

## EL INTERNET, LA CULTURA DEL MIEDO Y LA CRIMINALIDAD CIBERNÉTICA: ASPECTOS DE PRODUCCIÓN E INTERPRETACIÓN DEL DERECHO PENAL CONTEMPORÁNEO

Emerson Wendt<sup>1</sup>

Fecha de publicación: 01/11/2015

**SUMARIO: 1.** Introducción. **2.** El internet, su característica autopoiética sui generis y el Derecho. **3.** Internet y Cultura del Miedo. **4.** Análisis sobre la Ley 12.735/13 ("Ley Carolina Dieckmann"). **5.** Conclusiones. Referencias.

RESUMEN: Este texto analiza, a partir de la concepción del Internet (ciberespacio) como un sistema social sui generis, de la proliferación de la cultura del miedo con el uso de la (ciber)comunicación y el aumento de la sensación de inseguridad y, por consiguiente, la necesidad de crear mecanismos, por el Derecho (penal), del control y disminución de los riesgos, además de la necesidad de, no solamente para fines de la (re)creación del Derecho penal, como también de su (re)interpretación y (re)análisis, de considerar la esencia tecnológico-digital, la naturaleza, peculiaridades características propias de la sociedad digital, buscando preservar los derechos y garantías de los usuarios (sistemas psíquicos), incluyendo la expectativa referente a evolución de la red mundial de computadores.

**Palabras-llave:** Autopoiesis. Ciber-criminalidad. Cultura del miedo. Internet. Sociedad digital.

-

Cursando Master en Derecho y Sociedad (Facultad Unilasalle. Canoas, Rio Grande do Sul, Brasil). Delegado de la Policia Civil en el RS/Brasil. Lattes: http://lattes.cnpq.br/9475388941521093. E-mail: emersonwendt@gmail.com

# THE INTERNET, THE CULTURE OF FEAR AND THE CYBERNETIC CRIMINALITY: ASPECTS OF PRODUCTION AND INTERPRETATION OF CONTEMPORARY CRIMINAL LAW

**ABSTRACT:** Considering the conception of Internet (cyberspace) as a social system sui generis, this paper approaches the proliferation of the culture of fear through the use of cyber communication and the growing of insecurity sensation, and, consequently, the need to create mechanisms of control and reduction of risks through the Law (criminal). This text claims not only for a recreation of the criminal law, but it also claims for its reinterpretation and reanalysis considering the technological-digital essence, the nature, peculiarities and own characteristics of a digital society aiming to preserve the user's rights and guarantees (psychic systems), including the expectation about evolution of the world wide web.

**Keywords:** Autopoiesis. Cybercrime. The culture of fear. Internet. Digital society.

#### 1. Introducción:

La temporalidad y pérdida de la noción del espacio son las características principales de aquello que se tornó uno de los principales medios de comunicación en las últimas décadas: Internet. En Brasil, según datos del Comité Gestor de Internet<sup>2</sup> (2014), son más de 30 millones de domicilios con computador, siendo de éstos más de 27 millones con acceso a internet. De esta forma totalizando más de 85 millones de usuarios de internet. (Al tiempo que más de 143 millones de brasileños usan celular, de los cuales 52,5 millones son usuarios de internet usando esa modalidad).

La instantaneidad de las informaciones referente a los acontecimientos y a la proyección de esa comunicación más allá de la comprensión humana, atravesando barreras antes intransponibles, integran ese *medium* de comunicación ampliamente utilizado actualmente y que posee un único lenguaje comunicacional codificada (*bits* y *bytes*), (STOCKINGER, 2003), entre sus mecanismos de intercambios de informaciones, a través de los protocolos llamados de TCP/IP (*Transmisión Control Protocol/Internet Protocol*).

La comprensión de Internet como un sistema o subsistema autónomo, con características especiales, al mismo tiempo en que se caracteriza como un modulador actual principal de las comunicaciones entre los diversos subsistemas sociales, tales como de Derecho, de política, de religión, de moral, etc., es uno de los objetivos de este artículo. No se pretende agotar el asunto, sino traspasar esa nueva concepción, basada en Niklas Luhmann, idealizador de la Teoría de los Sistemas, para analizar no solamente la cultura del miedo, amplificada con el uso de la red mundial de computadores, como también la ciber-criminalidad, tanto bajo la óptica de los subsistemas de Derecho (principalmente) y de la política bajo la óptica del propio Internet, como subsistema con características *sui generis*.

### 2. El internet, su característica autopoiética sui generis y el Derecho:

La tecnología ha evolucionado con un ritmo frenético, tornándose cada vez más compleja. Junto con ella, desde los primeros pasos en la década del 70 del Siglo XX, surgió la idealización de Internet y sus peculiaridades

<sup>&</sup>lt;sup>2</sup> Esos datos y otros, recolectados por el Comité Gestor de Internet en Brasil, están disponibles en: <a href="http://cetic.br/publicacoes/2013/tic-domicilios-2013.pdf">http://cetic.br/publicacoes/2013/tic-domicilios-2013.pdf</a>. Último acceso en: 15 jul. 2014.

comunicativas dinámicas y constantes innovaciones, principalmente a partir de la década del 90, más específicamente después de la creación de la red "www" por Tim Berners-Lee. En Brasil, tuvo su impacto, principalmente después de 1995, cuando dejó de ser uso exclusivo de las universidades y pasó a tener acceso público y también, fue creado el Comité Gestor de Internet en Brasil, por la Portaría Interministerial n° 147, de 31 de mayo de 1995, alterada por el Decreto Presidencial n° 4.829, de 3 de setiembre de 2003.

Además de las varias características conocidas de Internet, que solidificó la llamada "Sociedad de Información<sup>3</sup>", como la masificación de las informaciones, el acceso a sistemas y datos, multidiversidad de asuntos, una "superhighway" (SYDOW, 2013, p. 31), etc., el autodesarrollo<sup>4</sup> es la principal característica. También, varios sectores mundiales y nacionales<sup>5</sup>, defienden la continuidad de la auto-regulación de la red mundial de computadores, Internet.

