Derecho Penal y ciberdelitos.
Breves aproximaciones dogmáticas.

Prof. Dr. Fabio Roberto D'Avila, PUCRS, Brasil[1]
Daniel Leonhardt dos Santos, PUCRS, Brasil[2]

Resumen: Nuestro tiempo no tiene una sola apariencia. Si por un lado es verdad que la informática está muy lejos de hacerse cargo de transformaciones tan numerosas y tan profundas, por el otro no se puede negar que haya cambiado radicalmente la manera como la humanidad se relaciona con el mundo y con el tiempo. La informática hizo con que el tiempo se volviera instantáneo, al paso que comprimió las nociones de espacio. Las comunicaciones ya no encuentran más fronteras físicas, y la velocidad guía a las relaciones humanas. A esta nueva y tan intensa dimensión relacional corresponden nuevos conflictos, que, a su vez, también recurren al Derecho Penal. De hecho, algunos de esos delitos ya son conocidos y regulados por la ley, una vez que ya existían y sólo encontraron en la informática un nuevo ambiente y nuevas formas de realización. Sin embargo, también hay nuevos delitos, dotados con nuevas características que traen dificultades no sólo para la definición de los términos de criminalidad, como incluso para la identificación de los valores protegidos por la norma. Dadas las condiciones todavía incipientes del derecho positivo, así como las condiciones locales de cada sistema jurídico, buscamos considerar algunos problemas comunes y particularmente sensibles a nuestras tradiciones jurídico penales, con referencia a las propuestas de la Convención de Budapest y la Decisión marco 2005/222/JAI del Consejo, pero sin dejar de lado el derecho positivo español y el brasileño.

Palabras clave: Derecho Penal; ciberdelitos; aplicación de la ley en el espacio; bien jurídico; ofensividad.

1. Nuestro tiempo y nuestro mundo.

"Todo el mundo es compuesto de mudanza", diría el gran poeta portugués Luís de Camões en su memorable obra *Sonetos*. No hay ninguna duda acerca de esto, sin embargo, hacer buen provecho de estos cambios a fin de darles características específicas, un exacto rostro frente al tiempo que vivimos, es una tarea notablemente difícil, si no imposible. Tanto sea porque para aquellos que viven mientras ocurren las mudanzas, los cambios

[1] Profesor Titular de Derecho Penal de la Universidad Católica de Rio Grande do Sul (PUCRS).
[2] Estudiante de doctorado del Programa de Posgrado en Ciencias Penales de la Universidad Católica de Rio Grande do Sul (PUCRS).

suelen mostrarse amorfos, – o por lo menos turbios, disfrazados en medio al constante flujo de la vida y su aparente normalidad – sea porque – tratándose justamente de los días actuales – ella toma, como nunca antes, un rostro multiforme, dotado de un caleidoscopio de aspectos verdaderamente intensos y no menos importantes. Así se da la coexistencia de tan variadas denominaciones: desde la "*sociedad del riesgo*", de Ulrich Beck,[3] a la "*civilización del espectáculo*" de Mario Vargas Llosa,[4] pasando por designaciones como "*sociedad de consumo*" o "*sociedad de la información*", y todavía por otras mucho más comprensibles y por eso consecuentemente multiformes, como *pos-modernidad, modernidad tardía* o *hipermodernidad*.[5]

En este contexto, defender la existencia de una *sociedad informática* no sería algo nuevo, tampoco raro. En los años 80, Adam Schaff[6] ya hacía uso de tal designación. Pero tomar solo un fragmento de algo como si eso fuera el "todo", es dejar escapar lo esencial. Esencial que se revela justamente por su complejidad y multiplicidad de formas, que no pueden ser aprehendidas ni aprisionadas en un único rostro. Nuestro tiempo definitivamente no tiene una sola apariencia, y eso de manera ninguna surge como un impedimento para que se siga con la tarea de constantemente vigilar[7] a las numerosas manifestaciones y frutos que resultan de eso, si no que sirve como un estímulo. Es justamente bajo esta perspectiva que se desarrollan las reflexiones presentes en este breve escrito.

Si por un lado es verdad que la informática está muy lejos de hacerse cargo de transformaciones tan numerosas y tan profundas, por el otro no se puede negar que haya cambiado radicalmente la manera como la humanidad se relaciona con el mundo y con el tiempo. La informática hizo con que el tiempo se volviera instantáneo, al paso que comprimió las nociones de espacio. Las comunicaciones ya no encuentran más fronteras físicas, y la velocidad guía a las relaciones humanas. Gracias al internet y a los smartphones, el hombre descubre una nueva forma relacional. Datos personales, bancarios, comerciales, y judiciales pasan a ser almacenados en la red; la economía y el mercado de capitales se hicieron tan virtuales a punto de que se cuestione el futuro del papel moneda; relaciones afectivas, amistades y también las relaciones de trabajo migran en gran medida a este nuevo mundo virtual. Nada parece escapar a la informática ni a la red mundial de computadoras.

Según la lógica, a esta nueva y tan intensa dimensión relacional corresponden nuevos conflictos, que, a su vez, también recurren al Derecho Penal. De hecho, algunos de esos delitos ya son conocidos y regulados por la ley, una vez que ya existían y sólo encontraron en la informática un nuevo ambiente y nuevas formas de realización. Sin embargo, también hay nuevos delitos, dotados con nuevas características que traen dificultades no sólo para la definición de los términos de criminalidad, como incluso para la identificación de los valores protegidos por la norma. Es por medio de dificultades como estas que surgen importantes problemas en la dogmática penal.

---

[3] BECK, Ulrich. *Risikogesellschaft.* Auf dem Weg in eine andere Moderne, Frankfurt am Main: Suhrkamp, 1986.

[4] VARGAS LLOSA, Mario. A civilização do espetáculo. Uma radiologia do nosso tempo e da nossa cultura. Trad. Ivone Benedetti, Rio de Janeiro: Objetiva, 2013.

[5] LIPOVETSKY, Gilles. *Os tempos hipermodernos*. Trad. Mário Vilela. São Paulo: Barcarolla, 2004.

[6] SCHAFF, Adam. *A sociedade informática*. As consequências sociais da segunda revolução industrial. Trad. Carlos Eduardo Jordão Machado e Luiz Arturo Obojes, 4.ª ed., São Paulo: Ed. UNESP, 1995.

[7] STEIN, Ernildo. *Uma breve introdução à filosofia*, Ijuí: Ed. UNIJUÍ, 2002, p. 22.

