HÁBEAS DATA Y DIRECCIÓN IP: UN MERCADO POTENCIALMENTE INSEGURO PARA LOS DATOS PERSONALES

ALVARO DE ANGULO SANZ

LUZ ANGELA DUARTE GONZÁLEZ

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS JURÍDICAS

MAESTRÍA EN DERECHO ECONÓMICO

BOGOTÁ, COLOMBIA

JULIO DE 2015

HÁBEAS DATA Y DIRECCIÓN IP: UN MERCADO POTENCIALMENTE INSEGURO PARA LOS DATOS PERSONALES

ALVARO DE ANGULO SANZ

LUZ ANGELA DUARTE GONZÁLEZ

TESIS, TRABAJO DE GRADO

Director de Tesis:

FERNANDO CASTILLO CADENA

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS JURÍDICAS

MAESTRÍA EN DERECHO ECONÓMICO

BOGOTÁ, COLOMBIA

JULIO DE 2015

RESUMEN

En el presente trabajo, se muestran los elementos jurídicos y microeconómicos que se consideran relevantes para tener en cuenta por parte del regulador en hábeas data, dado el mercado de la dirección IP; se realiza un análisis de diferentes teorías microeconómicas que permiten concluir que la clasificación formal de la dirección IP como dato personal, no es suficiente para garantizar la protección de la información personal que se comparte en Internet, siendo necesario una concientización por parte de los usuarios de Internet, de que toda la información al momento en que se comparte en la Red, adquiere el carácter de pública.

PALABRAS CLAVE: Dirección IP, hábeas data, privacidad, información personal, datos personales, mercado, regulación.

TABLA DE CONTENIDO

HÁBEAS DATA Y DIRECCIÓN IP: UN MERCADO POTENCIALMENTE INSEGURO PARA LOS DATOS PERSONALES

INTRODUCCIÓN

Actualmente, la humanidad se encuentra ante la peor crisis en materia de privacidad en toda la historia[1]. De hecho, Google es considerado como el mayor peligro en términos de hábeas data y existen fallos judiciales sobre el particular. En Colombia, y en razón al presente estudio, existe un Concepto del año 2015 en el cual la Superintendencia de Industria y Comercio sostiene que la dirección IP es un dato personal privado.

A nivel mundial se ha dado un intenso debate en términos de hábeas data y privacidad, sobre el tratamiento que se le debe otorgar a la dirección IP. En algunos países del mundo, ya se ha resuelto este interrogante y los diferentes tribunales o autoridades competentes se han pronunciado sobre el particular, aunque en diversos sentidos. Hay quienes consideran que la dirección IP no debe ser catalogada como un dato personal, ya que no se encuentra vinculada a una persona natural, sino que identifica a una máquina en internet[2]. Por otro lado, hay quienes sostienen que a través de la dirección IP se puede conocer hasta los aspectos más íntimos y sensibles de una persona[3].

---

[1] Tene, O. (2008). W*hat google knows: privacy and internet search engines.* Utah, Estados Unidos: Utah Lwa Review.
[2] En el capítulo Análisis Comparado se expondrá la sentencia del el Tribunal de Apelación de Paris.
[3] Como la Agencia de Protección de Datos Española.

El mercado de los datos personales ha tomado gran relevancia en la economía internacional y son considerados como la moneda de oro de la economía digital y el motor de la economía del siglo XXI[4].

En el presente trabajo se pretende brindar diferentes elementos de juicio, tanto jurídicos como económicos, para abordar un tema polémico y actual, como es la protección de datos personales en internet. Desde el punto de vista de los titulares de la información o los cibernautas en general, existe un desconocimiento o tolerancia excesiva frente al tratamiento que se les está otorgando a sus datos personales (este fenómeno se conoce como *the chilling effect*[5]).

Desde el punto de vista constitucional se requiere regular el tratamiento del dato personal, más aun cuando la dirección IP, como se expondrá en el presente trabajo, es solo una de las formas que debe regularse para garantizar el derecho al hábeas data como consecuencia de las tecnologías de la información y las comunicaciones.

Hoy en día es prácticamente imposible para una persona saber ¿qué datos se han recolectado sobre ella?, ¿quién los recolectó?, ¿qué usos le están dando a esa información?, ¿a quién le están permitiendo acceso a esa información?, o ¿a quién le están enviando o circulando sus datos personales? (Remolina, 2013, p. 2)

La hipótesis que se busca demostrar en el presente trabajo, es la siguiente: en Colombia existe un mercado de direcciones IP asociadas a personas determinadas o determinables; aquello que se intercambia es un dato compuesto por la dirección IP, y el usuario al que le otorgaron dicha dirección. Ese dato, al permitir identificar el sujeto que

---

[4] Remolina, N. (sin fecha determinada). 'Big data, big problema?'. *Ámbito Jurídico.* Recuperado de: http://www.ambitojuridico.com/BancoConocimiento/N/noti-130723-13big_data_big_problem/noti-130723-13big_data_big_problem.asp (Revisión 21/06/2015)13big_data_big_problem.asp

[5] Tene, O., *op. cit.*

navega e interactúa en internet, facilita acceder a los gustos y preferencias de los consumidores, por lo que tiene un valor intrínseco para las estrategias políticas, de mercadeo, religiosas, etc.

Para demostrar la mencionada hipótesis, se efectuará un análisis microeconómico del mercado de la dirección IP, entendida esta como un número asociado a una cuenta que identifica o podría identificar una persona[6], con el fin de concluir cómo éste podría resultar afectado según la regulación que se adopte sobre la materia en Colombia. Dentro de las diferentes posibilidades, en el presente trabajo se sostendrá que la dirección IP es un dato personal sensible que incluso podría estar asociado a menores de edad.

No obstante, no se puede perder de vista que la dirección IP es tan solo uno de los mecanismos con los que se puede asociar a una persona determinada en internet. Existen otras herramientas como cookies o mediante logging. Igualmente, desde el punto de vista técnico hay otras capas e identificaciones de un equipo en internet, como es el caso de la dirección MAC.

Por lo tanto, el presente trabajo abordará un análisis económico y desde la regulación de hábeas data de tan sólo una de las capas de identificación de un equipo en Internet (la dirección IP), dejando la preocupación abierta sobre la existencia de otras formas de conocer el comportamiento de un usuario en Internet.

[6] La mayoría de datos personales al analizarse de forma desagregada o individualizada, no tienen el potencial para determinar al titular de la información, aunque al agregarse, se produce el fenómeno conocido como BIG DATA.

1. Privacidad en Internet y Entendimiento de la Dirección IP

La información personal de los consumidores en términos de sus gustos y preferencias tiene un valor incalculable para las empresas y los departamentos de mercadeo.

Los consumidores, de forma algo desprevenida, dan su información personal a cambio de algún descuento o concurso, por nombrar algún ejemplo. Al momento de realizar las compras en el supermercado, si el consumidor está afiliado a algún programa de fidelidad, entregará toda la información relativa a sus gustos, preferencias, restricciones económicas etc., a cambio de un descuento o acumulación de puntos. Entre más información entregue el consumidor, mayor será el descuento o incentivo esperado.

En adición a la información personal que el usuario suministra de forma consciente y expresa, este tipo de registros en los supermercados genera un historial que permite garantizar una publicidad eficiente y dirigida al público correspondiente.

En la red sucede algo similar; los comerciantes se esfuerzan por tener la mayor cantidad de información posible. Desean conocer de qué pagina venimos, cuáles son los intereses del usuario, la capacidad adquisitiva, etc. En la web, la información es más dirigida. La idea es no perder recursos, por ejemplo, promocionando carteras a hombres o niños, no ofertar suntuosos hoteles a personas que no tienen la capacidad adquisitiva, o libros o música que no son de su preferencia.

Para no perder recursos con publicidad ineficiente, las empresas de mercadeo separan a sus clientes en “tribus”. Dependiendo de la “tribu” a la que pertenece, la publicidad se dirige en determinado sentido.

La información que se obtiene para poder clasificar a una persona dentro de determinada “tribu” radica en su comportamiento en internet. Hay empresas como Accenture[7] que dentro de sus servicios de consultoría incluye mercadotecnia basada en “perfiles virtuales”.

Teniendo claro lo anterior, en el presente capitulo se pretende evidenciar la tensión existente entre tecnología y privacidad y la dirección IP como un dato que permite identificar personas determinadas en la web. Para el efecto, se expondrán algunos casos ilustrativos como son: Caso What Google Knows y Caso Contiendas Electorales[8].

Posteriormente, se analizará el entendimiento de la dirección IP para los propósitos del presente trabajo, estudiando el alcance que podría tener en términos de identificación del usuario del mismo.

1.1. **Caso What Google Knows[9]**

Los motores de búsqueda son los actores centrales de internet y hoy en día Google es el rey indiscutible de las búsquedas. Google domina internet guiando usuarios a través del océano de datos no relacionados hacia la información buscada por el usuario con una precisión y velocidad sorprendente. Google juega con una interface simple y

[7] Accenture es una Compañía multinacional de consultoría de gestión, servicios tecnológicos y outsourcing.
[8] Baker, S. (2011) *Numerati. Lo saben todo de ti.* España: Seix Barral.
[9] Tene, O., *op. cit.*

amigable y un algoritmo complejo. Es evidente que Google es una poderosa herramienta que ha facilitado la forma en la que se navega en internet.

No obstante lo anterior, el poder que ha adquirido Google como el último árbitro en el éxito comercial de una empresa, ha llamado la atención hasta el punto que la existencia comercial de ésta depende de aparecer en los resultados de búsqueda de Google.

En igual sentido, existe una generalizada preocupación por el poder informático que ha adquirido Google, por la gran cantidad de datos personales que administra, convirtiéndose así en la base de datos central para usuarios de información personal.

No solamente porque registra las búsquedas realizadas por los usuarios, sino por que es quien almacena el correo electrónico (Gmail), la agenda (Calendar), las fotos (Picasa), videos (YouTube), blogs (Blogger), documentos (Docs y hojas de cálculo), redes sociales (Orkut), noticias (Reader), información de la tarjeta de crédito (Checkout); en términos generales, la vida digital de millones de usuarios.

El acceso y almacenamiento de grandes cantidades de información personal por parte de Google crea un serio problema en términos de privacidad. Edward Felten, científico en computación de Princeton, calificó esta situación como “el problema en términos de privacidad más complejo en toda la historia de la humanidad”[10]. Todos los días millones de usuarios proporcionan sin restricciones de ningún tipo, valiosa

[10] Baker, S., *op. cit.*

información personal relativa a intereses, necesidades, deseos, miedos, placeres e intenciones.

Que una empresa tenga tal poder sin mayores restricciones es una preocupación legítima, no solamente por el potencial "mal uso" que Google le pueda dar a esa información, sino por el "mal uso" que los Estados[11] o hackers[12] puedan realizar.

Como consecuencia de la regulación existente en Europa, Google ha accedido a disminuir el término de permanencia de la información recolectada mediante las búsquedas, de 18 a 9 meses. Google argumenta que uno de los insumos requeridos para que el motor de búsqueda funcione correctamente es el historial de búsquedas de los usuarios y se plantea el siguiente ejemplo: piénsese en un usuario que ingresa la siguiente búsqueda "Paris Hilton" en Google. Dependiendo de su historial de búsquedas Google va a lanzar resultados tales como: información de alojamientos en el hotel Hilton ubicado en Paris, o información relacionada con Paris Hilton. Google argumenta que su éxito depende del resultado de las búsquedas, que el historial es un factor determinante dentro del algoritmo desarrollado.

Privacy International, un reconocido grupo defensor de los derechos humanos, en el 2007 realizó un estudio comparando las políticas de privacidad de más de 20 proveedores de servicios en internet, incluyendo a Microsoft, Yahoo, Amazon e eBay[13]. En dicho estudio, Google fue el proveedor peor rankeado y Privacy International calificó

[11] Existe colaboración entre Google y el Gobierno de EEUU en materia penal y de inteligencia nacional.
[12] En reiteradas oportunidades los sistemas de seguridad de Google han sido superados por Hackers y ladrones de identidad.
[13] Tene, O., *op. cit*.

a Google como una amenaza endémica para la privacidad y criticó el uso agresivo e invasivo que por medio de la tecnología está realizando Google respecto a la información personal de los usuarios.

El 13 de mayo de 2014, en un polémico fallo, el Tribunal de Justicia de la Unión Europea resolvió un caso originado por la inconformidad de un ciudadano español frente al resultado de la búsqueda cuando alguien "googleaba" su nombre (arrojaba información relacionada a una deuda antigua).

En este caso, Google mencionaba que este buscador no realizaba tratamiento a ninguna información y que los contenidos no eran creados por Google. En esa medida ellos no se pueden hacer responsables frente al contenido de terceros que ha sido encontrado por el motor de búsqueda en Internet. El Tribunal, por el contrario, consideró que Google sí realizaba tratamiento de datos personales[14], toda vez que almacena las búsquedas realizadas y los resultados de dichas búsquedas.

> La actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales»"(Tribunal de Justicia de la Unión Europea, 1993).

[14] Según el artículo 3º de la Ley 1581 de 2012, en Colombia se entiende como Tratamiento, "Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."

En este caso, el Tribunal señaló que el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona, los vínculos a páginas web publicadas por terceros y que contienen información que afecte a esta persona; incluso, los motores de búsqueda deben eliminar esta información así ésta no haya sido borrada de la página del tercero.

1.2. **Caso Contiendas electorales**

Existe un fenómeno interesante en las últimas contiendas electorales en donde los hackers, la información personal, e Internet, juegan un papel importante.

Stephen Baker, señala que en las contiendas electorales, la minería de datos desempeña un rol importante desde diferentes ángulos.

Por un lado, las búsquedas, consultas, páginas visitadas y en general el comportamiento de las personas en Internet, permiten inferir las inclinaciones políticas de una persona determinada. Este tipo de información permite calificar a los potenciales electores en diferentes grupos.

El principal interés se centra en aquellos votantes indecisos a quienes se debe dirigir la mayor cantidad de recursos en las campañas.

Igualmente, dicha información permite realizar discursos de campañas enfocados a cada grupo dependiendo de sus intereses y necesidades.

De acuerdo con los casos mencionados, es claro que la información personal que revelan las personas a través de internet es explotada económicamente para diferentes

propósitos, tales como mercadeo, campañas políticas, o incluso relaciones interpersonales.

Se considera que esta información podría entrar en el marco de la regulación en materia de hábeas data, siempre y cuando se encuentre individualizada; de lo contrario es simple información estadística y uno de los mecanismos (no el único) para asociar a una persona con un comportamiento en internet es través de la dirección IP, toda vez que como se explicará a continuación, cada persona para ingresar a internet, requiere de una dirección que permita el intercambio de información en la red.

1.3. **Entendimiento de la dirección IP**

Para los fines planteados en el presente trabajo, es imprescindible entender que la dirección IP (siglas dadas por su significado en inglés “Internet Protocol”), es una de las herramientas esenciales que permiten la comunicación a través de internet.

La dirección IP es aquel número que da la ubicación del sujeto que envía un mensaje en la red, con el fin de que reciba su respuesta; incluso se podría asociar la IP con la dirección de correspondencia de cada usuario en la red.

La forma en que las máquinas conectadas a internet se comunican, es a través de la dirección IP, haciendo posible que la información sea enviada y recibida por su exacto destino en Internet.

