado, solo México con su reforma constitucional de 2009 deja de manera explícita el derecho fundamental a la "protección de los datos personales"

> Artículo 16. (...) toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (...)
> (Adicionado mediante decreto publicado en el diario oficial de la federación el 1 de junio de 2009)

El panorama general en Latinoamérica sobre la constitucionalización de la protección de datos personales se encuentra en la siguiente tabla:

Aspectos sobre protección de datos personales explícitamente incorporados en las constituciones latinoamericanas

Aspecto sobre protección de datos personales	País y artículo de la Constitución que explícitamente se refiere a cada aspecto
Mención de dato personal, información personal o dato	Argentina (Art. 43), Bolivia (Art. 130), Brasil (Art. 5, LXXII), Colombia (Art. 15), Ecuador (Art. 94), Honduras (Art. 182), México (Arts. 6, 16 y 20 Lit C –V–), Nicaragua (Art. 26), Paraguay (Art. 135), Perú (Art. 2 No. 6), República Dominicana (Art. 44 No. 2), Venezuela (Art. 28)
Derecho a la protección de datos personales	México (Art. 16)
Derecho a conocer datos contenidos en bases de datos públicos y privados	Argentina (Art. 43), Bolivia (Art. 130), Colombia (Art. 15), Ecuador (Art. 94), Honduras (Art. 182), México (Art. 16), Paraguay (Art. 135), República Dominicana (Art. 44 No. 2), Venezuela (Art. 28)
Aspecto sobre protección de datos personales	**País y artículo de la Constitución que explícitamente se refiere a cada aspecto**
Derecho a conocer datos contenidos solamente en bases de datos públicos	Brasil (Art. 5, LXXII), Guatemala (Art. 31), México (Art. 6), Nicaragua (Art. 26)
Derecho a conocer la finalidad del uso de los datos	Argentina (Art. 43), Ecuador (Art. 94), Guatemala (Art. 31), Nicaragua (Art. 26), Paraguay (Art. 135), República Dominicana (Art. 44 No. 2), Venezuela (Art. 28)
Derecho a conocer el uso que se le da a los datos	Paraguay (Art. 135), República Dominicana (Art. 44 No. 2), Venezuela (Art. 28)
Derecho a exigir actualización de los datos	Argentina (Art. 43), Colombia (Art. 15), Ecuador (Art. 94), Guatemala (Art. 31), Honduras (Art. 182), Paraguay (Art. 135), República Dominicana (Art. 44 No. 2 y 70), Venezuela (Art. 28)
Derecho a solicitar rectificación o corrección	Argentina (Art. 43), Bolivia (Art. 130), Brasil (Art. 5, LXXII), Colombia (Art. 15), Ecuador (Art. 94), Guatemala (Art. 31), Honduras (Art. 182), México (Art. 6, 16), Paraguay (Art. 135), República Dominicana (Art. 44 No. 2, 70), Venezuela (Art. 28)
Derecho a solicitar supresión, eliminación, destrucción o cancelación del dato	Argentina (Art. 43), Bolivia (Art. 130), Ecuador (Art. 94), Honduras (Art. 182), México (Art. 16), Paraguay (Art. 135), República Dominicana (Art. 44 No. 2), Venezuela (Art. 28)

Derecho a exigir confidencialidad sobre los datos	Argentina (Art. 43), Honduras (Art. 182), República Dominicana (Art. 70)
Derecho a impedir transmisión o divulgación de la información	Honduras (Art. 182)
Derecho de oposición	México (Art. 16), República Dominicana (Art. 44 No. 2)
Tratamiento de datos	Colombia (Art. 15), República Dominicana (Art. 44 No. 2)
Recolección de datos	Colombia (Art. 15)
Circulación de datos	Colombia (Art. 15)
Acción o garantía de hábeas data	Brasil (Art. 5, LXXII), Ecuador (Art. 94), Honduras (Art. 182), Paraguay (Art. 135), Perú (Art. 200, No. 3), República Dominicana (Art. 70), Venezuela (Art. 281)
Acción de amparo	Argentina (Art. 43)
Acción de protección de privacidad	Bolivia (Art. 130)
Principio de calidad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de licitud en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de lealtad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de seguridad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)
Principio de finalidad en el tratamiento de datos personales	República Dominicana (Art. 44 No. 2)

Fuente: Remolina, N. (2012). P. 209-211

Sin ser excepción el artículo 15 de la constitución política de Colombia versa sobre temas de datos personales, pero no lo menciona de manera explícita en el articulado, pero deja entre dicho la función del estado frente a estas menciones, ya que éste debe respetar, pero aún más importante es jugar como garante y hacer-los respetar incondicionalmente.