Ya podemos adelantar que, sin embargo, no se trata de un "nuevo" derecho penal, sino que solamente del normal progreso de la ley penal en un nuevo ambiente, marcado, *in casu*, por una complejidad especial y por particularidades relativas al *medio* de la informática.[8] Aunque haya diferencias importantes entre los conflictos denominados como ciberdelitos, no restan dudas de que existen fuertes líneas que los conectan, no apenas haciendo con que sea posible estudiarlos, sino que en realidad recomendando que sean estudiados de manera conjunta. Algunos de estos elementos son aquí objeto de nuestra atención: inicialmente, teniendo en cuenta sus especificidades, consideraremos algunos aspectos de la aplicación de la ley penal en los diferentes medios. En un segundo momento, propondremos una breve reflexión sobre el contenido del injusto en los delitos informáticos.

Dadas las condiciones todavía incipientes del derecho positivo, así como las condiciones locales de cada sistema jurídico, buscamos considerar algunos problemas comunes y particularmente sensibles a nuestras tradiciones jurídico penales, con referencia a las propuestas de la Convención de Budapest y la Decisión marco 2005/222/JAI del Consejo, pero sin dejar de lado el derecho positivo español y el brasileño.

2. La instantaneidad del tiempo y la compresión del espacio. El problema de la aplicación de la ley en el espacio.

Decíamos antes que la instantaneidad del tiempo y la compresión del espacio son marcas profundas de la delincuencia informática. En este exacto ámbito, una conducta delictuosa, *v.g.,* fragmentada en más de un país en Asia puede, a través del Internet, producir efectos en varios países europeos en el mismo momento en que se practica la conducta. Las tradicionales nociones de lugar y espacio ya no encuentran aquí aplicación apropiada, y conceptos fundamentales de territorio y soberanía se ven profundamente fragilizados.

En un primer momento, se podría pensar que, al igual que en muchos otros casos, como el narcotráfico, solamente se trata de un crimen potencialmente transnacional. Sin embargo, tras un análisis más atento, es posible darse cuenta de que, en el campo de los ciberdelitos, esas conductas se proyectan de manera totalmente única en cuestión de tiempo y espacio. Aquí estas nociones son verdaderamente redimensionadas y reconfiguradas, trayendo grandes repercusiones dogmáticas y político-criminales.[9]

Inicialmente, merecen destaque las fragilidades del derecho penal limitado al Estado-Nación. Una política criminal estrictamente nacional tiene poco que decir en respuesta a una criminalidad de ese tipo. Los esfuerzos político-criminales deben convertirse, obligatoriamente en esfuerzos de cooperación internacional, alineados por directrices para que puedan alcanzar a una deseada *política penal común*. Esto acaba por inserirla perfectamente dentro de las perspectivas del mundo globalizado y sus paradojos. Perspectiva esa donde, como destaca Faria Costa, fenómenos criminales exuberantemente globales se abordan con los limitados mecanismos nacionales, proporcionando "la

[8] FARIA COSTA, José Francisco de. *Direito penal da comunicação*: alguns escritos. Coimbra: Coimbra Editora, 1998, p. 119.
[9] FARIA COSTA, José Francisco de. *Direito penal e globalização*: reflexões não locais e pouco globais. Coimbra: Coimbra Editora, 2010, p. 17.

sensación de cierta paralización en las acciones de defensa contra el crimen".[10] Así surgen tanto la voluntad como la necesidad de que el derecho penal, a pesar de su tradicional y a veces inherente vocación *local,* se haga también *global*.

En ese contexto, el primer desafío es eliminar cualquier isla de impunidad, generalmente derivada de la falta de regulación o del fracaso de las leyes penales y procesuales ya existentes. Es con razón que la Convención de Budapest ha dedicado un gran esfuerzo para conseguir una armonización mínima de la legislación aplicable.[11] Como era de esperar, el texto convencional dedica, por un lado, un amplio espacio para la identificación y descripción de conductas criminales, dotadas de suficiente consenso. Por otro, también avanzan importantes disposiciones penales y procesuales penales relacionados, principalmente al resguardo de los elementos necesarios para la materialidad del delito, la competencia, la cooperación y la asistencia mutua.[12] Es preciso reconocer que, con la intención de evitar la impunidad, el ideal sería obtener una unificación reguladora y eficaz. Tal afirmación, sin embargo, como observa bien Marcelo Riquert, "aparece como una suerte de aspiración de imposible alcance – utópica en escala global, muy difícil a nivel regional".[13] El logro de la armonización mínima de las normas se muestra, pues, como el mejor de los caminos.

Una cuestión merece atención especial: el problema de la competencia.

No hay duda de que la armonización legislativa deseada permitiría un paso importante en el camino de evitar *conflictos negativos de competencia* a través de directrices comunes direccionadas a la aplicación de la ley penal en ese ámbito.[14] Con respecto a, p. ej., el principio de territorialidad, verdadero principio de los principios en el ámbito de la aplicación de la ley penal en el medio informático, se puede decir que la adopción de un amplio criterio de competencia territorial, iluminado por el principio de ubicuidad, sería suficiente para por lo menos cubrir casos en que el delito informático tocó de alguna manera el territorio nacional, despertando así su interés directo.[15]

---

[10] FARIA COSTA, José Francisco de. *Direito penal e globalização*: reflexões não locais e pouco globais. Coimbra: Coimbra Editora, 2010, p. 46 (traducción libre).

[11] Intento de armonización normativa necesaria para evitar la impunidad. (RIQUERT, Marcelo A. Repensando cómo funciona la ley penal en el ciberespacio. In: *Ciberdelitos*. Marcelo A. Riquert (org.), Buenos Aires: Hammurabi, 2014, p. 23). Esto fue reconocido por el Consejo de la Unión Europea en la Decisión-Cuadro 2005/222/JAI, de 24 de febrero de 2005, al exponer que: "Las considerables lagunas y diferencias entre las legislaciones de los Estados-Miembros, en este dominio, pueden obstar la lucha contra el crimen organizado y el terrorismo, además de que también pueden dificultar que haya una cooperación policial y judiciaria eficaz en el ámbito de ataques contra los sistemas de información. La naturaleza transnacional y sin límites de los sistemas de información modernos hace con que los ataques contra estos sistemas frecuentemente tengan una dimensión que ultrapasa esos límites, de manera que se torna evidente la urgente necesidad de seguir adelante con la armonización de las legislaciones penales en ese dominio." (CONSELHO DA UNIÃO EUROPEIA. Decisão-Quadro 2005/222/JAI de 24 de fevereiro de 2005. *Relativa a ataques contra os sistemas de informação*. Bruxelas: Jornal Oficial da União Europeia, 24 de fevereiro de 2005)

[12] CONSELHO DA UNIÃO EUROPEIA. Convenção de Budapeste, de 23 de novembro de 2001. *Convenção do Cibercrime*, Budapeste, 2001.

[13] RIQUERT, Marcelo A.. Repensando como funciona la ley penal en el ciberespacio. In: *Ciberdelitos*. Marcelo A. Riquert (org.), Buenos Aires: Hammurabi, 2014, p. 26.

[14] De esa manera, en la sección 3 da la Convención.

[15] En respeto a las teorías de delimitación del *locus commissi delicti*, se puede decir que la teoría pura de la ubicuidad es la menos vulnerable dentro de todas las teorías que intentan delimitar el lugar del crimen. Conforme enseñado por Hungria, la teoría "no exige transigencias de soberanía, y si no evita los conflictos positivos de la jurisdicción, elimina a los negativos, de manera a alejar al incómodo de una eventual

Con esta finalidad, sería necesario llevar en cuenta tanto el *lugar del hecho* como el lugar de acción, además de comprender las acciones participativas, como el lugar de los resultados, o todavía el lugar donde debería ocurrir el resultado. La legislación brasileña, por ejemplo, establece el lugar del crimen como el "lugar donde ocurrió la acción u omisión, como un todo o en parte, y donde se produce o se debe producir el resultado" (art. 6 CP brasileño). De manera similar, aunque no idéntica, el código penal alemán define el *lugar del hecho* como aquél en el que "el autor haya actuado o, en caso de comisión por omisión, en el que hubiera debido actuar, o en el que se produzca el resultado del tipo, que debería producirse conforme la representación mental del autor" (§ 9 I CP alemán). Con respecto a la legislación española, aunque no sea similar en términos de regulación,[16] generalmente también se interpreta de acuerdo con los parámetros del principio de ubicuidad.[17]

Sin embargo, no es infrecuente la ocurrencia de problemas dogmáticos de importante impacto en la práctica, lo que representa muy bien el caso de crímenes de peligro abstracto. Diferente de los delitos de daño o peligro real, para lo cual el resultado "daño" o "peligro" son indispensables al bien jurídico, los crímenes de peligro abstracto son mayoritariamente interpretados como delitos sin resultado (*erfolglos*). Por lo tanto, mientras que el principio de ubicuidad cubre sin problemas a los crímenes de daños y peligro, tanto en el lugar de la acción como en el lugar de su resultado, por otro lado, en los delitos de peligro abstracto se controvierte que el hecho de la competencia puede o no estar restringido a su lugar de acción, no cubriendo los lugares donde los efectos de la acción podrían proyectarse, ya que es consenso que esos efectos no constituyen un elemento de ese tipo. En términos más prácticos, esa situación podría hacer con que el Estado, atingido solamente por los efectos del crimen, se vea imposibilitado de aplicar sus leyes penales, dejando así lagunas de impunidad.

Este problema ha llamado la atención del penalista alemán Jörg Martin, dando lugar a un interesante estudio sobre la responsabilidad penal de los daños transfronterizos, *in casu*, bajo el punto de vista ambiental. La solución defendida por el consistía en también reconocer la existencia de resultados en los crímenes de peligro abstracto, constituyendo un riesgo para el bien jurídico, a ser evaluado por medio de un juicio *ex ante* bajo la perspectiva del autor.[18] De manera similar pero no coincidente, nosotros también hemos abogado por una lectura que considere a los crímenes de peligro abstracto como crímenes de resultado, sin embargo comprehendidos como una *posibilidad de daño al bien jurídico*, y verificados por un juicio *ex ante* de base total.[19] En los dos casos, el problema de competencia sería solucionado a través del reconocimiento de la existencia de un resultado en los crímenes de

---

impunidad del agente." Es justamente en este punto que la teoría se sobresale sobre las demás. (HUNGRIA, Nélson. *Comentários ao código penal*, volume I, tomo I: arts. 1º ao 10. 5ª ed. Rio de Janeiro: Forense, 1976, p. 162) (traducción libre).

[16] Vide art. 8.1 Codigo Civil e art. 23.1 LOPJ.

[17] PIFARRÉ DE MONER, María José. Spanien. Länderberichte. In: *Jurisdiktionskonflikte bei grenzüberschreitender Kriminalität*. Ein Rechtvergleich zum internationalen Strafrecht, Arndt Sinn (Hg.) Göttingen : V & R Unipress, 2012, p. 420 ss., 423.

[18] MARTIN, Jörg. *Strafbarkeit grenzüberschreitender Umweltbeeinträchtigungen*. Zugleich ein Beitrag zur Gefährdungsdogmatik und zum Umweltvölkerrecht, Freiburg i. B: Max-Planck-Institut, 1989, p. 83.

[19] D'AVILA, Fabio Roberto. *Ofensividade e crimes omissivos próprios*: contributo à compreensão do crime como ofensa ao bem jurídico. Coimbra: Coimbra Editora, 2005, p. 172.

peligro abstracto, también posibilitando la aplicación de la ley penal por parte del Estado exclusivamente afectado por los efectos de la actividad delincuente. Esta, por cierto, sólo es una posible forma de abordar este problema, cuyos desarrollos dogmáticos, por motivos obvios, lamentablemente no se pueden profundizar aquí.

Una vez resuelta la cuestión de los conflictos negativos de competencia – y por lo tanto de cualquier resquicio de impunidad –, por medio de un amplio ámbito de aplicación de las legislaciones nacionales surge otro problema: el conflicto positivo de la competencia y del *ne bis in ídem*.

El aumento de las competencias nacionales resulta en la coexistencia de diversos países interesados en juzgar un mismo delito informático. Este hecho requiere la inmediata adopción de criterios capaces de establecer reglas de preferencia, una vez que poner un hecho criminal bajo múltiples investigaciones y procesos judiciales coexistentes puede acarrear diversas órdenes de perjuicios en sus resultados, desde la recogida de pruebas y gastos innecesarios hasta el riesgo de una doble sentencia.

Conscientes de estas dificultades, dos modelos distintos tratan de proponer una solución. El primero, desarrollado por Arndt Sinn, defiende la adopción de criterios *vor der Tat*, es decir, la adopción de criterios previamente establecidos por la ley y que se aplican a todos los casos. En este sentido, Sinn propone que la preferencia en la aplicación del derecho penal sea definida a partir de un conjunto de reglas, por medio de las cuales algunos principios de aplicación de la ley penal se superponen a otros. Se daría prioridad al lugar de la práctica de la acción, seguido por el lugar que sufre el resultado, en el caso de la acción proyectarse a más de un país, y así por delante.[20] Bernd Hecker ofrece una segunda propuesta, en la cual el autor mezcla principios tradicionales y también primordiales en la aplicación de la ley penal (como el principio de la territorialidad, el principio de la personalidad activa y pasiva, etc.) con criterios materiales como, *v. g.*, el sitio con mayor daño, el interés de la víctima y el interés de los acusados, con el objetivo de tornar las cosas más concretas, y de esa forma determinar, caso por caso, a quien debe competir la preferencia.[21]

Las dos propuestas, ambas dotadas de ventajas y desventajas, corresponden a los modelos de resolución de conflictos de jurisdicción desarrollados por ZEIS (*Zentrum für Europäische und Internationale Strafrechtsstudien*) para crímenes transnacionales, entre estos, la delincuencia informática.[22] Sin embargo, a pesar de las dificultades habituales de aplicación, estas propuestas serían diseñadas fundamentalmente para la Unión Europea. Así que, aunque sean de enorme relevancia, esas propuestas todavía estarían lejos de hacerse cargo de la delincuencia informática a nivel global. Todo esto demostrando el nivel de complejidad y los desafíos que el enfrentamiento de este tipo de delito en particular puede traer en un futuro próximo.

---

[20] MODELLENTWÜRFE EINES REGELUNGSMECHANISMUS ZUR VERMEIDUNG VON JURISDIKTIONSKONFLIKTEN, in: *Jurisdiktionskonflikte bei grenzüberschreitender Kriminalität*. Ein Rechtvergleich zum internationalen Strafrecht, Arndt Sinn (Hg.) Göttingen : V & R Unipress, 2012, p. 585 ss.

[21] MODELLENTWÜRFE EINES REGELUNGSMECHANISMUS ZUR VERMEIDUNG VON JURISDIKTIONSKONFLIKTEN, in: *Jurisdiktionskonflikte bei grenzüberschreitender Kriminalität*. Ein Rechtvergleich zum internationalen Strafrecht, Arndt Sinn (Hg.) Göttingen : V & R Unipress, 2012, p. 581 s.

[22] MODELLENTWÜRFE EINES REGELUNGSMECHANISMUS ZUR VERMEIDUNG VON JURISDIKTIONSKONFLIKTEN, in: *Jurisdiktionskonflikte bei grenzüberschreitender Kriminalität*. Ein Rechtvergleich zum internationalen Strafrecht, Arndt Sinn (Hg.) Göttingen : V & R Unipress, 2012, p. 575 ss.

3. El injusto penal en los crímenes informáticos. Aspectos relativos al bien jurídico y a la ofensividad.

Los principales problemas del derecho penal en la sociedad contemporánea no son propiamente *cuantitativos*. No provienen ni de su expansión ni de su crecimiento en el ámbito de la regulación jurídico-penal, tampoco suceden gracias al simple hecho de que existe *más derecho penal*. El principal problema se encuentra, en realidad y en términos *cualitativos*, en la forma como ocurre esta nueva regulación.[23]

El espíritu de nuestro tiempo, todos sabemos, ha elevado las presunciones acerca de *eficiencia* y *seguridad* a la condición de valor supremo, de valor superior a todos los demás valores. Frente a esto, las libertades y las garantías penales, conquistadas por medio de mucho esfuerzo, hoy se ven no apenas debilitadas, como también muchas veces reprimidas, bajo el argumento de que para combatir al crimen es necesario optimizar las reivindicaciones político-criminales.[24] Es una especie de exaltación de la idea de seguridad que, de acuerdo con el contexto en que se proyecta, parece no conocer límites ni dogmáticos ni político-criminales, como se puede ver en el terrorismo.[25] Esto, evidentemente, no es admisible dentro de una ley penal democrática.[26] El derecho penal tiene la tarea intransferible de establecer límites para esa seguridad desmedida y, de esta forma reequilibrar la continua tensión entre la libertad y la seguridad. No por otro motivo, vivimos también en un tiempo en que la recuperación de la dimensión material del crimen asume un papel especialmente importante, tanto acerca de la delimitación del espacio en la legitimidad penal, cuanto a un entendimiento adecuado del injusto.

Aunque la teoría del crimen como una ofensa a los bienes jurídicos sea continuamente criticada, sobre todo bajo la llamada *Nebenstrafrecht*, tenemos la convicción de que todavía se hace indispensable como elemento para que se identifique y se comprehenda al contenido material del injusto, y de esa manera, también del ámbito del

---

[23] D'AVILA, Fabio Roberto. Liberdade e segurança em direito penal. O problema da expansão da intervenção penal. *Revista Síntese Direito Penal e Processual Penal*, v. 11, n. 71, dez./jan. 2012, Porto Alegre: IOB, p. 46). En un sentido similar, Nucci articula que la verificación del principio de la intervención mínima no significa necesariamente "la falta de criminalización de nuevas conductas que surgen a través de las relaciones sociales conforme avanzan los progresos tecnológicos. El Derecho Penal, como *ultima ratio*, tiene que estar presente en los casos que otros ramos del conocimiento jurídicos no lograron resolver. Se puede constatar que la tipificación de los delitos informáticos es indispensable, considerando el desarrollo notable de las computadoras en la vida de las personas y en la estructura administrativa del Estado." (NUCCI, Guilherme de Souza. Prefácio. In: SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013, p. 11) (traducción libre).

[24] Gonzalo Quintero Olivares hace una reflexión muy interesante acerca del tema y expone que "La tensión, pues, entre los afanes de control – sin entrar en su razón de ser – *y los derechos de los ciudadanos al plano ejercicio de sus derechos y libertades*, está en la escena del ciberespacio. Ni unos ni otros pueden tener legitimidad para todo lo que desean, y por eso se impone un equilibrio, *y es en ese equilibrio donde eventualmente se habrá de situar el derecho penal* que podrá criminalizar conductas porque en sí mismas son delictivas, *pero no porque el ciberespacio tenga la virtud de transformarlas en delictivas*. Es evidente que *no puede reconocerse ningún derecho subjetivo a hacer en el ciberespacio lo que no se puede hacer fuera de él*, al igual que es patente que la red puede multiplicar los efectos de las acciones delictivas" (QUINTERO OLIVARES, Gonzalo. Problemas de la perseguibilidad de los ciberdelitos. In: A. RIQUERT, Marcelo (Coord.). *Ciberdelitos*. Buenos Aires: Hammurabi, 2014, p. 175).

[25] Vide GRACIA MARTÍN, Luis. *O horizonte do finalismo e o direito penal do inimigo*. Trad. Luiz Regis Prado e Érika Mendes de Carvalho. São Paulo: Editora Revista dos Tribunais, 2007, p. 75-92

[26] MARINUCCI, Giorgio, DOLCINI, Emilio. *Corso di diritto penale*: le norme penali: fonti e limiti di applicabilità, il reato: nozione, estruttura e sistematica, vol. I. 3ª Ed. Milão: Giuffrè Editore, 2001, p. 451ss.

tipo. Esto no es todo. Esta teoría también es una fuerte expresión de un Modelo de Estado democrático, plural, multicultural, tolerante y establecido en los derechos y en las garantías fundamentales.[27] Son dos dimensiones de la misma idea que traen, cada una a su vez, desarrollos fundamentales.

El tipo penal, si lo comprehendemos bien, nada más es que la expresión legislativa de un ilícito que lo antecede, de una realidad no apenas negativamente valorada, pero también considerada sin valor, de tal forma que llega al punto de merecer la respuesta más dura por parte del Estado, la criminalización. Luego, si es así, hay que concluir que todo tipo es un tipo-de-ilícito, y que para que todos puedan ser definidos adecuadamente, es necesario que se pregunte acerca de los datos de realidad que le dan forma. La definición del alcance del tipo y de la materia de incriminación, dependen fundamentalmente de esto.

Cuando nos fijamos en los delitos informáticos nos damos cuenta de que, en parte, lo que se puede percibir es que estos delitos son viejos crímenes cometidos por un nuevo medio – el medio informático. Crímenes de honor hoy son practicados a través de las redes sociales, fraudes son cometidas por correo electrónico, además de delitos contra los derechos de autor, que ocurren cuando se disponen descargas no autorizadas de libros y música en el internet. Como señaló Faria Costa, se puede imaginar hasta mismo un homicidio por vía informática. Para tal, se propone la hipótesis de que eso podría ocurrir si alguien, a través de internet o incluso – agregamos nosotros – por medio del intranet de un determinado hospital, tuviera acceso a los dispositivos hospitalarios que mantienen una persona viva y los apagara, llevándola a la muerte.[28] Todavía en este sentido, es decir, en el sentido de viejos crímenes que ahora asumen nuevas características, la Convención de Budapest enlista el fraude informático, la falsedad informática, la pornografía infantil y medidas que violan los derechos de autor. Otros, como el propio homicidio, estarían encubiertos por la ley tradicional.

Como se ha señalado, el problema en eses casos no es tanto el contenido del injusto, pero si su forma de realización y los aspectos penales y de procedimiento que derivan de ello. Como dice un dicho, se trata de vino viejo en una nueva botella. Gracias a eso, a esta forma de delito le suelen llamar algunas veces de crímenes *impropiamente informáticos* o crímenes *relacionados con computadoras*.

Por otro lado, hay otro grupo de crímenes en que esa forma de conclusión no ocurre de manera tan inmediata, recibiendo, por parte de algunos, el nombre de crímenes *propiamente informáticos*. Ese tipo de delito en particular surge como la cosa *nueva* en la ley penal informática, es decir, una categoría de crímenes que fue efectivamente *abierta* por este nuevo marco, una vez que sólo podrían ser "practicadas a través de la informática".[29] Con

---

[27] En ese sentido, "un Estado que no desea ser liberticida, autoritario e intolerante, pero sí laico, plural y multicultural, erigido por las diferencias y comprometido con ellas, donde no haya espacio para que se persiga a nadie por su religión, color o clase, donde lo que se castigue no sean personas o grupos, solamente hechos. En resumen, un Estado donde todos, absolutamente todos, puedan valerse de su condición de ciudadano, e de esta forma, protegidos por la totalidad de derechos y garantías constitucionales, resistir a manifestaciones de autoritarismo inaceptables, que vez u otra, tanto por razones pragmáticas, cuanto por razones ideológicas, vuelven a surgir." (D'AVILA, Fabio Roberto. *Ofensividade em direito penal*: escritos sobre a teoria do crime como ofensa a bens jurídicos. Porto Alegre: Livraria do Advogado Editora, 2009, p. 68) (traducción libre).

[28] FARIA COSTA, José Francisco de. *Direito penal e globalização*: reflexões não locais e pouco globais. Coimbra: Coimbra Editora, 2010, p. 17.

[29] CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. Rio de Janeiro: Lumen Juris, 2001, p. 11; Cf. também, BARROS, Marco Antonio de, *et. al.* Crimes informáticos e a proposição

relación al Convenio de Budapest, se refieren a delitos de (I) acceso ilícito al sistema informático, (II) la interceptación ilegal de datos informáticos, (III) la interferencia con datos informáticos, (IV) la interferencia en el sistema informático y (V) uso abusivo del dispositivo informático. Eses delitos también aparecen fijados por la Decisión-marco 2005/222/JAI, en los artículos 2º (acceso ilegal a sistemas de información), 3º (interferencia ilegal en el sistema) y 4º (interferencia ilegal en datos).

El éxito o no de esa clasificación depende principalmente del contenido material del injusto, de aquello que pueda ser comprehendido como objeto bajo protección de las normas – algo que, en ese contexto, no es una tarea fácil. El hecho de que las conductas narradas corresponden a realidades específicamente informáticas, tales como el acceso al sistema informático o la interferencia en datos informáticos, acaban por nublar el bien jurídico tutelado por la norma penal y, por consecuencia, también el ámbito de incidencia del tipo. Por ejemplo, si recibiéramos al crimen de interferencia en datos informáticos (art. 4 de la Convención) como un delito de naturaleza exclusivamente patrimonial, similar al tradicional delito de daño, tendríamos que concluir que la conducta de "dañar, borrar, deteriorar, cambiar o eliminar datos informáticos" solo tiene relevancia penal cuando esos datos tienen valor económico, dejando aparte todo el resto, como datos personales o de carácter familiar (fotos, documentos personales, etc.).[30] No se trata solamente de eso. La indefinición del bien jurídico hace con que la identificación y el análisis de resultados sean inciertos, tornando inviable, p. ej., la implementación de requisitos usuales, como el de *daño grave* a delitos de interferencia de datos, previsto por el art. 4.2 de la Convención, o de *grave obstrucción* en el caso de delito de interferencia en los sistemas, previsto en el art. 5º de la Convención. A contra sensu, el reconocimiento de un posible *daño insignificante* u *obstrucción insignificante* incapaz de configurar el crimen es igualmente inviable, en función de la insignificancia de sus efectos.[31]

Las propuestas en esta área son las más variadas. Hay quien defienda la *seguridad informática* como bien jurídico, bajo el argumento de que "en la sociedad informatizada, la seguridad adentro del ciberespacio se convierte en un gran valor, siendo completamente

---

legislativa: considerações para uma reflexão preliminar. *Revista dos Tribunais*, vol. 865, p. 399, Nov. 2007; KERR, Vera Kaiser Sanches. *A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da internet*. Dissertação de Mestrado, São Paulo, 2011, p.19; VIANNA, Túlio Lima. *Fundamentos de direito penal informático*: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, p. 13; CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011, p. 63; COLLI, Maciel. *Cibercrimes*: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010, p. 42/44; VIANNA, Túlio; MACHADO, Felipe. *Crimes informáticos*. Belo Horizonte: Editora Fórum, 2013, p. 29; SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013, p. 55 e ss.

[30] En ese aspecto, hay aquellos que defienden que los bienes violados por un crimen informático no deben ser analizados considerando lo que representan economimicmente, solamente por su valor patrimonial, pero sí analizados conforme el valor que les es añadido por el individuo o por la sociedad empresarial que los utilizan. Para Barros, por ejemplo, el valor reside en la utilidad añadida al bien y en lo que representa, de manera general, en la vida de aquellos que usufructúan de él. (BARROS, Marco Antonio de, et. al. Crimes informáticos e a proposição legislativa: considerações para uma reflexão preliminar. *Revista dos Tribunais*, vol. 865, p. 399, Nov. 2007). Zanelatto, en el mismo sentido, expone que el valor de un bien informático es su utilidad inherente, de manera que no debe ser valorado solamente por aspectos económicos. (ZANELLATO, Marco Antonio. Condutas ilícitas na sociedade digital. *Revista de Direito do Consumidor*, vol. 44, p. 206, out. 2002).

[31] Ver el dispositivo del relatório.

merecedora de tutela jurídica",[32] como también hay quien sustente un concepto de "libertad informática", eso es, una idea de que los delitos informáticos serían delitos "característicos de las distintas libertades que pueden surgir por medio del uso de las tecnologías".[33] También hay aquellos que proponen que las nociones de i*nviolabilidad de la información automatizada* reconozcan a los datos informáticos como bienes jurídicos, de manera a incluir y proteger también a los programas de computadora, una vez que también son datos.[34] Y, siguiendo una línea similar, hay quien defina al bien jurídico como el *dato informático* y el *sistema informático*.[35]

Desde el principio es necesario considerar que la teoría moderna del crimen como un ataque al bien jurídico comprende al todo y no es compatible ni con bienes jurídicos fugaces ni con bienes de fronteras fluidas, como es el caso de la seguridad, y como se puede ver en los ejemplos mencionados anteriormente, también de la supuesta libertad informática.[36] Ese tipo de bienes defraudan a la capacidad crítica necesaria del bien jurídico-penal. También se puede levantar una objeción similar en contra de las propuestas de datos y sistemas informáticos. Por un lado, no parece que estos elementos puedan tener valor en sí mismos, sino que sólo en la medida de aquello que informan (para los datos) o que ofrecen (para el sistema). Por otro, considerar al propio dato y al sistema como bienes jurídicos sería como sacralizar a los elementos informáticos, permitiendo que cualquier tipo de contacto pueda constituirse en un crimen. Una constatación así no sólo perjudica la naturaleza crítica de la teoría, sino que también perjudica la graduación del delito por medio de los efectos que el ataque produce a los datos y al sistema.

Debido a eso, se ven mejores los intentos de identificar a los intereses legales a partir del *valor que expresan* o *resguardan* los elementos informáticos a los cuales recae la acción. Los datos informáticos y el sistema informático sin duda consisten en el *objeto de la acción,* y pueden corresponder simultáneamente al *objeto del bien jurídico – eso* es, a la materialización del valor que la norma busca resguardar – pero definitivamente no son un bien jurídico. Una carta de amor, una foto de familia o un video erótico producido por una pareja son datos palpables llenos de valor personal, y materializan valores como la intimidad, la privacidad y la libre disposición de la propia imagen. Esto no es diferente cuando se realiza a través de los datos informáticos en forma de una foto, un e-mail o de un vídeo digital, de manera que tanto el acceso indebido a eses datos cuanto su destrucción, daño o robo constituyen crímenes contra esos mismos valores personales, corporificados en estos datos.

En contrapartida, el resguardo de datos y sistemas informáticos de valor económico, como los datos o sistemas de una empresa, se encuadran mejor entre las nociones de delitos contra la propiedad. Ataques continuos a empresas virtuales, de manera que permanezcan inactivas por un par de horas o días, dan lugar a lo que se llama de *denegación de servicio* (denial of service - DoS), y caracterizan fundamentalmente una agresión de carácter patrimonial, que puede generar grandes pérdidas. Lo mismo parece ocurrir cuando

---

[32] BRITO, Auriney. *Direito penal informático*. São Paulo: Saraiva, 2013, p. 45 (traducción libre).

[33] SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013, p. 84 (traducción libre).

[34] VIANNA, Túlio; MACHADO, Felipe. *Crimes informáticos*. Belo Horizonte: Editora Fórum, 2013, p. 21.

[35] SANTOS, Daniel Leonhardt dos. *Crimes de informática e bem jurídico-penal:* contributo à ofensividade em direito penal. Dissertação de Mestrado, Porto Alegre, PUCRS, 2014, p. 90.

[36] En ese sentido, FARIA COSTA, José Francisco de. *Direito penal da comunicação*: alguns escritos. Coimbra: Coimbra Editora, 1998, p. 109.

el delito de acceso al sistema informático tiene como objetivo, *v. g.*, alcanzar un particular secreto comercial. Aun que haya un elemento de confidencialidad en juego, es el valor económico del secreto que se destaca.

Como consecuencia, el legislador español hizo bien en separar a los problemas de acceso al sistema, interceptación ilegal e interferencia en los datos por medio de títulos distintos, uno dedicado a la intimidad y a la imagen (art. 197), y otro dedicado a la propiedad (art. 264). Aunque se pueda cuestionar si eso comprende adecuadamente a todos los elementos de valor, no hay duda de cómo se define el objeto de tutela, permitiendo tanto la verificación de la infracción como la graduación del injusto. Sin embargo, no se puede decir lo mismo acerca de la Convención de Budapest. Es cierto que, al caracterizar de manera genérica a los delitos informáticos como infracciones contra la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos,[37] la Convención de Budapest llega a un amplio espectro de inclusión y garante mayor libertad de configuración a los países firmantes. Pero también es cierto que al hacerlo perdió una oportunidad única de guiar enteramente a las legislaciones nacionales, generando importantes repercusiones para la armonización legislativa en ámbito internacional.

Para nosotros, la Convención también se equivoca al avanzar en la criminalización de actos simplemente preparatorios. En su art. 6, intitulado de "uso abusivo de los dispositivos", es recomendado la criminalización de la fabricación y la venta de dispositivos maliciosos, es decir, direccionados a la práctica de delitos informáticos, así como la mera posesión de estos dispositivos. Se trata de actos preparatorios a delitos informáticos y, de esa manera, vacíos de lesión o peligro de lesión para el objeto tutelado por la norma. Sabiendo que existen muchos ejemplos similares en el tráfico de drogas y en el terrorismo, hay que llevar en cuenta que su recepción defrauda las exigencias de legitimidad material para ofensas a bienes jurídicos, de manera que el injusto penal equivale a una mera infracción de deber – línea ideológica propia de modelos de Estado autoritarios. Basta recordar el concepto de injusto defendido por la Escuela de Kiel durante el período nacionalsocialista.[38] Además, bajo una perspectiva de proporcionalidad, esos dispositivos enfrentan dificultades enormes,[39] una vez que crímenes mucho más graves, como el homicidio, no tienen un espectro punitivo tan largo.

Es posible encontrar otro exceso similar por parte de la Convención en lo que atañe a la penalización de la pornografía infantil en el medio informático. Nadie discute la dignidad y la necesidad de que haya protección penal para los niños contra la explotación sexual. En este sentido la Convención fue muy adecuada, en especial al considerar que el anonimato en el internet, asociado a los elementos espaciales de la delincuencia informática anteriormente citados, son grandes facilitadores para el mercado de pornografía infantil. El mayor problema se encuentra específicamente en hechos que son solamente simulaciones:

---

[37] Cap. II, Sección 1, Título 1 de la Convención.

[38] Ver MARINUCCI, Giorgio, DOLCINI, Emilio. *Corso di diritto penale*: le norme penali: fonti e limiti di applicabilità, il reato: nozione, estruttura e sistematica, vol. I. 3ª Ed. Milão: Giuffrè Editore, 2001, p. 439.

[39] La ley especial contra los delitos informáticos en Venezuela, por ejemplo, en su artículo 10, prevé, bajo una pena de tres a seis años de cárcel, el crimen de la fabricación, distribución o la venda de dispositivos destinados a eliminar o tornar más vulnerable a la seguridad de cualquier sistema que utilice tecnologías de la información. (VENEZUELA. Lei n. 48, 30 de octubre de 2001. *Lei especial contra los delitos informáticos*. Gaceta Oficial n. 37.313, 30 oct. 2001). Es una pena demasiadamente severa para un acto preparatorio. A título de comparación, en el mismo país la sentencia para el crimen del hurto es de seis meses hasta tres años de cárcel.

cuando se aprehende material pornográfico en que hay alguien que aparenta ser menor de edad cuando en realidad no lo es, o entonces cuando las imágenes parecen ser reales, pero no lo son, siendo editadas por medio de la computadora o producidas enteramente de esta forma (art. 9.º 2 Conv.).[40]

En ninguno de los dos casos hay un menor involucrado. El bien jurídico no es perjudicado ni expuesto al peligro, aunque todavía se vea dentro de los amplios límites de los crímenes de peligro abstracto. Lo que hay en este caso es la prohibición de una conducta inmoral que emana un *derecho penal de autor*, que consecuentemente no se puede encuadrar en el derecho penal democrático, una vez que simples inmoralidades, carentes de una peligrosidad objetiva mínima, no pueden ser objeto de criminalización.[41] El argumento defendido por el Reporte Explicativo de la Convención, de que la pedofilia simulada podría seducir e incentivar los niños a participaren en actos similares,[42] es un total equívoco. Si el objetivo es tornar crimen la seducción de niños, el comportamiento a ser criminalizado debe ser ese – la seducción – y no otro. Suponer efectos – que nada más son que suposiciones – no puede sustituir a la criminalización directa de lo que se quiere prohibir, principalmente cuando su descripción típica claramente se ve desconectada de la conducta (seducir) y de los efectos (riesgo de ser seducido) que se buscan evitar. Es necesario observar que en ningún momento ese dispositivo menciona esta supuesta pretensión final, mencionada solamente sólo en el Reporte Explicativo. Todo indica que, al fin y al cabo, de hecho, esta es una prohibición de orden puramente moral.

4. A título de conclusión:

"Vino viejo en una nueva botella" es un dicho que, aunque ilustre muy bien el tema de los delitos cibernéticos, por veces acaba por disminuir el impacto que su regulación y expresión concreta pueden producir en elementos tradicionales de la dogmática penal.

La informática trae consigo una reformulación de las perspectivas de tiempo y espacio tradicionales, reivindicando una nueva mirada acerca de la aplicación de las reglas de competencia del derecho penal y su coexistencia internacional. Reglas que acaban por cuestionar incluso la manera como se comprehenden usualmente las figuras dogmáticas, como los crímenes de peligro abstracto. Por otro lado, el rescate de la dimensión material del crimen, muchas veces descuidada en tiempos como los nuestros – donde se exaltan las ideas de seguridad y eficiencia –, es esencial para que sea posible reequilibrar la tensión continua que hay entre libertad y seguridad. La teoría del crimen como ofensa al bien jurídico, a pesar de las críticas específicas acerca del *Nebenstrafrecht*, sigue siendo absolutamente indispensable como elemento para que se identifique y comprehenda el contenido material del injusto y, por lo tanto, también del tipo de los ciberdelitos.

---

[40] De manera similar, en Brasil el Estatuto da Criança e do Adolescente, en su artículo 241-C, criminaliza la conducta de simulación de niños o adolescentes en sexo explícito o pornográfico, sea por medio de adulteración, montaje o edición fotográfica, de video o de cualquier otra forma de representación visual. Para constituir al tipo penal no es necesaria la práctica de cualquiera de las conductas descritas por parte del niño o del adolescente, una vez que la utilización de su imagen, de forma simulada o adulterada, es suficiente.

[41] FIGUEIREDO DIAS, Jorge de. *Direito penal*: parte geral: tomo I: questões fundamentais. 2ª Ed. Portugal: Coimbra Editora, 2007, p. 111-112.

[42] COE, Introducción, n. 102.

Estos son sólo algunos de los aspectos dogmáticos particularmente relevantes traídos por los llamados crímenes de informática, que, dentro de las limitaciones de este escrito, fueron nuestro objeto de reflexión. Reflexión esta que, sin embargo, parte de una premisa específica. El avance inevitable de la ley penal a nuevas áreas de conflicto no significa y tampoco debe significar la erosión de los conceptos y elementos básicos que le atribuyen identidad, al contrario. La idea de desarrollo inherente a cualquier ciencia con el fin de afrontar los desafíos de su tiempo, sólo tiene sentido mientras se respeten los límites formales y materiales que le dan forma e identidad. Este es el verdadero desafío. Un desafío no solamente marcado por la responsabilidad y por el equilibrio, sino también, de manera fundamental, por el respeto de los derechos y garantías que garantizan forma al derecho penal de la época.

5. Referencias

BARROS, Marco Antonio de, *et. al.* Crimes informáticos e a proposição legislativa: considerações para uma reflexão preliminar. *Revista dos Tribunais*, vol. 865, p. 399, Nov. 2007.

BECK, Ulrich. *Risikogesellschaft.* Auf dem Weg in eine andere Moderne, Frankfurt am Main : Suhrkamp, 1986.

BRITO, Auriney. *Direito penal informático*. São Paulo: Saraiva, 2013.

CASTRO, Carla Rodrigues Araújo de. *Crimes de informática e seus aspectos processuais*. Rio de Janeiro: Lumen Juris, 2001.

COLLI, Maciel. *Cibercrimes*: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá Editora, 2010.

CONSELHO DA UNIÃO EUROPEIA. Convenção de Budapeste, de 23 de novembro de 2001. *Convenção do Cibercrime*, Budapeste, 2001.

CONSELHO DA UNIÃO EUROPEIA. Decisão-Quadro 2005/222/JAI de 24 de fevereiro de 2005. *Relativa a ataques contra os sistemas de informação*. Bruxelas: Jornal Oficial da União Europeia, 24 de fevereiro de 2005

CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011.

D'AVILA, Fabio Roberto. Liberdade e segurança em direito penal. O problema da expansão da intervenção penal. *Revista Síntese Direito Penal e Processual Penal*, v. 11, n. 71, dez./jan. 2012, Porto Alegre: IOB.

___. *Ofensividade e crimes omissivos próprios*: contributo à compreensão do crime como ofensa ao bem jurídico. Coimbra: Coimbra Editora, 2005.

___. *Ofensividade em direito penal*: escritos sobre a teoria do crime como ofensa a bens jurídicos. Porto Alegre: Livraria do Advogado Editora, 2009.

FARIA COSTA, José Francisco de. *Direito penal da comunicação*: alguns escritos. Coimbra: Coimbra Editora, 1998.

FIGUEIREDO DIAS, Jorge de. *Direito penal*: parte geral: tomo I: questões fundamentais. 2ª Ed. Portugal: Coimbra Editora, 2007.

GRACIA MARTÍN, Luis. *O horizonte do finalismo e o direito penal do inimigo*. Trad. Luiz Regis Prado e Érika Mendes de Carvalho. São Paulo: Editora Revista dos Tribunais, 2007.

HUNGRIA, Nélson. *Comentários ao código penal*, volume I, tomo I: arts. 1º ao 10. 5ª ed. Rio de Janeiro: Forense, 1976.

KERR, Vera Kaiser Sanches. *A disciplina, pela legislação processual penal brasileira, da prova pericial relacionada ao crime informático praticado por meio da internet*. Dissertação de Mestrado, São Paulo, 2011.

LIPOVETSKY, Gilles. *Os tempos hipermodernos*. Trad. Mário Vilela. São Paulo: Barcarolla, 2004.

MARINUCCI, Giorgio, DOLCINI, Emilio. *Corso di diritto penale*: le norme penali: fonti e limiti di applicabilità, il reato: nozione, estruttura e sistematica, vol. I. 3ª Ed. Milão: Giuffrè Editore, 2001.

MODELLENTWÜRFE EINES REGELUNGSMECHANISMUS ZUR VERMEIDUNG VON JURISDIKTIONSKONFLIKTEN, in: *Jurisdiktionskonflikte bei grenzüberschreitender Kriminalität*. Ein Rechtvergleich zum internationalen Strafrecht, Arndt Sinn (Hg.) Göttingen : V & R Unipress, 2012, p. 585 ss.

NUCCI, Guilherme de Souza. Prefácio. In: SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013.

PIFARRÉ DE MONER, María José. Spanien. Länderberichte. In: *Jurisdiktionskonflikte bei grenzüberschreitender Kriminalität*. Ein Rechtvergleich zum internationalen Strafrecht, Arndt Sinn (Hg.) Göttingen : V & R Unipress, 2012, p. 420 ss.

QUINTERO OLIVARES, Gonzalo. Problemas de la perseguibilidad de los ciberdelitos. In: A. RIQUERT, Marcelo (Coord.). *Ciberdelitos*. Buenos Aires: Hammurabi, 2014.

RIQUERT, Marcelo A.. Repensando como funciona la ley penal en el ciberespacio. In: *Ciberdelitos*. Marcelo A. Riquert (org.), Buenos Aires: Hammurabi, 2014.

SANTOS, Daniel Leonhardt dos. *Crimes de informática e bem jurídico-penal:* contributo à ofensividade em direito penal. Dissertação de Mestrado, Porto Alegre, PUCRS, 2014.

SCHAFF, Adam. *A sociedade informática*. As consequências sociais da segunda revolução industrial. Trad. Carlos Eduardo Jordão Machado e Luiz Arturo Obojes, 4.ª ed., São Paulo : Ed. UNESP, 1995.

STEIN, Ernildo. *Uma breve introdução à filosofia*, Ijuí : Ed. UNIJUÍ, 2002.

SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013.

VARGAS LLOSA, Mario. A civilização do espetáculo. Uma radiologia do nosso tempo e da nossa cultura. Trad. Ivone Benedetti, Rio de Janeiro : Objetiva, 2013.

VIANNA, Túlio Lima. *Fundamentos de direito penal informático*: do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003.

VIANNA, Túlio; MACHADO, Felipe. *Crimes informáticos*. Belo Horizonte: Editora Fórum, 2013.

ZANELLATO, Marco Antonio. Condutas ilícitas na sociedade digital. *Revista de Direito do Consumidor*, vol. 44, p. 206, out. 2002.