Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

COMENTARIO A LA SENTENCIA T-020 DE 2014 DE LA CORTE CONSTITUCIONAL COLOMBIANA. APUNTES SOBRE EL "TRATAMIENTO ESTRUCTURADO DE DATOS PERSONALES"

*Juan Carlos Upegui Mejía**

I. Descripción del caso de la sentencia T-020 de 2014

En la sentencia T-020 de 2014, en una decisión 2-1, una sala de revisión de la Corte Constitucional colombiana ordenó a la Relatoría de la Corte Suprema de Justicia alterar el texto de una sentencia de casación en firme que esta unidad había publicado en su página web en cumplimiento del mandato de publicidad de las decisiones judiciales. La orden de alteración fue sencilla: reemplazar el nombre de la persona que resultó condenada por "una serie de letras o números que impidan su identificación". Con esto, la Corte Constitucional perseguía impedir que la información personal que dicha sentencia revela(ba) pudiese ser accedida de forma indiscriminada, vía Internet, mediante el buscador de Google. La favorecida con la orden de amparo en el caso había sido condenada, en 1998, por los delitos de "concusión, falsedad material de particular en documento público y fraude procesal, en su calidad de Fiscal 34 de la Unidad de Delitos contra el Patrimonio Público". Para el momento de la solicitud de amparo, la pena impuesta había sido cumplida y los derechos de la peticionaria restablecidos.

La mayoría de la Corte Constitucional fundamentó su decisión en el régimen del *habeas data*. Para la Corte, "aun cuando se entiende que las sentencias son públicas, y así deben seguir siéndolo, la información perso-

* Es doctorando en el Instituto de Investigaciones Jurídicas de la UNAM; maestro en derecho público y abogado por la Universidad Externado de Colombia, *juan.upegui@uexternado.edu.co*.

Fecha de recepción: 16 de enero de 2017.
Fecha de dictamen: 14 de marzo de 2017.

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

nal en ellas contenida está sometida a los principios de la administración de datos". Consideró que la información personal relacionada con condenas judiciales en materia penal es del tipo "información semi-privada", y está sometida a los principios de "circulación restringida" y "finalidad", propios del *habeas data*.

Gabriel Mendoza, integrante de la Sala, salvó el voto. Según Mendoza, la información contenida en las sentencias judiciales es, por definición legal, información pública, y en ninguna fuente del derecho, incluidos tratados internacionales, existía una causal que, en este caso específico, reservara la información contenida en la sentencia. La sentencia judicial, consideró, es un "documento público y [según] las normas que permiten su divulgación a través de medios informáticos, sin que exista reserva legal, no puede la Corte ordenar su modificación". Para Mendoza, "[l]a Corte Suprema de Justicia no es una entidad que administre datos, maneje información personal o antecedentes judiciales".

El salvamento de voto no comparte los dos presupuestos de la sentencia: que el archivo de la relatoría de la Sala Penal de la Corte Suprema de Justicia sea una base de datos personales, y que la información contenida, en esa particular sentencia de casación, sea información semi-privada.

En términos jurídico constitucionales, el desencuentro entre minoría y mayoría puede ser expresado como un problema del ámbito de aplicación del derecho fundamental al *habeas data*; esto es, un desencuentro en torno al fenómeno específico que constituye el objeto de regulación de dicho derecho.

II. El ámbito de aplicación del *habeas data* según la jurisprudencia y la ley

La jurisprudencia constitucional, en un escenario pre-Internet, consideró que el ámbito de aplicación del derecho al *habeas data* era la administración de información personal a partir de archivos o bases de datos personales. Las bases de datos personales son entendidas como dispositivos tecnológicos o archivísticos que permiten el surgimiento del "poder informático". Lo que a su vez está determinado por la posibilidad de acumular y de disponer de una importante cantidad de información personal. Esta fue la concepción de la Corte en la seminal sentencia T-414 de 1992, que inaugura e inspira la jurisprudencia constitucional colombiana sobre el *habeas data*.