Actualmente, existen dos tipos de direcciones IP en uso: IPv4 e IPv6.

La primera de ellas (IPV4), fue desarrollada inicialmente el 1º de enero de 1983, y es la versión más usada (IANA); está compuesta por 32-bits que se divide en dos partes: el número de red y el número de computadora. Asimismo, los 32 bits son divididos en 4

grupos de 8 bits, separados por puntos, y son representados en formato decimal (por ejemplo, 181.129.79.193). Cada bit en el octeto tiene un peso binario. El valor mínimo para un octeto es 0 y el valor máximo es 255 (Network Information Center Mexico, S.C.).

La segunda versión de la dirección IP, denominada IPv6, se generó en el año 1999, en atención a que la IPv4 no estaba siendo suficiente para la alta demanda de direcciones IP. La IPv6 está compuesta por un número de 128 bits, lo cual permite 360 sextillones de direcciones IP, mientras que la IPv4 permitía un máximo de 4.294.967.296 direcciones IP (ICANN).

Para el desarrollo de toda la dinámica que implica la comunicación en internet, se han constituido varios organismos que garantizan un Internet seguro, estable y adaptable a las diferentes tecnologías que se vayan desarrollando.

Es así como se constituye la Corporación para la Asignación de Nombres y Números en Internet – ICANN, como una organización internacional sin ánimo de lucro que integra a representantes gubernamentales y no comerciales, al sector industrial y a particulares con el objetivo de discutir, debatir y desarrollar políticas sobre la coordinación técnica del sistema de nombres de dominio de internet (ICANN).

Como una dependencia de la ICANN, se encuentra la Autoridad de Números Asignados en Internet – IANA, la cual es la responsable de la coordinación global de las direcciones IP. La IANA ubica las dirección IP a los diferentes Registros Regionales de Internet[15], quienes a su vez, asignan las direcciones IP a los PSI (Proveedores de Servicios de Internet).

[15] Existen cinco (5) Registros Regionales de Internet: AFRINIC, APNIC, ARIN, LACNIC y RIPE NCC.

La asignación de este número a cada equipo es efectuada por el PSI, quien es el encargado de escoger la dirección IP que asignará a cada usuario. De esta forma, quien conozca qué dirección IP tiene asignada una máquina, podrá determinar con sólo rastrear la dirección IP, el comportamiento que ha tenido en Internet.

Si bien la dirección IP puede ser dinámica (cambia cada vez que se ingresa a internet) o estática, el PSI siempre tiene la posibilidad de conocer qué usuarios han accedido a Internet con determinada dirección IP.

Aterrizando lo anterior a una realidad más cercana, imagínese que por la dirección IP que es asignada a su teléfono inteligente de su propiedad (información que es conocida y puede ser transada por el PSI) se puede identificar de una forma más detallada (incluso, más privada) verificando las páginas electrónicas que se han visitado, los correos que se han enviado, incluso los mensajes instantáneos que se han compartido, y por supuesto, la información personal que se ha puesto a disposición de la red.

Así, es en razón a la posibilidad que tienen diferentes sujetos de acceder a una información tan personal, como la que se asocia a los teléfonos celulares, que es imprescindible analizar si la dirección IP es o no un dato que por ser asociable a una persona, pueda ser considerado como un dato personal, como se expondrá a continuación.

2. El hábeas data en Colombia y la dirección IP

En el presente capítulo se pretende realizar una contextualización en materia de hábeas data, tener un entendimiento del objeto de estudio y del problema que se busca resolver en el presente trabajo.

Para el efecto, en primer lugar, se realizará una descripción de la evolución en materia legal y jurisprudencial frente el derecho al hábeas data. En segundo lugar, se expondrá el problema existente entre protección de datos personales y la dirección IP como herramienta para identificar técnicamente a “equipos” en internet; se planteará cómo se ha resuelto el interrogante en otros países y se expondrá el caso colombiano.

En tercer lugar, se explicará que la dirección IP en algunos casos se encuentra asociada a información sensible del titular e incluso vinculada a menores de edad.

2.1. El hábeas data en Colombia

El derecho fundamental al hábeas data ha ganado protagonismo tanto en el escenario internacional, como en el doméstico.

La Sentencia proferida por el Tribunal de Justicia de la Unión Europea, del 13 de mayo de 2014, es un caso interesante de estudio ya que evidencia un debate profundo entre el ejercicio de un derecho abstracto contra realidades técnicas y tecnológicas que dificultan su protección.

En Colombia podemos evidenciar un cambio profundo a partir de la expedición de la Ley 1581 de 2012 y su respectiva reglamentación. Dicho cambio se puede ver en el

ejercicio de las empresas[16] quienes solicitan autorizaciones para realizar tratamiento de datos personales, cuentan con políticas para la realización de dicho tratamiento y, en general, han adoptado mayores estándares de protección, y mejores prácticas corporativas sobre el particular.

Adicionalmente, es claro el papel dinámico de la Superintendencia de Industria y Comercio (en adelante SIC), quien ha tomado polémicas decisiones que afectan tanto al Estado como a los particulares. Igualmente, en Colombia se incorporó un novedoso mecanismo de supervisión y vigilancia (responsabilidad demostrada o accountability) y recientemente se sumó a pronunciamientos proteccionistas que han considerado la dirección IP como un dato personal.

Existen condenas en materia penal y actualmente hay ciudadanos pagando condenas restrictivas de la libertad, por conductas que atentan el derecho al hábeas data[17].

En el presente capítulo se pretende describir la evolución del derecho al hábeas data en Colombia de manera esquemática. Para el efecto se dividirá el proceso en tres etapas: (i) Periodo comprendido entre la promulgación de la C.N. y la sanción de la Ley 1266 de 2008[18]; (ii) periodo comprendido entre la sanción de la Ley 1266 de 2008 y la

[16] Algunas empresas tenían incorporados estándares de protección, incluso con anterioridad a la sanción de la Ley 1266 de 2008, en cumplimiento a pronunciamientos jurisprudenciales emitidos por la Corte Constitucional en sede de tutela. No obstante, estas prácticas se encontraban solamente en algunos sectores de la economía, principalmente centrales de información.
[17] Sentencia del trece (13) de septiembre de dos mil once (2011), de la Corte Suprema de Justicia, Sala de Casación Penal, M.P., Magistrado Ponente, Fernando Alberto Castro Caballero.
[18] Con anterioridad a la Constitución de 1991 existían normas que protegían datos personales sectoriales, tales como historias médicas (Ley 23 de 1981) y datos referentes a la identidad de las personas, como son sus datos biográficos, su filiación y fórmula dactiloscópica (Ley 96 de 1985).

sanción y reglamentación de la Ley 1581 de 2012 y; (iii) Desde la Sanción de la Ley 1581 de 2012 a la actualidad.

Lo anterior, con el propósito de brindar elementos de juicio mediante una aproximación al estado del arte en materia de hábeas data en Colombia.

2.1.1. Periodo comprendido entre la promulgación de la C.N. y la sanción de la Ley 1266 de 2008 (1991-2008).

Con la promulgación de la Constitución de 1991 se reconoció el derecho al hábeas data y se le otorgó el rango de derecho fundamental. No obstante, fue hasta la sanción de la Ley 1266 de 2008 (para el dato de contenido crediticio, comercial y financiero) y particularmente hasta la sanción de la Ley 1581 de 2012, que se contó con una Ley Estatutaria que desarrollara la materia frente a la universalidad de datos personales.

> "El artículo 15 significó un antes y un después en la materia, no solo por su novedad en aquella época, sino por su actual relevancia social y económica, porque estamos en la denominada "sociedad de la información" o "era de la información", en la que los datos personales son el eje de muchas actividades y la moneda de la economía digital" (Remolina, 2013, p. XXI).

Esta etapa se caracteriza por un importante desarrollo jurisprudencial, ya que al no existir una norma estatutaria, la protección de este derecho se ejercía mediante acciones de tutela que carecían de efectos erga omnes (lo anterior sin prejuicio de la Sentencia

SU 082 de 1995) cuyo desarrollo es principalmente la jurisprudencia constitucional en sede de tutela. En esta etapa se establecen los aspectos fundamentales del derecho, así como algunas reglas concretas, siendo destacable lo siguiente:

- ***Entendimiento del derecho al hábeas data como un derecho autónomo.***

En un comienzo, la Corte Constitucional no entendió el derecho al hábeas data como un derecho autónomo; en su defecto la Corte consideró que era parte del derecho a la intimidad, la honra y el buen nombre.

A partir de la Sentencia T-094 de 1995[19], la Corte cambió su posición y reconoció al hábeas data como un derecho autónomo. No obstante, lo trataba como una garantía, ya que lo consideraba como un instrumento para la protección de derechos, tales como la intimidad, la honra y el buen nombre.

En 1995, con la sentencia SU-082 de 1995, la Corte reconoció el derecho al hábeas data como un derecho independiente en los siguientes términos:

> A diferencia de lo que ocurre en otras legislaciones, en Colombia el hábeas data está expresamente establecido en la Constitución. Al respecto, el artículo 15, después de consagrar los derechos de todas las personas a la intimidad y al buen nombre, agrega: "De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido

[19] Colombia. Corte Constitucional. Sentencias T-094 de 1995, T-097 de 1995 y T-119 de 1995.

sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Este, concretamente, es el derecho al hábeas data.

En la Sentencia T-552 de 1997, la Corte precisó las diferencias entre el derecho a la intimidad y el hábeas data, después de que la relación entre ambos se había manejado como de género a especie, desde el año de 1992[20].

En dicha sentencia la Corte señaló que "El derecho al hábeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa..." (Corte Constitucional, Sentencia T-552 de 1997).

Con posterioridad, la Corte reafirmó este punto señalando: "De otra parte, la Corporación debe reiterar, una vez más su doctrina jurisprudencial, en el sentido de que el artículo 15 superior establece tres derechos con sus dimensiones específicas a saber: el derecho a la intimidad, al buen nombre y al hábeas data" (Corte Constitucional, Sentencia T-527 de 2000).

- ***Conceptualización, delimitación y alcance del derecho fundamental.***

[20] Colombia. Corte Constitucional. Sentencia T-729 de 2002 M.P. Magistrado Ponente: Dr. Eduardo Montealegre Lynett.

En este periodo, la Corte señaló los aspectos determinantes del derecho al Hábeas Data, los cuales siguen vigentes en la actualidad y se encuentran replicados en las leyes estatutarias que desarrollan dicho derecho. En este sentido se conceptualizó el alcance y definición propia del derecho, se estableció cuál es el núcleo esencial del mismo y las prerrogativas y contenidos mínimos.

La Corte Constitucional en esta etapa señaló, que entre las prerrogativas-contenidos mínimos- que se desprenden de este derecho, se encuentran las siguientes: (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 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 por que 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 de 2011).

- ***Núcleo esencial del derecho.***

La Corte Constitucional en el periodo descrito, estableció que el núcleo esencial del derecho al hábeas data es la autodeterminación informativa, entendida como “la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso

y circulación, de conformidad con las regulaciones legales" (Corte Constitucional, Sentencia SU-082 de 1995).

- ***Reglas específicas frente al tratamiento de datos personales.***

La Corte Constitucional, particularmente frente al dato de contenido comercial, crediticio y financiero, mediante sentencias de unificación, fijó las reglas específicas frente al tratamiento de los datos personales. Entre dichas reglas, se encuentran las siguientes:

- Término de caducidad de la información negativa (derecho al olvido): "*El término para la caducidad del dato lo debe fijar, razonablemente, el legislador. Pero, mientras no lo haya fijado, hay que considerar que es razonable el término que evite el abuso del poder informático y preserve las sanas prácticas crediticias, defendiendo así el interés general. Si el pago se ha producido en un proceso ejecutivo, es razonable que el dato, a pesar de ser público, tenga un término de caducidad, que podría ser el de cinco (5) años. Sin embargo, cuando el pago se ha producido una vez presentada la demanda, con la sola notificación del mandamiento de pago, el término de caducidad será solamente de dos (2) años, es decir, se seguirá la regla general del pago voluntario.*"
- Principio de la Libertad informática: "*En relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes, a las centrales de información que para el efecto se han creado, así como la facultad de reportar a quienes incumplan las obligaciones con ellos contraídas, tiene como base fundamental y punto de equilibrio, la*

autorización que el interesado les otorgue para disponer de esa información, pues al fin y al cabo, los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar. Autorización que debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho."

Los aspectos tratados y desarrollados desde este periodo y que han sido reiterados en muchas sentencias posteriores son:

- La dignidad humana como supremo principio de la Constitución de 1991.
- La definición de una cuarta generación de derechos.
- Creación de la regla jurisprudencial que establece la prevalencia del derecho a la intimidad sobre el derecho a la información.
- Creación de la regla jurisprudencial que señala que el titular de la información es el propietario de sus datos personales.
- Incorporación en la jurisprudencia de conceptos de libertad informática, hábeas data, derecho constitucional informático, cárcel del alma, perfiles de personas virtuales, poder informático, y derecho al olvido.
- Establecimiento de la necesidad de la autorización previa del titular del dato como requisito para el tratamiento de datos personales, cumplimiento del "debido proceso informático" y del uso responsable de la informática. (Remolina, 2013, p. 31.)

2.1.2. Periodo comprendido entre la sanción de la Ley 1266 de 2008 y la sanción y reglamentación de la Ley 1581 de 2012 (2008-2012)

Este periodo comienza con la sanción de la Ley Estatutaria 1266 de 2008 y termina con la sanción de la Ley Estatutaria 1581 de 2012.

En virtud de la Ley 1266 de 2008, los conceptos, definiciones, principios para la administración de datos personales, así como la adopción de reglas concretas para la caducidad del dato negativo, quedaron estipuladas en una norma estatutaria.

En igual sentido, la Corte Constitucional, al realizar el análisis previo de constitucionalidad a la Ley Estatutaria, mediante la Sentencia de Constitucionalidad C-1011 de 2008, realizó una recopilación de la jurisprudencia de dicha Corte sobre la materia, elevando los efectos de la jurisprudencia de la Corte en sede de tutela, a sentencia de constitucionalidad con efectos erga omnes.

La Ley 1266 de 2008, estableció los derechos y deberes correspondientes a cada actor involucrado en el tratamiento de datos personales (Titular de la Información, Operador de la información, Fuentes de la Información y Usuarios de la Información); señaló las reglas específicas frente al término de permanencia de la información negativa, dispuso un proceso especial para las peticiones, consultas y reclamos de los titulares, y creó una autoridad en materia de hábeas data, con facultades de inspección, control y vigilancia, y con capacidad para imponer sanciones pecuniarias (la Ley asignó estas competencias a la Superintendencia de Industria y Comercio)[21].

[21] La Superintendencia Financiera conservó estas facultades, frente a las entidades vigiladas por ésta. Esta situación, es decir, dos Superintendencias ejerciendo una vigilancia sobre el mismo aspecto legal,

Durante este periodo existió ambigüedad frente al ámbito de aplicación de la norma como se procederá a explicar.

- ***Ambigüedad teórica frente al ámbito de aplicación de la Ley 1266 de 2008.***

El artículo 2º de la Ley 1266 de 2008, estableció el ámbito de aplicación de la norma señalando que "La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada. (…)".

