CRIMEN Y CASTIGO[23]: ¿RÉGIMEN INTERNACIONAL DE CIBERCRIMINALIDAD?

CRIME AND PUNISHMENT: INTERNATIONAL REGIME OF CYBER CRIMINALITY ?

Entregado (22-02-2016 – Revisado 17-06-2016)

DANIEL ANDRÉS JIMÉNEZ MONTALVO (AUTOR)

Bacharel en Relaciones Internacionales e Integración por la Universidade Federal da Integração Latino-americana (UNILA) en Foz do Iguaçu – Brasil.

****JAIME EDGAR MAXIMILIANO JIMÉNEZ VILLARREAL (CO-AUTOR)***

Maestro en Ciencias Políticas por la Facultad Latinoamericana de Ciencias Sociales (FLACSO) Sede en Ecuador.

*Universidade Federal da Integração Latino-americana (UNILA) – Brasil
**Universidad Politécnica Estatal del Carchi (UPEC) – Ecuador
*daniel.montalvo@aluno.unila.edu.br
**emjimenezv@hotmail.com

RESUMEN

El presente artículo tiene por finalidad presentar argumentos para la constitución de un régimen internacional de cibercriminalidad. Esencialmente, este artículo está centrado en la concepción de que los Estados, al someter de forma voluntaria el interés nacional y la maximización de su poder, generan regímenes internacionales. Al partir de esa concepción, el trabajo se estructura de tres capítulos y un epílogo: El primer capítulo comprende los instrumentos analíticos sobre regímenes internacionales y los conceptos que estructuran el cibercrimen. El segundo capítulo desarrolla una argumentación analítica sobre el Convenio del Cibercrimen y su protocolo adicional. El tercer capítulo evidencia las acciones de las organizaciones internacionales como sustento a la lucha de la cibercriminalidad. Finalmente, se realiza un epílogo sobre el hacktivismo de Edward Snowden. En cuanto al referencial teórico se instrumentalizará el concepto de regímenes internacionales, en las perspectivas de Stephen Krasner y Robert Keohane. En referencia a la metodología se hará uso del análisis de contenido y el método de process tracing. En tanto, las fuentes bibliográficas primarias se enfocan en el Convenio sobre cibercriminalidad y su Protocolo Adicional, y los documentos sobre las acciones del cibercrimen de la Naciones Unidas (ONU); Unión Africana (UA); Organización Internacional de Policía Criminal (INTERPOL); Organización para la Cooperación y el Desarrollo Económico (OCDE); y la Organización de Estados Americanos (OEA), y las fuentes secundarias enfocan críticamente el cibercrimen. Lo que se torna posible, para enfatizar la

[23] Título de la famosa obra de Fiodor Dostoievski escrita en 1886; este título se torna una analogía, en cuanto muestra la cibercriminalidad como un delito, y como tal debe ser castigado, como fue el caso de Raskólnikov (personaje principal de la obra) quien para salir de la pobreza asesino y robo a una usurera por lo cual fue condenado y castigado.

necesidad de la creación de un régimen internacional sobre cibercriminalidad como fruto de la voluntad de los Estados.

Palabras clave: *Consejo de Europa, Cibercrimen, Regímenes Internacionales, organizaciones internacionales*

ABSTRACT

This article aims to present arguments for the establishment of an international cybercrime regime. Essentially, this article focuses on the idea that states submit voluntarily to the national interest and maximizing their power generating international regimes. Based on this conception, the work is divided into three chapters and an epilogue: The first chapter covers the analytical instruments on international regimes and concepts that structure cybercrime. The second chapter develops an analytical argument on the Convention on Cybercrime and its additional protocol. The third chapter evidence the actions of international organizations and support to fight cybercrime. Finally an epilogue on hacktivism Edward Snowden is performed. As for the theoretical framework the concept of international regimes shall be implemented on the prospects for Stephen Krasner and Robert Keohane. Referring to the methodology will use content analysis and process tracing method. Meanwhile, the primary literature sources focus on the Convention on Cybercrime and its Additional Protocol, and documents on the actions of cybercrime the United Nations (UN); African Union (AU); International Criminal Police Organization (INTERPOL); Organization for Economic Co-operation and Development (OECD); and the Organization of American States (OAS) and secondary sources critically focused cybercrime. Turning all possible, stressing the need for the creation of an international regime on Cybercrime as a result of the will of States.

Keywords: *Council of Europe Cybercrime, international regimes, international organizations*

1. INTRODUCCIÓN

El presente artículo tiene por finalidad presentar argumentos empíricos acompañados de análisis teórico para la constitución futura de un régimen internacional de Cibercriminalidad; por lo que se ha planteado demostrar que los Estados al someter de forma voluntaria el interés nacional y la maximización de su poder, pueden generar regímenes internacionales, los cuales generan agendas de actuación conjunta y coordinada con la finalidad de alcanzar metas en común.

El presente artículo se compone de tres capítulos y un epílogo. El primer capítulo comprende los instrumentos analíticos sobre regímenes internacionales bajo la perspectiva de Krasner (2012) y Keohane (1982) y los conceptos que componen el mundo de la cultura internet: el cibercrimen; la ciberseguridad; la pornografía infantil; el *cyberbullying, copyright, phishing,* el hacktivismo y el *hacker.* El segundo capítulo desarrolla una argumentación empírica-analítica sobre el Convenio de Cibercrimen y su Protocolo Adicional para demostrar que puede ser constituido por principios, normas, reglas, y procesos de toma de decisiones en un área determinada de las relaciones internacionales (Krasner, 2012, p.93).

Paralelamente, el tercer capítulo pretende evidenciar las acciones de las organizaciones internacionales como sustento a la lucha de la cibercriminalidad, en donde se destaca la actuación de la ONU por medio de la Cumbre Mundial de la Sociedad de la Información, el Foro para la Gobernanza del Internet y la Unión Internacional de Telecomunicaciones; así mismo, se destaca el

papel de la Organización de las Naciones Unidas para las Drogas y el Crimen; la Unión Africana y la Organización de los Estados Americanos; y, finalmente un epílogo sobre el *hacktivismo* de Edward Snowden con la intención de evidenciar el estudio de las variables causales como la ética dentro de los regímenes internacionales.