Esta situación, sin embargo, no se modifica en la jurisprudencia post-Internet, ni post-web 2.0. Tanto en la sentencia T-729 de 2002 como en

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

la SU-458 de 2012, casos en que se debatía sobre el alcance del derecho de acceso a información personal vía Internet, la Corte insistió en que el ámbito de aplicación del derecho del *habeas data* es el del tratamiento de información personal a partir de la existencia de archivos o bases de datos personales. En esta última sentencia, consideró (considerando 5, sentencia SU-458 de 2012, MP Adriana Guillén):

> [E]l derecho al *habeas data* opera en el contexto determinado de la administración de bases de datos personales. Por tanto, su ejercicio es imposible jurídicamente en relación con información personal que no esté contenida en una base o banco de datos, o con información que no sea de carácter personal. Estos presupuestos han permitido que esta Corte descarte la invocación del *habeas data* por ejemplo para proteger información personal que conste en distintos soportes, no organizados en una base de datos o en un fichero, o para proteger información de otro carácter, como información académica, científica, técnica, artística que, a pesar de estar contenida en base de datos o archivos, esté desvinculada de personas naturales o jurídicas.

Para la Corte, el *habeas data* no tiene como objeto de protección la información personal *per se*. Se protege, en cambio, el derecho a que la información personal sea objeto de tratamiento según una serie de reglas y de principios bajo la consideración de que la información personal integra una base de datos, la cual a su vez es ordenada según estas reglas y principios.

Sin embargo, la Ley 1581 de 2012 tiene otra aproximación al fenómeno. El título de la ley es revelador: "Por la cual se dictan disposiciones generales para la protección de datos personales". Es, como su nombre lo dice, una ley de "protección de datos personales" y no una ley de *habeas data* como tal. El objeto de la ley es la protección de "los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada". Hay un cambio, en apariencia sutil, del ámbito de protección con énfasis en el tratamiento de la información personal, y un repliegue de la importancia de la existencia de una base de datos personales. En la nueva ley, dada la amplitud en la definición de la expresión "tratamiento" y la irrelevancia de la naturaleza de la base de datos en cuestión (que puede ser "cualquiera" según la ley), la información personal parece devenir objeto de protección *per se*. La Ley 1581 de 2012, avalada en su constitucionalidad por la sentencia C-748 de 2011, está inspirada en el modelo europeo de protección de datos personales y rompe, en alguna medida, la tradición del modelo local que se había

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

perfilado a partir de: *a*) el énfasis en el *habeas data* orientado a favorecer la participación del titular de la información personal en las actividades de tratamiento de dicha información, *b*) en los ámbitos específicos del despliegue del poder informático, y *c*) a partir de la existencia de un archivo o de una base, específicamente, de datos personales.

La diferencia entre la forma de aproximarse al fenómeno en la jurisprudencia y en la ley puede reducirse a una constatación elemental: si es relevante considerar que en el origen de los problemas y de los derechos presuntamente afectados está o no una base de datos personales. Para la Ley 1581 de 2012 esto dejó de ser relevante. Así, por la vía de la interpretación amplia de la expresión "tratamiento", cualquier operación realizada sobre datos personales determina la aplicación de sus reglas. Esta posición fue secundada por la Corte Constitucional al examinar la constitucionalidad de la expresión "tratamiento", en donde afirmó que el propósito de la ley era regular "todas las operaciones y conjunto de operaciones con los datos personales" (sentencia C-748 de 2011, considerando 2.5.9). Esta visión maximalista de la Ley 1581 rompe con la visión acotada de la jurisprudencia constitucional, para la cual la existencia de una base de datos personales es un presupuesto indispensable para la aplicación del régimen de *habeas data*. Para esta última, el ámbito de aplicación del *habeas data* es el del tratamiento de información personal a partir de la existencia de una base de datos personales, entendida como un conjunto de información organizada, por medios físicos o tecnológicos, que tiene como objeto principal la captura, organización, almacenaje y divulgación de datos personales.