La Corte Constitucional, en el respectivo análisis previo de constitucionalidad, consideró que el ámbito de aplicación era exclusivamente frente a los datos de contenido comercial, crediticio y financiero relacionados con el cálculo del riesgo crediticio.

> La dicotomía existente en el Proyecto entre disposiciones de carácter general, que por su naturaleza regularían todo el espectro de relaciones derivadas de la administración de datos personales y normas particulares, destinadas a prever las reglas para la gestión de datos relacionados con el cálculo del riesgo creditito es, en criterio de la Corte, apenas aparente. Ello en tanto concurren varios argumentos para concluir que el proyecto de ley estatutaria objeto de examen constituye una regulación parcial del derecho fundamental al hábeas data, concentrada en las reglas para la administración de datos personales de carácter financiero destinados al

---

pero dependiendo de la actividad de la persona objeto de la vigilancia, puede generar una suerte de arbitramento regulatorio donde un actor podía encontrar ventajas regulatorias, dependiendo de quién lo vigile.

cálculo del riesgo crediticio, razón por la cual no puede considerarse como un régimen jurídico que regule, en su integridad, el derecho al hábeas data, comprendido como la facultad que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos y bancos de datos de naturaleza pública o privada. Para sustentar esta conclusión existen argumentos de carácter sistemático, teleológico e histórico, como pasa a explicarse.

(…)

Las consideraciones expuestas demuestran que el Proyecto de Ley tiene un propósito unívoco, dirigido a establecer las reglas para la administración de datos personales de contenido financiero y crediticio. Esta comprobación, como lo han puesto de presente algunos de los intervinientes y el Ministerio Público, plantea dos aspectos que deben analizarse de forma específica: (i) la legitimidad que el legislador estatutario realice regulaciones de los derechos fundamentales, aplicables de manera sectorial; y (ii) la objeción fundada en que regulaciones de esta naturaleza violan la Constitución, en tanto incurren en una omisión legislativa relativa."

(Corte Constitucional, Sentencia C-1011 de 2008)

No obstante lo anterior, la Corte Constitucional en la parte resolutiva de la Sentencia declaró la constitucionalidad del artículo 2º sin ninguna condición[22].

[22] Parte motiva de la Sentencia C-1011 de 2008 "Segundo.-Declarar EXEQUIBLES los artículos 1º, 2º, 4º, 7º, 8º, 9º, 10, 11, 12, 15, 16, 18, 19, 20, 21 y 22 del Proyecto de Ley Estatutaria objeto de revisión".

El hecho de que la Corte hubiese declarado exequible el artículo 2º del Proyecto de Ley Estatutaria, sin ningún tipo de condicionamiento, a pesar de que en la parte motiva dispuso que se trataba de una norma sectorial, generó incertidumbre frente al ámbito de aplicación de la norma. Por lo tanto, al no existir relación entre la parte motiva y la resolutiva, se puede entender como obiter dicta o obiter dictum, perdiendo así fuerza vinculante.

Este argumento cobra mayor relevancia si se tiene en cuenta que mediante el Auto Aclaratorio 159 de 2009, la Corte aclaró y corrigió algunos aspectos de la Sentencia C-1011 de 2008. Dichos aspectos, aclararon y corrigieron el contenido de la Sentencia, tanto en la parte motiva como resolutiva. En este Auto Aclaratorio, la Corte no se pronunció frente al “error” anteriormente mencionado.

Siendo así las cosas, podría interpretarse válidamente que la intensión de la Corte no fue delimitar el ámbito de la Ley, y dentro de la disquisición realizada por ésta, los argumentos expuestos en la parte motiva, que restringen el ámbito de aplicación de la Ley, es simple obiter dicta sin poder vinculante.

Este periodo es importante ya que además de contar con la primera Ley Estatutaria que desarrollara el artículo 15 de la Constitución Política, en materia de hábeas data, en enero de 2009, se sancionó la Ley de delitos informáticos la cual introdujo el siguiente tipo penal:

> 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. (Congreso de la República de Colombia, Ley 1273 de 2009)

Por último, es pertinente señalar, que al crearse una autoridad en materia de hábeas data, se generó una nueva fuente de derecho (fuente auxiliar) consistente en la doctrina de la Superintendencia de Industria y Comercio a través de los conceptos expedidos por ésta.

2.1.3. Desde la Sanción de la Ley 1581 de 2012 hasta la actualidad.

En este subcapítulo se pretende abordar el periodo comprendido entre el 18 de octubre de 2012 (sanción de la Ley 1581 de 2012) hasta la actualidad. En primer lugar se mencionarán las principales razones que dieron origen a la Ley 1581. En segundo lugar, se pretende mencionar algunos impactos que ha tenido dicha normatividad y, por último, se mencionará el nuevo sistema de inspección, control y vigilancia introducido por el Decreto 1377 de 2013.

- ***Principales razones que dieron origen a la Ley 1581 de 2012.***

Según Nelson Remolina, las principales razones que dieron origen a la Ley 1581 de 2012, fueron las siguientes:

- Insuficiencia y deficiencia de la Ley Estatutaria 1266 de 2008 para proteger los datos personales diferentes a los de índole comercial y financiera.
- Necesidad de establecer reglas obligatorias, generales e integrales para el tratamiento de datos personales que respondan a la reglamentación integral de un derecho fundamental.
- Generación de un marco legal para que Colombia obtenga el nivel adecuado de protección frente a las autoridades europeas y cuente con un marco legal competitivo que facilite la realización de negocios que impliquen tratamiento de datos personales. (Remolina, 2013, p. 82)

Respecto al primer punto, como se mencionó anteriormente, la Corte Constitucional restringió el ámbito de aplicación de la Ley Estatutaria 1266 (independientemente de la discusión señalada frente al poder vinculante de dicha restricción), generando así la necesidad de contar con otra Ley que desarrolle el artículo 15 de la Constitución, pero frente a todos los datos personales y no solamente respecto a los datos de contenido comercial, financiero y crediticio.

Con la sanción de la Ley 1581 de 2012, terminó la ambigüedad señalada anteriormente, por lo que en la actualidad Colombia cuenta con dos leyes estatutarias que desarrollan el derecho al hábeas data: una de aplicación general (Ley 1581 de 2012) y otra de carácter sectorial (Ley 1266 de 2008).

En cuanto al segundo y tercer punto mencionado por el profesor Remolina, es importante tener en cuenta la importancia de contar con reglas generales, integrales y obligatorias frente al tratamiento de datos personales, y poder ser considerado como un país con un nivel adecuado en la materia. Entre otros aspectos, tener un nivel adecuado

permite la transferencia internacional de datos personales con países que sí cuentan con un nivel adecuado. Sobre el particular, la exposición de motivos del proyecto de Ley 046 de 2010 de la Cámara de Representantes (previo tránsito por el Congreso y revisión por parte de la Corte, este proyecto fue sancionado como la Ley Estatutaria 1581 de 2012) dispuso lo siguiente:

> Por último es importante mencionar que en la actualidad Colombia es considerada como un país no seguro en protección de datos por la Comunidad Europea. Este hecho se traduce en un obstáculo comercial a la transferencia de datos personales de ciudadanos europeos para que sean tratados en Colombia y limita sustancialmente el crecimiento del sector de tercerización de procesos de negocio (BOP&O), identificado por el gobierno como un sector de clase mundial en el marco del Programa de Transformación Productiva (Exposición de Motivos de la Cámara de Representantes, Proyecto de Ley 046 de 2010)

Este proyecto incorpora en su articulado las mejores prácticas internacionales en materia de protección de datos; estas prácticas se encuentran contempladas en el Convenio 108 de 1981 del Consejo de Europa, la Directiva Europea 95/46 de 1995, la Resolución 45/95 de 1990 de la ONU y la Resolución de Madrid de 2009. El esfuerzo del Estado por expedir esta Ley Estatutaria, tuvo como objetivo lograr la acreditación de Colombia por parte de la Unión Europea, como un país seguro en la protección de datos y así poder acceder al mercado europeo sin restricciones atrayendo inversión extrajera

y generando nuevos empleos[23].

- ***Algunos Impactos de la Ley 1581 de 2012.***

Con la sanción de la Ley 1581 de 2012, y en particular con la expedición del Decreto 1377 de 2013, las empresas[24] comenzaron a solicitar autorizaciones en adelante y tuvieron que subsanar la situación frente a los datos recolectados antes de la su expedición.

Esto significó que cada empresa que contara con bases de datos o archivos con datos personales (piénsese en clientes, proveedores o usuarios) tuviese que tratar de contactarse con cada uno para solicitar autorización, salvo que demostrara una imposibilidad para requerir el consentimiento uno a uno, caso en el cual debía informar al titular de la información utilizando medios de comunicación masivos.

Lo anterior implicó que durante el segundo semestre del año 2013 cada titular de la información (prácticamente cualquier persona) recibiese diferentes solicitudes de autorizaciones a través de correos electrónicos, correspondencia postal, mensajes de texto, llamadas telefónicas y que además viese anuncios en las páginas web, periódicos, revistas etc.

[23] Colombia. Cámara de Representantes. Exposición de Motivos del Proyecto de Ley Estatutaria 046 de 2010, Gaceta del Congreso No. 488 de 2010.
[24] Con excepción de aquellas empresas que se encontraban obligadas en virtud de la Ley 1266 de 2008, las cuales ya contaban con autorizaciones.

Igualmente, diferentes empresas y entidades públicas han adoptado altos estándares de protección de datos personales y han capacitado a sus respectivos empleados para tal fin[25].

Esto ha significado un avance hacia una cultura de protección de datos personales, lo cual se puede evidenciar en los diferentes casos que se presentan ante los jueces o la superintendencia, como se demostrará a continuación.

Al revisar la jurisprudencia de la Corte Constitucional, se evidencia que con anterioridad a la Ley 1581 de 2012, la gran mayoría de casos presentados surgen con ocasión al tratamiento de datos personales de contenido comercial, crediticio y financiero (DATACREDITO-CIFIN).

Se trata, en términos generales, de titulares de la información, reclamando por los datos que sobre ellos reposan en las centrales de información.

Con posterioridad, se presentaron ante las Cortes y Superintendencia, diferentes casos con supuestos fácticos diversos. A manera de ejemplo se presentaron en sede de tutela casos relacionados con los siguientes datos personales:

- Datos contenidos en bases de datos de EPS´s relacionados con preexistencias médicas (Corte Constitucional, Sentencia T-802/13).
- Datos relativos a imágenes con fines publicitarios (Corte Constitucional, Sentencia T-634/13)

[25] Sobre el particular es pertinente señalar que la SIC cuenta con programas de capacitaciones para las empresas.

- Datos relativos a los certificados laborales para la emisión del bonos pensionales (Corte Constitucional, Sentencia T-592/13).
- Datos contenidos en las bases de datos de las universidades para la generación de certificaciones académicas (Corte Constitucional, Sentencia T-058/13).
- Datos contenidos en la base de datos de la Procuraduría General de la Nación para la generación de certificados de antecedentes disciplinarios (Corte Constitucional, Sentencia T-699/14).
- Datos contenidos en la base de datos en la "Lista Clinton" (Corte Constitucional, Sentencia T-363/14).
- Datos contenidos en la base de datos DEFENCARGA y COLFECAR relativo a los de incidentes presentados (Corte Constitucional, Sentencia T-176A/14).

Igualmente, es importante mencionar que la Superintendencia de Industria y Comercio en comunicado del 23 de enero de 2014 le pide a la Corte Suprema de Justicia "suprimir datos de menores de edad en versiones públicas de las sentencias"[26].

- ***Nuevo sistema de inspección, control y vigilancia: responsabilidad demostrada frente al tratamiento de datos personales.***

Con anterioridad al Decreto 1377 de 2013, para que una empresa fuese sancionada por la SIC, el caso objeto de reclamación debía ser interpuesto en primer

[26] Igualmente, es importante mencionar que la Superintendencia de Industria y Comercio en comunicado del 23 de enero de 2014 le pide a la Corte Suprema de Justicia "suprimir datos de menores de edad en versiones públicas de las sentencias" http://www.sic.gov.co/drupal/noticias/node/7038 (Revisado 21/06/2015).

lugar, frente al Responsable o el Encargado del Tratamiento y en caso de que el reclamo subsistiera, el titular podía acudir a la SIC para que investigara y tomara una decisión.

Con el nuevo sistema de inspección, control y vigilancia, la SIC a su completa discreción, puede investigar a cualquier empresa y será la empresa la encargada de demostrar su diligencia y cuidado.

Este cambio implica, en primer lugar, una variación en el rol de las empresas, pasando de un rol reactivo (su actuar inicia con un reclamo o queja) a un rol proactivo, ya que en cualquier momento puede ser objeto de una investigación, y teniendo en cuenta que la carga de la prueba la asume la empresa, ésta deberá demostrar que se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012.

Dichas medidas, y en general el estándar de cuidado esperado, depende de los criterios establecidos en el mismo: naturaleza jurídica, tamaño de la empresa, naturaleza de los datos objeto de tratamiento, el tipo de tratamiento y el riesgo potencial del tratamiento sobre los derechos del titular.

En segundo lugar, este cambio implica el inicio de un modelo que promueve la autorregulación de las empresas en materia de protección de datos personales. Este tipo de modelo, conocido como “accountability”, obliga a la empresa a demostrar su responsabilidad, cuidado y diligencia, promueve la autorregulación y ha demostrado ser

un modelo exitoso para alcanzar un nivel adecuado en materia de protección de datos personales[27].

Por último, se presenta un cuadro que resume la evolución en materia de protección de datos personales en Colombia.

Tabla 1
Evolución del Hábeas Data en Colombia[28]

	1991-2008	2008-2012	2012 a la fecha
▪ **Norma Constitucional**	x	x	x
▪ **Principios básicos jurisprudenciales**	x	x	x
▪ **Principios Legales**		x	x
▪ **Normas Sectoriales**		x	x
▪ **Norma General**			x
▪ **Autoridad de control, inspección y Vigilancia**		x	x
▪ **Norma Penal**		x	x
▪ **Sistema de supervisión y control basado en la diligencia probada**			x

2.2. Entendimiento de la dirección IP como dato desde la regulación de hábeas data.

La Ley 1581 de 2012 define dato personal como “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”.

[27] Ornelas, L. G., Higuera, M. (2013). *La autorregulación en materia de protección de datos personales: la vía hacia una protección global.* (Spanish). *Revista De Derecho Comunicaciones Y Nuevas Tecnologías*, (9), 1-30.
[28] Fuente de la Tabla: Elaboración propia

En igual sentido la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, define dato personal como “toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”.

La pregunta que surge es si la dirección IP en los términos expuestos constituye un dato personal o no. Esta cuestión ha sido objeto de diferentes pronunciamientos por parte de diversas autoridades en varios Estados, que se expondrán en el capítulo Análisis Comparado.

La respuesta tiene implicaciones importantes ya que una decisión en uno u otro sentido significa la aplicabilidad de las normas en la materia frente a este dato.

En caso de que sea considerado como un dato personal, esto implica que los PSI tienen la calidad de responsables del tratamiento y deben cumplir con una serie de obligaciones cuyo cumplimiento implica toda clase de retos en términos tecnológicos.

Sobre el particular, es de considerar importante la posición de Google sobre la dirección IP en términos de protección de datos personales, así como de la SIC.

2.2.1. Posición de GOOGLE[29].

Google, a través de su blog oficial emitió un comunicado sentando su posición frente a si la dirección IP debe ser considerada como un dato personal.

En términos generales, Google tiene una posición mixta bajo el entendido de que en algunas ocasiones la dirección IP es un dato personal y en otras no.

Google explica que la dirección IP le permite a una página enviar la información (piénsese en el resultado de una búsqueda) al equipo correcto. Igualmente, señala que la dirección IP es un recurso escaso y, en consecuencia, los PSI maximizan su utilidad reasignando la misma dirección IP a varios usuarios (lo anterior, teniendo en cuenta que no todos los usuarios se conectan al mismo tiempo).

Igualmente, señala que una misma dirección IP puede ser utilizada por varias personas si el equipo o la conexión a internet se comparte con varias personas.

Dado lo anterior, una misma dirección IP puede ser asignada a múltiples personas, y varias personas pueden conectarse utilizando la misma dirección IP, por lo que no siempre es posible asociar una dirección IP a una persona específica.

No obstante lo anterior, Google reconoce que en algunos contextos la dirección IP sí es un dato personal, y esto sucede cuando un PSI asigna una dirección IP a un equipo que se conecta con una cuenta de suscripción particular y en consecuencia la dirección IP se asocia con una persona específica. No obstante, las direcciones IP

---

[29] Whitten, A. (22 de febrero de 2008). Are IP addresses personal? Recuperado de: http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html (Revisado 21/06/2015).

registradas por cada sitio web sin información adicional no deben considerarse datos personales, debido a que estos sitios web por lo general no pueden identificar a los seres humanos que se encuentran detrás de estas cadenas de números.

2.2.2. Posición de la Superintendencia de Industria y Comercio – SIC.

En el marco de la presente investigación, se presentó una consulta a la SIC en los siguientes términos:

> ¿La Dirección IP en Colombia es considerada como un dato personal?
>
> En caso afirmativo ¿Debe ser considerada como un dato público, semiprivado, privado o sensible?

En respuesta a la consulta presentada, la SIC en concepto del 30 de enero de 2015 señaló lo siguiente:

> (…) En este orden de ideas, se considera dato personal toda pieza de información relativa a una persona natural determinada o determinable mediante “identificadores”, por ejemplo, a titulo enunciativo, una dirección “IP”(1), en la medida en que cada vez que una persona natural accede a Internet puede ser identificado por la dirección “IP” atribuida por el proveedor de acceso a Internet.
>
> Hay que señalar que el Grupo de Trabajo del artículo 29 (2), en el informe No. 37, indicó que la dirección “IP” sí es un dato personal. Dijo el órgano: los proveedores de acceso a Internet y los administradores de redes locales

> pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor http.
>
> En ese escenario, la dirección "IP" es un dato personal, siempre y cuando: (i) este vinculada a una persona, o (ii) pueda realmente identificar a la persona, con independencia del tipo de IP. (SIC, 2015)

Respecto al segundo interrogante la SIC señaló que se trata de un dato personal privado, en los siguientes términos: "En ese contexto, en consonancia con las normas y criterios jurisprudenciales, el dato personal se clasifica en: (i) dato público; (ii) dato semiprivado; y, (iii) dato privado, tales como la dirección "IP".

Es pertinente señalar que la SIC llega a esta conclusión utilizando como fuentes la doctrina de la Agencia Española de Protección de Datos, la Directiva 95/46/CE de 1995 y la Directiva 97/66/CE de 1997 y el Grupo de Trabajo del artículo 29.[30]

De las definiciones normativas expuestas, la posición de Google y de la SIC sobre la connotación del dato "dirección IP" se desprende la siguiente conclusión:

La dirección IP es un dato personal privado, cuando se encuentra asociado a una persona particular. En ese sentido una lista con diferentes direcciones IP que le son

[30] Este Grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente sobre la protección de datos y la intimidad

entregadas a un PSI no contiene datos personales y no se rige por la Ley 1581 de 2012. No obstante, la lista de las direcciones IP otorgadas a usuarios determinados, sí se rige por la Ley Estatutaria. Lo anterior, teniendo en cuenta que si puedo asociar la direcciones IP utilizadas por personas determinadas, es posible conocer su comportamiento en la red y tener acceso a diferente aspectos íntimos de esta persona.

2.2.3. Análisis Comparado

En materia de protección de datos personales/privacy existe una tensión entre Europa y EEUU. Aunque en ambos modelos existen normas que protegen los datos personales, el enfoque y concepción misma del derecho es diferente.

La tensión que existe entre ambos sistemas tiene relevancia para Colombia teniendo en cuenta, en primer lugar, que la legislación Colombiana ha seguido el modelo Europeo y como se describió anteriormente, la Ley 1581 de 2012 incorporó “en su articulado las mejores prácticas internacionales en materia de protección de datos contempladas en Convenio 108 de 1981 del Consejo de Europa, la Directiva Europea 95/46 de 1995, la Resolución 45/95 de 1990 de la ONU y la Resolución de Madrid de 2009 .” (Cámara de Representantes. Exposición de Motivos del Proyecto de Ley Estatutaria 046 de 2010)

En segundo lugar, al Estado Colombiano, le debe interesar quién tiene la mayor cantidad de información personal, incluso sensible, (afectan la intimidad del titular en los términos del artículo 5 de la Ley 1581) de los titulares de la información nacionales. Sobre el particular, es pertinente recordar que Facebook y Google son empresas

norteamericanas, que cotizan en el mercado norteamericano y cuya propiedad accionaria se encuentra en cabeza de miles de inversionistas norteamericanos. El principal activo de estas compañías son los datos personales de millones de usuarios, una decisión que afecte este activo, afecta a la economía norteamericana (Suuberg, 2013).

Estados Unidos fue visto como un líder a nivel mundial en materia de protecciones sobre privacidad. Esta posición de liderazgo la perdió durante la década de los 70`s, periodo en el cual varios países europeos adoptaron legislaciones en materia de protección de datos personales. La Ley Hesse de 1970 de Alemania fue la primera Ley en materia de protección de datos personales, y con posterioridad diferentes países de Europa (Suiza y Dinamarca en los 70`s; Noruega y Finlandia 80`s; Luxemburgo, Bélgica, España y Portugal 90´s,). Los últimos países en adoptar estas medidas en Europa fueron Italia y Grecia quienes lo hicieron con posterioridad a la Directiva del 95. (Suuberg, 2013, p. 274)

Respecto a la evolución de la protección de datos personales, se menciona que existen dos generaciones. La primera generación se preocupaba por posibles abusos del Estado frente a los ciudadanos en términos de la información solicitada por los Estados de Bienestar. La segunda generación, centró su atención en la autodeterminación informativa y dotó al ciudadano de diferentes instrumentos para poder ejercer su derecho.

En EEUU la legislación en materia de protección de datos personales no ha tenido este mismo proceso en parte, como consecuencia de un fuerte cabildeo “lobby” ejercido por empresas como Google, Facebook, Ebay, Amazon, y un grupo industrial incluyendo

Microsoft, Cisco, Intel, I.B.M., Oracle, Motorola Mobility, Texas Instrumments, Dell. (Suuberg, 2013, p. 270)

En términos generales puede señalarse que las principales diferencia entre estos modelos son:

- En el sistema de EEUU la protección de datos personales es vista como un derecho del consumidor. En el sistema europeo se entiende como un derecho fundamental.
- En EEUU existen normas de carácter sectorial. En Europa existen normas generales y sectoriales. En consecuencia, en Europa todo dato personal es protegido, mientras que en EEUU solamente se protegen aquellos datos personales señalados en las normas.
- En el sistema europeo existe una autoridad en materia de protección de datos personales con facultades sancionatorias. En el modelo de EEUU no existe una autoridad como tal, aunque la Comisión Federal del Comercio tiene pronunciamientos sobre el particular.

A continuación, se expondrán diferentes pronunciamientos de distintas autoridades frente al entendimiento de la dirección IP como dato personal.

- ***Caso España.***

La Agencia de Protección de Datos Española en el 2003 señaló que la dirección IP es un dato personal en los siguientes términos:

> Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos."[31]

En igual sentido en octubre de 2014, se pronunció el Tribunal Supremo de España[32], frente a un caso relacionado con redes P2P en el siguiente sentido:

> Esta Sala estima que las direcciones IP son datos personales, en el sentido del artículo 3 LOPD, ya que contienen información concerniente a personas físicas "identificadas o identificables". El hecho a que alude la parte recurrente, de no tener al alcance de su mano la identificación del titular de los datos por medios y plazos razonables, no es obstáculo para la conclusión que mantenemos de que se trata de datos personales, pues de conformidad con la definición de datos personales del artículo 2.a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de

---

[31] Agencia Española de Protección de datos. (2013) Informe 327/2003, Recuperado de: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf

[32] España. Tribunal Supremo de España. Sala de lo Contencioso Administrativo, Sentencia del 03 de octubre de 2014. Recuperado de: http://www.poderjudicial.es/cgpj/es/Poder%2DJudicial/Sala%2Dde%2DPrensa/Notas%2Dde%2Dprensa/El%2DTS%2Dprohibe%2Da%2DPromusicae%2Dusar%2Dlos%2Ddatos%2Dde%2Dlos%2Dusuarios%2Dde%2Dredes%2Dde%2Dintercambio%2Dde%2Darchivos%2Dsin%2Dsu%2Dconsentimiento (Revisado 21/06/2015).

octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por dato personal habrá de entenderse, al igual que señala el artículo 3.a) LOPD antes citado, toda información sobre una persona física identificada o identificable, añadiendo el artículo 2.a) de la Directiva 95/46 que "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación.

- ***Caso Francia.***

El Tribunal de Apelación de París en dos sentencias del 27 de abril y del 15 de mayo de 2007, en un caso también relacionado con el uso de tecnología p2p, consideró que la dirección IP no es un dato personal. Esta sentencia permitió a los titulares de los derechos de autor, identificar a los usuarios no autorizados para descargar el contenido. El Tribunal argumentó que la dirección IP no identifica personas sino máquinas en internet[33].

- ***Unión Europea***

En el informe No. 37 del Grupo de Trabajo del artículo 29, grupo creado en virtud de la Directiva 95/46/CE, se estableció lo siguiente:

[33] L'adresse IP n'est pas une donnée indirectement nominative. (29 de junio de 2007). *Legalis*. Recuperado de http://www.legalis.net/spip.php?page=breves-article&id_article=1956 (Revisado 21/06/2015).

> “los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor http”.

2.3. La dirección IP como un dato personal de carácter sensible

Como se mencionó anteriormente, la SIC mediante concepto del 30 de enero de 2015, señaló que la dirección IP en Colombia es considerada como un dato personal privado.

Se procederá a plantear que la dirección IP dependiendo del contexto puede ser considerada como un dato personal sensible e incluso datos personales asociados a menores.

La Ley 1581 define dato sensible en los siguientes términos:

> “Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos

> políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.” (Congreso de la República, 2012)

Si por medio de la dirección IP es posible conocer el comportamiento de una persona, entonces la dirección IP debe ser considerada como un dato personal sensible, por lo menos frente a aquellos casos en los cuales la dirección IP revele aspectos íntimos del titular (tendencias, hábitos sexuales), orientación política (Blogs que frecuenta, noticias que elige), relativos a la salud (búsquedas a través de Google), vida sexual (Búsquedas y páginas que visita), etc.

El artículo 7º de la Ley 1581 establece que en el tratamiento de datos personales se respetará los derechos de los niños y adolescentes y prohíbe el tratamiento de estos datos, salvo los de naturaleza pública[34].

Ahora bien, ¿qué sucede si la persona que se encuentra detrás del computador o Smartphone es un menor de edad? La respuesta es sencilla: se realiza tratamiento de datos de menores de edad. ¿cómo pueden hacer los responsables de tratamiento para asegurar que las direcciones IP objeto de tratamiento no corresponden a usuarios menores de edad? Es técnicamente muy difícil.

Así las cosas, es preciso advertir que la dirección IP en algunos casos es un dato personal de carácter sensible, que incluso puede estar asociado a niños, para abordar el análisis económico del mercado cuyo bien transable es precisamente, la dirección IP.

[34] La Corte Constitucional en la Sentencia C-748 de 2011, matizó la prohibición señalada permitiendo el tratamiento siempre y cuando prevalezca el interés superior del niño.

3. Análisis económico del mercado de la dirección IP

La información es el activo más valioso que puede tener una empresa; se sostiene que la información personal es el petróleo en internet[35]. La red contiene enormes e incalculables cantidades de datos personales que son utilizados, entre otros, para fines publicitarios, políticos, personales, etc. En razón a ello, existe un mercado de la información personal al ser aprovechada por las Compañías que la poseen, como lo es Google.

Así lo expone Litvinov, al afirmar que la infraestructura existente está sobrecargada y requiere una gran inversión de capital, pero los usuarios no están dispuestos a pagar más por un servicio más rápido. Por ello los PSI han reconocido un mercado derivado de la transacción de secretos de los usuarios por dinero, un mercado en el cual Compañías como Google han tenido un éxito increíble (Litvinov, 2013, p. 585).

En atención a que los datos personales son el negocio de los negocios y lo que se diga o no se diga en las normas afectará a algunas industrias, se considera que el regulador debe tener en cuenta el análisis económico que pueda efectuarse del mercado de la información personal, y mucho más concreto, de la dirección IP.

---

[35] Kineva, M. European Consumer Comissioner. *Rountable keynote speech.* Bruselas, 31 de marzo de 2009.

Para tal fin, a continuación se analizará el mercado de la información personal y de la dirección IP; posteriormente, se dará aplicación a la teoría del consumidor y se concluirá con un análisis de las formas de intervención del Regulador y de los costos de producción de direcciones IP.