Después de 1980, entidades no gubernamentales asumieron, no oficialmente, la reglamentación del ciberespacio, estableciendo padronizaciones y reglas. Dos de esas entidades son ICANN – *Internet Corporation for Assigned Names and Numbers* – e IANA – *Internet Assigned Numbers Authority* –, esta última responsable por la distribución/organización de "números" en Internet, como las direcciones

\_

<sup>&</sup>lt;sup>3</sup> Borges (2000, p. 29) sintetizó las características de la Sociedad de Información, como consecuencia de la sociedad Post-industrial, asi resumidos: la información es un producto y el saber un factor económico; la distancia y el tiempo entre la información y el destinatario no tiene más sentido, o sea, hay pérdida de noción de tiempo y espacio; hay "valor agregado" a la información, revolucionado por las tecnologías de información y comunicación que, además de revolucionar el mercado, creando nuevos servicios, empresas, empleos, transformaron el mundo en una "aldea global" (McLuhan); el "ciclo informativo" se transformó, pues además del usuario también se convertir en productor, hay para eso un bajo costo, mismo cuando se trata del almacienamiento de gran volumen de datos; el procesamiento, recuperación y acceso a las informaciones se tornó más rápido, seguro y eficaz, posibilitando el monitoramiento y evaluación de los datos/informaciones.

<sup>&</sup>lt;sup>4</sup> Luhman hace referencia a la "autoreproducción". Puede decirse, no obstante, que el Internet posee las dos características: autodesenvolvimiento e autoreproducción. Las ideas que se conciben a partir del uso e interacciones acaban por propiciar el desarollo y aprimoramiento de la red; el autoreproducirse, en el caso de la red, ocurre siempre en el sentido de que un (micro)sistema, como el microblog Twitter, que para continuar a evolucionar, acaba por necesitar otras aplicaciones y complementos, que hace con que no solo él, como también la propia red Internet, puedan perfeccionarse y reproducirse, a través de otras aplicaciones que interaccituan con él (Twitter). Podriamos ejemplificar, como las aplicaciones de fotos y videos para Twitter, además de los servicios para acortar las URLs (links), facilitando los tweets, limitados a 140 caracteres.

<sup>&</sup>lt;sup>5</sup> En el Brasil, el Comité Gestor de la Internet prima por la libertad de la evolución de la misma.

de los protocolos de internet – IP – y portas de comunicación (SYDOW, 2013).

Además de eso, como un (sub)sistema autónomo, *sui generis* en referencial de Stockinger (2003)<sup>6</sup>, el Internet tiene sus propias reglas y está cerrado operativamente, pero teniendo en su entorno los sistemas psíquicos (usuarios) y utilizando también, la comunicación para interactuar con los demás sistemas sociales (Derecho, moral, economía, etc.), influenciándolos o siendo influenciado.

Es un (sub)sistema auto-organizado, pues ha construido sus propias estructuras de funcionamiento y funcionalidad, que se iniciaron en 1969 con ARPANET<sup>7</sup> y, después de una división con la creación de Milnet<sup>8</sup>, en inicio de 1980 y posterior inter-ligación (1986) con los supercomputadores de NSF<sup>9</sup>, se creó la «espina dorsal» de una red formada por computadores súper potentes (*blackbones*), que evolucionó y continua evolucionando a través del tiempo, de acuerdo con las necesidades de otros (sub)sistemas, principalmente el económico.

Gottfried Stockinger (2003), apoyado en la teoría de los sistemas de Niklas Luhmann, ve el ciberespacio como un sistema autónomo (*sui generis*) y no apenas como un nuevo *medium* (medio por el cual pasan las comunicaciones), en el decir de referido autor "é – funcionalmente falando – um mensageiro" (STOCKINGER, 2003, p.162) que amplía la comunicación social. Es autopoiético, pues produce elementos para continuar produciendo más elementos estando, como referido, autoorganizado, a ejemplo de la extensa red mundial ("www") lanzada en 1992 y con estructuras y elementos definidos en cuanto a la distribución de dominios y conjuntos de protocolos de internet (IP) por todo el mundo. Por otra parte, desde el punto de vista, por ser un proceso de comunicación, entre los (sub)sistemas, puede ser tenido como un *super* mecanismo de acoplamiento estructural entre ellos (los sistemas), no solo por la agilidad de transmisión de datos, como por la instantaneidad y por el traspaso de barreras físicas, antes intransponibles o difíciles de ser derrumbadas.

La interdependencia de los sistemas, ponderada en la importante

<sup>&</sup>lt;sup>6</sup> La identificación como sistema autónomo *sui generis* es dada por Stockinger para explicar la diferencia con los demás (sub)sistemas. Puede parecer contracditorio con la teoría luhmaniana, puesto que un sistema siempre es diferenciado de los demás. No existen apesar de ello, estudios posteriores que trabajen esta cuestión de Internet como sistema y, por esto, preferimos, en este estudio, repetirla.

<sup>&</sup>lt;sup>7</sup> Advanced Research Projects Agency Network.

<sup>&</sup>lt;sup>8</sup> La Milnet es una red exclusiva para intercambio de datos militares.

<sup>&</sup>lt;sup>9</sup> National Science Foundation.

contribución de Stockinger (2003, p. 184) sobre la interacción entre los sistemas a través de la comunicación vía Internet, refuerza la concepción de su fundamento, estableciendo una especie de "ciber-dependencia":

Quando sistemas sociais passam a usar a autopoiese, elementos e relações comunicativas eletrônicos (por exemplo *e-mails*), estes farão, daqui em diante, parte integrante das ações e comunicações sociais. A interpenetração chega a tal ponto que a autopoiese de sistemas sociais passa a depender da cibercomunicação. Do mesmo modo, os cibersistemas concebidos em forma de mídia, "vivem" do seu uso por sistemas sociais. Tal dependência mútua também se reproduz e passa, assim, a fazer parte de cada sistema, através da interpenetração e acoplamento estrutural.

Específicamente sobre la interacción de los usuarios (sistemas psíquicos), Stockinger (2003, p. 185), enfatiza que ya "não são os usuários que estabelecem os limites e o horizonte da comunicação. É um sistema operacional eletrônico, em relação ao qual os usuários formam apenas o seu ambiente". En otros términos, los usuarios se utilizan de las aplicaciones de la red, como Twitter, Facebook, Flickr, YouTube, e-mails, etc., que son los elementos para interactuar en la red, permaneciendo, así mismo, en su entorno.

Así, dada la característica autopoiética *sui generis* de Internet, con capacidad de "fazer emergir construções culturais e sociais inéditas, que se transformam praticamente em sujeito" (STOCKINGER, 2003, p. 185), se tiene, por lo tanto, la existencia de un sistema complejo.