Es frente a esta especial organización de la información, que llamamos "archivo o base de datos personales", que la jurisprudencia constitucional colombiana reconoció los llamados "principios de la administración de datos" en su sentencia T-729 de 2002. En efecto, la existencia de este tipo específico de organización de la información personal es un presupuesto del reconocimiento del llamado "poder informático" y del fundamento del *habeas data* como una "libertad informática". Los llamados principios de la administración de datos se organizan en clave constitucional como una forma de limitar el ejercicio de este poder y de favorecer el ejercicio de esta libertad. El principio de finalidad sólo tiene sentido si partimos de la existencia de una base de datos personales; de lo contrario, su poder normativo es difícil de articular y puede llevar a situaciones absurdas. Piénsese, por ejemplo, la pretensión de aplicar el principio de finalidad a los archivos periodísticos que están plagados de información personal, pero cuyo criterio organizativo no es la información personal.

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

III. La distinción entre tratamiento estructurado y no estructurado de datos personales

La distinción entre información personal sometida a tratamiento independientemente de su relación con una base de datos personales, e información personal sometida a tratamiento a partir de una base de datos personales puede ser una herramienta analítica útil para definir el alcance, por lo menos, del derecho fundamental al *habeas data* en Colombia. Esta distinción podría articularse con una tesis defendida por el académico sueco Sören Öman.

Öman ha defendido la tesis de restringir el ámbito de protección del derecho a la protección de datos personales (y su artillería de principios) a aquellas actividades de tratamiento que hayan sido estructuradas para facilitar el conocimiento y la comunicación de datos personales (Öman, 2002 y 2004). Para ello, Öman distingue, por un lado, el tratamiento de datos personales del tratamiento de textos que contienen datos personales, y, por el otro, la finalidad del archivo centrada en la organización de información personal, de aquella centrada en la organización de documentos. Bajo estas diferencias (elementales) sugiere que los principios de la protección de datos personales son adecuados y pertinentes para el primero de los casos, pero no para regular el procesamiento de datos de forma no estructurada (Öman, 2002).

Su argumento es pragmático: aplicar el sistema comprensivo de reglas del tratamiento de datos a cada pieza documental que contenga datos personales supone una carga burocrática altísima para prevenir los pocos casos en que dicho tratamiento pueda causar daños. A esto suma tres argumentos. Uno histórico: los principios de la protección de datos fueron pensados para el tratamiento estructurado de información personal, no para regular la protección de información personal contenida en cualquier documento; uno sistémico: la necesidad de evitar colisiones con el derecho a la libertad de expresión en el contexto de la sociedad de la información post-web 2.0, y el último relacionado con el efecto útil: la percepción pública de que requerir la aplicación de dichos principios cada vez que cualquier persona produce un documento es absurda y puede llevar a su pérdida de eficacia en aquellos casos en que sí sea necesaria (Öman, 2002 y 2004).

IV. Crítica a la sentencia T-020 de 2014

Las posiciones enfrentadas al resolver el caso de la sentencia T-020 de 2014 descansan sobre distintas concepciones de cómo debe protegerse la infor-

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

mación personal: una ligada al derecho de *habeas data* y otra ligada al derecho a la protección de datos. La posición minoritaria diagnostica el caso como uno de acceso a la información pública, en el cual, frente al carácter incidental de los datos personales en la actividad de tratamiento, no son aplicables las reglas del *habeas data*. La posición mayoritaria lo diagnostica como uno de protección de datos, en donde la información como tal es el centro de la cuestión. Esto parece ser así ante la urgencia de activar mecanismos de protección de los derechos involucrados frente al poder que supone el uso del buscador de Google. Esta situación lleva a la mayoría a forzar los elementos de la dogmática propia del derecho de *habeas data*.

Por otra parte, es muy problemática la caracterización del nombre de una persona que ha sido condenada, contenido en una sentencia de casación penal, como "información semi-privada". Buena parte del análisis de la posición mayoritaria se concentra en defender el carácter "semi-privado" de la información personal con el propósito de hacerle aplicable el principio de circulación restringida, y poder, en últimas, fundamentar la orden de anonimización. Sin embargo, una correcta lectura de la sentencia SU-458 de 2012, empleada para fundamentar esta postura, permite desvirtuar esta estimación. De hecho, la consideración de la información sobre antecedentes como información pública fue uno de los elementos más problemáticos de la sentencia de unificación. Esta información es información personal pública, porque se le comunica el carácter público de la sentencia en firme. Según la Corte (considerando 6, sentencia SU-458 de 2012, MP Adriana Guillén):

> ...los antecedentes penales tienen el carácter de información pública. La información en qué consisten está consignada (soportada, escrita, contenida) en providencias judiciales en firme, expedidas por autoridades judiciales competentes, y caracterizadas por su carácter público, entendido este, como la condición de accesibilidad de su contenido, por cualquier persona, sin que medie requisito especial alguno.