3.1. Determinación de los mercados

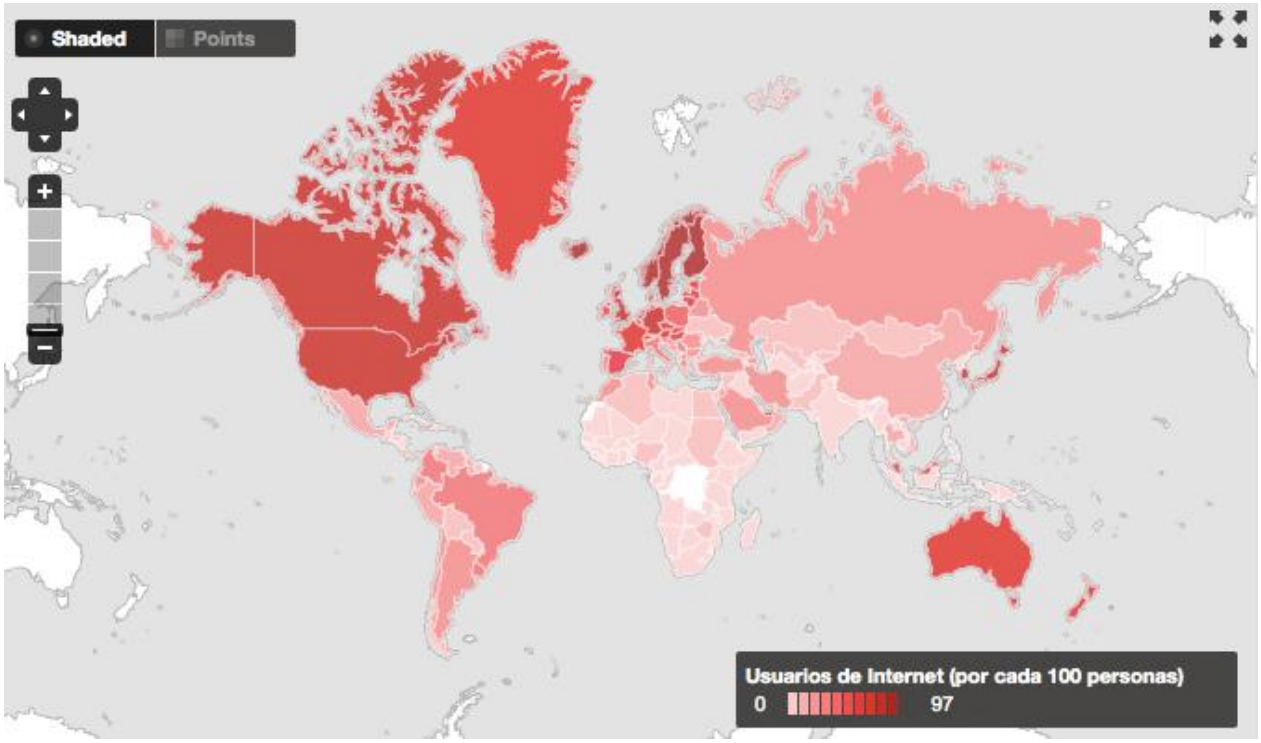
De conformidad con lo estudiado hasta el momento, se puede afirmar que quien tenga más información y datos que adquieran la capacidad de generar una ventaja comercial o incluso política, tendrá mayor poder en el mercado.

Sin embargo, acceder a la información directamente no es fácil, por lo que a lo largo de los años se han creado diferentes maneras para ello, unas más efectivas que otras, tales como encuestas, censos, sondeos, etc.

Uno de los mecanismos que se han utilizado desde las últimas dos décadas para obtener información personal, es a través de Internet. En el presente trabajo se considera que este medio ha sido preferido para acceder a la información, por dos razones. La primera de ellas, es porque la información que se conoce a través de los censos no puede incluir información personal no pública, datos que sí pueden accederse a través de Internet; cuando los usuarios acceden a Internet, no tienen ningún tipo de limitante o de precaución con respecto al rastro de sí mismos que están dejando en la red, razón por la cual se pueden conocer hasta las inclinaciones sexuales que se tienen, si se accede a las páginas de Internet que se visitan por una persona determinada.

La segunda razón por la que se considera que es más eficiente acceder a la información personal no pública de los usuarios a través de Internet, es por el mismo

alcance que éste tiene a nivel mundial. Para el año 2014, según el Banco Mundial, en los lugares del mundo donde se presenta una mayor densidad en el uso de Internet, de cada 100 personas, 97 son considerados como usuarios de Internet, así:



Fuente: Banco Mundial. http://datos.bancomundial.org/indicador/IT.NET.USER.P2/countries?display=map

Se ha evidenciado que la forma más eficiente para satisfacer la necesidad de conocer la información personal de la mayor cantidad de personas, tales como sus gustos, preferencias, hábitos, necesidades, etc., es a través de aquel mecanismo que permite la interacción en Internet, y que es el rastro del camino seguido por un usuario en la Red: la dirección IP.

En esa medida, con el fin de entender la necesidad y el impacto de una regulación en materia de hábeas data en este mercado, es importante conocer cuáles son las variables

que tienen un efecto directo e indirecto en el mercado de las direcciones IP, y cómo se caracteriza. En razón a ello, éste análisis se adelantará a continuación en lo que se ha denominado para el presente trabajo, *estudio del mercado de la dirección IP*.

Adicionalmente, es importante recordar que la dirección IP por sí misma no es apetecida por sus compradores; de hecho, el interés de los compradores por la dirección IP es totalmente indirecta y es utilizada como un medio. A las Compañías les interesa aquella información (personal) del usuario a quien le ha sido asignada una dirección IP. A los compradores de esta dirección, no les interesa conocer esa combinación de números que permite interactuar en Internet (dirección IP), les interesa conocer el usuario: sus gustos, preferencias, hábitos, inclinaciones políticas, e incluso sexuales.

Así es como se hace evidente la necesidad de entender un segundo mercado cuyo análisis es imprescindible: *el mercado de la información personal*.

De acuerdo con lo anterior, a continuación se efectuará el análisis de cada uno de los mercados mencionados anteriormente, empezando por el *mercado de la información personal,* el cual determinará el alcance del *mercado de la dirección IP*, permitiendo conocer hasta dónde puede intervenir el regulador de hábeas data.

3.1.1. El mercado de la información personal

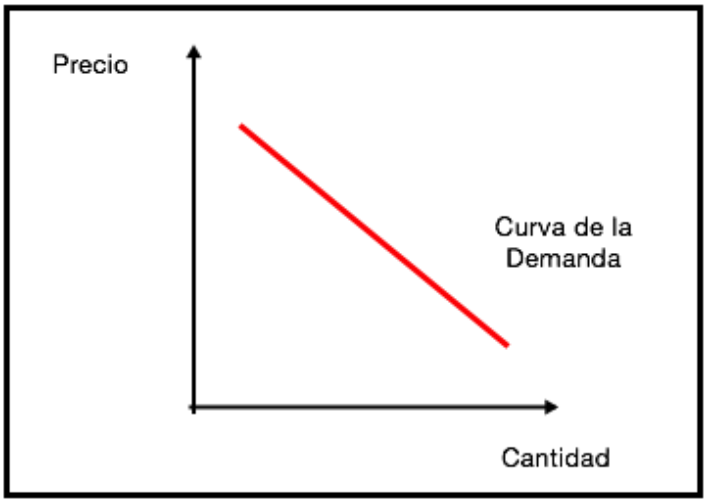
El mercado de la información personal se delimita por la transacción de éste tipo de información de los usuarios, concretamente hablando, como lo sería la asociación entre un nombre, con un correo electrónico, número celular, hábitos en internet, intereses políticos, comerciales y sexuales, etc.

Es un mercado que no tiene fronteras espaciales ni temporales, como el ámbito del Internet mismo; por esto, la regulación de este mercado requiere de una cooperación y armonía internacional entre las leyes existentes en la materia en los diferentes países. Una regulación que no cumpla con estas características, está destinada a resultar insuficiente.

Los demandantes de la información privada de las personas, son aquellos que requieren tomar decisiones con base en ésta, tales como Compañías de Publicidad, Partidos Políticos, Comerciantes, o incluso Desarrolladores de Aplicaciones Móviles. En atención al valor inherente de la información personal, y a los altos costos de su producción derivados de la dificultad de obtenerla en grandes cantidades, esta no puede ser comprada por todos sus demandantes.

En atención a ello, los demandantes que no pueden acceder a la información personal por la falta de capacidad económica para adquirirla directamente, genera que los demandantes deban acudir a otro mercado para obtenerla a través de la dirección IP, como se explicará en el siguiente aparte. Incluso, y en caso en que los demandantes de la información personal, tampoco puedan alcanzar el precio para adquirir la dirección IP, es claro que no podrían satisfacer su necesidad y se encontrarían por fuera de los dos mercados.

Entre mayor sea el precio de la información personal para conseguir en el mercado, menor será la demanda, si todo lo demás permanece constante, por lo que la gráfica de esta curva sería la siguiente:



Gráfica 1: Curva de la Demanda del Mercado de la Información Personal

Conforme con la gráfica, asumimos una curva ordinaria de demanda con pendiente negativa, donde la función de demanda depende del precio: $f(d) = d(p)$

Con respecto a los oferentes, se considera que se trata de una pluralidad de actores, que no tienen poder para la determinación del precio del mercado. Está conformado por todo tipo de agentes que por su actividad, tienen acceso a la información personal, y que por medio de la venta de esta información, tienen una nueva fuente de ingresos. En este escenario se encuentran Compañías que tienen la autorización de los dueños de la información para este tipo de tratamiento (entiéndase una Compañía que contando con la autorización del usuario, obtiene la información y la vende), o aquellas que se encuentran por fuera de la regulación.

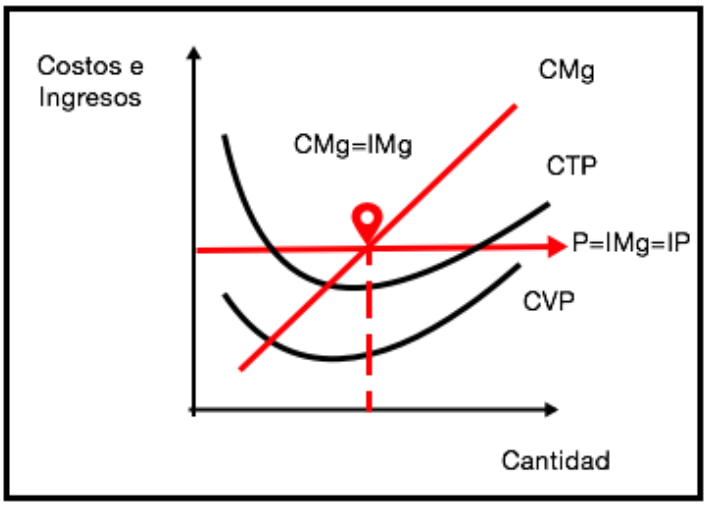
En este último escenario, encontramos las Compañías que tienen su domicilio o su actividad en un país con una regulación en hábeas data más flexible, que permite realizar transacciones con la información personal sin contar con autorización del titular de la misma.

Adicionalmente, puede ocurrir que los oferentes de la información personal, o incluso de la dirección IP, en algunos casos, son a su vez demandantes de la misma; en otras palabras, pueden existir agentes cuyo objeto principal es obtener la información personal directamente del usuario, y sin necesidad de venderla, la usan para diferentes fines. Así, esta clase de agentes no se encontrarían en el mercado de la información personal, sino que harían parte del mercado de servicios. En este escenario, se encuentran, por ejemplo, compañías que desarrollan aplicaciones móviles o programas de internet y que a través de estas, obtienen información personal de los usuarios (como lo sería Instagram) y son éstos quienes se encargan de publicarlas en la red.

En atención a que en el último escenario planteado, encontramos Compañías que son productoras y a su vez demandantes de la información personal, es claro que no tendrían la necesidad de acudir al mercado para satisfacer su necesidad de obtener este tipo de información, por lo que el análisis que se realizará a continuación no las incluirá.

Con base en lo mencionado, se considera que el mercado de la información personal, es un mercado que se encuentra en competencia perfecta, toda vez que por la cantidad de agentes que interactúan en el mismo (demandantes y oferentes), éstos son tomadores de precios. Asimismo, se entiende que el bien que se tranza en el mercado es homogéneo, al estudiarlo desde un punto de vista global como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012). Y por último, se encuentra que el mercado de la información personal no presenta barreras para su ingreso o salida, dadas las diferentes formas de acceder a la información, como se explicó anteriormente.

Para determinar la cantidad de información personal que el oferente debe poner en el mercado, se debe recordar que los oferentes buscan maximizar sus beneficios. En razón a ello y dado que el precio es dado por el mercado, se debe encontrar cuál es la cantidad de bienes cuya producción maximizan la utilidad del productor. Para tal fin, hemos incluido la siguiente gráfica que permite solucionar este problema:

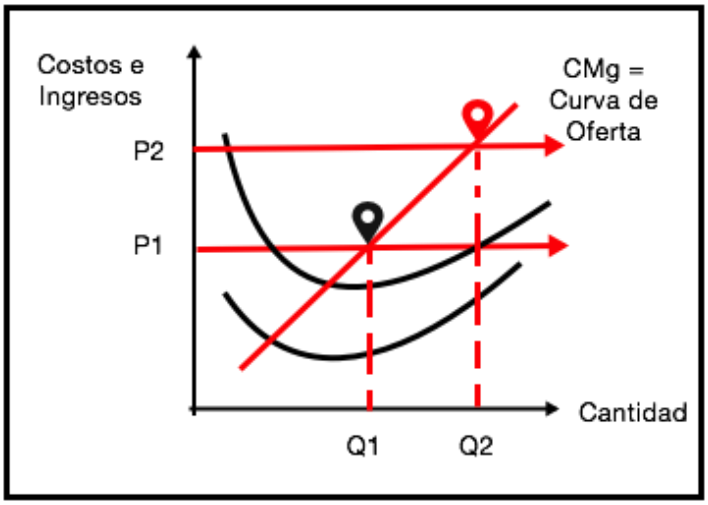


Gráfica 2: Punto de maximización de beneficios para un Oferente en competencia perfecta

Así, el precio en el que el oferente de información personal maximiza su utilidad, es aquel donde el ingreso marginal, se cruza con el costo marginal, como se evidencia en la gráfica (CMg = IMg). Lo anterior permite encontrar la curva de la oferta de este oferente, al analizar las diferentes decisiones que toma el productor frente a una variación en el precio.

Supongamos que el precio sufre un aumento por un desplazamiento (incremento) de la curva de demanda, por lo que el oferente encontrará que la producción inicial dada, no maximiza su utilidad, dado que el ingreso marginal se encuentra por encima del costo marginal que se deriva de este nivel de producción. En razón a ello, el productor debe

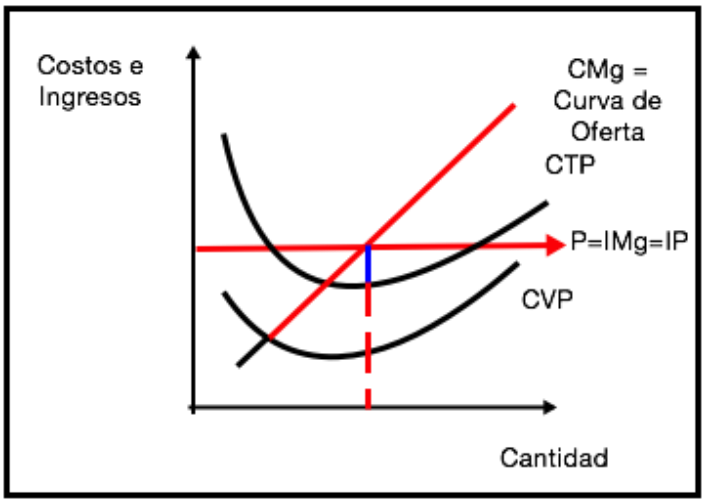
reacomodar su nivel de producción nuevamente según el precio dado por el mercado, hasta que éste se cruce una vez más con la curva de costo marginal. Dado que los productores en un mercado de competencia perfecta, como el que se analiza, son tomadores de precio, la curva de la oferta es equivalente a la curva de costo marginal, sobre la curva de costos variables promedio, así:



Gráfica 3: Curva de la Oferta de un Oferente y Curva de Costos Marginales

Hasta este punto se ha analizado la curva de la oferta de un oferente individualmente considerado. Sin embargo y siguiendo el análisis propuesto por Mankiw, para determinar la curva de la oferta del mercado, es importante tener en cuenta que los distintos oferentes, no tienen el mismo comportamiento con respecto a sus costos, por lo que los diferentes movimientos del precio en el mercado puede originar una salida de aquellas empresas cuyos costos totales promedio sean inferiores al precio (ingreso marginal) obligándolas a salir del mercado. Asimismo, dados los beneficios que se dan en el mercado, puede generarse un incentivo para el ingreso de nuevas empresas.