En cuanto al referente teórico se instrumentalizará el concepto de regímenes internacionales y la orientación estructural modificada de Stephen Krasner (2012), siendo reforzado por la variable de voluntad de Robert Keohane (1982) dentro de los regímenes internacionales. En referencia a la metodología se hará uso del análisis de contenido y el método de *process tracing*; en tanto que las fuentes bibliográficas primarias se enfocan en el contenido del Convenio sobre cibercriminalidad y su Protocolo Adicional, y los documentos sobre las acciones del cibercrimen de la ONU, UA, INTERPOL, OCDE, y la OEA; además de las fuentes secundarias bajo una revisión crítica se enfocan en la comprensión sobre el cibercrimen. Es nuestra intención y por medio de una presentación argumentativa enfatizar en la necesidad de creación de un régimen internacional sobre cibercriminalidad como fruto de la voluntad de los Estados.

2. INSTRUMENTOS Y CONCEPTOS ANALÍTICOS

a. Regímenes Internacionales

Los regímenes internacionales son conceptualizados como principios, normas, reglas y procedimientos de la toma de decisiones en los cuales los intereses de los actores (Estados) convergen en un área dada de las relaciones internacionales[24] (Krasner, 2012, p.93). Sin embargo, es esencial especificar que las normas son conceptualizadas como padrones de comportamiento definidos en cuanto derechos y obligaciones; por su parte los principios (propósitos) se definen como creencias de hechos y causalidad; por un lado; y, por otro, las reglas (detalles de los derechos y las obligaciones) se consideran como prescripciones o proscripciones para las acciones, y los procedimientos decisorios permiten la implementación de las elecciones colectivas o en otras palabras, marcar los procesos para la posibilidad de implementación de los principios y la alteración de las reglas (Safarti, 2005, p.58).

De tal forma, que los regímenes internacionales al impactar en los Estados, "los controles nacionales en un área específica en relación a acuerdos específicos entre los Estados"[25] (*Ibidem,* p.59), bajo una perspectiva realista estructural convencional, permiten evidenciar a los Estados soberanos como actores que buscan maximizar sus intereses y poderes[26]. No obstante, esta visión realista del Estado, que al ser compactada por una concepción neoliberal, considera a los regímenes internacionales como el surgimiento de la acción voluntaria de los Estados para poder alcanzar sus objetivos, o en otras palabras constituye una visión estructural modificada de los regímenes internacionales (Krasner, 2012, p.97) – como lo expone la figura 1.

[24] Debe tomarse en cuenta que no existe una gran diferencia entre las normas y las reglas, por lo que para este artículo se considera a las normas como un conjunto de reglas de conducta con la finalidad de dar cumplimiento a un precepto legal (Cabanellas, 1993, p. 214). Por lo que, las reglas constituirían la descripción de las normas o mejor dicho del contenido.

[25] Traducción libre del autor, en el original: "*os controles nacionais em uma dada área, especialmente em relação a acordos específicos entre os Estados*" (Safarti, 2005, p.59)

[26] Este tipo de concepción sobre los regímenes internacionales está presente en los trabajos de Keohane (1982) y Stein (1982).

Por ello, es argumentable que los regímenes internacionales son vistos como un significativo censo de voluntad, los cuales son distinguidos por dos aspectos: (1) la imposición de límites y (2) la toma de decisiones (Keohane, 1982, p.330). Es decir, los regímenes internacionales se los expone como la acción voluntaria de los Estados a los cuales se impone límites aceptados, por un conjunto de Estados, con la finalidad de consolidar acuerdos que tienden a institucionalizar las relaciones internacionales para la constitución de reglas y procesos de normas orientadas para la continuación del buen censo en el régimen internacional (*Ibidem*, p.331).

Por tanto, la visión estructural convencional constituye la relación directa entre el interés, el comportamiento y el poder de los Estados, para concebir a los regímenes internacionales como variables intervinientes, resultantes de las acciones voluntarias y coordinadas de los Estados soberanos, donde es sometido el interés nacional[27] y la maximización de su poder[28] con la finalidad de alcanzar una meta común[29] (Krasner, 2012, p.98).

b. Conceptos de la cultura del internet[30]:

1. Cibercrimen:

El cibercrimen o *cybercrime* es definido como toda actividad criminal efectuada a través del ciberespacio[31] o el internet. Se acota que las actividades cibercriminales incluyen actividades ilegales, ilícitas, irregulares o no contempladas que tiene por finalidad la utilización de apartados digitales y electrónicos, televisión y redes de comunicación para afectar la integridad del individuo o conjunto de individuos, organizaciones o Estados. En otras palabras el cibercrimen constituye actividades no contempladas por la ley por medio del internet (Ghernaouti, 2013, p.25-26).

2. Ciberseguridad:

La ciberseguridad es definida como los asuntos para la protección de la información para los gobiernos, las organizaciones, y los individuos que instrumentalizan tecnologías de información y comunicación con la tecnología del internet. Dicho de otra forma, la ciberseguridad concreta una dimensión estratégica de la infraestructura y de servicios de las tecnologías de información y comunicación en respeto de la soberanía estatal, la eficacia de las organizaciones, y la seguridad humana (Ghernaouti, 2013, p.330-331).

[27] Para este trabajo el interés es visto como cálculos racionales de los actores, los cuales llevan a abandonar la toma de decisiones independiente para favorecer la toma de decisiones colectiva (Stein, 1982, p.316).

[28] El poder es definido desde una perspectiva cosmopolita e instrumental, que lo define como el poder utilizado para asegurar resultados óptimos, y la maximización conjunta de las ganancias, es decir el poder obedece al servicio del bien común (Krasner, 2012, p 103).

[29] Las metas son definidas como "resultados futuros conscientemente deseados, condiciones o estados finales, los cuales a menudo tiene valores intrínsecos (pero diferentes) para miembros de partes particulares" (Demmers, 2012, p.6).

[30] Este tipo de cultura es definida como la cultura de los creadores del internet, la cual se entiende como un conjunto de valores y creencias provenientes de la tecnomeritocracia (ciencia-tecnología y el mundo académico); de la cultura *hacker* (libertad de información); y de los emprendedores del internet (negocios-internet) (Castells, 2001, p. 77). En otras palabras la cultura de internet se compacta de las innovaciones del mundo académico y científico tecnológico, que se compacta con la libertad de la información con la finalidad de concretizar espacios de un nuevo quehacer económico-político.

[31] El ciberespacio o espacio cibernético es conceptualizado como el conjunto de actividades con un singular régimen híbrido de propiedades físicas y virtuales (información) (Nye, 2012, p.162). En otra visión, concretiza el ambiente digital creado por medio de la interconexión de los sistemas de computación por el internet (Ghernaouti, 2013, p.403).