La clasificación de la información personal contenida en sentencias judiciales condenatorias, adoptada por la mayoría del caso del 2014, es contradictoria con la clasificación unánime de la misma información en la Sala Plena del 2012, y con lo dispuesto en artículo 3o., literal f, de la Ley 1266 de 2008, que define como públicos, "entre otros, los datos contenidos en… sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva".

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

Es también problemática la caracterización del principio de finalidad de la base de datos de las sentencias publicadas por la relatoría de la Sala Penal de la Corte Suprema. Lo es porque la finalidad de esta base de datos es la publicidad y la difusión de las sentencias, precisamente porque esa base de datos no es en estricto sentido una base de datos personales. Esto explica que la Corte haya tenido dificultades para caracterizar el principio de finalidad en función de los datos personales contenidos en las sentencias. De hecho, no hay una afirmación clara en todo el texto de la sentencia de cómo, en este caso, se desconoce el principio de finalidad del tratamiento. Ello puede explicarse porque en este caso la información personal es incidental y no el objeto de la base de datos.

La asimilación del caso de la sentencia T-020 de 2014 con el resuelto en la SU-458 de 2012 falla además en un elemento fundamental. En ésta, la Corte se pronuncia sobre una típica base de datos personales: la que contiene los "antecedentes judiciales"; en aquélla, no. Que funcionalmente la base de datos de la Relatoría de la Sala Penal de la Corte Suprema de Justicia pueda operar como una "nueva forma de consulta de antecedentes judiciales", vía su inserción en un portal y la ayuda del buscador de Google, no cambia la naturaleza de la información ni convierte la base de datos en una de datos personales a la que se le aplica el régimen del *habeas data*. La mayoría resulta seducida, por alcanzar la decisión perseguida, a forzar los elementos de la dogmática del *habeas data*.

Además, el de la T-020 de 2014 era un mal caso para sugerir la anonimización de las decisiones judiciales, porque la peticionaria fue condenada en su "calidad de Fiscal 34 de la Unidad de Delitos contra el Patrimonio Público", como figura en los hechos del texto de la sentencia. Se extraña en el análisis de la Corte al menos una mención a esta circunstancia, pues a pesar de no ser una "figura pública", en los términos de la jurisprudencia constitucional colombiana, no es menos cierto que a los servidores públicos les es exigible una mayor responsabilidad frente a sus conductas oficiales y privadas. De otra parte, el asunto no era ni de lejos uno de los que ha justificado la reserva de esta información, como en el caso de delitos contra la libertad o el pudor sexual, información sobre el estado de salud de una persona, o asuntos relacionados con derecho de familia. Tampoco se trataba de un titular, sujeto de especial protección, niño, niña o adolescente, o una persona con identidad sexual diversa, casos en los cuales el fundamento de la decisión pudo haberse anclado en el contenido de los derechos a la intimidad y a la no discriminación, y no como en éste, en las reglas del *habeas data*. Finalmente, en este caso la Corte no despliega un

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

análisis concreto de la afectación de los derechos alegada por la peticionaria. No se demuestra cómo, en qué circunstancias y por quién en concreto ha sufrido discriminación, o cómo y en qué circunstancias precisas la posibilidad de hallar la información por la vía del motor de búsqueda la ha privado de "oportunidades laborales y comerciales". La posición mayoritaria parte de la veracidad de estas afirmaciones, y por esta vía termina por afirmar la tesis de que la información personal es un bien protegido *per se*; un objeto de protección que es extraño en el contexto de la jurisprudencia constitucional del *habeas data* en Colombia, en donde la información personal ha sido protegida en relación con un contexto más o menos determinado a partir de la lectura en clave constitucional de la bina poder informático-libertad informática.