El Habeas Data aparece como una creación jurisprudencial dándose tres etapas de este derecho a través de las sentencias de constitucionalidad, inicialmente se le interpretó como una garantía al derecho a la intimidad, en la segunda etapa se interpreta como manifestación del derecho al libre desarrollo de la personalidad, respecto a su contenido la Honorable Corte Constitucional se ha referido de la siguiente manera

> **"(i)** el derecho de las personas a **conocer** - acceso- la información que sobre ellas está recogida en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; **(ii)** el derecho a un **incluir** nuevos datos con el fin de que se provea una imagen completa del titular; **(iii)** el derecho a **actualizar** la información, es decir, a poner al día el contenido de dichas bases de datos; **(iv)** el derecho a que la información contenida en bases de datos sea **rectificada o corregida**, de tal manera que concuerde con la realidad; **(v)** el derecho a **excluir** información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa." Corte Constitucional. Sentencia C-748/11. (Magistrado Ponente Jorge Ignacio Pretelt Chaljub; 6 de octubre de 2011).

Conviene señalar, que este derecho fundamental que se consagró en nuestra constitución y en otras legislaciones internacionales, no busca proteger los intereses de los administradores datos personales o archivos, sino por el contrario, está encaminado a que el tratamiento de los datos personales, se realice de la mejor manera posible y no se vulneren los derechos fundamentales de los titulares de la información.

Por eso "se propone entender por derecho a la protección de datos a la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas con el tratamiento de los datos personales" (Puccinelli, 2004). Ya que esta es una herramienta jurídica que debe garantizar a la persona su protección del tratamiento indebido o ilegal que se le pueda dar a sus datos personales y sea exigible al administrador o responsable del tratamiento que cumpla con su tarea de manera legal y ética.

Análogamente la Corte Constitucional ha señalado que "En concepto de esta Corporación existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante". Corte Constitucional. Sentencia T- 227/03. (Magistrado Ponente Eduardo Montealegre Lynett; 17 de marzo de 2003), debido que su finalidad es asegurar los intereses morales de los titulares de la información ya que estos no pueden

renunciar del todo a su intimidad ya que este acto sería nulo.

Al llegar aquí, es cuando encontramos la problemática de las redes sociales y el fenómeno de la recolección internacional de datos, a esto se añade que la regla general en las redes sociales es la falta de garantías, en cuanto al uso y manejo de los datos personales de aquellos usuarios que depositan su información sin tener en cuenta los riesgos a la que la dejan expuesta y sin saber que es muy poco probable poder responsabilizar al administrador de los datos o a un tercero que no se encuentra dentro del territorio nacional.

4. EL STRIPTEASE INFORMÁTICO Y LA PESCA DE INFORMACIÓN.

A menudo los usuarios del internet y en especial de las redes sociales, al ingresar a éstas no se toman la molestia de plantearse la idea de que ninguna red social es gratuita, ya que los datos personales son el principal insumo de éstas, es decir, se ha vuelto la industria del dato, debido a que la información que se encuentra en las redes sociales se usa como referente para el marketing, ya que es más fácil saber que desean las personas y estas a su vez son blanco de publicidad.

A consecuencia de esta situación, la gente deposita cantidades inimaginables de información, (cabe anotar que no toda información es un dato personal) ahora bien en las redes sociales si fluyen muchos datos personales y como agravante son datos que por lo general son de carácter sensible, estos últimos son aquellos que por su importancia pueden afectar la esfera más íntima de la persona o de lugar a su discriminación lo que da lugar a perfiles virtuales que dan idea de quién es una persona pero que en realidad se convierten en una huella digital que permiten menoscabo.

Un concepto más amplio lo trae el Tribunal Constitucional Federal Alemán con la sentencia de 15 de diciembre de 1983 que

> "configuro a partir del derecho general a la personalidad que consagra el artículo 2.1 de la Ley Fundamental de Bonn, la facultad del individuo derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida (...) el grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad. Hace falta, mas bien, conocer la relación de utilización de un dato para poder determinar sus implicaciones para el derecho de la personalidad." (Escobar, 2004).

Si bien el Doctor Remolina N. hace hincapié en este hecho al decir "Estos usuarios prácticamente se desnudan en internet, sin saber que están condenados a ser esclavos vitalicios de la información que publiquen así traten de eliminarla (...)" (p. 12). Ya que en la mayoría de redes sociales, por ejemplo Facebook a pesar de cerrar la cuenta del usuario, la red social guarda una copia de seguridad, lo que evita que el usuario que realmente desea retirar su información y salir de red social, no lo pueda hacer de forma completa lo que igualmente vislumbra el denominado derecho al

olvido, que básicamente se refiere a la cancelación, rectificación, oposición y por ende desvinculación de datos personales perjudiciales a la persona real.

A esto se añade el riesgo que implica tratamiento inadecuado de los datos personales, y para dar una idea de a qué se expone el usuario, el GECTI (2005) recalca que

> La peligrosidad del uso inadecuado de las tecnologías de la información para algunos derechos humanos se pone de manifiesto, básicamente, a través de las siguientes circunstancias: (1) La publicación de datos que por su naturaleza pertenecen a la esfera íntima de la persona o que pueden ser tomados como elementos para prácticas discriminatorias; (2) La publicación de información errónea, inexacta, incompleta, desactualizada, parcializada, etc.; (3) La potencialidad de la informática para recopilar y almacenar masivamente datos de cualquier naturaleza sobre las personas y la facilidad para acceder a esa información; (4) La manipulación y/o "cruce" de los datos almacenados que permiten crear perfiles virtuales de las personas (conocer sus pautas de comportamiento, sus tendencias políticas, religiosas, sexuales, entre otras), que pueden resultar valoradas, bien o mal, para las más diversas actividades públicas o privadas; (5) el riesgo de que la información de las personas sea conocida y manipulada por grupos ilegales para diferentes fines (terrorismo, chantajes, extorsiones, saboteos, discriminaciones, etc.) y (6) La utilización de la información para fines no permitidos por la ley o no autorizados por el titular del dato. (p. 8)

De lo dicho, se puede inferir que si bien el usuario es el titular de la información, se le debe garantizar el buen tratamiento a sus datos personales, o de lo contrario se le estarían violentando más derechos de carácter fundamental, que afectan tanto su honor como la buena imagen que él como persona ha de tener frente a la sociedad.

La mayoría de las características anteriormente mencionadas, se materializan cuando la buena fe y la confianza de los usuarios lleva a compartir información privada o de carácter sensible, asumiendo que no se utilizaran en forma maliciosa, pero usurarios malintencionados suelen crear perfiles con identificaciones falsas o de terceros o empresas usando hasta información real o manipulada para chantajear a los demás usuarios o simplemente con el fin de generar un perjuicio a su buen nombre, el concepto de este acción lo trae la doctora Yolanda Guerra cuando explica que "En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos."(p. 65)

No obstante el usuario y titular de los datos, deseara que se elimine la información errónea o falsa que se ha subido a su nombre y que le está perjudicando, ya que se están usando para un fin que no fue autorizado por él, y ahondando un poco más lo lógico de este razonamiento es que se encuentre un responsable ya sea directo o indirecto que pueda explicar lo sucedido e indemnizar el daño.

Colombia cuenta con herramientas jurídicas para que el usuario que se vea afectado pueda defender sus derechos siempre y cuando el usuario malintencionado se encuentre dentro del territorio nacional, pero al ser una red social de carácter global el daño lo puede ocasionar un tercero de otro país, es decir alguien estando A toma los datos de cualquier persona que se encuentra en B, y hace de esta información un mal uso y como la red social no es un administrador responsable se facilita la tarea de recolección de la información directamente de las personas. Este fenómeno es lo que se conoce como pesca de información.

Los ejemplos abundan, empezando por el dueño y creador de Facebook, Mark Zuckerberg, quien fue víctima de los hackers que ingresaron a su cuenta e hicieron pública información y fotografías. La compañía no dio ningún comentario después del incidente, sin embargo el hecho de que la propia página del creador de la red social haya sido hackeada despierta alertas en torno a la seguridad que ofrece el sitio, igualmente a finales del 2010 Facebook admitió que a través de sus aplicaciones se han transmitido datos confidenciales a empresas de publicidad y otras de rastreo en la web.

5. ¿QUIÉN SE HACE RESPONSABLE?

Ahora bien, cabe señalar que al realizarse este tipo de conductas pueden tener consecuencias civiles y hasta penales dentro ámbito nacional, pero el fenómeno del flujo de datos transfronterizos se ve limitado el actuar del estado y del individuo afectado, a esto se añade la falta de compromiso de la red social, en este caso de la más grande del mundo Facebook, que resulta irrisorio cuando en su *Declaración de derechos y responsabilidades* (2012), da una posición *de agradezca que lo dejamos usar la red social y que nos dé sus datos personales* cuando dice "2.5 Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello (del mismo modo que tú no tienes obligación de ofrecerlos)." A esto se añade que todas las autoridades policiales y judiciales del mundo tienen acceso a los datos que se encuentran en poder de Facebook, ya que es la fuente más completa de datos sobre cada individuo, sus gustos, actividades, posturas políticas, creencias religiosas entre otras, y cuando Facebook recibe una solicitud de información de una autoridad judicial no está obligada a notificar al titular de la información.