Sin embargo, la salida y el ingreso de empresas en el mercado es limitada en el corto plazo, por lo que la curva de la oferta es equivalente a la curva de costo marginal que es superior a los costos variables promedio (señalada en rojo); de esta forma y como se observa en la gráfica 4, la curva de la oferta tiene pendiente positiva (entre mayor precio, mayor cantidad los oferentes quieren poner en el mercado), así:



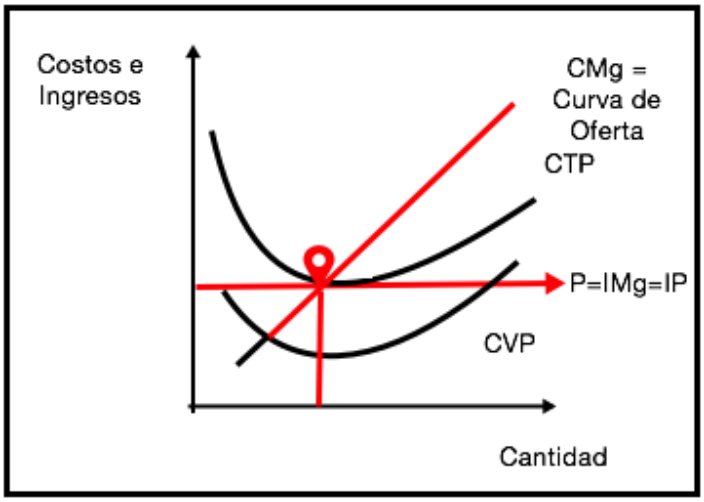
Gráfica 4: Curva de la Oferta del Mercado a Corto Plazo

Como se puede evidenciar de la gráfica, el hecho de que el ingreso marginal (precio) sea superior a los costos totales promedio (fragmento en azul), implica la generación de rentas económicas, por lo que hay un incentivo para el ingreso de nuevas empresas en el mercado.

Ahora, dado que en el largo plazo la salida y el ingreso de empresas sí ocurre y tiene incidencia en el mercado, la curva de la oferta en este mercado competitivo debe tener en cuenta las implicaciones de las decisiones de los agentes en el mercado. Supongamos que las Compañías oferentes tienen las mismas curvas de costos, por lo que la decisión de entrar o salir depende de los incentivos que tenga el mercado. Así, los

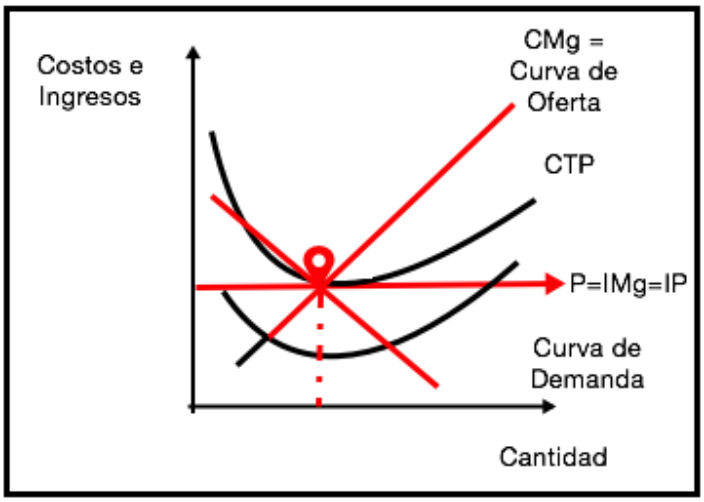
beneficios en el mercado van a generar atracción a nuevas empresas, quienes al ingresar al mercado, van a tener un impacto directo en el precio del bien disminuyéndolo, y con ello reduciendo los beneficios que se obtienen del mercado. Esto implicará que otras empresas decidan salir, y el precio vuelva a acomodarse.

Al final de estos movimientos en el mercado, las empresas deberán obtener cero beneficios económicos contables, dado que si existen beneficios económicos positivos, ello generará el ingreso de nuevas empresas y así un nuevo movimiento del precio y de las curvas en el mercado; esto implicará un nuevo desplazamiento del precio hasta encontrar el equilibrio donde se encuentran el precio y el costo total promedio, y en el cual las empresas deben actuar de forma eficiente para que el costo marginal y el costo total promedio sean iguales. Este precio corresponde al valor mínimo del costo total promedio, haciendo que el precio reduzca a cero la puja económica, así:



Gráfica 5: Eliminación de las rentas económicas por un movimiento en el precio al largo plazo

De acuerdo con lo mencionado, las características de este mercado se identifican a las de un mercado en competencia perfecta, al haber pluralidad de agentes, libre ingreso y retiro de empresas y un bien homogéneo; en esa medida, la gráfica del mercado de la información personal, sería la siguiente:



Gráfica 6: Gráfica del Mercado de la Información Personal

Como se observa en la gráfica, y siguiendo lo concluido anteriormente, el comportamiento del mercado de la información personal es un mercado en competencia perfecta, al reunir los tres (3) requisitos esenciales para ello.

Para los propósitos planteados en el presente trabajo, se considera esencial entender cómo reacciona el mercado de la información personal, según la regulación existente. Para este análisis, se ha aplicado la teoría de la elasticidad precio de la demanda y de la oferta, en lo que sea denominado como *elasticidad regulación de la demanda y de la oferta*, la cual mide qué tan dispuestos están los demandantes a

comprar información personal, y los oferentes a venderla, de acuerdo con la dureza de la regulación para ello.

Así, un análisis de la elasticidad de la oferta, desde el punto de vista de la regulación, debe tener en cuenta que ésta genera un incremento en los costos del productor, por lo que desincentiva su participación en el mercado y podría generar incluso su salida del mismo. En esa medida, un incremento en la regulación disminuiría la oferta, lo cual es una regulación inversa a la existente con el precio, donde su relación es directa, así: $Q_o = O(-R, +P)$

Se debe recordar lo mencionado en el capítulo anterior, donde se dejó claro que quienes hagan tratamiento de información personal de un usuario, sin contar con la debida autorización para ello, podrán ser investigados y juzgados ante la jurisdicción penal por el tipo de *Violación de Datos Personales* (artículo 269-F CP).

Por lo tanto, el precio final para acceder a la información personal debe tener en cuenta esta carga adicional para los oferentes y demandantes, de verificar que la información que está adquiriendo de cada persona, cuenta con la autorización de su propietario para ello. Para evaluar esta carga, se debe tener en cuenta que la pena máxima que se impondría a los que resulten culpables por cometer este tipo penal, sería de ocho (8) años.

De acuerdo con lo anterior, es claro que los oferentes de la información personal reducirán el nivel de oferta, entre mayor regulación en materia de habeas data exista.

Con respecto a la elasticidad de la demanda, encontramos que los demandantes tienen a su vez una carga de verificar que el tratamiento de la información personal se hizo en cumplimiento de los parámetros legales para tal fin. En razón a ello,

consideramos que esto genera un desincentivo para los demandantes, quienes podrían preferir ver incluida esta carga en el precio, sin tener la necesidad de asumir una obligación personal y propia sobre el particular. Sin embargo, y dado que el tipo penal mencionado no permite el traslado de la responsabilidad entre oferentes y demandantes de información personal, se considera que mayor regulación en materia de habeas data, disminuye la demanda de este bien, con el fin de preferir otros bienes sustitutos (como se analizará más adelante).

En esa medida, consideramos que la ecuación sería la siguiente: $Q_D = D(-R, -P)$

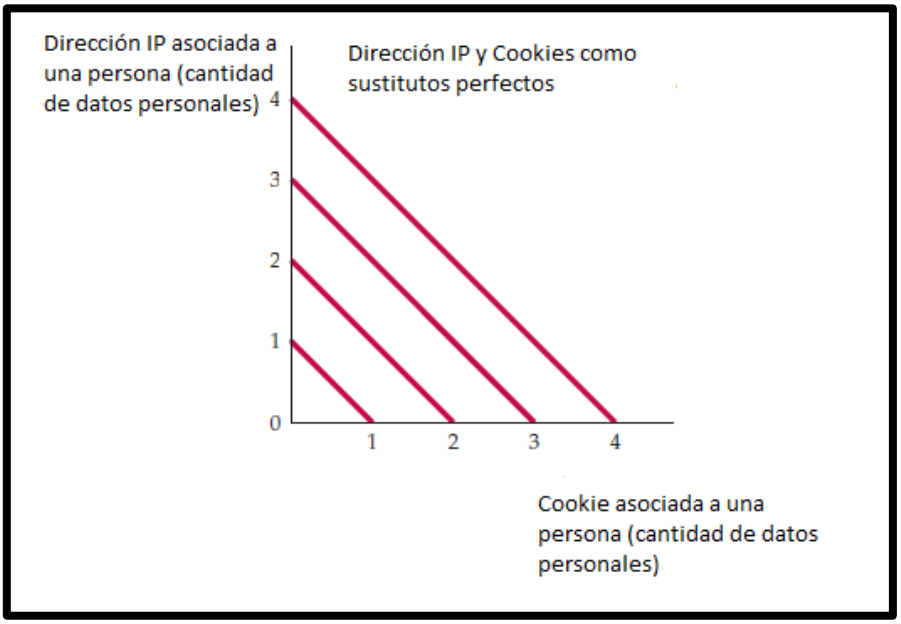
Así, aquellos agentes en el mercado que no puedan acceder al precio de equilibrio, o que si bien pueden acceder a este precio, no pueden asumir la carga de revisar o contar con cada una de las autorizaciones que deben otorgar los propietarios de la información, deben salir del mercado y acudir a los bienes sustitutos de la información personal: la dirección IP.

Así las cosas, se considera que la oferta y la demanda del mercado de la información personal, son absolutamente inelásticos en caso de que la regulación imponga tales obligaciones, que hagan su cumplimiento tan gravoso que resulte más eficiente acudir al mercado de la dirección IP, que asumir la carga impuesta por la regulación.

Respecto a la categorización del bien dirección IP asociado a una persona determinada o determinable, es pertinente señalar que Robert S. Pindyck y Daniel L. Rubinfeld señalan que cuando para el consumidor es totalmente indiferente la elección entre un bien u otro, dichos bienes son sustitutos perfectos, es decir, la relación marginal de sustitución de uno por otro es una constante. (pag. 85)

La dirección IP, es un mecanismo utilizado para obtener información personal, conociendo el comportamiento de los usuarios en internet. No obstante, es preciso advertir que la dirección IP no es el único mecanismo. Mediante la utilización de Cookies también es posible conocer el comportamiento de los usuarios en la Web por lo que debe entenderse como un bien sustituto de la dirección IP.

En razón a ello, en la gráfica 7 se ha graficado el comportamiento entre el uso de la dirección IP y de las cookies, como sustitutos perfectos, así:



Gráfica 7: Sustitución perfecta entre Cookies y la Dirección IP

Este es un factor que debe tener en cuenta regulador al momento de crear restricciones respecto a la dirección IP, ya que puede incentivar la utilización de las Cookies y no conseguir el objetivo buscado.

Si el regulador considera que la dirección IP en todos los casos es un dato personal sensible que puede estar asociado a menores de edad, esta definición implica un

aumento en el precio de dicho bien generando así, un incentivo para la utilización de Cookies como mecanismo para obtener datos personales.

3.1.2. El mercado de la dirección IP

Se considera que el mercado de la dirección IP se caracteriza por tener un bien idéntico. Recuérdese que la dirección IP es sólo un medio para obtener un bien final, esto es, el conocimiento de la información personal de los usuarios que tienen asignada una dirección IP; por lo tanto, es claro que es indiferente cuál es la dirección IP que se adquiere. El valor subyacente que tiene la dirección IP, depende de la cantidad de usuarios de los cuales puedo conocer su comportamiento en Internet a través de esta dirección. Así, entre mayor sea el tamaño de la "lista" de direcciones IP asociadas a sus correspondientes usuarios, mayor valor tendrá para el demandante de este bien.

Habiendo entendido la categorización del bien que se transa en este mercado, es importante conocer las características de sus oferentes y demandantes. Los demandantes de la dirección IP, son aquellos agentes en el mercado que están interesados en acceder a la información personal de los usuarios de Internet, pero no pueden acceder a ella de forma directa por el alto costo de ésta información. En razón a ello y de forma subsidiaria, estos demandantes acuden al mercado de la dirección IP.

Este mercado se caracteriza por estar compuesto por muchos demandantes. Dichos actores, demandan información personal (piénsese en las preferencias de los consumidores), y teniendo en cuenta sus restricciones técnicas y económicas, acuden al mercado primario, para obtener su materia prima: direcciones IP asociadas a personas

identificadas o identificables. Por lo tanto, la gráfica de la curva de la demanda es la misma que para el mercado de la información personal (gráfica 1).

De otro lado, los oferentes de direcciones IP (con su correspondiente asociación a un usuario), son los proveedores de servicio de internet (PSI); en Colombia, los PSI no son más de 20 empresas en todo el país, por lo que se considera pocos, en comparación con los productores de bienes de la canasta familiar (como lo sería la papa o el azúcar). Esta circunstancia se sustenta en la existencia de barreras de entrada y salida para los oferentes, al requerir la infraestructura necesaria para ofrecer internet a los usuarios (altos costos de ingreso), y en algunos casos, un permiso para el uso del espectro radioeléctrico[36].

En esa medida, al haber pocos oferentes en el mercado, y tener barreras de entrada, se considera que el mercado de la dirección IP se encuentra entre la competencia perfecta, y el monopolio: es un oligopolio.

En este punto, es importante mencionar que para el caso de un PSI de naturaleza pública, podría interferir una falla del mercado: la corrupción; esto, por la posibilidad de suministrar (o proveer) direcciones IP por fuera del ámbito mercantil con fines privados. Así, se considera que esta falla del mercado reduciría la demanda (ya que parte de ella se encontraría satisfecha a través de la corrupción generada por los PSI públicos) y con ello se podría afectar.

No obstante, y dada la cantidad de demandantes existentes en el mercado de la dirección IP, se considera que el impacto de la corrupción en la disminución de la demanda, no generaría un efecto en el precio, al ser un mercado oligopólico en el que

[36] Artículo 11, Ley 1341 de 2009.

los oferentes actúan de forma cooperativa, como se evidenciará más adelante, asimilando su comportamiento al de un monopolista.

Cualquier decisión que tomen los oferentes en el mercado, tendrá implicaciones directas en el precio del bien (dirección IP) y por supuesto, en su nivel de utilidades. El reducido grupo de oferentes tiene la capacidad de actuar como un cartel e imponer un precio monopólico determinado que represente el máximo beneficio para estos. Sin embargo, la legislación en materia de competencia es clara en prohibir cualquier tipo de prácticas que tengan como objeto un acuerdo de precios.

Por lo tanto, es imperioso actuar de forma estratégica con el fin de que todos los oferentes alcancen el máximo nivel de beneficio, sin generar un cartel de precios. Para ello, es necesario acudir a la teoría de juegos, en virtud de la cual cada agente interactúa en el mercado asumiendo su mejor decisión, teniendo en cuenta las estrategias tomadas por los demás agentes en el mercado. Con el fin de maximizar sus beneficios en el mercado, los agentes analizan las opciones que tienen los demás agentes, y así garantizar que sus decisiones sean armónicas y permitan obtener la mayor utilidad del mercado. No se toman decisiones independientes o ajenas que puedan afectar la utilidad global de los agentes, dado que esto implica una pérdida de beneficio irrecuperable.

Es así como se alcanza un equilibrio de Nash y a su vez, la respuesta para que en un oligopolio se alcance el mejor equilibrio. Se podría decir incluso que el comportamiento de los agentes se asimila al de un monopolio, dado que las decisiones de los agentes, al tener como fin alcanzar el mayor beneficio de todo el mercado, resultan homogéneas.

Con el fin de tener un mejor entendimiento de la aplicación de la teoría de juegos en el caso que nos ocupa, se supondrá que el mercado está compuesto por dos PSI, que se encuentran en la decisión de incrementar o no la oferta de direcciones IP en el mercado; para entender esto, procederemos a generar la siguiente matriz de ganancias:

Tabla 2
Matriz de Ganancias entre PSI[37]

		PSI 2	
PSI 1		Incrementar la oferta de direcciones IP	No Incrementar la oferta de direcciones IP
	Incrementar la oferta de direcciones IP	5, 5	20, 5
	No Incrementar la oferta de direcciones IP	5, 20	10, 10

De acuerdo con la matriz de ganancias anterior, encontramos que una decisión fundamentada en obtener el mayor beneficio para cada PSI, partiendo de que los otros PSI actuarán de forma racional y maximizando utilidades, dadas las opciones de los otros oferentes, implicaría asumir la decisión de no incrementar la producción por encima del punto de equilibrio (punto donde se cruza el ingreso marginal con el costo marginal).

Para verificar que este punto es efectivamente un equilibrio de Nash, y siguiendo a PYNDICK, debe verificarse si hay incentivos para los PSI de modificar su decisión, con el fin de obtener una mayor ganancia. Analizando la matriz de ganancias, es claro que si PSI 1 decidiere incrementar el número de direcciones IP que pone en el mercado, si bien le generaría un mayor beneficio, esta decisión depende de que PSI 2 no incremente la

[37] Fuente de la Tabla: Elaboración propia

producción; por lo tanto, si PSI 2 decidiere a su vez incrementar el número de direcciones IP que pone en el mercado, esto implicaría una pérdida mayor tanto para PSI 1 como para PSI 2.

De esta forma, es claro que el equilibrio de Nash se encuentra en la decisión de no incrementar el número de direcciones IP que se ponen a disposición del mercado; los PSI han tomado la mejor decisión que pueden tomar, dadas las mejores opciones de los otros PSI.

Los oferentes de direcciones IP, no van a tener ningún estímulo para moverse del equilibrio alcanzado mediante el análisis de la estrategia de los demás oferentes, toda vez que en cualquier otro punto, dadas las elecciones de los demás oferentes, se alcanza una menor utilidad que en el punto del equilibrio.

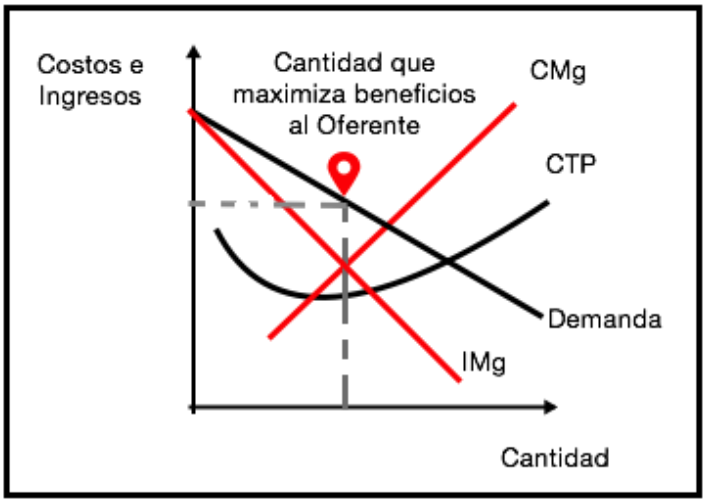
No obstante, se deben recordar las características del bien (dirección IP), cuyo mercado se está estudiando. Si bien se trata de un bien que es ofrecido de forma idéntica por sus oferentes, en los términos explicados anteriormente, la producción del mismo está limitada para cada oferente – PSI.

Como se explicó en el primer capítulo del presente trabajo, las direcciones IP son asignadas por la IANA a los Registros Regionales de Internet, y son éstos quienes acceden a las solicitudes de los diferentes PSI para la entrega de las direcciones IP. En esa medida, la cantidad de direcciones que cada oferente pueda poner en el mercado, está limitado por las que le han asignado, y las que éste a su vez, tiene en uso.

Así las cosas, se considera que el comportamiento que mejores resultados le traería a los oferentes del mercado de la dirección IP, sería aquel que implique una cooperación entre todos, sin buscar un interés propio, dada su limitación de producir más cantidad del

bien apetecido en el mercado. A los oferentes les interesa alcanzar la mayor utilidad posible con las direcciones IP que tienen asignadas, por lo que la opción más viable es mantener un Equilibrio de Nash, conforme se explicó anteriormente.

De conformidad con lo anteriormente descrito, y teniendo en cuenta que los oferentes podrían actuar de forma estratégica por el bienestar común, se considera que el comportamiento de los oferentes se asimilaría a la de un monopolio, por lo que la cantidad de direcciones IP que se pondrían en el mercado para maximizar los beneficios de los oferentes, dependen del punto en donde se cruce el ingreso marginal con el costo marginal, así:



Gráfica 8: Cantidad donde los Oferentes maximizan beneficios

Con base en lo anterior, se puede concluir que la oferta de dirección IP en este mercado, estará impuesta por los oferentes que, actuando de forma estratégica, lograrían beneficios de un monopolio al imponer el precio en el mercado. Así, el precio de mercado será impuesto por los oferentes, y la demanda deberá ajustarse a este valor para adquirir las direcciones IP.

Ahora, el escenario planteado hasta el momento, no ha tenido en cuenta los impactos que la regulación en hábeas data de la dirección IP podría tener en el mercado.

Por lo tanto, considerando que el regulador decida finalizar definitivamente toda discusión con respecto a la naturaleza de la dirección IP como dato personal, es claro que el valor de mercado tendría que incluir la carga de contar con las autorizaciones de los usuarios de las direcciones IP para poder hacer cualquier tratamiento sobre las mismas (lo cual incluye, por supuesto, la compra y venta). Lo anterior generaría un incremento en los costos que asumen los oferentes, que en últimas, por ser un oligopolio, sería trasladado a los demandantes.

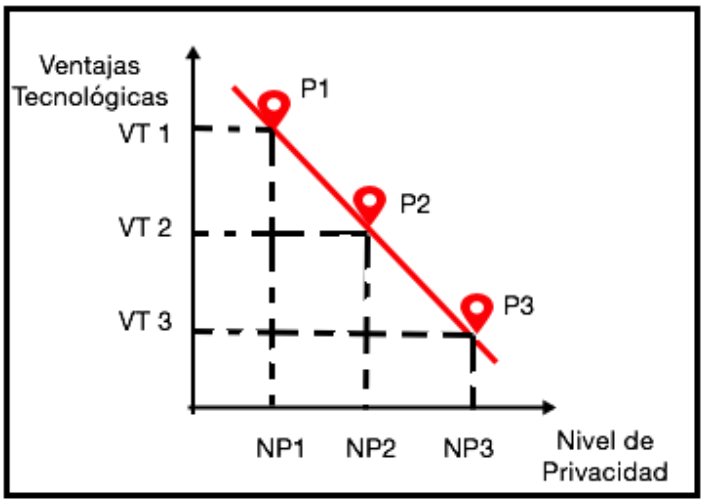
3.2. Análisis de la Elección del Consumidor de Información Personal

En este capítulo se argumentará que la herramienta más eficiente para garantizar el derecho al hábeas data de los titulares, consiste en promover la igualdad de información de los agentes del mercado, buscando autorizaciones consentidas por parte de los titulares.

Los titulares de la información son propietarios de una información valiosa para diferentes agentes del mercado. Existe un mercado de información personal donde los demandantes de información personal “compran” esta información a cambio de unas “ventajas tecnológicas”. Cuando una persona utiliza los servicios de Facebook o Google, intercambia datos personales a cambio de unas ventajas tecnológicas. En igual sentido sucede con aplicaciones como Waze que intercambian datos personales (ubicación personal geo-referenciada) a cambio de ahorro de tiempo en trayectos vehiculares.

Existe una relación inversa entre ventajas tecnológicas y niveles de privacidad, donde a mayores ventajas tecnológicas, menores niveles de privacidad por parte de los titulares. Dado lo anterior, los titulares deben elegir entre mayores niveles de privacidad o acceso a ventajas tecnológicas.

En la gráfica 9 se evidencian tres puntos que corresponden a diferentes combinaciones entre ventajas tecnológicas y niveles de privacidad.



Gráfica 9: Combinación de elecciones entre Ventajas Tecnológicas y Niveles de Privacidad

El primer punto (p1), corresponde a una combinación en la cual el titular elige total acceso a las ventajas tecnológicas sacrificando su información personal y escogiendo el nivel más bajo de privacidad.

A título de ejemplo, piénsese en un titular que tiene los niveles de privacidad más bajos en sus equipos, permite el acceso público de su perfil en Facebook, utiliza Aplicaciones (App's) que requieren de información relativa a su ubicación geo-referenciada y utiliza sistemas P2P para intercambio de archivos.

El segundo punto (p2), corresponde a una combinación en el cual el titular ha decidido reducir las ventajas tecnológicas a cambio de un mayor nivel de privacidad.

Este punto corresponde a un titular que en algunos casos prefiere conservar su privacidad a cambio de menos ventajas tecnológicas. Seguramente optará por configuraciones con mayor privacidad, preferirá el uso de buscadores con estándares más altos en sus políticas de privacidad y se abstiene de divulgar información personal por redes sociales.

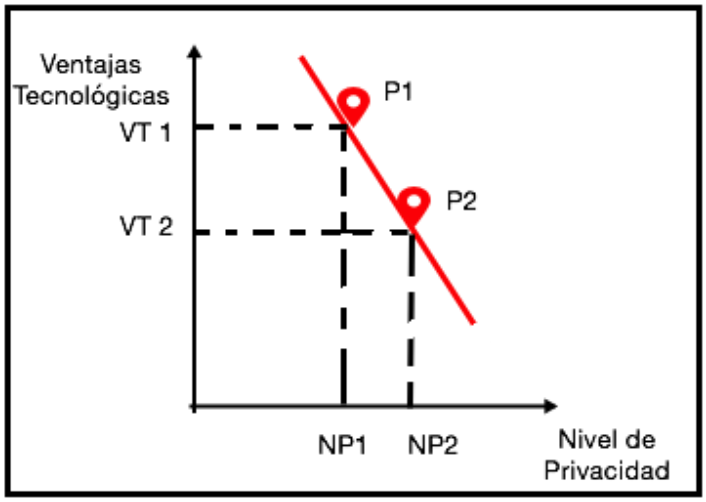
El tercer punto (p3), corresponde a una combinación en la cual el titular elige el nivel más alto de privacidad a cambio de no tener acceso a las ventajas tecnológicas.

En el anterior análisis se utilizó una pendiente igual a 1, en donde una unidad adicional de privacidad, implica una unidad menos de ventajas tecnológicas.

No obstante, existe la posibilidad de un usuario que esté dispuesto a renunciar a más de una unidad de ventaja tecnológica por obtener una unidad de privacidad (usuario adverso al riesgo) y usuarios con mayor apetito al riesgo que se encuentran dispuestos a sacrificar varias unidades de privacidad a cambio de una unidad de ventaja tecnológica. En este sentido la pendiente de la curva determina el nivel de indiferencia del usuario, generando una pendiente (negativa en todo caso) igual al impacto de la variación la variación de las ventajas tecnológicas, sobre los niveles de privacidad, así:

$$M = \frac{VT2 - VT1}{NP2 - NP1}$$

De acuerdo con lo anterior, la gráfica de la curva de combinación de elecciones de un usuario con aversión al riesgo, sería de la siguiente manera conforme la explicación precedente:



Gráfica 10: Usuario adverso al riesgo.

Desafortunadamente, en el mercado de la información personal existe una asimetría de la información entre demandantes y oferentes de este tipo de información, ya que el titular no suele ser consiente del precio real de su información personal y no suele consultar los términos y condiciones de los servicios que utiliza.

En ese sentido, la autoridad en materia de protección de datos personales debe propender por una regulación que incentive las autorizaciones consentidas y sancione el tratamiento de datos no autorizados. Para el efecto, la autorización debe contener las finalidades específicas, señalar si la información será compartida con terceros y el término de caducidad de dicha información.

En términos de Remolina, “La cuestión no es el uso de la tecnología, sino el abuso en el uso de ella” (Remolina, 2013, p. 28)

3.3. Formas de intervención del Regulador y Análisis de los costos de producción de direcciones IP

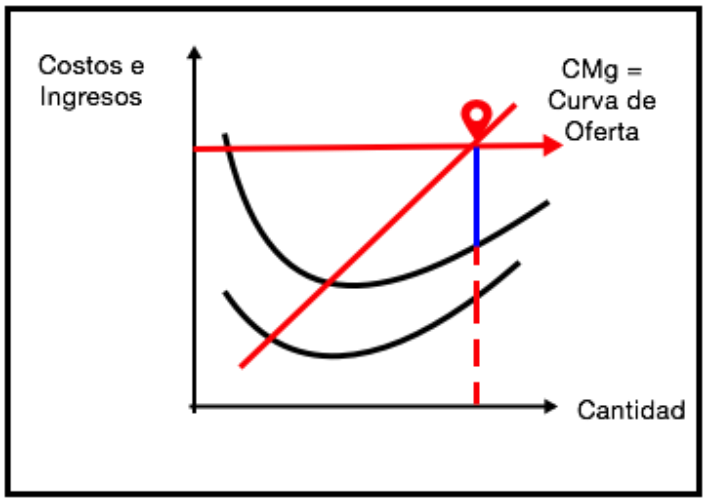
Como un análisis económico adicional para entender cómo solucionar el conflicto entre el derecho a la privacidad e Internet Libre, tenemos el análisis de los costos de producción de direcciones IP.

Uno de los primeros análisis que el productor realiza para determinar el valor de los bienes que ofrece, se fundamenta en los costos de producción de determinado bien. Para los PSI, la producción de direcciones IP asociadas a un usuario no genera un costo adicional al que implica su actividad principal: proveer el servicio de Internet. La venta de direcciones IP con la identificación de su usuario para un momento determinado, es un segundo uso que se le da a este protocolo asignado a los usuarios que permite su interacción en Internet.

De esta forma, los costos que se generan para los PSI por la venta de direcciones IP, actualmente, implica la preparación de la información de forma tal que sea de valor para los demandantes. Así, se podría decir válidamente que la mayor parte del ingreso que provenga de la venta de direcciones IP, es un beneficio para el oferente, así:

$$BT = IT – CT$$

De manera gráfica, se podría decir que el mercado de la dirección IP tiene un gran incentivo para el ingreso de nuevas empresas al mismo, al presentar rentas económicas importantes en comparación con otros mercados (franja azul), como se observa en la gráfica 11:



Gráfica 11: Rentas económicas.

De acuerdo con ello, el hecho de generar grandes rentas económicas a los oferentes del mercado de la dirección IP, implica un incentivo para el ingreso de nuevas empresas oferentes, y con ello la posibilidad de transformación del mercado a una competencia perfecta en el largo plazo, generando comportamientos como los explicados anteriormente para el mercado de la información personal.

Este análisis sería suficiente, si la regulación en hábeas data no pudiera intervenir incrementando (generando) los costos de producción para efectuar la venta de direcciones IP. Así, en caso en que el regulador decidiere asumir formalmente que la dirección IP es un dato personal, los PSI deberán contar con la autorización de cada uno de los usuarios para tales efectos, entre otro tipo de obligaciones formales detalladas en la Ley 1581 de 2012.

En esa medida, y analizando algunos de los modelos de contratos que actualmente se suscriben por parte de los usuarios con los PSI para la contratación de servicios de

Internet[38], se evidenció que ninguno de estos cuenta con algún tipo de alusión a la posibilidad de efectuar tratamiento de la dirección IP.

En razón a ello, es claro que la adaptación a la regulación por parte de los PSI generaría un costo que implicaría modificar todos los contratos de prestación de servicios vigentes a la fecha, y a futuro. Sin embargo, más allá de esta modificación y de otro tipo de obligaciones formales, los PSI no tendrían que asumir mayor carga.

Se considera que la inclusión de esta autorización en los contratos de prestación de servicios que se suscriben con los PSI, sería tratado como los *Términos y Condiciones* que regulan el alcance para acceder a determinado lugar en Internet o hacer uso de un software. Los usuarios no están manifestando su verdadera voluntad, ni siquiera conocen las implicaciones de este tipo de documentos; esta aceptación es un click más que tiene que hacer el usuario para alcanzar su fin real, que en este caso sería, acceder a los servicios de Internet.

Así las cosas, este tipo de regulación no tendría el verdadero efecto buscado: que los PSI sólo puedan transar aquellas direcciones IP sobre las cuales, los usuarios han autorizado su transacción, con total voluntad y de forma consciente de que a través del conocimiento de la dirección IP, se puede acceder a información personal e incluso íntima de los usuarios.

Por lo tanto, y de la misma forma en que se concluyó en el aparte anterior, la regulación podría no ser suficiente para proteger el derecho a la privacidad de los internautas. Los usuarios deben ser conscientes de que toda la información que se divulgue o se consulte por Internet, tiene el carácter de pública.

---

[38] Se revisaron los contratos de adhesión establecidos por CLARO, UNE, ETB, MOVISTAR, y EPM.

4. CONCLUSIONES

Habiendo explicado cómo nos encontramos frente a una de las mayores crisis en matera de privacidad de la historia, es necesario entender el alcance que la regulación en hábeas data puede tener, frente al intercambio de información personal que se realiza por Internet.

Colombia actualmente cuenta con normatividad en materia de hábeas data, la cual incluye, la consagración de orden constitucional como derecho fundamental, leyes estatutarias sectoriales y generales, y amplia jurisprudencia que desarrolla el derecho. El legislador colombiano optó por el modelo europeo, se cuenta con una autoridad de control, inspección y vigilancia que la ejerce a través del sistema de supervisión y control basado en la diligencia probada, y normas penales que tutelan el bien jurídico datos personales.

De acuerdo con ello, la autoridad en materia de datos personales en Colombia ha catalogado la dirección IP como un dato personal privado, cuando se encuentra asociado a una persona particular. En ese sentido una lista con diferentes direcciones IP que le son entregadas a un PSI no contiene datos personales y no se rige por la Ley 1581 de 2012. No obstante, la lista de las direcciones IP otorgadas a usuarios determinados, sí se rige por la Ley Estatutaria. Lo anterior, teniendo en cuenta que si puedo asociar la direcciones IP utilizadas por personas determinadas, es posible conocer su comportamiento en la red y tener acceso a diferentes aspectos íntimos de esta persona.

Por lo tanto, del estudio de las herramientas microeconómicas que otorgan una ayuda al ente regulador para que su intervención en el mercado de la información personal y de la dirección IP, se realice de forma consciente y responsable desde el punto de vista económico, se puede concluir lo siguiente:

- Aquellos agentes en el mercado de la información personal que no puedan acceder al precio de equilibrio, o que si bien pueden acceder a este precio, no pueden asumir la carga de revisar o contar con cada una de las autorizaciones que deben otorgar los propietarios de la información, deben salir del mercado y acudir a los bienes sustitutos de la información personal: la dirección IP.
- Considerando que el regulador decida finalizar definitivamente toda discusión con respecto a la naturaleza de la dirección IP como dato personal, es claro que el valor de mercado tendría que incluir la carga de contar con las autorizaciones de los usuarios de las direcciones IP para poder hacer cualquier tratamiento sobre las mismas (lo cual incluye, por supuesto, la compra y venta). Lo anterior generaría un incremento en los costos que asumen los oferentes, que en últimas, por ser un oligopolio, sería trasladado a los demandantes.
- Se considera que la inclusión de una autorización para el tratamiento de la dirección IP en los contratos de prestación de servicios que se suscriben con los PSI, sería tratado como los *Términos y Condiciones* que regulan el alcance para acceder a determinado lugar en internet o hacer uso de un software. Los usuarios no están manifestando su verdadera voluntad, ni siquiera conocen las implicaciones de este tipo de documento; esta aceptación es un click más que

tiene que hacer el usuario para alcanzar su fin real, que en este caso sería, acceder a los servicios de Internet.

- La regulación podría no ser suficiente para proteger el derecho a la privacidad de los internautas. Los usuarios deben ser conscientes de que toda la información que se divulgue o se consulte por Internet, puede llegar a ser pública.

5. BIBLIOGRAFÍA

- Agencia Española de Protección de datos. (2013) Informe 327/2003, Recuperado de: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf (Revisado 21/06/2015)
- Baker, S. (2011) Numerati. Lo saben todo de ti. España: Seix Barral.
- Banco Mundial. Gráfica de Cobertura de Internet. Recuperado de: http://datos.bancomundial.org/indicador/IT.NET.USER.P2/countries?display=map (Revisado 21/06/2015)
- Bercica, B., George, C. Investigating the legal protection of data, information and knowledge under the EU data protection regime ,International Review of Law, Computers & Technology, Vol. 23, No. 3, November 2009, 189–201.
- *Beware of Web Profiling* GEEK.COM (Oct. 28, 1999, 7:35 AM), http://docs.law.gwu.edu/stdg/gwilr/PDFs/45-3/5-%20Litvinov.pdf (Revisado 21/06/2015)
- Call, Steven T.; Holahan, William L. Microeconomía. Grupo Editorial Iberoamérica. (CH)
- Colombia, Asamblea Nacional Constituyente. Constitución Política de Colombia. 1991

- Colombia. Cámara de Representantes. Exposición de Motivos del Proyecto de Ley Estatutaria 046 de 2010, Gaceta del Congreso No. 488 de 2010.
- Colombia. Congreso de la República. Ley 1266 de 2008
- Colombia. Congreso de la República. Ley 1581 de 2012
- Colombia, Corte Constitucional, Sentencia C-1011/08
- Colombia, Corte Constitucional, Sentencia C-748/11
- Colombia. Corte Constitucional. Sentencias T-094 de 1995, T-097 de 1995 y T-119 de 1995.
- Colombia. Corte Constitucional. Sentencia T-729 de 2002 M.P. Magistrado Ponente: Dr. Eduardo Montealegre Lynett.
- Colombia. Superintendencia de Industria y Comercio. Concepto del 31 de enero de 2015.
- Cooper, E., A Smarter Rule for Smarter Phones: Why SILA Does Not Protect Our Smartphones and Why the California Legislature Should, McGeorge Law Review / Vol. 44 29/03/2013 University of the Pacific CALIFORNIA.
- España. Tribunal Supremo de España. Sala de lo Contencioso Administrativo, Sentencia del 03 de octubre de 2014. Recuperado de: http://www.poderjudicial.es/cgpj/es/Poder%2DJudicial/Sala%2Dde%2DPrensa/Notas%2Dde%2Dprensa/El%2DTS%2Dprohibe%2Da%2DPromusicae%2Dusar%2Dlos%2Ddatos%2Dde%2Dlos%2Dusuarios%2Dde%2Dredes%2Dde%2Dintercambio%2Dde%2Darchivos%2Dsin%2Dsu%2Dconsentimiento. (Revisado 21/06/2015)
- Ferguson, C. E.; Gould, J. P. Teoría microeconómica. Fondo de Cultura Económica.

- Fleischer, P. We Need a Better, Simpler Narrative of U.S. Privacy Laws, (Mar. 12, 2013, 4:37 PM), http://peterfleischer.blogspot.com/2013/03/ we-need-better-simpler-narrative-of-us.html (Revisado 21/06/2015)
- Garriga-Domínguez, A. (2004) *Tratamiento de datos personales y derechos fundamentales.* Madrid, España.
- Gómez, J., Pinnick, T., Soltani, A. KNOWPRIVACV 4 (Univ. of Cal. at Berkeley, Sch. of Info. 2009), Recuperado de: *at* http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf. (Revisado 21/06/2015)
- Hirshleifer, Jack y David. Microeconomía: teoría del precio y sus aplicaciones. Prentice Hall.
- Howe, J., *Online Privacy and BehavicrrProfilingV'RSMKÎl.'WiSi* (July 1, 2011), http://www.privatewifi.com/online-privacy-and-behavior-profiling. (Revisado 21/06/2015)
- IANA. Recuperado de: https://www.iana.org (Revisado 21/06/2015)
- ICANN. Recuperado de: https://www.icann.org (Revisado 21/06/2015)
- Kineva, M. European Consumer Comissioner. Rountable keynote speech. Bruselas, 31 de marzo de 2009.
- Krugman, Paul; Wells, Robin; Olney, Martha L. Fundamentos de economía. Reverté. (KWO)
- L'adresse IP n'est pas une donnée indirectement nominative. (29 de junio de 2007). Legalis. Recuperado de http://www.legalis.net/spip.php?page=breves-article&id_article=1956 (Revisado 21/06/2015)

- Leyden, J. US Warrantless Wiretapping Predates 9/11, THE REGISTER (London), Dec. 18, 2007, http://www.theregister.co.uk/2007/12/18/warrantless_wiretapping_latest/ (Revisado 21/06/2015)
- Liât, C. U.S. Privacy Advocates Head to Brussels in Show of Support, WIRED.CO.UK. (Jan. 22, 2013), http://www.wired.co.uk/news/archive/2013-01/22/us-eu-data-protection-advocates. (Revisado 21/06/2015)
- Litvinov, A. (2013) The data protection directive as applied to internet protocol (ip) addresses: uniting the perspective of the european commission with the jurisprudence of member states. *The George Washington University Law School*. Recuperado de: http://docs.law.gwu.edu/stdg/gwilr/PDFs/45-3/5-%20Litvinov.pdf
- Mankiw, N. Gregory. Principios de economía. McGraw Hill. (M)
- McCullagh, D., Anger Grows over NSA Surveillance Report, CNETNEWS, May 11, 2006, http://news.cnet.com/2100-1028_3-6071525.html (Revisado 21/06/2015)
- McGonville, R., *Telcos Show Their Google Envy,* LIGHT READING (Apr. 8, 2008), http://www.lightreading.com/document.asp?doc_id=150479 (Revisado 21/06/2015)
- Megias, J. *Privacidad en la Sociedad de La Información.* Universidad de Cádiz
- Miller, Roger Leroy. Microeconomía moderna. Harla.
- Mills, E. Google Buys Ad Firm DoubleClick for $3.1 billion, CNET NEWS, Apr. 13, 2007, http://news.cnet.com/2100-1024_3-6176079.html. (Revisado 21/06/2015)

- Network Information Center Mexico, S.C. Recuperado de: http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4 (Revisado 21/06/2015)
- Nicholson, Walter. Teoría microeconómica. McGraw Hill.
- Ornelas, L. G., Higuera, M. (2013). La autorregulación en materia de protección de datos personales: la vía hacia una protección global. (Spanish). Revista De Derecho Comunicaciones Y Nuevas Tecnologías, (9), 1-30.
- Parkin, Michael y Gerardo Esquivel. Microeconomía, versión para latinoamérica. Addison Wesley. (PE).
- PCWorld Staff, Private Lives? Not Omsl, PCWORLD (Apr. 18,2000,12:00 AM), http://www.pcworld.com/article/16331/article.html (Revisado 21/06/2015)
- Pindyck, R., Rubinfeld. D. Microeconomía. Ed. Séptima: 2009. Pearson Prentice Hall
- Popkin, H. Privacy Is Dead on Facebook Get over It, TECHNOTICA ON NBCNEWS.COM (Jan. 13, 2010, 8:56 AM ET), http:// www.nbcnews.com/id/34825225/ns/technology_and_science-tech_and_gadgets/. (Revisado 21/06/2015)
- Remolina, N. ¿Tiene Colombia un nivel adecuado de protección de datos personales?. *Revista Colombiana de Derecho Internacional.* Marzo de 2010.
- Remolina, N. *Cláusulas contractuales y transferencia internacional de datos personales,* en *Obligaciones y contratos en el derecho contemporáneo,* 357-419
- Remolina, A. (2013) *Tratamiento de datos personales.* Bogotá, Colombia: Legis Editores S.A.

- Remolina, N. (sin fecha determinada). 'Big data, big problema?'. Ámbito Jurídico. Recuperado de: http://www.ambitojuridico.com/BancoConocimiento/N/noti-130723-13big_data_big_problem/noti-130723-13big_data_big_problem.asp (Revisado 21/06/2015)
- Robayo, E., Varela, E., una colisión *peer to peer: hábeas data versus* derechos de autor, Vniversitas. Bogotá (Colombia) N° 120: 237-252, enero-junio de 2010.
- Salvatore, D. Microeconomía. McGraw Hill. (S)
- Solove, D., A Taxonomy of Privacy, 154 U. PA. L. REV. 477, 479–87, 507–50 (2006) (attempting to classify types of privacy harms for study).
- Stein, J., *Data Mining: How Companies Now Know Everything About You,* TIME MACAZINE (Mar. 10, 2011), http://content.time.com/time/magazine/article/0,9171,2058205,00.html (Revisado 21/06/2015)
- Stankey, R. Data Protection Regulation Proposal Approved by the European Parliament, LEXOLOGY (Oct. 30, 2013), http://www.lexology.com/library/detail.aspx?g=38c769f6-77d8-4e7d-b968-89cb242c6114. (Revisado 21/06/2015)
- Stiglitz, Joseph E. Microeconomía. Ariel Economía.
- Suuberg, A. The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law
- Tene, O. (2008). What google knows: privacy and internet search engines. Utah, Estados Unidos: Utah Lwa Review.

- Tribunales Constitucionales y autoridades en materia de hábeas data o privacy de diferentes países, entre otros, Francia, Canadá, Alemania, EEUU.
- Unión Europea. Tribunal de Husticia. Gran Sala. Sentencia del 13 de mayo de 2014. Asunto C-131/2012. Recuperado de: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES (Revisado 21/06/2015)
- Varian, H., Microeconomía intermedia. Antoni Bosch.
- Whitten, A. (22 de febrero de 2008). Are IP addresses personal? Recuperado de: http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html (Revisado 21/06/2015)