3. Pornografía infantil:

La pornografía infantil es definida como todo material pornográfico, que contenga una representación visual de menores de edad[32] (hombres o mujeres) que han adoptado comportamientos sexuales explícitos o personas que simulan ser menores de edad adoptando un comportamiento sexual. Todo ello con la finalidad de mostrar imágenes realistas que presenten menores de edad en situaciones que contengan comportamientos sexuales explícitos (Council of Europe, 2001, p.7).

4. *Cyberbulling:*

El *cyberbulling* es definido como actos de índole intencional y repetido daño infligido a niños/as, preadolescentes o adolescentes, a través del uso de los computadores, celulares o cualquier dispositivo o medio electrónico (Hinduja; Sammer, 1978, p. 5).

5. *Copyright:*

El *copyright* se define como la copia ilegal o al acto de piratear los datos de información o en efecto generar una réplica del producto original de contenidos digitales. No obstante, este acto ilegal en el caso de propiedad intelectual es considerado un crimen fraudulento por la adquisición de las ideas, invenciones o las expresiones creativas de un individuo o un conjunto de individuos, organizaciones o Estados (Ghernaouti, 2013, p.107).

6. *Phishing:*

El *phishing* se refiere a los ataques que usan programas de correo electrónico para atraer usuarios *web* dentro de información relativamente importante con la finalidad de concretizar propósitos criminales como el fraude o malversación de los datos de información económicos (*Ibidem*, p.210).

7. *Hacktivismo:*

Es conceptualizado como el activismo político y la protesta social que hace uso del *hacking* u operaciones destinadas a generar brechas en el sistema de información tecnológica (*Ibidem*, p.433). Por lo que cabe decir que el *hacktivismo* es considerado como una forma de protesta que usa la información con objeticos políticos y un cierto grado de desobediencia civil (*Ibidem*, p.165).

7.1. *Hacker:*

La cultura *hacker* constituye un conjunto de valores y creencias que surgieron de las redes de programadores informáticos, que interactúan *online* para la autonomía de los proyectos de información y que implementan la conexión informática como base material y tecnológica (Castells, 2001, p.57). Además de ello, la cultura *hacker* constituye un sentimiento comunitario el cual se basa en la pertenencia activa a una comunidad que se estructura por medio de costumbres y principios de una organización informal de tipo global y virtual (*Ibidem*, p. 63).

[32] En la definición de menor de edad se comprende a los individuos menor de 18 años, pero que según el Consejo de Europa los Estados Miembros podrán definir la edad inferior al mínimo de 16 años (Council of Europe, 2001, p.7).

CONSTRUYENDO ESFUERZOS CONJUNTOS: INICIOS DEL RÉGIMEN INTERNACIONAL DE CIBERCRIMINALIDAD:

El Convenio sobre el Cibercrimen y su Protocolo Adicional[33]:

El Convenio sobre el Cibercrimen o también denominado Convenio de Budapest[34] retrata el interés de los Estados Miembros del Consejo de Europa y los Estados signatarios del Convenio, por la intensificación de la cooperación contra el cibercrimen (Council of Europe, 2001, p.2) Tal interés demuestra un censo de voluntad entre los Estados adscritos al Consejo de Europa y al Convenio, lo que muestra en la visión de Keohane (1982, p.331) la aceptación de límites diseñados por un conjunto de Estados para regular determinada área de las relaciones internacionales, en este caso el cibercrimen.

No obstante, no sólo la necesidad, sino también el interés de los Estados, provee bases iniciales para la emergencia de un régimen internacional, que debe estar cimentado y tener como sustento mayor a los principios rectores de cooperación, solidaridad y reciprocidad. En el caso del Convenio de Budapest los intereses compilan: la aplicación de una política penal para proteger la sociedad, la preservación de las redes informáticas y la información electrónica, el aumento de la cooperación entre los Estados Partes y el sector privado, la protección de los intereses legítimos de la utilización y el desarrollo de las tecnologías de la información (Council of Europe, 2001, p.2). En complementación, el Protocolo Adicional al Convenio evoca el respeto a los derechos humanos, condenación de los actos racistas y xenófobos que amenazan el Estado de Derecho y la estabilidad democrática, el reconocimiento de la libertad de expresión como reflejo de la sociedad democrática (Consejo de Europa, 2003, p.2-3). Por lo tanto, al preocuparse de estos principios los Estados del Convenio de Budapest según Krasner (2012, p.94) se unen propósitos para una actuación conjunta sobre el cibercrimen.

En tal panorama, el Convenio de Budapest se marca por la convergencia voluntaria de los Estados y empieza a ganar fuerza por la consolidación de principios o propósitos para actuar en intereses comunes. Sin embargo, la consolidación de normas constituye, para Krasner (2012, p.95) la implementación de un sentido de obligación general o según Keohane (1982, p.331), la imposición de limitaciones para el comportamiento de los actores internacionales con la finalidad de cimentar un régimen internacional. En esa visión, el Convenio de Budapest delimita la actuación de los Estados por un conjunto de obligaciones por medio de la aplicación nacional de penalidades hacia la utilización de datos[35] y sistemas informáticos,[36] (Council of Europe, 2001, p.4) con la finalidad de efectuar actividades cibercriminales.

Por ello, el Convenio de Budapest, para dar una contestación efectiva al cibercrimen, expresa en su art.2, la condena al acceso ilícito o ilegítimo a un sistema informático, así mismo en su art.3 censura la interceptación ilícita de datos informáticos no públicos por medios técnicos (*Ibidem*, p.4-5). Por otra parte, en su art. 4 considera que los ataques a la integridad de los datos serán considerados como delitos, o en otras palabras, el daño, la supresión, el deterioro y la alteración de los datos de información será considerada un delito. En complementación, el art. 5 considera un delito el

[33] Para un panorama detallado sobre la adhesión al Convenio de Cibercrimen y el Protocolo Adicional ver anexos.
[34] Se firmó firmado el 23 de octubre de 2001 y entró en vigor el 1 de julio de 2004.
[35] Por datos informáticos se comprende al conjunto de hechos, información o conceptos presentes en un programa (Council of Europe, 2001, p.4).
[36] Los sistemas informáticos constituyen dispositivos interconectados individuales o en su conjunto cuya función es el tratamiento de los datos ejecutados por un programa (*Ídem).*

funcionamiento ilegítimo de un sistema informático mediante el daño la supresión, alteración o deterioro de los datos informáticos (*Ibidem*, 2001, p.5).

En tanto, si el Convenio de Budapest es la convergencia voluntaria de los Estados que limitan su actuación por propósitos y obligaciones, para Krasner (2012, p.95) tal Convenio se constituiría como un régimen internacional por ser compuesto de principios y normas que por efecto convergen en un premisa de obligación general entre los Estados, siendo para Jervis (1982, p.357), esta premisa la reciprocidad y la cooperación que es más que la continuación del interés propio a corto plazo, porque plantea el sacrificio del interés propio por motivar a otros actores en actuación conjunta siendo esta acción iniciativa propia y no necesariamente por la obligatoriedad de una norma específica. En otras palabras, el Convenio de Budapest puede ser catalogado como un régimen internacional, por componer "la combinación de comportamientos con principios y normas que distinguen las acciones estatales gobernadas por regímenes de la actividad más convencional guiada exclusivamente por la estricta evaluación de intereses"[37] (Krasner, 2012, p.95).

Por consiguiente, al evidenciar el Convenio de Budapest como un régimen internacional, es esencial mencionar que la limitación de actuación de los Estados es voluntaria para alcanzar metas en común, o en palabras de Krasner (2012, p.93) la convergencia en un área dada de las relaciones internacionales. Tal concepción da paso a visualizar las problemáticas para alcanzar el interés común, que en el caso del Convenio de Budapest están centradas en: la pornografía infantil; el *cyberbullying*; el *copyright;* y el *phishing.*

En atención, al primer problema se debe mencionar que el art. 9 del Convenio de Budapest, considera a la pornografía infantil como un delito, por lo que condena expresamente la producción y la intención de difusión; el ofrecimiento y la puesta de disposición, la transmisión, la adquisición y la posesión de pornografía infantil por medio de sistemas informáticos o dispositivos de almacenamiento de datos informáticos (Council of Europe, 2001, p.6). Por otra parte, el *cyberbullying* es regulado por el Protocolo Adicional[38] al Convenio de Budapest que en su art. 3 condena la difusión de material racista y xenófobo[39] mediante sistemas informáticos; complementado en su art.4 penaliza las amenazas por medio de sistemas informáticos a las personas de diferente raza, color, ascendencia u origen étnico del agresor (Consejo de Europa, 2003, p.4), y seguidamente, el art 5 prohíbe los insultos que tengan por finalidad la agresión a grupos raciales o étnicos (*Ibidem*, p.5).

De igual importancia, el *copyright* según el Consejo de Europa (2001, p.7) es considerado como una infracción a la propiedad intelectual, a los derechos afines, y penalizado por el art. 10 conforme a las obligaciones detalladas en la Acta de París (1971), el Convenio de Berna sobre la propiedad de las obras literarias y artísticas, el Acuerdo sobre el derecho de la propiedad intelectual y el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre el derecho de autor. Finalmente, como última problemática, el *phishing* es condenado por el Convenio de Budapest, bajo el art.8, que

[37] Traducción libre del autor, em el original: "*mistura de comportamentos com princípios e normas que distingue as ações estatais governadas por regimenes da atividade mais convencional guiada exclusivamente pela estreita avaliação de interesses*" (Krasner, 2012, p.95).

[38] El Protocolo Adicional al Convenio sobre el Cibercrimen relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos se firmó firmado el 28 de enero de 2003 y entró en vigor el 1 de marzo de 2006.

[39] Por material racista y xenófobo debe comprenderse todo material escrito, difundido por imágenes o alguna representación de ideas que tenga por finalidad promover agresión, discriminación, odio o violencia con individuos o grupo de individuos de una determinada raza, ascendencia u origen étnico (Consejo de Europa, 2003, p.4).

considera al fraude informático como una acción dolosa,[40] con beneficio económico que causa perjuicio patrimonial a una persona jurídica mediante la "introducción, alteración, borrado o supresión de datos informáticos y "cualquier interferencia en el funcionamiento de un sistema informático" (Council of Europe, 2001, p.6). Sin duda alguna, la creación de agendas de actuación por los actores internacionales contra las problemáticas comunes para alcanzar una meta en conjunto, permite demostrar la existencia de la vinculación directa entre la moderación de los Estados y sus intereses para evocar un régimen internacional (Jervis, 1982, p. 357).

Sin embargo, la continuación de los principios, normas y reglas provenientes del Convenio de Budapest, debe ser acompañada por la concretización del proceso de toma de decisiones, con la finalidad de posibilitar la implementación de los principios y la alteración de las normas y reglas dentro del régimen internacional (Safarti, 2005, p.58). Por esta razón, el Convenio de Budapest concretizó sus esfuerzos mediante el Comité para la Convención de Cibercriminalidad, el cual tiene por finalidad facilitar el uso y la aplicación efectiva del Convenio; permitir el intercambio de información sobre el desarrollo legal, policial o tecnológico sobre el cibercrimen; y formular posibles enmiendas para la Convención sobre el cibercrimen (Council of Europe, 2014, p.2).

En consecuencia, este Comité se refuerza, mediante el art.13 del Convenio, porque considera la implementación de sanciones para los delitos previstos en los artículos 2 al 11[41], que están sujetos a "sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad" (*Ibidem*, p.8). En otras palabras, se impondrá sanciones o medidas penales a las personas jurídicas[42], conforme al art. 12 que expresa la responsabilidad de la persona jurídica por los delitos previstos en el presente Convenio. Por ello, según Keohane (1982, p. 331) la presencia del Comité facilitó la institucionalización del proceso decisorio, que guía la constitución e implementación de las normas para la continuación de censo en el régimen internacional.

En conclusión, ante las pruebas empíricas y analíticas presentadas en este capítulo, el Convenio de Budapest constituye un cuerpo robusto de principios, normas, reglas, procedimientos y de toma de decisiones que conforman así, un régimen internacional según la argumentación teórica de Krasner (2012); y aún más, este Convenio entrama un tipo de régimen internacional de visión estructural convencional, por constituir una acción voluntaria y coordinada que somete el interés nacional y la maximización del poder, con la finalidad de alcanzar una meta común que permite la institucionalización de las relaciones internacionales para regular acciones de los Estados en la perspectiva de Keohane (1982).

PIEZA A PIEZA SE ARMA UN ROMPECABEZAS: COMPLETANDO EL RÉGIMEN INTERNACIONAL DE CIBERCRIMINALIDAD:

Comparativamente al anterior capítulo, las organizaciones internacionales[43] constituyen un espacio de convergencia de los Estados, lo que permite la actuación conjunta en áreas determinadas de las Relaciones Internacionales. En este caso, en base a los mismos lentes analíticos de los regímenes

[40] Ejecución de un acto típicamente antijurídico con conocimiento y voluntad de la realización (Cabanellas, 1993, p. 147-148).
[41] En este trabajo no son considerado, para fines de este trabajo, los artículos: 6 (Abuso de los dispositivos), y 11 (Tentativa y complicidad) dispuestos en el Convenio de Ciberdelincuencia de 2001 del Consejo de Europa.
[42] En este punto es esencial evidenciar de que se trata de una personalidad jurídica internacional, en la cual se torna sujeto del derecho el Estado que se abstiene a derechos y obligaciones en el plano internacional (Amaral Junior, 2012, p. 40).
[43] Son definidas como como el conjunto de Organizaciones Intergubernamentales Internacionales (OIG) formadas por Estados y las Organizaciones no Gubernamentales Internacionales (ONGIS) que son formas institucionalizadas de legitimación y cooperación internacional (Herz; Hoffmann, 2004, p.9-10).

internacionales, las organizaciones internacionales parten de una visión estatocéntrica, la cual según Waltz (1988, p. 145), considera los Estados como actores principales de las organizaciones que actúan por su propio interés y buscan maximizar sus capacidades, sin embargo esta concepción se compacta por un visión neoliberal que según Herz & Hoffmann (2004, p. 45) las instituciones internacionales facilitan la cooperación y permiten la circulación del poder y la información. Por ello, se considera a las organizaciones internacionales como el fruto de las decisiones de los Estados, en las cuales se busca legitimar la búsqueda de la cooperación, el poder y sus intereses para una meta en común[44].

De tal manera, que ese tipo de interacción entre los Estados para alcanzar sus intereses es evidente en el caso de la ONU[45], que como meta común entrama la lucha al cibercrimen por medio de la aprobación de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en 2001 en dos fases: la (1) en Ginebra en 2003; y la (2) en Túnez en 2005. Por su parte, la Cumbre de Ginebra[46] de 2003 compiló el deseo la creación de una Sociedad de la Información para que la información y el conocimiento a nivel global en base a la Carta de las ONU y la Declaración Universal de los Derechos Humanos (CMSI, 2004). Por medio del fomento de la confianza y la seguridad en la utilización de las Tecnologías de la Información y la Comunicación (TIC) con la finalidad promover una cultural global de ciberseguridad en cooperación con Estados y organismos internacionales. (*Ídem*). Y por su parte, la Cumbre de Túnez en 2005 consolidó el papel de las TIC para afianzar la seguridad de la información y de las redes, para promover la paz, la seguridad, y la estabilidad a una escala nacional y global (CMSI, 2006).

Por esta razón, se puede evidenciar según Nye & Keohane (1971, p.332) la existencia de una interacción trasnacional[47] genera una interdependencia, que en la perspectiva de Waltz, (1988, p.153) permite que los Estados se preocupen por consolidar las relaciones con otros Estados para alcanzar intereses comunes. En esa visión, un resultado de la convergencia de los Estados Miembros de la CMSI dieron paso al nacimiento del Foro para la Gobernanza del Internet (IGF), el cual congrega un espacio de debate sobre cuestiones de política pública relacionadas con el internet, la gobernanza del internet, y facilita la participación de los Estados en instituciones y acuerdos existentes sobre el internet para identificar problemas en torno de la ciberseguridad y el cibercrimen dentro de la comunidad internacional (IGF, 2011).

En complementación, la Unión Internacional de Telecomunicaciones (UIT)[48] sustenta la lucha contra el cibercrimen por medio de la Agenda sobre la Ciberseguridad Global (GCA) lo que constituyó un marco teórico para la cooperación internacional, con la finalidad de promover la ciberseguridad, y la confidencia y seguridad de la Sociedad de la Información (GCA, 2007, p.2). Además de ello, permitió el desarrollo técnico de Fórums Internacionales sobre telecomunicaciones para el incremento de la seguridad y la capacidad de creación de información, en las redes por parte de los Estados, y la promoción del trabajo conjunto, con la comunidad global sobre las estructuras internacionales, regionales y nacionales que envuelvan ciberseguridad (*Ibidem*, p.15-16).

[44] La selección de las organizaciones internacionales para este apartado se basaron en la participación del Comité de la Convención de Budapest (Council of Europe, 2014, p.7).
[45] La Cumbre Mundial sobre la Sociedad de la Información fue aprobada bajo la resolución 56/183 del 2001 (WSIS, 2006) por la Asamblea General de las Naciones Unidas.
[46] Desarrollada del 10 al 12 de diciembre del 2003 (CMSI, 2004).
[47] Referida a aquellas interacciones que envuelven actores no gubernamentales como organizaciones internacionales, donde el Estado es apenas una unidad que facilita la interacción dentro de las interacciones transnacionales (Nye; Keohane, 1971).
[48] La Unión Internacional de Telecomunicaciones se creó en 1932 y se convirtió en un agencia especial de las Naciones Unidas en 1947 (Herz; Hoffmann, 2004, p.113)

En consecuencia, a una mayor interdependencia entre los Estados para la lucha contra la cibercriminalidad, se produce para Waltz (1988, p.154-155) una especialización que permite el establecimiento de una división de tareas. Básicamente esta idea de división de tareas se evidencia, en la actuación contra el cibercrimen lo que produce nuevas agendas o problemáticas dentro de la cibercriminalidad. Específicamente esta división de tareas se ve reflejada, en la Oficina de las Naciones Unidas para las Drogas y el Crimen (UNODC), la cual comprende el cibercrimen como un crimen emergente encajado dentro del crimen organizado trasnacional[49]. Este organización actúa sobre los delitos, sobre la identidad, lavado de dinero, fraudes y movimientos irregulares de transacciones económicas, tráfico de bienes culturales, el crimen del medio ambiente que concentra la caza furtiva y venta a gran escala de especies marinas y silvestres en extinción, el tráfico de órganos que constituye un mercado ilícito para la venta de órganos con la finalidad de lucro económico, y la medicina fraudulenta (UNODC, 2015). Por lo cual, la UNODC para frenar este crimen emergente enfatiza en la creación de un capacidad sostenible contra el cibercrimen por medio de apoyo a estructuras y acciones nacionales para la implementación de sistemas penales que permitan la cooperación internacional para la investigación y análisis del cibercrimen (*Ídem*).

Sin duda alguna, esta división de tareas puede verse como el establecimiento de una reciprocidad en palabras de Jervis (1982, p.357), donde los Estados sacrifican sus intereses como una iniciativa propia y no como una imposición de una norma específica (Krasner, 2012, p.95). Es ejemplo de ello, los Estados Miembros de la Unión Africana (UA) que se suscribieron al combate del cibercrimen por medio del Proyecto de la Convención de la UA sobre la Confianza y la Seguridad en el Ciberespacio con la finalidad de producir una legislación cibernética (INFOSOC, 2015). Para mostrar así que el proyecto de la UA ante el cibercrimen refuerza los sistemas de información, el patrimonio digital y cultural; la continuidad y la soberanía de los Estados; y la ciberseguridad como voluntad política.

Por tanto, como resultado de este proyecto se concretó una agenda de actuación sobre la ciberseguridad, la cual formula leyes de responsabilidad conjunta que tiene por finalidad el combate al cibercrimen y la promoción de la protección de la infraestructura de la información por medio de la cooperación internacional (*Ídem*, 2015), para atender los déficits de seguridad tecnológica; y edificar una Sociedad de la Información que preserve los derechos y las libertades (AUC, 2012).

Por consiguiente, la reciprocidad y la suscripción a un interés común por parte de los Estados permite un camino de actuación conjunto que en palabras de Waltz (1988, p.155) se denomina de integración que en un sistema de división de tareas crea un beneficio para todos los Estados. Esto es visto en la Organización de los Estados Americanos (OEA) que en 2004 aprueba la Estrategia Interamericana para Combatir las amenazas a la ciberseguridad (OEA, 2015b). De tal forma, que efectiviza la cooperación con entidades nacionales y regionales de sectores privados y públicos para implementar espacios de discusión política y técnica, para la seguridad de la información y la comunicación en las Américas (OEA, 2015a). Se complementa, la estrategia para combatir la ciberseguridad por medio del Comité Interamericano contra el Terrorismo (CICTE), el cual trata la ciberseguridad desde una óptica de Equipos de Respuesta a Incidentes (CSIRT) para promover el desarrollo de Estrategias Nacionales sobre Ciberseguridad y fomentar la "Seguridad Cibernética en el Hemisferio" de las Américas (OEA, 2015b).

Por lo anteriormente dicho, cabe concluir que las organizaciones internacionales, desde el punto de vista neorrealista (Waltz, 1988) y neoliberal (Keohane; Nye, 1979) las organizaciones internacionales constituyen un espacio de convergencia voluntaria de los Estados para el desarrollo de actividades conjuntas, para alcanzar una meta en común (Krasner, 2012). Por esta razón, la mayor

[49] Definido como actividades legítimas para fines delictivos en un escala global (UNODC, 2015).

contribución de las organizaciones internacionales para el régimen internacional de cibercriminalidad, consiste en crear espacios de diálogo político entre los Estados, que puedan operativizar e instrumentar la cooperación internacional, la interdependencia, la especialización en las actividades cibercriminales y fortalecer las acciones conjuntas con la finalidad de promover la ciberseguridad como regulación y el combate de las actividades cibercriminales.

¿CRIMEN Y CASTIGO?: El *HACKTIVISMO* DE SNOWDEN

Al haber sustentado teórica y empíricamente la conformación de un régimen internacional de cibercriminalidad, cabe preguntarse ¿si tal régimen – suponiendo que a futuro se concretice – podría ser implementado en el caso de Edward Snowden? Con el recuerdo que el personaje de Snowden toma fuerza y visibilidad internacional por medio de la divulgación del espionaje realizado por la Agencia Nacional de Seguridad (NSA) y la Sede de Comunicaciones del Gobierno (GCHQ). Ante ello Snowden expone que teóricamente estas agencias deberían apenas recolectar información para objetivos estratégicos denominados SIGINT, pero en la práctica estas agencias de espionaje, recolectan la información de norteamericanos como registros telefónicos, "títulos de los e-mails, líneas de asunto, todo llevado sin autorización o consentimiento"[50] (Harding, 2014, p.14). Tales prácticas permiten a los Estados Unidos y al Reino Unido la interceptación de información de las redes de datos y comunicación a escala global.

Por ello, según la perspectiva de Snowden, la comunidad de inteligencia de los Estados Unidos está cometiendo una flagrante infracción a la Constitución de los Estados Unidos y principalmente al derecho de la privacidad (*Ídem*). Sin embargo, tras la difusión de esta información por medio de Laura Poitras, Ewen MacAskill y Glenn Greenwald, Edward Snowden fue el hombre más buscado internacionalmente por los Estados Unidos y el Reino Unido acusado de terrorismo y su postura aleñada al *hacktivismo.*

Ante esto, el régimen internacional de Cibercriminalidad penalizaría las acciones de Snowden por catalogar su difusión de información de la NSA como acceso ilícito o ilegítimo a un sistema informático contemplado en el art.2 del Convenio de Budapest. Pero si se refiere a este punto debe pensarse dos caminos: El primero estaría enfocado a contemplar la evidencia expuesta por Snowden, por intermedio de Comité del Convenio de Budapest para condenar a la NSA, por el uso inapropiado de los datos e información en Estados Unidos, y el segundo contempla la condena expresa de Edward Snowden por el uso ilícito e ilegítimo de la información de la NSA para exponer el espionaje mundial de los Estados Unidos.

Por consiguiente, hay que replantearse el problema de la aplicación de crimen y castigo del régimen internacional para los dos casos, por medio de variables causales que permiten la conformación de la voluntad de los Estados, complementados por la ética y moral como un valor que regule el comportamiento de los actores y de paso a ún régimen internacional (Thomson, 200, p. 292).

CONCLUSIONES:

El Convenio de Budapest debe ser considerado como un "régimen internacional" según la perspectiva de Krasner (2012), porque se compone de principios enmarcados en el fortalecimiento de la cooperación internacional, y la necesidad de constituir un cuerpo jurídico que regule las

[50] Traducción libre del autor, en el original: "*cabeçalhos de e-mail, as linhas de assunto, tudo levado sem autorização ou consentimento"* (Harding, 2014, p.14)

actividades cibercriminales; así mismo, está compuesto por normas y reglas que penalizan la pornografía infantil, el *cyberbullying,* el *copyright* y el *phishing*, y concreta un cuerpo institucionalizado del proceso de toma de decisiones por medio del Comité para la Convención de Cibercriminalidad.

Por otro lado, el Convenio de Budapest se cataloga como una variable interviniente de orientación estructural modificada, en cuanto surge como acción voluntaria de los Estados, según Keohane (1982), que en este caso constituyen los países parte de la Unión Europea, y como un variable de reciprocidad para Jervis (1982), que permite la acción conjunta y coordinada de los Estados, para alcanzar una meta en común que somete así el interés nacional y la maximización del poder, en la visión de Krasner (2012).

No obstante, cabe señalar que las agendas o problemáticas penalizadas por el Convenio de Budapest promueven un cierto tipo de *spillover* (Mitrany, 1946), es decir que el trasbordamiento de un área de interés para otra. Siendo así que la pornografía infantil y el *cyberbullying* como parte de un futuro régimen internacional de Cibercriminalidad pueden vincularse al régimen internacional de Derechos Humanos, y en el caso del *copyright* y el *phishing,* se vinculan perfectamente al régimen internacional de crimen transnacional. Por estas razones se puede evidenciar que los regímenes internacionales evocan un principio de cooperación, para alcanzar metas comunes y beneficiarse de la formación de una interdependencia.

A manera de colofón, cabe decir que las organizaciones internacionales juegan un papel importante en el impulso de los regímenes internacionales, en cuanto crean espacios de diálogo e interacción entre los Estados, con la finalidad de promover agendas de actuación conjunta, lo que representa un censo de voluntad y coordinación según Keohane (1982), y la congregación en torno de la cooperación para promover convergencia en metas comunes.

BIBLIOGRAFÍA

- African Union Commission (AUC). (2012) *Projecto de Convenção da Union Africana sobre a adopção de um quadro jurídico sobre a ciberseguridad em África ou Projeto de Convenção da Union Africana sobre a confiança e a seguridade n ciberespaço***.** Recuperado de: <http://au.int/en/sites/default/files/AU%20Convention%20%28Portuguese%29%20%2813-11-2012%20CSD%29.pdf>.
- Amaral Junior, Alberto. (2012). A Personalidade Jurídica**.** En Amaral Junior, Alberto. *Manuel do Candidato: noções de direito e direito internacional*. (4ª Ed) p.37-44. Brasilia: FUNAG.
- Cabanellas, Guillermo. (1993). *Diccionario Jurídico Elemental***.** p. 147-148; 210-214. Argentina: Editorial Heliasta S.R.L.
- Carvalho, Ernani. (2010). Krasner e os regimenes internacionais**.** En Medeiros, Marcelo de Almeida (*et al)*. *Clássicos das relações internacionais*. p. 208-216. São Paulo: Hucitec.
- Castells, Manuel. (2001). *La Galáxia Internet***.** (1ª. Ed.). p. 51-67. Barcelona, España: Areté.
- Consejo de Europa. (2003). *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos***.** Serie de Tratados europeos n°189. Estrasburgo: Ministerio de Asuntos Exteriores y de Cooperación, p. 1-9. Recuperado de: <http://www.plataformaong.org/conferencia/wp-content/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf>.

- Council of Europe. (2014). Cybercrime *Convention Commitee (T-CY): T-CY rules of Procedure***.** Strasbourg, p. 1-7. Recuperado de: <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY (2013)25%20rules_v14.pdf>.
- _____. (2001). *Convenio sobre la Ciberdelincuencia***.** Serie de Tratados Europeos, n°185, Budapest, p. 1-26. Recuperado de: < http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF>.
- Cumbre Mundial sobre la Sociedad de la Información (CMSI). (2006). *Compromiso de Túnez***.** Recuperado de: <http://www.itu.int/wsis/docs2/tunis/off/7-es.pdf>.
- _____ (CMSI). (2004). *Declaración de Principios/ Construir la Sociedad de la Información: Un desafío Global para el Nuevo Milenio***.** Recuperado de: < http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-S.pdf>.
- Demmers, Jolle. (2012) *Theories of Violent Conflict: An Introduction***.** p. 1-20. New York: Routledge.
- Division of Information Society (INFOSOC). (2015). Cyber Security**.** African Unión Commission 2015. Recuperado de: <http://pages.au.int/infosoc/cybersecurity>.
- Dostoievski, Fiodor. (2005). *Crimen y Castigo***.** España: Editorial Cátedra.
- Ghernaouti, Solange. A Global Approach to Cybersecurity**.** En Ghernaouti, Solange. (2013). *Cyber Power/ Crime, Conflict and Security in Cyberspace*. p. 330-336. Switzerland: EPFL Press.
- _____. Cyberconflicts, Cyberwars and Cyberpower**.** En Ghernaouti, Solange. (2013). *Cyber Power/ Crime, Conflict and Security in Cyberspace.* p. 163-167. Switzerland: EPFL Press.
- _____. Cybercrimes against Persons**.** En Ghernaouti, Solange. (2013). *Cyber Power/ Crime, Conflict and Security in Cyberspace*. p. 91-107. Switzerland: EPFL Press.
- _____. Cyberspace and Internet: a New Paradigm for Crime and Conflicts**.** En Ghernaouti, Solange. (2013). *Cyber Power/ Crime, Conflict and Security in Cyberspace.* p. 23-28. Switzerland: EPFL Press.
- _____. Glossary of main cybercrime and Cybersecurity related terms. En Ghernaouti, Solange. (2013). *Cyber Power/ Crime, Conflict and Security in Cyberspace.* p. 425-442. Switzerland: EPFL Press.
- _____. The Cybercriminal's Toolkits**.** En Ghernaouti, Solange. (2013). *Cyber Power/ Crime, Conflict and Security in Cyberspace.* p. 210-216. Switzerland: EPFL Press.
- Global Cybersecurity Agenda (GCA). (2007). *Report of the Chairman of Hleg***.** p.1-21. Recuperado de: <http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf>.
- Harding, Luke. (2014). *Os arquivos Snowden/ A história do homem mais procurado do mundo.* Traducción de Alice Klesck, Bruno Correia. p. 7-85. Rio de Janeiro: LeYa.
- Henriques, Anna Beatriz Leite; Leite, Alexandre Cesar Cunha; Júnior, Augusto Wagner Menezes Teixeira. (2015). Reavivando o método qualitativo: as contribuições do Estudo de Caso e do Process Tracing para o estudo das Relações Internacionais. *Revista Debates: Porto Alegre*, vol. 9 (n° 1), p. 9-23.
- Herz, Mônica; Hoffmann, Andrea Ribeiro. Contribuições Teóricas para o Estudo de Organizações Internacionais**.** En Herz, Mônica; Hoffmann, Andrea Ribeiro. (2004). *Organizações Internacionais: História e Práticas*. p. 33-50. Rio de Janeiro: Elsevier.
- _____. Organizações Internacionais: Definição e História**.** En Herz, Mônica; Hoffmann, Andrea Ribeiro. (2004). *Organizações Internacionais: História e Práticas*. P.9-20. Rio de Janeiro: Elsevier.