Después de esa aclaración hay que formularse dos preguntas ¿a quién le regalé mis datos personales? y ¿Qué términos de uso acepte? Lo que lleva a determinar el tipo de contrato en el usuario y la red social (Facebook).

El contrato que es común en internet y las redes sociales, es el contrato por adhesión online, donde la relación jurídica nace de la prestación del servicio entre la empresa titular del sitio web y el usuario. Los contratos por adhesión son aquellos en los cuales el contenido contractual ha sido determinado con prelación, por uno solo de los contratantes, al que se deberá adherir el co-contratante que desee formalizar la relación jurídica obligatoria.

Es decir el usuario no tiene otra medida al realizar el proceso de registro en sitios tales

como Facebook, Hi5, Orkut, que aceptar o rechazar el contenido contractual; pero uno de los elementos contractuales es la capacidad jurídica, a esto Facebook hace claridad que " si eres menor de 13 años no usarás Facebook" , pero el problema continua ya que la capacidad jurídica en Colombia se adquiere a los 18 años, la doctora Rocío M. (2003) ratifica la idea cuando dice "un contrato por medios electrónicos, siguiendo las leyes tradicionales, será jurídicamente nulo en el caso de incapacidad absoluta o relativa de cualquiera de las partes." (Rocío, 2003).

A esto se añade otra problemática jurídica, y es, hasta qué punto si hay un verdadero consentimiento por parte del usuario al aceptar las cláusulas del contrato, ya que la mayoría de los usuarios no suelen leer con detenimiento los términos y condiciones de uso de la red social, además de la falta de conocimiento técnico y jurídico cuando se enfrentan a este tipo de situaciones. Es normal que en este tipo de contratos estén presentes cláusulas abusivas que buscan reducir su responsabilidad en perjuicio del usuario final, es decir violando derechos de este último, lo que genera una situación de desequilibrio.

La jurisdicción pactada (como cláusula abusiva) en el contrato generalmente son países extranjeros, por ejemplo la cláusula de Facebook (2012)

> 16.1 Resolverás cualquier demanda, causa de acción o conflicto (colectivamente, "demanda") que tengas con nosotros surgida de o relacionada con la presente Declaración o exclusivamente con Facebook en un tribunal estatal o federal del condado de Santa Clara. Las leyes del estado de California rigen esta Declaración, así como cualquier demanda que pudiera surgir entre tú y nosotros, independientemente de las disposiciones sobre conflictos de leyes. Aceptas someterte a la competencia de los tribunales del condado de Santa Clara, California, con el fin de litigar dichas demandas.

Esta prórroga resulta inaccesible para el contratante débil, es decir el usuario, lo que niega la posibilidad de poder ejercer sus derechos, ya que tiene una excesiva onerosidad por la distancia y que además hace litigar en una jurisdicción distinta a la natural, lo que hace ilusorio tener protección frente a los derechos vulnerados. Ahora interesa extraer de lo dicho el modo de endilgar responsabilidad tanto al usuario mal intencionado, como a la red social que cuenta con nuestros datos. Entonces los elementos básicos para que exista responsabilidad son tres: "el daño, la imputación de éste a un autor específico, mediando una relación de causalidad al desempeño de una actividad peligrosa o la existencia de un riesgo". (Peña, 2003).

A si bien, se pueden determinar dos tipos de responsabilidades, una objetiva (directa) al poder imputársele a un autor en específico (usuario mal intencionado), y una subjetiva (indirecta) ya que media una relación de causalidad al desempeño de la actividad (red social o el proveedor de servicios de internet). Lo que conlleva a la afección o el daño al usuario que puede ser de dos tipos: "de carácter patrimonial, es decir lucro cesante y daño emergente; Extrapatrimoniales, que se refiere al daño moral, a la proyección de la persona y su integridad afectiva (…)" (Peña, 2003).

Siguiendo con los tipos de responsabilidad, la primera es la objetiva es imputable a un autor específico que puede ser el PSI o la red social al hacer directamente mal uso de los datos personales o un tercero, en este caso el perjuicio lo genera un tercero al realizar una conducta punible como un delito informático, y estos a su vez generan la segunda clase de responsabilidad subjetiva ya que la red social o los PSI generan el espacio para que terceros coloquen el contenido mal intencionado y además permiten el acceso de terceros al contenido, pero esta segunda clase es más compleja para dar unos ejemplos de cómo se genera la responsabilidad subjetiva se puede apelar al sistema Español y el Americano.

En el primer sistema es necesario que para endilgar la responsabilidad al PSI debido a un tercero, la persona afectada acuda ante el órgano competente y exponga su situación, y si el órgano competente determina la ilicitud de los contenidos, ordene el retiro de la información o se imposibilite el acceso a ésta; Por el lado del sistema Americano a primera vista se ve más ágil y garantista, ya que el particular acude ante el PSI y expone su situación de la cual está siendo afectado y el PSI debe mirar si es realmente perjudicado e inmediatamente retirar los contenidos, de no ser así es cuando se genera la responsabilidad ya que no toma las medidas para que no se siga con tal infracción es lo que se ha denominado "notice and takedown"

Frente a estos sistemas surgen interrogantes, ¿Qué pasa con el principio de continuidad de la protección cuando la información va del país A al B o al C?, ¿Será que nuestro aparato judicial puede resolver estos casos cuando este fenómeno no le da la competencia? y ¿Qué pueden hacer los Estados frente a recolección de datos personales extraterritoriales?

6. REGULACIÓN O AUTORREGULACIÓN

Hasta aquí podemos percibir las irregularidades que se presentan frente a la protección de los datos personales en las redes sociales (Facebook y otros), ahora hay que concentrarse en regulación que se le da al tema o la autorregulación que debe tener la red social y por ende el usuario cuando está a punto de ingresar a ésta.

Este fenómeno ha obligado a varios Estados a regular el tema, es el caso de la denominada Ley Facebook que se crea en Alemania, debido a que los empleadores le solicitaban a sus trabajadores la clave de acceso a Facebook, para revisar los datos personales o les exigían que aceptaran su jefe entre su grupo de amigos con el fin de poder determinar qué actividades realizaba el empleado. Frente a esta situación Alemania expide esta ley con el fin de limitar esta arbitrariedad no solo por violación a la intimidad, sino como medida para evitar la discriminación de personas que son competentes para el cargo, pero que por la información de su perfil no coincidan con las del empleador. Estados Unidos tiene la misma iniciativa habrá que ver qué resultados se generan.

En Colombia, la ley 1266 de 2008 se ve muy relegada frente a esta situación, empezando porque es una legislación sectorial, no brinda protección en el sector de las comunicaciones electrónicas, carece de herramientas jurídicas para proteger al titular contra el uso abusivo de las

tecnologías de la información. No es sino hasta con la promulgación de la ley 1273 de 2009 que modifica el código penal, en su artículo 53 dando como agravante el uso de medios informáticos, electrónicos o telemáticos para la realización de conductas punibles, e incluye el capítulo "de la protección de la información y de los datos" como solución a esta problemática creando delitos como los siguientes: Obstaculización ilegítima de sistema informático o red de telecomunicación (Artículo 269B); Interceptación de datos informáticos (Art. 269C); Daño informático (Art. 269D); Uso de software malicioso (Art. 269E); Violación de datos personales (Art. 269F); Suplantación de sitios web para capturar datos personales (Art. 269G). En el capítulo segundo se incorporaron estos tipos penales: Hurto por medios informáticos y semejantes (Art. 269I) y Transferencia no consentida de activos (Art. 269J).

Ahora bien, artículo 269 F es lo más cercano, pero aun así no se sabe si quedan por fuera los datos de carácter sensible que se han usado de manera errónea por fuera del estado ya que el artículo 10 del código penal exige que la conducta debe ser definida de manera "inequívoca, expresa y clara".

> Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Entonces, si por el mal uso de datos personales de carácter sensible que son los que fluyen en las redes sociales, el titular de la información tiene como herramienta el título v del código penal que versa sobre "delitos contra la integridad moral", esto siempre y cuando el tercero que genera el perjuicio esté en territorio nacional, igualmente podrá hacer uso del título I del Libro II del Código Penal que con ley 1482 de 2011 introduce el Capítulo IX que versa sobre "De los actos de discriminación", pero como el fenómeno va más allá se ve limitado cuando la conducta punible es transfronteriza.

Por el contrario hay leyes con la iniciativa transfronteriza para afrontar estas problemáticas como lo es la Ley 679 de 2001 cuando en su artículo 13 sobre acciones de cooperación internacional dice "El Gobierno Nacional tomará las medidas necesarias para defender los derechos fundamentales de los niños y aumentar la eficacia de las normas de la presente ley, mediante acciones de cooperación internacional acordes con el carácter mundial del problema de la explotación sexual, (...)"; esta disposición es a la que debe apuntar la legislación del habeas data a la cooperación internacional y se tomen medidas tecnológicas como en el caso de derechos de autor, para bloquear o rastrear al pescador de información, garantizando así que la protección sea integral, debido que al ser todas leyes sectoriales y muchas acomodándolas a la realidad dejan un gran

margen de desprotección para el titular de la información.

Ahora resulta necesario, decir que el internet no solo puede regirse por códigos de conducta o listados de ética, que si bien mencionan cómo sería un uso responsable no brinda una herramienta jurídica coercitiva, más bien debería generarse una legislación que sea coercitiva, eficiente y eficaz basada en la tecno ética, la doctora Guerra, Y. la define como

> Una combinación de la mente con la tecnología y su objetivo es establecer principios que procuren controlar el alcance arrasador de la información, pretendiendo el control de una *sociedad de conocimiento* gestionada con reglas éticas. La combinación de contrastes como el pasado y el futuro, lo natural y lo artificial, lo espiritual y lo material han surgido en esta nueva sociedad y es necesario, redefinir los objetivos, usos y alcances de la tecnología en convivencia con el ser humano. (p. 68)

La Honorable Corte Constitucional con la primera sentencia que profiere referente a este tema deja en claro la escasa regulación y conocimiento jurídico sobre estos casos refiriéndose en los siguientes términos

> "En lo que respecta a la posible vulneración del derecho fundamental al habeas data, entendido éste como la garantía de protección de datos, y en el caso específico de las redes sociales digitales, de la protección de datos personales y de datos sensibles, no existe mayor normatividad en la legislación nacional que regule lo referente a la protección de los mismos en casos de menores de edad.(…) se precisa que la resolución de la situación fáctica puesta en conocimiento de esta Sala se resolverá a partir de las disposiciones constitucionales y de la posible afectación de derechos fundamentales contenidos tanto en el ordenamiento interno como internacional y, no a partir de la regulación establecida por la red social Facebook, pues la vulneración del contenido de un derecho fundamental no depende de la transgresión o acatamiento de éstas". Corte Constitucional. Sentencia T 260/12. (Magistrado Ponente Humberto Antonio Sierra Porto; 29 de marzo de 2012).

A estos requerimientos parece que responde el proyecto de ley estatutaria a la que se refiere la sentencia T 260 de 2012. En la actualidad ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", cuando en su artículo 2 sobre el Ámbito de aplicación, dice "(…)La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.(…)"; el artículo 5 versa sobre los Datos sensibles; el artículo 6 sobre el Tratamiento de datos sensibles, prohibiendo tratamiento de estos salvo unas causales específicas contenidas en el mismo artículo; el artículo 12 versa sobre deber de informar al titular, para que van hacer usados sus datos; el artículo 19 sobre Autoridad de protección de datos, que

designa a la súper intendencia de industria y comercio para que a través de ésta se genere una delegatura encargada de la protección de datos personales; en cuanto al fenómeno de flujo internacional de datos personales aparece el artículo 26, que prohíbe la transferencia a países que no tengan el nivel adecuado de protección igualmente dice "(…)Esta prohibición no regirá cuando se trate de: a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia. (…)"; cuando dice expresa e inequívoca tal vez cabe la posibilidad de generar responsabilidad o anular el contrato con Facebook.

A través del comunicado No. 40 de 2011 los magistrados María Victoria Calle Correa, Jorge Iván Palacio Palacio y Luis Ernesto Vargas Silva, realizan el salvamento de voto en la sentencia C – 748 de 2011 frente a varios puntos del proyecto de ley por ejemplo

> El inadecuado "trasplante normativo" que hizo el legislador estatutario, llevó a que se fijara como autoridad de control para el tratamiento de datos personales a la Superintendencia de Industria y Comercio, entidad perteneciente a la Rama Ejecutiva del Poder Público. Además de las incontables dificultades prácticas que eso genera, la ausencia de una autoridad independiente es manifiestamente contraria al principio de imparcialidad que informa a la función pública, por la sencilla razón que buena parte del tratamiento de datos personales es efectuado por autoridades estatales, tanto a nivel nacional como territorial. Esto exigía que la autoridad colombiana de protección de datos, como sucede con sus pares en el derecho comparado, no hiciera parte del Ejecutivo.

En la sentencia mencionada se declara la exequibilidad del proyecto de ley salvo algunos artículos o palabras, es de esperar los resultados que esta ley pueda llegar a brindar a la protección de los datos personales y en el caso en que se regule la materia de forma específica se deben atender las recomendaciones hechas en el memorándum de Montevideo (2009) principalmente las siguientes:

- "Fortalecer el uso de la responsabilidad civil extracontractual objetiva como mecanismo regulatorio para garantizar los derechos fundamentales en las aplicaciones en la Sociedad de la Información y Conocimiento, Internet y redes sociales digitales.
- Desarrollarse y difundirse una base de datos sobre casos y decisiones (fallos judiciales o resoluciones administrativas anonimizadas) vinculada a la Sociedad de la Información y el Conocimiento, en especial a Internet y las redes sociales digitales, que sería un instrumento para que los jueces puedan apreciar el contexto nacional e internacional en el que están decidiendo." (P.8)

Y las recomendaciones hechas por la Agencia Española de Protección de Datos (2009) En especial el reconocimiento que hace a la aplicación legal frente aquellos prestadores o redes sociales cuyos domicilios no se encuentren dentro del estado pero que se puede determinar que prestan el servicio en el mismo.

"la LSSI-CE (Ley de Servicios de la Sociedad de Información de España) contempla su aplicación a "los prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo". Así, su artículo 4 dispone que a estos prestadores les sea de aplicación los artículos sobre la libre prestación de los servicios y sobre colaboración de los prestadores de servicios de intermediación para interrumpir el servicio o retirar determinados contenidos cuando lo haya declarado un órgano español competente sobre la licitud de los mismos.

Para determinarlos se tendrá en cuenta:

- Si disponen de la extensión de nombre de dominio. Es registrada ante Nic. estos operan a través de nombres de dominio "es.redsocial.com" o "redsocial.com/es"

- Si el sitio web se encuentra en castellano.

- Si tiene política de privacidad específica.

- Si el sitio web, por su apariencia y contenido, pudiera llegar a dar a entender que se dirige al territorio de España.

- Si la publicidad realizada es de productos y servicios distribuidos desde España." (P. 108)

Todo lo anterior, para saber que si se permite la autorregulación, se atenderán primero las exigencias y necesidades de la industria y muy difícilmente la de los individuos que son los que han dado el insumo, lo que hace aún más amplio su ámbito de desprotección legal debido a que los usuarios no cuentan con el presupuesto, tiempo ni el conocimiento para determinar el nivel de seguridad que ofrece cada página o red social, a diferencia de una regulación gubernamental que puede ofrecer confianza y un marco legal estable homogéneo internacionalmente en el mejor de los casos y con las herramientas para efectivizarlo.

7. CONCLUSIONES

En esta época de la globalización y el uso de las nuevas tecnologías a la vez que han contribuido a mejorar las condiciones de vida del ser humano, también se han generado complicaciones al momento de relacionarnos, comunicarnos y entendernos, lo que da lugar a un conjunto de relaciones altamente complejas y asimétricas tanto con la red social como entre usuarios.

Al ser este un fenómeno global, no se puede tratar de solucionar con legislación local, es decir de nada sirve la inflación legislativa sobre el tema si no existe un elemento común entre los estados que sea vinculante para la debida protección de los datos personales y los datos personales sensibles ante cualquier situación, porque no puede seguir la situación jurídica de que existen muchos países, muchas leyes y un solo internet.

De lo cual surge la necesidad de crear una convención internacional de protección de datos, donde impere la cooperación internacional de cada estado y así darle jurisdicción a un ente judicial existente para que conozca de estos casos, dando

como resultado mecanismos y autoridades que realmente velen y garanticen por la protección de los datos personales al ser un derecho fundamental.

Igualmente es necesaria la educación sobre el tema para concientizar, ya que no puede ser solo políticas restrictivas sino por el contrario, mejorar la eficiencia al ser políticas paralelamente preventivas para que el ciudadano común entienda los riesgos que corre, el tratamiento y destinación que tienen sus datos, en este caso en las redes sociales. Pero la educación no puede ser solo para los usuarios, se debe formar en el derecho informático a jueces, magistrados, es decir al aparato judicial en general.

Otra solución es la presión gubernamental, Brasil está entre los puestos más altos de estados que solicitan a Google, que retire contenidos de usuarios falsos o perfiles de la red social Orkut que promueven la prostitución y el turismo sexual en su país, Google no dio respuesta hasta que el gobierno de Brasil amenazara con cancelar el funcionamiento de sus instalaciones en el país, solo así Google dio respuesta positiva a las peticiones de dicho país. Igualmente los estados en la legislación pueden adoptar medidas "Opt In", es decir son medidas que propenden por la solicitud expresa de autorización previa al hecho de recolección.

Ahora bien, el uso de las redes sociales también puede ayudar a estar en contacto con los ciudadanos, ya que esta información o datos personales son el insumo del gobierno electrónico, lo que facilita en alguna medida la toma de decisiones o simplemente como medio para estar en contacto con la población y sus necesidades. Aquellos que pensaban que la vigilancia permanente que se mostraba en la obra *1948 de George Orwell* era distante, es probable que justo ahora tenga una cuenta activa en una red social. Es esta situación la que obliga a mirar la dignidad del ser humano y su protección desde el prisma de la justicia internacional, y como bien se sabe con el internet pasa igual que con la hidra mitológica, si se le cortaba una cabeza, rebrotan siete.

8. REFERENCIAS BIBLIOGRÁFICAS

- Agencia Española de Protección de Datos. (2009). *Estudios sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line. Instituto Nacional de Tecnologías de la Comunicación. INTECO.*
- Carta de derechos humanos de la unión Europea. Tomado el 15 de febrero de 2012, http://www.europarl.europa.eu/charter/pdf/text_es.pdf
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. 5 de enero de 2009.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. 31 de diciembre de 2008
- Ley 1482 de 2011. Por medio de la cual se modifica el Código Penal y se establecen otras disposiciones. (ley antidiscriminación). 30 de noviembre de 2011.
- Ley 679 de 2001. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la

explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. 3 de agosto de 2001.
- Constitución de la República Dominicana. Tomado el 25 de enero de 2012, http://www.jmarcano.com/mipais/politicos/title2.html#title2_1
- Constitución Política de Colombia. 20 de julio de 1991.
- Constitución Política de los estados Unidos Mexicanos. Tomado el 9 de febrero de 2012, http://info4.juridicas.unam.mx/ijure/fed/9/
- Corte constitucional. Sentencia T- 227/03. (Magistrado Ponente Eduardo Montealegre Lynett; 17 de marzo de 2003).
- Corte constitucional. Sentencia C-748/11. (Magistrado Ponente Jorge Ignacio Pretelt Chaljub; 6 de octubre de 2011).
- Corte constitucional. Sentencia T-260/12. (Magistrado Ponente Humberto Antonio Sierra Porto; 29 de marzo de 2012).
- Declaración de Santa Cruz de la Sierra de los jefes de estado y de gobierno de los países iberoamericanos (2003). Tomada el 12 de marzo de 2012, http://www.oei.es/xiiicumbredec.htm
- Declaración universal de los derechos humanos de 1948. Tomado el 23 de marzo de 2012, http://www.derechoshumanos.net/normativa/normas/1948-DeclaracionUniversal.htm?gclid=CKzrpaOata8CFRNS7Aod0B6-lA
- Escobar, E., Marulanda, L. (2004). *El derecho a la intimidad, segunda edición. Bogotá:* Ediciones Doctrina y Ley LTDA.
- *Facebook. (2012). Actualización de la Declaración de derechos y responsabilidades.* Tomado 14 de abril de 2012, https://www.facebook.com/note.php?note_id=10151417207465301
- Grupo de estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática. (2005, 20 de octubre). Documentos GECTI sobre el habeas data y la protección de datos personales. Bogotá, Author.
- Guerra, Y. (2012).*Derecho y tecnología.* Centro de investigaciones socio-jurídicas, Universidad Santo Tomás, Tunja.
- Madrid, A., Zubieta, H., Rocío, M., Peña, D. & Burgos, A. (2003). *El contrato por medios electrónicos.* Colombia: Departamento de derecho de los negocios, Universidad Externado de Colombia, Bogotá.
- Memorándum de Montevideo. *(2009). Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes.* Instituto de investigación para la justicia.
- Piñar, J., Remolina, N., Puccinelli, O. (2004). *Foro sobre protección de datos personales.* Colombia: Defensoría del pueblo.
- proyecto de ley estatutaria número 184 de 2010 senado, 046 de 2010 cámara. "por la cual se dictan disposiciones generales para la protección de datos personales"
- Remolina, N. (2010). *¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?*, International Law, Revista Colombiana de Derecho Internacional, 16, 489-524.
- Remolina, N. (2010, 15 al 28 de Noviembre). "striptease" informativo, redes sociales, ley de protección de datos personales y ética empresarial. Ámbito jurídico, p. 12.
- Remolina, N. (2010, 31 al 13 de Junio). Captura internacional de datos, un elemento que pone a prueba la capacidad de los estados. Ámbito jurídico, p.14.
- Remolina, N. (2012). *Insuficiencia de la regulación latinoamericana frente a la recolección internacional de datos personales a través de internet.* RevistaColombiana Quaestiones Disputatae 2, 179-226, Pontificia Universidad Javeriana, Bogotá.
- Téllez, J. (1987). *Derecho informático.* México: Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México.