Para Teubner (2005, p. 37) eso no significa que no pueda haber (intervenção humana ativa), caracterizada por un (intervencionismo estatal ativo). Además, dado el pluralismo jurídico en la sociedad post-moderna, mismo con reglas propias, un determinado (sub)sistema (en el caso, el Internet o el Ciberespacio), como enfatiza Teubner (2005, p. 29), no puede valerse de la "clausura operacional da autopoiese", o sea, de estar inmunizada contra el Derecho. Éste (el Derecho), necesariamente causará influencias en él (Internet) y lo contrario también sucede.

La idea de intervencionismo, propuesta por Teubner (2005, p. 37-38), sería posible delante del surgimiento de la idea de "atratores", elemento nuevo/agregado en el estudio de la teoría de los sistemas. Las diferentes posibilidades de solución son llamadas de "atratores". Los sistemas auto-organizacionales son, por sí solos y secuencialmente, estables, recursivos. En ese punto es que entra el Derecho, puesto que, según Teubner (2005, p. 38),

o direito pode tentar, por produção normativa geral ou por atos jurídicos especiais, produzir perturbações de forma orientada e, apesar de todo o caos individual, irritar os sistemas recursivos de maneira que eles consigam mudar de um estado atrator a outro, com o qual o objetivo legal seja, pelo menos, compatível.

En ese acto intervencionista se puede conseguir así, la regulación jurídica contextual, necesaria y objetivadora del comportamiento deseable por parte del sistema recursivo. El Internet no escapa a la regla y, mismo que *diferencialmente* autopoiética y vista como sistema social *sui generis*, está dentro del contexto y del pluralismo jurídico.

También no es diferente, por lo tanto, el racionamiento en el contexto del Derecho Penal, porque mismo que tenga sus propias reglas, el Internet genera situaciones y comportamientos de sus usuarios (sistemas psíquicos), operadores de su entorno (ambiente), "compatíveis", por así decirlo con los tipos penales existentes en las más variadas legislaciones o, aún, comportamientos, positivos o negativos, que pueden generar daños y/o que tengan o vengan a tener reflejo en el contexto del proceso legislativo, generando la necesidad de su regulación, penal o no, pero de una racionalidad legislativa, pues, conforme Lira (2014, p. 82), "o processo de irritação/(des)juridificação é cíclico<sup>10</sup>".

Algunas legislaciones internacionales, incluso, mismo desde el punto de vista penal, han reducido el tiempo de reacción en relación a las evoluciones de ahí advenidas, influenciando el (sub)sistema político para atender a las expectativas normativas, generando Derecho, el que no es necesariamente el caso de Brasil, cuyos (comportamientos) legislativos del sistema político son más lentos, mismo que en fraccionamiento con el sistema de Derecho, hay una rapidez para criminalizar comportamientos (producir más Derecho), mucho más rápido del que para descriminalizar conductas (LIRA, 2014, p. 81), o sea, la des-juridificación es más lenta<sup>11</sup>. Italia, por ejemplo, modificó su código penal, enfocando determinados delitos para el combate a los delitos informáticos en 1993, mientras que Alemania lo hizo ya en 1986, el Reino Unido en 1990 y Holanda en 1992 (CRESPO, 2011). Esos países pueden inclusive ser referencia en materia legislativa respecto al asunto, pero lo que debe ser llevado en cuenta es la propia evolución de Internet en Brasil, a partir de 1995, momento en que se acentuó el ritmo de la evolución tecnológica y se somatizaran las

<sup>&</sup>lt;sup>10</sup> Sobre las fases de racionalidad legislativa, ver Lira (2014, p. 109-143).

<sup>&</sup>lt;sup>11</sup> *V.g.*, con respecto del adulterio, que desde 1977 la regulación pasó a ser civil, pero solo en 2005 hubo la descriminalización, juntamente con el delito del rapto consensual.

circunstancias necesarias y provocadoras de la contingencia jurídico-penal. Así, en comparación con las realidades (económicas, de evolución tecnológica, etc.) enfrentadas por los países, se puede citar a Argentina, que en 2008 modificó su código penal e introdujo los "delitos informáticos" (CRESPO, 2011, p. 150-153), y Colombia, que hizo las modificaciones legislativas en 2009, con «la protección de la información y de los datos» (COLOMBIA, 2009).

De cierta forma, la omisión legislativa específica no aleja el (re)análisis y (re)definición de la legislación penal y su aplicación, por el Judiciario, en relación a las conductas practicadas vía Internet, preservándose derechos y garantías fundamentales. La tendencia es que haya un refuerzo en el Derecho penal<sup>12</sup> en vista de la propaganda «sociedad de riesgo» (donde los riesgos "extrapolam as realidades individuais e até mesmo as fronteiras territoriais e temporais", conforme Giddens (*apud* VIEIRA; ROBALDO, 2007, p. 2)) y la proliferación de la cultura del miedo en Internet.

#### 3. Internet y Cultura del Miedo

#### 3.1 La cultura del miedo en la era de Internet:

El miedo no puede ser definido correctamente, sino cuando comparado con su ausencia (BAUMAN, 2008). A pesar de él estar asociado directamente a la presencia de algunos factores, como la existencia de un mal (visible o no) y/o un riesgo.

Según Costa (2011, p. 220), cuanto mayor el miedo (sensación de inseguridad) de una sociedad, mayor es el "controle social formal" por el Derecho, principalmente el Derecho Penal. Tal vez por esto de que el Estado no consiga satisfacer y restablecer por otros mecanismos la sensación de seguridad y relativizar el miedo, se acaba no solamente "privatizando" medios de seguridad (fragmentación de los espacios urbanos, por ejemplo), pero también focalizando su acción para la contingencia legislativo-normativo, como una forma de mostrar su parte de acción.

Desde el punto de vista tecnológico, se puede afirmar que el aspecto principal en relación al miedo está en la victimización, o sea, el riesgo, en la potencialidad de transformarse víctima en cuanto al uso de los recursos basados en tecnologías digitales. Esa sensación es mayor o menor cuanto

<sup>&</sup>lt;sup>12</sup> Ese refuerzo, necesariamente, debe ser comprendido como la creación de nuevos tipos penalis y/o agravamiento de las penas en los tipos penales ya existentes.

más representativo el proceso de percepción/pensamiento luhmanianos y las respectivas comunicaciones (GUIBENTIF, 2012), o sea, cuando el *medium* (en el caso Internet) adquiere forma (por la repetición de los procesos de percepción/pensamiento) y sentido, se vislumbra una mayor o menor sensación de miedo (de victimización).

A pesar que, es obvio que la mayor o menor percepción (exterior, con delimitación del objeto) y consecuente asimilación (pensamiento, interior, con calificación del objeto), dependen no solamente de la utilización de la tecnología como del conocimiento que las personas van adquiriendo, por el uso o por repase por medios de comunicación. Así, el (no) acceso a las herramientas tecnológicas, derivado o no por condiciones sociales, personales, económicas, políticas etc., hace con que se pueda establecer una mayor o menor sensación de miedo. Ella puede ser aumentada, también, por los medios de comunicación en masa, principalmente TV y periódicos, por la difusión de noticias de los riesgos en el área tecnológica.

Como observa Costa (2011, p. 229), las percepciones sobre la inseguridad consecuente, mismo la derivada del uso de Internet, y las dimensiones del miedo no son lineares, ya que, conforme explicitado, "as reações psicológicas e comportamentais são variáveis" y porque no decir inestables, pues pueden ser alteradas a cualquier nueva noticia sobre virus, caballos de Troya, ataques cibernéticos, guerra cibernética, violaciones de la privacidad/intimidad, etc.

Por otra parte, se podría afirmar que la fragmentación de los conocimientos, en especial el tecnológico y sobre Internet, hace con que en su paradoja, el no conocimiento, provoque sentimientos/sensaciones de inseguridad, proliferándose el miedo. De Giorgi (2013, entrevista), revela que el riesgo está en no tener conocimiento. Tal sensación de inseguridad sobresale en los llamados "delitos de intervenção", en que el tipo penal no presupone que la víctima participe en el comportamiento, bastando la acción unilateral del autor (SYDOW, 2013, p. 112).

Parameetrizando el tema, tratándose de las relaciones del riesgo con los sistemas, expone De Giorgi (1998) que mismo un disturbio de pequeña importancia puede traer consecuencias incontrolables, lo que ocurre no solamente en los sistemas sociales como también en las organizaciones de los sistemas complejos de la tecnología moderna (léase y compréndase, actualmente, el Internet). Es el riesgo, entonces, una acción evolutiva del tratamiento de las contingencias que, se excluye toda seguridad, excluye también todo destino. Él se diferencia (el riesgo, como modalidad de vínculo con el tiempo) del Derecho, pues éste fija "os pressupostos que permitem a orientação das proprias expectativas no futuro"; también se

diferencia de la economía, pues ella es la que determina las modalidades de acceso a los bienes (DE GIORGI, 1998, p. 198). Así, el riesgo torna evidente los límites con que se deparan estos sistemas referentes a la construcción de vínculos con el futuro, que se efectúa en el *médium* de la probabilidad/improbabilidad, teniendo este "médium" como referencia la incertidumbre, el no conocimiento y la fatalidad.

De Giorgi (1998, p. 198) también puntualiza que el riesgo es modalidad de distribución de "bads" y no de "godos", pues se basa "na suportabilidade, na aceitação e não na certeza das próprias expectativas". En razón de esto, los riesgos no pueden ser transformados en Derecho, mismo que puedan ser monetarizados. De lo contrario, la inserción de riesgo en Derecho causa su sobrecarga, con inserción de reglas normativas que, en verdad son apenas estrategias de retardamiento del riesgo y no de estrategias que evitan el riesgo. Por otra parte, es necesaria una continua repolitización de riesgos, mismo que sea, para la política, arriesgada tanto la situación que se decide como la que no se decide sobre los riesgos, pues en este caso se puede, inclusive, estar sobre la auto-evolución de los conocimientos en Internet, como la opción de criminalizar la conducta de creación de software capaz de ser utilizado para invadir dispositivo informático (Art. 154-A, Código Penal).

Por otra parte, también en Internet pueden/están siendo creados los llamados "grupos de risco", no solamente creados por la mídia – medios de comunicación en masa (COSTA, 2011, p. 236), como también por la propia Internet. Al igual que los espacios urbanos, el Internet también es segregativa, no apenas socialmente sino también culturalmente, donde los códigos binarios bello/feo, divertido/aburrido (cool/not cool), cierto/errado, acceso/no acceso, funcional/no funcional, por ejemplo, son constantes de auto-selección de sus usuarios (sistemas psíquicos), cada cual con sus criterios de valoración y concepción de verdad. Eso, por otro lado, puede ser una falla (de los usuarios de Internet) en la percepción y provocar un sentido diferente de lo real, de lo correcto, puesto que la sensación (concepción) de (supuesto) anonimato es una de las principales características del uso de la web, pudiendo tener consecuencias dañinas y no necesariamente generar la sensación de miedo, que hace con que se reconozca el riesgo. Es, una vez más, el no-conocimiento!

Concluyendo esta parte, hay que tener en mente que, usando no solamente los raciocinios de De Giorgi (1998) y Bauman (2006), como también de Costa (2011), que el simbolismo de eventual legislación penal aplicable a Internet no puede surtir el efecto necesario: generar seguridad o, al menos, proporcionar sensación de ésta. La contingencia jurídica, que deberá valerse/ser avaluado no solo del punto de vista social,

principalmente tecnológico-jurídico, no evitará el riesgo; pero será la respuesta de (sub)sistema político a la indeterminación o indeterminaciones en el campo de la tecnología (digital), modificando el Derecho. Son, por lo tanto, las influencias de un (sub)sistema en el otro, produciendo las alteraciones necesarias basadas en sus co-evoluciones (principalmente, Internet, Derecho y Política).

Por otro lado, nos preocupa también esa forma de reacción de sistema político en relación en las evoluciones de ritmo frenético de los otros subsistemas sociales, que puede causar el aumento de edición de normas penales en blanco, con tipos penales abiertos.

# 3.2 Los efectos de la cultura del miedo en Internet frente a La producción legislativa penal brasileña:

Muchas innovaciones, principalmente del área de informática y comunicaciones, ya son incluidas y comprendidas en nuestro ordenamiento jurídico (v.g., las directrices referente a la actuación en Comercio Electrónico, con el Código de Defensa del Consumidor, Ley 8.078/90, y su reglamentación, el Decreto 7.962/13). También, varios tipos penales ya previenen expresamente: la violación/adulteración de bancos de datos de la administración pública (arts. 313-A e 313-B, del Código Penal); la interceptación ilegal de datos telemáticos/informáticos (art. 10 de la Ley 9.296/96); el fraude o violación de sistemas de votación (art. 72 de la Ley 9.504/97 - Ley Electoral - y art. 266, §1°, del Código Penal, respectivamente) y protegen, penalmente, la libertad sexual, de niños y adolescentes (arts. 241-A y siguientes de la Ley 9.069/95 - Estatuto del Niño y del Adolescente). A pesar de esto, la mayoría de los tipos penales brasileños no son producto de la contemporaneidad y, por eso, no contemplan bienes jurídicos tales como la protección de informaciones y de datos, así como son preceptos descriptivos compuestos por elementos objetivos que no describen las conductas humanas asociadas a las prácticas realizadas en internet, o mediante recursos tecnológicos.

Es cierto que algunas áreas del Derecho, como las del consumidor y tributaria, *v.g.*, están sujetas a una adaptación/evolución más rápida en relación a la evolución de las tecnologías digitales. Por otro lado, la evolución tecnológica (digital) y su consecuente utilización en la práctica de delitos, ha traído al intérprete de las normas sancionadoras y restrictivas de la libertad a la ansiedad por intentar comprender el "que", el "como" y el "porque" de determinados elementos (tecno-digitales) innovadores.

Esa búsqueda puede escapar a la hermenéutica penal tradicional, por lo cual tipos penales creados antes de la evolución tecnológica actual

pueden quedar no comprendidos o hasta inaplicables, por la no comprensión del "aspecto tecnológico" usado/visado en la práctica delictiva. Eso se justifica porque, justamente, son conceptos no pertinentes al ramo/sistema del *Derecho* y sí a la *Tecnología* o, más específicamente, a Internet (ciberespacio).

El legislador brasileño, en muchos casos, se ha valido de su "poder de legislar" y utilizado en el cuerpo de la Ley o sus anexos un "Glosario" de términos y conceptos, que serían interpretativos del contexto de la norma. En otros casos, sin valerse de esa actitud, para algunos violadora del Principio de legalidad, traer conceptos inciertos o distantes de la unanimidad, principalmente los que se refieren a cuestiones técnicas, como, v.g., la llamada "Ley Carolina Dieckmann", Ley 12.737/12, que posee innúmeros elementos normativos de tipos penales que no contienen un concepto uniforme en el contexto técnico, además de poseer defectos en la redacción de la Norma.

En ambos casos, cabera al intérprete, sea doctrinador, sea juzgador – o, porque no, el aplicador de la Norma -, de acuerdo con la hermenéutica penal y contexto social y tecnológico actual, el enfrentamiento de la misión de, partiendo del hecho penal relevante y de la forma/medio como fue practicado, comprender los aspectos tecnológicos digitales y buscar alinear perfectamente la Ley a la quaestio facti. En el caso que no sea posible, no podrá valerse de la analogía. A la par de estos factores, tendrá también que considerar las principales características de la criminalidad informática, por Sydow interactividad, ponderadas (2013): la la movilidad (portabilidad), la sociabilidad, la conectividad, la mundialización, la fraccionalidad, la divisibilidad, la intangibilidad, la disponibilidad, la pluralidad, la ubicuidad (simultaneidad), el anonimato, y, la velocidad (de las conexiones)<sup>13</sup>.

# 4. Análisis sobre la Ley 12.735/13 ("Ley Carolina Dieckmann"):

Además del derecho a la libertad y la anterioridad de la Ley, innúmeros aspectos están envueltos cuando se trata de interpretación en Derecho Penal. La voluntad del legislador, en la época de la «construcción» legislativa, la interpretación dada por los doctrinadores y/o por los magistrados en casos concretos, son parámetros claros de los paradigmas de la hermenéutica penal. La propia evolución del contexto social ha arraigado debates y construcciones hermenéuticas importantes a la evolución del Derecho, en especial el Penal. Notablemente, los métodos

<sup>&</sup>lt;sup>13</sup> Sobre el asunto, ver Sydow (2013, p. 88-110).

clásicos ya no son más aplicables para auxiliar al intérprete, que debe abrirse a otros contextos del mundo globalizado y *tecnológico digital*.

No siempre la intención inicial del legislador, que estaría en Ost (1999) en la "memoria" del Derecho, sea la principal salida para la interpretación del tipo penal o tipos penales que él redactó, principalmente en vista de las innovaciones en el campo social y tecnológico.

El momento y factores que son relativos a la creación del proyecto de Ley, su motivación, sus encaminamientos, los debates que lo envolvieron hasta su aprobación, son válidos, principalmente, para la comprensión histórica de ella, pero ya no pueden auxiliar ni tener valor decisivo en la interpretación de los textos legales penales. Es a ella que Marques (1997, p. 208) se refiere como *«interpretación case auténtica»*.

Más eficaz, es aún la interpretación *auténtica*, que también parte del propio legislador, cuando él lo hace en el propio cuerpo de la Ley, teniéndose la interpretación contextual. A pesar de que, por el contexto de la evolución actual, esa interpretación, cuando existe, puede provocar la no aplicación de la Ley Penal al caso concreto y, cuando inexistente, puede provocar interpretaciones diversas referidas a la finalidad de vocablo o vocablos usados por el legislador.

Para ejemplificar, el art. 154-A, adicionado al Código Penal por la Ley 12.737/12, trajo innúmeros conceptos nuevos, no «explicados» por el legislador. Dice el texto legal:

Invadir *dispositivo informático* alheio, conectado ou não à rede de computadores, mediante violação indevida de *mecanismo de segurança* e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (destaques nossos).

Se destacó, en la citación del texto legal, dos conceptos: dispositivo informático y mecanismo de seguridad. Ninguno de ellos fue definido por el legislador y dejó a los intérpretes, léase aplicadores de la Ley Penal, la función de hacerlo. Pensar en dispositivo informático no lleva a imaginar un computador, un pen drive, un smartphone, etc. ¿Pero estaría el legislador también intentando proteger dispositivos y/o aplicativos que ruedan en la computación en nube en Internet? ¿El Facebook, como aplicación en la red mundial de computadores, estaría incluido? ¡No quedó claro ni evidente! Referente al mecanismo de seguridad, sería éste restricto a apenas algunas formas de protección, ¿o debería englobar todo mecanismo computacional, desde una seña o un antivirus hasta la tecnología más moderna de detección de intrusiones e invasiones?

Otras observaciones también podrían ser hechas en relación a las manifestaciones sociales a través de Internet, por los grupos de activistas, actuación denominada de *hacktivismo*, pues si esas acciones afectan sites y servidores de datos públicos, a través, por ejemplo, de ataques de negación de servicio(cuando el site y/o servicio queda fuera del aire) dependiendo del contexto y de «servicio» público ofrecido, si solamente de informaciones, conforme redacción del §1º del art. 266 del CP14, o de carácter esencial para la sociedad, conforme el art. 265 del CP<sup>15</sup>, podemos tener interpretaciones diferentes en cuanto al tipo penal adecuado. Por cuanto, el análisis debe ser pormenorizado y avaluado desde el punto de vista técnico para la adecuada adaptación al tipo penal previsto. Por otra parte, esa misma acción (ataque de negación de servicio), cuando es dirigida a particulares, principalmente empresas, tendrá otra adecuación penal, en vista de los tipos penales existentes en Brasil y su (in)evolución legislativa en el área o, hasta mismo, a ningún tipo penal corresponderá, principalmente si no es tangible el daño impuesto con la conducta dañosa.

#### **5 Conclusiones:**

Comprender el ciberespacio como un sistema autónomo, de vida propia, en el cual los usuarios forman apenas su entorno y ya no establecen los límites y el horizonte de comunicación, puede parecer – y para algunos parecerá – algo anacrónico, pues se desfocalizaría la atención de los sistemas psíquicos como aspecto central. Por otro lado, ayuda a comprender cómo demás sistemas interactúan e inter-penetran, usando (ciber)comunicación, influenciando y siendo influenciados. reproduciéndose y co-evolucionando. No se concibe más la existencia de los sistemas sociales (Derecho, Economía, Política) sin la cibercomunicación y, por eso, los mismos deben adaptarse y absorber las influencias de uno en el otro<sup>16</sup>.

El aspecto central del Internet como (sub)sistema está justamente en el almacenamiento de datos (una foto, un documento, un video, una aplicación, etc.), en *bits* y *bytes*, cuya interacción se da por los aplicativos

\_

<sup>&</sup>lt;sup>14</sup> Redacción del § 1° del art. 266 del CP: "quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento".

<sup>&</sup>lt;sup>15</sup> Dispone el art. 265 del CP: "Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública".

<sup>&</sup>lt;sup>16</sup> El Internet brasileño, después de largo debate iniciado por el Ministerio de Justicia, tuvo su «Marco Civil» aprobado por el legislativo brasileño y sancionado por el ejecutivo. La Ley 12.965/14 es un demostrativo de la interacción/irritación entre los sistemas sociales.

(visualizador de fotos, editor de texto, reproductor de videos, redes sociales, respectivamente, de acuerdo con los ejemplos anteriores), pues estos serán los *medios*, los instrumentos, las herramientas utilizadas por los usuarios para operar en su entorno y realizar la comunicación, con intercambio de datos e informaciones. En ese proceso, por el uso de las aplicaciones, en especial las de red y las específicas de los medios de comunicación en masa (periódicos, TVs, midia online, etc.), es que surge y se agrega a la cultura del miedo, la sensación de inseguridad y de incertidumbres, que hace con que los usuarios tiendan a exigir mayor atención de otros sistemas, como el político (en la elaboración de nuevas leyes, previniendo los riesgos) y el de Derecho («reparando» los riesgos creados por los usuarios y por el propio subsistema de Internet).

Por lo tanto, a respecto del recorte específico de este análisis – cibercriminalidad, como a la producción y interpretación del Derecho Penal –, la (re)interpretación y el (re)análisis y, por qué no, a (re)creación de tipos penales ya con base en la «esencia tecnológica» es importante en varios aspectos, entre los cuales: claridad de la Norma; actualidad de la Norma Penal en vista del tiempo y de la evolución; anterioridad A PRIORI de la Ley Penal; preservación de derechos y garantías fundamentales, o sea, respecto a los principios constitucionales; y, finalmente, contribuiría para una cultura de seguridad (no-miedo).

El mejor ejemplo de esa *quaestio* es la modificación/inclusión de dispositivos en el Estatuto del Niño y del Adolescente en 2008<sup>17</sup>. Existía la duda, en los tribunales, con respecto a la aplicabilidad de la antigua redacción para las comunicaciones hechas vía internet y, sabiamente, los tribunales acabaron por adoptar el entendimiento de que, sí, el reo cometía el crimen cuando hacia la divulgación y/o transmisión de fotos y videos de escenas de sexo con niños y adolescentes. La nueva redacción vino aclarada y con interpretación auténtica, ya señalando lo que entiende por «escena de sexo explícito o pornográfica»:

Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais (Incluído pela Lei nº 11.829, de 2008).

\_

<sup>&</sup>lt;sup>17</sup> La Ley nº 11.829, de 2008, modificó la redacción de la Ley 8.609/90 y acrescentó nuevos tipos penales (arts. 241-A a 241-E).

A pesar de esto, otros dispositivos penales aún no fueron actualizados y pueden generar un análisis interpretativo complexo y divergente, frente a las cuestiones técnicas del área tecnológico-cibernética. Como ser, *e.g.*, el art. 202 del Código Penal, bajo el Título IV (DE LOS CRÍMENES CONTRA LA ORGANIZACIÓN DEL TRABAJO):

Invasão de estabelecimento industrial, comercial ou agrícola. Sabotagem.

Art. 202 - Invadir ou ocupar estabelecimento industrial, comercial ou agrícola, com o intuito de impedir ou embaraçar o curso normal do trabalho, ou com o mesmo fim danificar o estabelecimento ou as coisas nele existentes ou delas dispor:

Pena - reclusão, de um a três anos, e multa.

La comprensión lógica, actual, para la mayoría de los brasileños que usan Internet es que el concepto de «establecimiento comercial» es perfectamente creíble y usual en el contexto digital, o sea, la existencia de Comercio Electrónico o e-commerce y su utilización por los usuarios de Internet. Las dificultades quedan a cargo de los conceptos de «invadir» u «ocupar» el «establecimiento comercial», «digital» o «electrónico». Así, como forma de conducta humana, alguien con conocimiento técnico necesario, puede generar un ataque DoS<sup>18</sup> o DDoS<sup>19</sup>, contra el site de Comercio Electrónico, generando su indisponibilidad de acceso a terceros e impidiendo que los responsables por el site y sus empleados puedan recibir encomiendas, empaquetar productos y enviarlos a los compradores<sup>20</sup>. El contexto del ataque debe ser comprendido para la correcta interpretación y aplicación del tipo penal en cuestión, ya que él no genera una «invasión» (no hay violencia), pero una «ocupación» de todo el servicio del site de Comercio Electrónico, que queda impedido de realizar el comercio (electrónico), o sea, queda indisponible en virtud de la ocupación de todos los espacios (caminos) para llegar hasta el sitio electrónico de la empresa.

El alcance de esta Norma es la protección a las organizaciones de trabajo y de los trabajadores, que también quedan afectados con la «acción» de atacar el site, retirándolo del acceso público e impidiendo ventas. Por lo tanto, la aplicación, de tipo penal, pasa desde el análisis de la

<sup>&</sup>lt;sup>18</sup> Denial of Service – Ataque de Negación del Servicio.

<sup>&</sup>lt;sup>19</sup> Distributed Denial of Service – Ataque de Negación del Servicio Distribuido.

<sup>&</sup>lt;sup>20</sup> Según Jorge y Wendt (2013, p. 240-1), "o ataque DDoS ou de negação de serviço é uma modalidade de *ciberataque* que se caracteriza pelo envio simultâneo de requisições de serviços para um determinado recurso de um servidor, por exemplo, um site. Em razão de não suportar essa quantidade de requisições, o recurso torna-se indisponível".

finalidad de la Norma hasta el medio utilizado y, por esto, no puede ser descartada la mera intención de causar daño (art. 163 del CP) y no de impedir el trabajo (art. 202 del CP). Por lo tanto, no significa que en interpretación judicial, en juzgamientos aislados, no se pueda dar exegesis diferente.

De otra forma, tanto Marques (1997) como Palazzo (1989) afirman la indudable relación entre el elemento político-social y la construcción hermenéutica de las Normas Penales. Palazzo (1989, p. 16) enfatiza la estrechísima relación e influencia de los «valores constitucionales» en el sistema penal, lo cual ocurre en el campo de las relaciones entre Política y Derecho Penal. A pesar de esto, también se refiere a que es una zona conflictiva.

En ese campo existe el gran y más evidente conflicto: de un lado, el individuo que practica una acción delictiva afrontará el bien o los bienes tutelados por el Estado; de otro lado, la sanción criminal impuesta por el Estado caracteriza la intervención máxima en la esfera individual, la de la libertad. Esa relación, necesaria y conflictiva, tiene sobre todo la preservación de la persona humana, entre otros aspectos, reglas y principios pertinentes y previstos constitucionalmente. De otro punto de vista, la creación de nuevos tipos penales debe ponderar la eventual violación de derechos y garantías fundamentales, como la de acceso a Internet, a la libertad de manifestación y, en el caso de la red mundial de computadores, la creación/producción de aplicaciones/sistemas capaces de auxiliar en el desenvolvimiento constante de la humanidad.

Esos límites constitucionales, garantidores – por así decir –, principalmente establecidos en las Constituciones modernas, son el contrapunto al peligro de la instrumentalización política del Derecho Penal, a la pena a cualquier costo. La hermenéutica constitucional frente a la legislación penal debe ser instrumento, especialmente, a la libertad individual contra las diversas agresiones, sea del Estado, o de particulares (PALAZZO, 1989). La regla, por lo tanto, debe ser la preservación de derechos y garantías fundamentales.

Palazzo (1989, p. 18), citando Woesner, hace referencia a "a legislação penal deve – por natureza – ser *lei de atuação* da Constituição, concretizando, necessariamente, uma relação entre indivíduo e autoridade, cujas linhas de fundo são traçadas na Constituição".

Así, tanto el análisis de los tipos penales ya existentes como la remodelación o creación de nuevos, deberán adecuarse y, en la selección de las conductas dañinas y que merecerán la atención del legislador para transformarse en delitos, respetar fundamentalmente los derechos y garantías de los usuarios de Internet, atentándose también para con la

naturaleza, peculiaridades y características propias de la sociedad digital, siempre en evolución y transformación, donde, según Castells (2003, p. 29), el "processo de aprendizagem pelo uso, e de produção pelo uso, é extraordinariamente abreviado". Existe, por lo tanto, la necesidad de un "constante reexame e transformação das normas penais para adequá-las ao contexto social presente e futuro" (LIRA, 2014, p. 83), sin que, por eso, pueda ese proceso ser utilizado como espectacularización del sistema político para responder a un deseo del sistema social, que espera resolver los problemas de la sensación de inseguridad y del miedo en tiempos de evolución de la tecnología digital.

#### Referencias

- BAUMAN, Zygmunt. **Tempos líquidos**. Rio de Janeiro: Zahar, 2007.
- \_\_\_\_\_. **Medo Líquido**. Rio de Janeiro: Zahar, 2008.
- BORGES, Maria Alice Guimarães. A. G. A compreensão da Sociedade da Informação. Ciência da Informação, v. 29, p. 25-32, 2000.
- BRASIL. Lei 8.069, de 13 de julho de 1990. **Portal da Legislação**. Disponível em: <a href="http://www.planalto.gov.br/ccivil\_03/leis/18069.htm">http://www.planalto.gov.br/ccivil\_03/leis/18069.htm</a>. Acesso em: 31 jul. 2014.
- BRASIL. Código Penal. **Portal da Legislação**. Disponível em: <a href="http://www.planalto.gov.br/ccivil\_03/Decreto-lei/Del2848.htm">http://www.planalto.gov.br/ccivil\_03/Decreto-lei/Del2848.htm</a>. Acesso em: 31 jul. 2014.
- BRASIL. Lei 12.737, de 30 de novembro de 2012. **Portal da Legislação**. Disponível em: <a href="http://www.planalto.gov.br/ccivil\_03/\_ato2011-2014/2012/lei/l12737.htm">http://www.planalto.gov.br/ccivil\_03/\_ato2011-2014/2012/lei/l12737.htm</a>. Acesso em: 31 jul. 2014.
- CASTELLS, Manuel. A Galáxia da Internet. Rio de Janeiro: Zahar, 2003.
- CABETTE, Eduardo Luís Santos. **O novo crime de invasão de dispositivo informático**. Disponível em: <a href="http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico">http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico</a>>. Acesso em: 15 maio 2013.
- COLÔMBIA. Ley 1273 de 2009 (Enero 05). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Disponível em:

- <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3449">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3449</a></a>>. Acesso em: 15 jul. 2014.
- COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa TIC Domicílios 2013.** Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação no Brasil. Disponível em: < http://cetic.br/publicacoes/2013/tic-domicilios-2013.pdf>. Acesso em: 15 jul. 2014.
- COSTA, Renata Almeida. Cultura do medo e espaço urbano: um olhar reflexivo sobre a sensação social de insegurança. In: Albert Noguera Fernández; Germano Schwartz. (Org.). Cultura e identidade em tempo de transformações: reflexões a partir da teoria do Direito e da Sociologia. 1 ed. Curitiba: Juruá, 2011, v. 1, p. 219-239.
- CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.
- \_\_\_\_\_\_. O Direito da Tecnologia da Informação: noções essenciais. In: **Âmbito Jurídico, Rio Grande, XIII**, n. 79, Ago. 2010. Disponível em: <a href="http://www.ambito-juridico.com.br/site/index.php?n\_link=revista\_artigos\_leitura&artigo\_id=7974">http://www.ambito-juridico.com.br/site/index.php?n\_link=revista\_artigos\_leitura&artigo\_id=7974</a>>. Acesso em: 18 Nov. 2013.
- \_\_\_\_\_. **Os crimes digitais e as Leis 12.735/2012 e 12.737/2012**. Boletim IBCCRIM Ano 21 nº 244 Março 2013.
- DE GIORGI, Raffaele. **Direito, Democracia e Risco.** Vínculos com o futuro. Porto Alegre: SAFE, 1998.
- GLOECKNER, Ricardo Jacobsen. Funcionalismo jurídico-penal e a teoria dos sistemas sociais: um diálogo frustrado. In: SCHWARTZ, Germano Deoderlein. (Org.). **Juridicização das Esferas Sociais e Fragmentação do Direito na Sociedade Contemporânea**. Porto Alegre: Livraria do Advogado, 2011, v. 1, p. 241-285.
- GUIBENTIF, Pierre. Os direitos subjetivos na teoria dos sistemas de Niklas Luhmann. In: SCHWARTZ, Germano Deoderlein. (Org.). **Juridicização das Esferas Sociais e Fragmentação do Direito na Sociedade Contemporânea.** Porto Alegre: Livraria do Advogado, 2011, v. 1, p. 171-198.
- JORGE, Higor Vinícius Nogueira; WENDT, Emerson. **Crimes Cibernéticos**. Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro: Ed. Brasport, 2013.

- LÉVY, Pierre. **As tecnologias da Inteligência.** O futuro do pensamento na era da informática. Rio de Janeiro: Ed. 34, 1993.
- LIRA, Cláudio Rogério Sousa. **Direito Penal na Pós-Modernidade.** A Racionalidade Legislativa para uma sociedade de Risco. Curitiba: Juruá, 2014.
- LUHMANN, Niklas. **Sociologia do Direito II**. Rio de Janeiro: Tempo Brasileiro, 1983.
- \_\_\_\_\_. **A realidade dos meios de comunicação**. 2. ed. São Paulo: Paulus, 2011.
- LYRA, José Francisco Dias da Costa. A moderna sociedade do risco e o uso político do controle penal ou a *Alopoiesis* do Direito Penal. In: Mauro José Gaglietti e Florisbal de Souza Del'Olmo. (Org.). **Diálogo** e **Entendimento**. Rio de Janeiro: GZ Forense Editora, 2011, v. 3, p. 91-118.
- MACHADO, Marta Rodrigues de Assis. **Sociedade do Risco e Direito Penal.** Uma avaliação de novas tendências político-criminais. São Paulo: IBCCRIM, 2005.
- GIORGI, Raffaele de Sociólogo e filósofo italiano. Entrevista ao Programa de TV Mãos e Mentes, Porto Alegre: TV Com/RS/RBS TV, 20 de janeiro de 2013.
- MARQUES, José Frederico. **Tratado de Direito Penal**. Edição Revista, Atualizada e Amplamente Reformulada por Antônio Cláudio Mariz de Oliveira, Guilherme de Souza Nucci e Sérgio Eduardo Mendonça de Alvarenga. Campinas: Bookseller, 1997.
- OST, François. **O tempo do direito**. Traduzido por Maria Fernanda Oliveira. Lisboa: Instituto Piaget, 1999.
- PALAZZO, Francesco C. Valores Constitucionais e Direito Penal. Tradução Gérson Pereira dos Santos. Porto Alegre: Sérgio Antônio Fabris Editor, 1989.
- PANNARALE, Luigi. **Il diritto e le aspetattive**. Bari: Scientifiche Italiane, 1988.
- PASTANA, Débora Regina. **Cultura do Medo.** Reflexões sobre violência criminal, controle social e cidadania no Brasil. São Paulo: IBCCRIM, 2003.

- ROCHA, Leonel Severo. "A construção do tempo pelo direito". **Anuário do Programa de Pós-graduação em Direito**. Mestrado e Doutorado. São Leopoldo: EdUnisinos, 2003, p. 309-20.
- ROZA, Fabrízio. **Crimes de Informática**. Campinas: Ed. Bookseller, 2002.
- SANTOS, André Leonardo Copetti; OLIVEIRA JR, Paulo Eduardo Duarte. O favelado/diferente como inimigo: a seletividade criminalizante e o papel da mídia na difusão do medo como estratégia de controle social. In: Mauro José Gaglietti e Florisbal de Souza Del'Olmo. (Org.). **Diálogo e Entendimento**. Rio de Janeiro: GZ Forense Editora, 2011, v. 3, p. 47-65.
- STOCKINGER, Gottfried. **A sociedade da comunicação:** o contributo de Niklas Luhmann. Rio de Janeiro: Papel Virtual, 2003.
- SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. Coordenadores Alice Bianchini, Ivan Luís Marques e Luiz Flávio Gomes. São Paulo: Saraiva, 2013.
- TEUBNER, Gunther. **Direito, sistema e policontexturalidade**. Piracicaba: Unimep, 2005.
- VIEIRA, Vanderson Roberto; ROBALDO, José Carlos de Oliveira. A sociedade do risco e a dogmática penal. In: Âmbito Jurídico, Rio Grande, X, n. 38, fev 2007. Disponível em: <a href="http://www.ambito-juridico.com.br/site/index.php?n\_link=revista\_artigos\_leitura&artigo\_id=3593">http://www.ambito-juridico.com.br/site/index.php?n\_link=revista\_artigos\_leitura&artigo\_id=3593</a>. Acesso em: jul. 2014.