- Hinduja, Sammer; Patchin, Justin. (1987). Cyberbullying: The New Adolescent Aggression. En Hinduja, Sammer; Patchin, Justin. *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying*. p.5-16. United States of America: SAGE.
- International Criminal Police Organization (INTERPOL). *Cybercrime***.** (2015). Recuperado de: <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>.
- International Telecommunication Union (UIT). (2015). *Global Cybersecurity Agenda (GCA).* Recuperado de: http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx**>.**
- Internet Governance Forum (IGF). (2011). *What is the Internet Governance Forum?* Recuperado de: < http://www.intgovforum.org/cms/aboutigf>.
- Jervis, Robert. (1982). Security Regimes. *International Organization*. vol. 36 (n. 2), p. 357-378.
- Keohane, Robert O. (1982). The Demand for Internacional Regimes. *Internacional Organization*. vol. 36 (n° 2), p.325-333.
- Krasner, Stephen D. (2012). Causas estruturais e consequências dos regimes internacionais: regimes como variáveis intervenientes. *Revista de Sociologia e Política, Curitiba*, vol. 20 (n° 42), p.93-110.
- Mitrany, David. (1946). *A Working Peace System***.** Londres: Royal Institute of International Affairs.
- Nye, Joseph S. (2012). Deslocamentos do poder: difusão e transições**.** En Nye, Joseph S. *O Futuro de Poder*. Traducción de Magda Lopes. P.151-192. São Paulo: Benvirá.
- Nye, Joseph S. (2015). *International Norms in Cyberspace***.** Project and Syndicate/ The World´s Opinion Page: Innovation & Technology. Recuperado de: <http://www.project-syndicate.org/print/international-norms-cyberspace-by-joseph-s--nye-2015-05>.
- Nye, Joseph; Keohane, Robert O. (1971). Trasnational Relations and World Politics: An Introduction**.** *International Organization*, vol. 25 (n°3), p. 332-342.
- Organization for Economic Co-operation and Development (OECD). (2015). *Comparative analysis of national cybersecurity strategies***.** Recuperado de: <http://www.oecd.org/sti/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm>.
- Organización de los Estados Americanos (OEA). (2015b). *Seguridad Cibernética***.** Recuperado de: <https://www.sites.oas.org/cyber/Es/Paginas/default.aspx>.
- _____. (2015a) *Temas***.** Recuperado de: <http://www.oas.org/es/temas/seguridad_cibernetica.asp>.
- Sarfati, Gilberto. (2005). Regime internacional e cooperação**.** Em Sarfati, Gilberto. *Teoria das relações internacionais*. p.55-62. São Paulo: Saraiva.
- Stein, Arthur. A. (1982). Coordination and Collaboration: Regimes in an Anarchic World. *International Organization*. vol. 36 (n. 2), p. 299-324.
- Thomson, Janice E**.** (2000). Explicando a regulamentação de práticas transnacionais: uma abordagem construtiva com referência ao Estado. En Rosenau, James N; Czempiel, Ernst-Otto (orgs.). *Governança sem Governo: ordem e transformação na política mundial*. p. 263-294. Brasília, Editora Universidade de Brasília.
- Unión Internacional de Telecomunicaciones (UIT). (2015). *Visión General***.** Recuperado de: <http://www.itu.int/en/about/Pages/overview.aspx>.
- United Nations Office on Drugs and Crime (UNODC). (2015). *Emerging Crimes***.** Recuperado de: <https://www.unodc.org/unodc/organized-crime/emerging-crimes.html>.
- Waltz, Kenneth N. (1988). Estruturas Políticas**.** En Waltz, Kenneth N. *Teoría de la Política Internacional*. p. 119-144. Colección de Estudios Internacionales. Buenos Aires, Argentina: Grupo Editor Latinoamericano S.R.I.

- World Summit on the Information Society (WSIS). (2006). *Basic Information: About WSIS*. Recuperado de: < http://www.itu.int/wsis/basic/about.html>.
- Zabalete, Mariana Souto. (2013). Régimenes internacionales y gobernanza global: una mirada desde los aportes de la aproximación constructivista**.** En Rascovan, Alejandro (*et. al.)*. *Relaciones internacionales: teorías y debates*. p.255-278. Buenos Aires: Eudeba.

ANEXOS

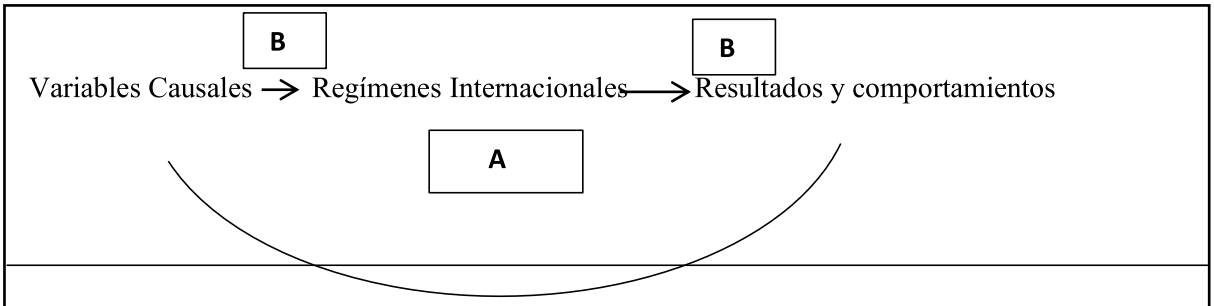

Figura N° 1
Fuente: adaptación de Krasner, Stephen D. (2012). *Causas estruturais e consequências dos regimes internacionais: regimes como variáveis intervenientes*, p.98.