V. Tratamiento no estructurado de datos e indexación por buscadores

El caso de la sentencia T-020 de 2014 es revelador del problema de la migración de archivos, y especialmente de los archivos públicos, a la Internet. Los "buscadores" vuelven la Internet *de facto* una base de datos personales. Pero la Internet no es por definición una base de datos, y las operaciones de indexación de los buscadores son actividades muy complejas de tratamiento de datos personales, no orientadas, en principio, por una finalidad diferente a la ordenación del criterio de búsqueda que consta en contenidos de portales de acceso abierto, según el diseño de algoritmos con múltiples variables.

Los problemas de afectación de derechos fundamentales y de los valores de las sociedades democráticas y pluralistas que supone esta migración deben ser resueltos con herramientas jurídicas y dogmáticas especiales. Para impulsar esta reflexión puede ser de alguna utilidad reconocer los límites del derecho al *habeas data* como un derecho y como un régimen jurídico pensado y articulado para resolver los problemas del tratamiento estructurado de datos personales. Esto es, a partir de la existencia de una base de datos personales *per se*, concebida, diseñada y operada para el tratamiento de datos personales, y no apto para resolver los nuevos problemas que engendra la migración masiva de información a la Internet.

Por ejemplo, reconocer los límites del ámbito de aplicación del *habeas data* permite articular mejor sus relaciones con los derechos a la libertad de expresión y al acceso a la información pública, centrales en la operación de las democracias contemporáneas y muy importantes en el funcio-

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

namiento de la sociedad de la información. Todo esto va sin negar que sea necesario diseñar nuevos instrumentos para proteger los derechos fundamentales de titulares de información personal en un escenario post-web 2.0, y donde es impensable una Internet funcional, abierta y robusta sin indexación ni motores de búsqueda.

Para resolver problemas como el de la sentencia T-020 de 2014, aceptando que sean verdaderos problemas de discriminación o de afectación de la dignidad de una persona, podría hacer uso del derecho a ser desindexado como un derecho especial y autónomo en este nuevo contexto. Sobre todo si aceptamos que lo que causa los problemas es la indexación de resultados por parte de un motor de búsqueda. También se pueden tomar decisiones políticas más extremas, como entronizar el derecho a la protección de datos personales como valor superior y proceder a anonimizar, "testar" o verter en "versiones públicas" todas las sentencias judiciales para proteger *in ovo* y desde la fuente, los posibles derechos que puedan afectarse con la eventual accesibilidad del nombre de las personas vía Internet, como ha sido política federal en México desde la década pasada; o seguir una posición más moderada, orientada por el "equilibrio" entre transparencia y acceso a la información, y protección a la intimidad y a los datos personales, como el que subyace a las Reglas de Heredia, acordadas en el 2003. En todo caso, es necesario un debate abierto sobre el tema, que consulte la forma como la cultura jurídica colombiana lo ha enfrentado y la forma en que la sociedad le gustaría que fuera tratado. No creo que sea buena idea impulsarlo como una forma de política judicial, y menos teniendo como fundamento un uso antitécnico de las categorías centrales del *habeas data* que tanto ha costado perfilar.

VI. Fuentes de información

Corte Constitucional de Colombia, Sentencia T-414 de 1992, MP Angarita Barón, Ciro.

———, Sentencia T-729 de 2002, MP Montealegre, Eduardo.

———, Sentencia C-748 de 2011, MP Pretelt Chaljub, Jorge Ignacio.

———, Sentencia SU-458 de 2012, MP Guillén Arango, Adriana.

———, Sentencia T-020 de 2014, MP Guerrero, Luis Guillermo.

Reglas de Heredia, 2003, *Reglas mínimas para la difusión de información judicial en Internet*.

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

Esta revista forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM
http://www.juridicas.unam.mx/ https://biblio.juridicas.unam.mx/bjv https://revistas.juridicas.unam.mx/
DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.4.11522

Sören Öman, 2004, "Implementing Data Protection in Law", *Scandinavian Studies in Law*, Peter Wahlgren, vol. 47.

———, 2002, "Protection of Personal Data: But How?", en *Law and information Technology-Swedish views,* Stockholm, IT Law Observatory, Peter Seipel.

BJV, Instituto de Investigaciones Jurídicas-UNAM, 2017
https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive