DIREITO PENAL E CRIMINALIDADE INFORMÁTICA. BREVES APROXIMAÇÕES DOGMÁTICAS

CRIMINAL LAW AND CYBERCRIMES. BRIEF DOGMATIC APPROACHES

Fabio Roberto D'Avila[1]
PUC/RS
Daniel Leonhardt dos Santos[2]
PUC/RS

Resumo

Nosso tempo não tem uma única feição. Se, por um lado, é verdade que a informática longe está de dar conta de tantas e tão profundas transformações, por outro, não se pode negar que ela mudou, de forma radical, o modo do homem relacionar-se com o mundo e com o tempo. A informática permitiu o tempo instantâneo e, simultaneamente, a compressão do espaço. As comunicações já não encontram fronteiras físicas. A velocidade passa a pautar as relações humanas. A essa nova e tão intensa dimensão relacional corresponde, por decorrência lógica, novos conflitos, a que é chamado também o direito penal. Parte deles, é verdade, já conhecidos e regulados pela legislação penal. Delitos que encontram na informática apenas um novo espaço e novas formas de realização. Outros, porém, dotado de novas características, colocam dificuldades não só na delimitação da matéria de incriminação, como, até mesmo,

[1] Pós-doutor em Ciências Criminais pela Johann Wolfgang Goethe Universität, Frankfurt am Main, Alemanha. Doutor em Ciências Jurídico-Criminais pela Faculdade de Direito da Universidade de Coimbra, Portugal. Professor Titular da Faculdade de Direito e do Programa de Pós-Graduação em Ciências Criminais (Mestrado e Doutorado) da PUCRS. Presidente do Instituto Eduardo Correia (IEC). Advogado criminal em Porto Alegre.

[2] Doutorando (2015 -) e Mestre em Ciência Criminais pela Pontifícia Universidade Católica do Rio Grande do Sul (2014), especialista em Ciências Penais (2013) e Bacharel em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul (2012). Bolsista integral CAPES (2015-), bolsista integral FAPERGS (2013-2014) e bolsista de Iniciação Científica (2010-2012). Pesquisador.

na identificação dos valores tutelados pela norma. Tendo em vista o estado ainda insipiente do direito positivo, bem como as particularidades locais de cada ordem jurídica, buscamos ter em conta alguns problemas comuns e particularmente sensíveis a nossa tradição jurídico-penal, tendo como referência as proposições da Convenção de Budapeste e a Decisão-quadro 2005/222/JAI do Conselho, sem, todavia, descuidar do direito positivo brasileiro.
Palavras-chave
Direito Penal. Ciberdelitos. Bem jurídico. Ofensividade.

Abstract
Our time doesn't have only one feature. If, on the one hand, it is true that computer science is far from managing so many and so profound changes, on the other hand, we cannot deny that it has changed radically man's way to relate himself with the world e with the time. The computer science enabled the instantaneous time and, simultaneously, the compression of space. Communications don't have physical boundaries anymore. The speed is what guide now the human relations. To this new and so intense relational dimension corresponds, by logical consequence, new conflicts, by which is also called for the criminal law. Some of them, indeed, already known and regulated by criminal law. Offenses that find in the computer science only a new space and new ways of realization. Others, however, equipped with new features, pose difficulties not only in the delimitation of the object of incrimination, but also in identifying the values protected by the rule. Given the incipient state of the positive law, as well as the local conditions of each legal system, the research have in mind some common and particularly sensitive problems to our criminal legal tradition, having as reference the propositions of the Budapest Convention and the Framework Decision 2005/222/JAI from the European Council, without, however, neglecting the Brazilian law.
Keywords
Criminal Law. Cybercrimes. Juridical good. Offensiveness.

1. O nosso tempo e o nosso mundo.

"*Todo o mundo é feito de mudanças*", diria o grande poeta português LUÍS DE CAMÕES, em seu memorável *Sonetos*. Quanto a isso não há a menor dúvida. Todavia, apreender corretamente estas mudanças, de modo a atribuir uma precisa feição, um preciso rosto ao tempo em que vivemos, é tarefa acentuadamente difícil, senão

mesmo impossível. Seja porque, para aquele que vive a mudança, ela costuma mostrar-se amorfa ou, ao menos, turvada, disfarçada pelo contínuo fluxo da vida e sua aparente normalidade; seja porque – e isso no que tange precisamente aos nossos dias – ela assuma, como nunca antes, uma feição poliforme, caleidoscópica, dotada de múltiplos aspectos verdadeiramente intensos e não menos importantes. Daí a convivência de tão variadas designações. Da "*sociedade do risco*" de ULRICH BECK[3] à "*civilização do espetáculo*" de MARIO VARGAS LLOSA,[4] passando por denominações como "*sociedade do consumo*" ou "*sociedade da informação*", ou ainda, por outras bem mais compreensivas e, daí, também poliformes, como *pós-modernidade*, *modernidade tardia* ou *hipermodernidade*.[5]

Defender, nesse contexto, a existência de uma *sociedade informática* não seria algo novo ou mesmo incomum. Já na década de 80, Adam Schaff[6] valia-se de tal designação. Contudo, tomar o fragmento como se o todo fosse é deixar escapar o essencial. Essencial que se revela justamente na complexidade e multiplicidade de formas, insusceptíveis de ser apreendidas e aprisionadas em um único rosto. O nosso tempo, definitivamente, não possui uma única feição. O que não nos impede, é claro, mas, pelo contrário, nos obriga a contínua tarefa de vigiar[7] as suas inúmeras manifestações e os frutos que nos são por ela legados. E é

[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.

sob essa precisa perspectiva que se colocam as reflexões desse breve escrito.

Se, por um lado, é verdade que a informática longe está de dar conta de tantas e tão profundas transformações, por outro, não se pode negar que ela mudou, de forma radical, o modo do homem relacionar-se com o mundo e com o tempo. A informática permitiu o tempo instantâneo e, simultaneamente, a compressão do espaço. As comunicações já não encontram fronteiras físicas. A velocidade passa a pautar as relações humanas. O homem descobre uma nova dimensão relacional aberta pela internet e potencializada pelos smartphones. Dados pessoais, bancários, comerciais, judiciais passam a ser armazenados na rede. A economia e o mercado de capitais virtualizam-se a ponto de colocar em dúvida o futuro da moeda em papel. Relações afetivas, relações de amizade ou laborais migram, em grande medida, para esse novo mundo virtual. Nada parece escapar à informática e à rede mundial de computadores.

A essa nova e tão intensa dimensão relacional corresponde, por decorrência lógica, novos conflitos, a que é chamado também o direito penal. Parte deles, é verdade, já conhecidos e regulados pela legislação penal. Delitos que encontram na informática apenas um novo espaço e novas formas de realização. Outros, porém, dotado de novas características, colocam dificuldades não só na delimitação da matéria de incriminação, como, até mesmo, na identificação dos valores tutelados pela norma. Dificuldades essas das quais advém importantes problemas de dogmática penal.

Não se trata, porém, e isso já podemos adiantar, de um "novo" direito penal, mas apenas do usual avanço do direito penal em novos espaços de conflitualidade, marcados, *in casu*, por uma muito especial complexidade e por particularidades atinentes ao

espaço no qual ele se projeta, a informática.[8] Conquanto haja importantes diferenças entre os denominados crimes informáticos, não resta dúvida de que há linhas fortes que os unem, não só permitindo, mas, de fato, recomendando o seu estudo conjunto. Alguns desses elementos serão aqui objetos da nossa atenção. Inicialmente, dadas as suas especificidades, iremos nos ocupar de alguns aspectos relativos à aplicação da lei penal no espaço. E, em um segundo momento, propomos uma breve reflexão sobre o conteúdo do injusto nos crimes informáticos.

Tendo em vista o estado ainda insipiente do direito positivo, bem como as particularidades locais de cada ordem jurídica, buscamos ter em conta alguns problemas comuns e particularmente sensíveis a nossa tradição jurídico-penal, tendo como referência as proposições da Convenção de Budapeste e a Decisão-quadro 2005/222/JAI do Conselho, sem, todavia, descuidar do direito positivo brasileiro.

2. A instantaneidade do tempo e a compressão do espaço. O problema da aplicação da lei penal no espaço.

A instantaneidade do tempo e a compressão do espaço – dizíamos antes – são marcas profundas da criminalidade informática. Nesse preciso âmbito, uma conduta delituosa, *v. g.*, fragmentada em mais de um país da Ásia, pode, por meio da internet, produzir efeitos em diversos países da Europa, e tudo no preciso instante em que a conduta é praticada. As tradicionais noções de lugar e espaço já não encontram aqui adequada aplicação. Conceitos fundamentais de território e soberania veem-se profundamente fragilizados.

[8] FARIA COSTA, José Francisco de. *Direito penal da comunicação*: alguns escritos. Coimbra: Coimbra Editora, 1998, p. 119.

Em um primeiro momento, poderia se pensar tratar-se de uma simples criminalidade potencialmente transnacional, como tantas outras, a exemplo do próprio tráfico de drogas. Um olhar mais detido, contudo, é capaz de perceber que, em âmbito informático, as condutas projetam-se em termos temporais e espaciais de forma absolutamente singular. Tempo e espaço são, aqui, verdadeiramente redimensionados, reconfigurados, com importantes repercussões dogmáticas e político-criminais.[9]

De pronto, merece destaque as fragilidades de um direito penal limitado ao Estado-Nação. Uma política criminal estritamente nacional muito pouco tem a dizer em resposta a uma tal criminalidade. Os esforços político-criminais devem converter-se, obrigatoriamente, em esforços de cooperação internacional, alinhados por diretrizes de uma desejada *política criminal comum*. Insere-se, pois, com perfeição, no horizonte do mundo globalizado e seus paradoxos. Horizonte em que, bem salienta Faria Costa, fenômenos criminais exuberantemente globais são enfrentados por meio de limitados mecanismos nacionais, a ensejar "a sensação de uma certa paralisia na acção de defesa para com o crime".[10] Daí a vontade e a necessidade do direito penal fazer-se também *global*, a despeito da sua tradicional, por vezes, inerente vocação *local*.

O primeiro desafio, nesse sentido, consiste em eliminar eventuais ilhas de impunidade, normalmente oriundas da falta de regulamentação ou de falhas da legislação penal e processual penal já existente. Não por outra razão é que a Convenção de Budapeste imprimiu um grande esforço no sentido de obter uma

[9] FARIA COSTA, José Francisco de. *Direito penal e globalização*: reflexões não locais e pouco globais. Coimbra: Coimbra Editora, 2010, p. 17.
[10] FARIA COSTA, José Francisco de. *Direito penal e globalização*: reflexões não locais e pouco globais. Coimbra: Coimbra Editora, 2010, p. 46

harmonização mínima da legislação aplicável.[11] Como era de se esperar, o texto convencional dedica, por um lado, um largo espaço à identificação e descrição de comportamentos criminosos dotados de suficiente consenso. E, por outro, avança também importantes disposições penais e processuais penais atinentes, principalmente, ao resguardo dos elementos necessários à materialidade do crime, à competência, à cooperação e ao auxílio mútuo.[12] É preciso reconhecer que o ideal, com vistas a evitar a impunidade, seria a obtenção de uma efetiva unificação normativa. Tal pretensão, todavia, bem observa Marcelo Riquert, "aperece como una suerte de aspiración de imposible alcance – utópica en escala global, muy difícil a nível regional".[13] A obtenção de parâmetros mínimos de harmonização mostra-se, pois, como o melhor dos caminhos.

Uma questão merece especial destaque: o problema da competência.

---

[11] Esforço de harmonização normativa necessário para evitar a impunidade (RIQUERT, Marcelo A.. Repensando como funciona la ley penal en el ciberespacio. In: *Ciberdelitos*. Marcelo A. Riquert (org.), Buenos Aires: Hammurabi, 2014, p. 23). Nesse mesmo sentido reconheceu o Conselho da União Europeia, na Decisão-Quadro 2005/222/JAI, de 24 de fevereiro de 2005, ao expor: "As consideráveis lacunas e diferenças entre as legislações dos Estados-Membros neste domínio podem entravar a luta contra a criminalidade organizada e o terrorismo e podem dificultar uma cooperação policial e judiciária eficaz no âmbito de ataques contra os sistemas de informação. A natureza transnacional e sem fronteiras dos modernos sistemas de informação implica que os ataques contra esses sistemas têm frequentemente uma dimensão transfronteiriça, evidenciando assim a necessidade urgente de prosseguir a harmonização das legislações penais neste domínio" (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.

Não há dúvida que a desejada harmonização legislativa permitiria um passo importante no sentido de evitar *conflitos negativos de competência*, por meio de diretrizes comuns voltadas à aplicação da lei penal no espaço.[14] No que tange, p. ex., ao princípio da territorialidade, verdadeiro princípio dos princípios em âmbito de aplicação da lei penal no espaço, pode-se afirmar que a adoção de um amplo critério de competência territorial, iluminado pelo princípio da ubiquidade, seria já suficiente para ao menos cobrir os casos em que o crime informático, de algum modo, tocou o território nacional, despertando, assim, o seu interesse direto.[15]

Para tanto, seria necessário considerar o *lugar del hecho* tanto o lugar da ação, no todo ou em parte, a compreender inclusive as ações de participação, como o lugar do resultado, no todo ou em parte, ou ainda, o lugar em que deveria ocorrer o resultado. A legislação brasileira, por exemplo, define o lugar do crime como o "lugar em que ocorreu a ação ou a omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado" (art. 6. CP brasileiro). De forma semelhante, embora não idêntica, o código penal alemão define o *lugar del hecho* como aquele em que "el autor haya actuado o, en caso de comisión por omisión, en el que hubiese debido actuar o en el que se produzca el resultado del tipo o que debía producirse conforme a la representación mental del autor" (§ 9 I CP alemão). E, no que se refere à legislação espanhola,

[14] Assim, secção 3 da Convenção.

[15] Das teorias de delimitação do *locus commissi delicti*, pode-se dizer que a teoria pura da ubiquidade é a menos vulnerável dentre as teorias que buscam delimitar o lugar do crime. Conforme já bem ensinava Hungria, a teoria "não exige transigências de soberania e, se não evita os conflitos positivos de jurisdição, elimina os negativos, conjurando o desconforto de eventual impunidade do agente". E é especificamente nesse ponto que essa teoria se sobressai sobre as demais (HUNGRIA, Nélson. *Comentários ao código penal*, volume I, tomo I: arts. 1º ao 10. 5ª ed. Rio de Janeiro: Forense, 1976, p. 162).

embora não guarde a mesma semelhança em termos de regulação,[16] também ela vem sido usualmente interpretada segundo os parâmetros do princípio da ubiquidade.[17]

Todavia, ainda assim, não é incomum a ocorrência de problemas dogmáticos de importante repercussão prática, o que tão bem ilustra o caso dos crimes de perigo abstrato. Diferentemente dos crimes de dano ou de perigo concreto, para os quais o resultado "dano" ou "perigo" ao bem jurídico são indispensáveis, os crimes de perigo abstrato são interpretados, em termos majoritários, enquanto delitos desprovidos de resultado (*erfolglos*). Logo, se para os crimes de dano e perigo concreto o princípio da ubiquidade cobre, sem problemas, tanto o lugar da ação como o lugar do seu resultado, nos delitos de perigo abstrato é controvertido o fato da competência estar ou não restrita ao lugar da ação, deixando a descoberto o lugar onde os efeitos da ação viessem a se projetar, uma vez que esses efeitos, segundo o entendimento majoritário, não constituiriam um elemento do tipo. Em termos práticos, tal situação levaria à impossibilidade do Estado atingido apenas pelos efeitos do crime aplicar a sua lei penal, resultando em lacunas de impunidade.

Essa questão chamou a atenção do penalista alemão JÖRG MARTIN, dando origem a um interessante estudo sobre a punibilidade de danos transfronteiriços, *in casu*, sob a perspectiva ambiental. A solução por ele defendida consiste em reconhecer a existência de resultado também em crimes de perigo abstrato, consistente em um *risco* ao bem jurídico, avaliado por meio de um

---

[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.

juízo *ex ante* e sob a perspectiva do autor.[18] De forma semelhante, conquanto não coincidente, também nós temos defendido uma leitura dos crimes de perigo abstrato como crimes de resultado, esse entendido, porém, como uma *possibilidade de dano ao bem jurídico*, verificada por um juízo *ex ante* de base total.[19] Tanto numa como noutra, o problema da competência viria solucionado pelo reconhecimento da existência de um resultado nos crimes de perigo abstrato, a colocar a possibilidade de aplicação da lei penal também pelo Estado afetado exclusivamente pelos efeitos da ação criminosa. Essa é, por certo, apenas uma possível forma de enfrentamento do problema cujos desdobramentos dogmáticos, por razões óbvias, e lamentavelmente, não podem ser aqui aprofundados.

De outra parte, uma vez resolvido a questão de conflitos negativos de competência – e, portanto, de eventuais lacunas de impunidade – por meio de um amplo alcance das respectivas legislações nacionais, outro problema se coloca, o problema do conflito positivo de competência e do *ne bis in idem*.

O resultado imediato do aumento das competências nacionais é a coexistência de vários países interessados em julgar o mesmo crime informático. Fato esse que requer a imediata adoção de critérios aptos a definir regras de preferência, sob pena da coexistência de múltiplas investigações e processos sobre o mesmo fato, com resultados prejudiciais das mais variadas ordens, desde a coleta da prova a gastos desnecessários, passando pelos riscos de uma dupla punição.

---

[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.

Atentos a tais dificuldades, dois modelos diversos buscam propor uma solução. O primeiro, desenvolvido por Arndt Sinn, defende a adoção de critérios *vor der Tat*, ou seja, a adoção de um critério preestabelecido pela lei e válido a todos os casos. Nesse sentido, propõe Sinn que a preferência na aplicação da lei penal seja estabelecida mediante uma série de regras, a partir das quais alguns princípios de aplicação da lei penal se sobreporiam a outros. Maior peso seria conferido ao lugar da prática da ação, seguido pelo lugar do resultado, no caso da ação se projetar em mais de um país, e assim por diante.[20] Uma segunda proposta é oferecida por Bernd Hecker. Nesta o autor combina tradicionais princípios reitores da aplicação da lei penal (princípio da territorialidade, princípio da personalidade ativa e passiva, etc.) com critérios materiais como, *v. g.*, o local do maior dano, o interesse da vítima, o interesse do acusado, entre outros, tendo como objetivo determinar à luz do caso concreto e, portanto, caso a caso, a quem deve competir a preferência.[21]

Ambas as propostas, dotadas de vantagens e desvantagens, corresponde aos modelos de solução de conflitos de jurisdição, desenvolvidos pelo ZEIS (*Zentrum für Europäische und Internationale Strafrechtsstudien*) para crimes transnacionais, dentre os quais, a criminalidade informática.[22] Tais propostas, contudo, a despeito das

---

[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: *Jurisdiktionskon-*

usuais dificuldades de implementação, estariam pensadas fundamentalmente para a União Europeia. Assim, embora de indiscutível relevo, estariam ainda muito distante de dar conta da dimensão efetivamente global da criminalidade informática. Tudo a demonstrar o nível de complexidade que coloca o enfrentamento dessa específica criminalidade e os desafios de enfrentamento obrigatório em um futuro próximo.

3. O injusto penal nos crimes informáticos. Aspectos atinentes ao bem jurídico e à ofensividade

Os principais problemas do direito penal na sociedade contemporânea não são propriamente *quantitativos*. Não decorrem da sua simples expansão, do simples aumento da área de regulação jurídico-penais ou ainda, de forma muito breve, do simples fato de haver *mais direito penal*. O grande problema reside, isto sim, na forma como se dá, em termos *qualitativos*, essa nova regulação.[23]

O espírito do nosso tempo, todos sabemos, tem elevado as pretensões de *eficiência* e *segurança* a condição de valor dos valores,

---

flikte bei grenzüberschreitender Kriminalität. Ein Rechtvergleich zum internationalen Strafrecht, Arndt Sinn (Hg.) Göttingen : V & R Unipress, 2012, p. 575 ss.

[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). Em sentido semelhante, Nucci expõe que a verificação do princípio da intervenção mínima não significa, necessariamente, "a ausência de criminalização de condutas novas, que emergem nas relações sociais, conforme se avança no progresso tecnológico em geral. O Direito Penal, como *ultima ratio*, precisa fazer-se presente nos cenários onde outros ramos do conhecimento jurídico não conseguiram solucionar. Portanto, constata-se a indispensabilidade da tipificação dos delitos de informática, tendo em vista o desenvolvimento acentuado dos computadores na vida das pessoas e na estrutura administrativa do Estado" (NUCCI, Guilherme de Souza. Prefácio. In: SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013, p. 11).

de valor que a tudo subjuga. Diante delas, as liberdades e garantias penais, a tanto custo conquistadas, veem-se hoje fragilizadas e não raramente são afastadas, sob o argumento da necessidade de otimização das pretensões político-criminais de combate à criminalidade.[24] Uma espécie de entronização da ideia de segurança que, por vezes, a depender do âmbito em que se projeta, como, aliás, bem ilustra o terrorismo, parece não conhecer limites dogmáticos ou político-criminais.[25] E isso, por certo, não é admissível nos quadros de um direito penal democrático.[26] É tarefa intransponível do direito penal estabelecer limites de contenção dessa desmedida vontade de segurança e, assim, reequilibrar a perene tensão entre liberdade e segurança. Não por outra razão, vivemos também um tempo em que o resgate da dimensão material do crime assume um papel de particular importância, no que tange tanto à delimitação do espaço de legitimidade do direito penal, quanto à correta compreensão do injusto.

---

[24] Gonzalo Quintero Olivares faz uma interessante reflexão sobre o tema, expondo 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] Ver 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.

Conquanto a teoria do crime como ofensa a bens jurídicos seja continuamente objeto de críticas, principalmente no âmbito do denominado *Nebenstrafrecht*, temos a convicção profunda que ela ainda se faz indispensável como elemento de identificação e compreensão do conteúdo material do injusto e, assim, também do âmbito do tipo. Mas não só. É, também, expressão forte de um Modelo de Estado democrático, plural, multicultural, tolerante e estabelecido nos direitos e garantias fundamentais.[27] Duas dimensões da mesma ideia. E que colocam, por sua vez, desdobramentos fundamentais.

O tipo penal, se bem vemos, nada mais é do que a expressão legislativa de um ilícito que o antecede, de um dado de realidade não apenas valorado negativamente, mas considerado de tal forma desvalioso, a ponto de merecer a mais dura resposta do Estado, a criminalização. Logo, se isso é assim, é preciso concluir que todo tipo é tipo-de-ilícito, que todo e qualquer tipo, para ser corretamente delimitado, exige que se pergunte sobre o dado de realidade que lhe confere forma. A definição do âmbito do tipo, da matéria de incriminação, depende fundamentalmente disso.

Quando olhamos para a criminalidade informática, percebemos que, em parte, o que se encontra são velhos crimes cometidos por um novo meio, o meio informático. Tradicionais

---

[27] Nesse sentido, "um Estado que se quer não-liberticida, autoritário, intolerante, mas sim, laico, plural e multicultural, erigido a partir da diferença e com ela comprometido, em que não há espaço para perseguições de credo, cor ou classe, em que não se punem pessoas ou grupos, mas apenas fatos. Enfim, um Estado em que todos, absolutamente todos, podem valer-se da condição de cidadãos e, assim, resguardados pela totalidade dos direitos e garantias constitucionais, resistir às manifestações de inaceitável autoritarismo que, sazonalmente, quer por razões de cunho meramente pragmático, quer por razões ideológicas, insistem em tenta-lo" (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).

crimes contra honra são hoje praticados pelas redes sociais, crimes de fraude são praticado por e-mail ou, ainda, crimes contra os direitos autorais dão-se na forma de disponibilização não autorizada para *downloads* de livros e músicas. É possível imaginar, até mesmo, como observa Faria Costa, um homicídio por via informática. Para tanto, cogita ele a possibilidade de alguém, por meio da internet ou, ainda – acrescentamos nós –, da intranet de um determinado hospital, ter acesso aos aparelhos que mantêm uma pessoa viva, vindo a desligá-los, produzindo, assim, a sua morte.[28] Nesse mesmo sentido, i.e., no sentido de velhos crimes agora com nova roupagem, a Convenção de Budapeste elenca a burla informática, a falsidade informática, a pornografia infantil e as ações violadoras de direitos autorais. Outros, como o próprio homicídio, estariam cobertos pela legislação tradicional.

O problema aqui, como se percebe, não é tanto o conteúdo do injusto, mas a forma de realização e os aspectos penais e processuais dela decorrentes. Como usualmente se diz: vinho velho em garrafa nova. Razão pela qual este tipo de criminalidade é designada, por vezes, de crimes *impropriamente informáticos* ou de crimes *relacionados com computadores*.

Em contrapartida, há um outro grupo de crimes em que essa mesma conclusão não se coloca de forma imediata, merecendo, de alguns, a denominação de crimes *propriamente informáticos*. Essa específica criminalidade é apresentada como o *novo* do direito penal informático, como crimes efetivamente *inaugurados* pelo esse novo âmbito. Crimes, enfim, que só poderiam ser "praticados através da informática".[29] Dizem respeito, no que tange à Convenção de

[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,

Budapeste, aos delitos de *(i)* acesso ilegítimo a sistema informático, *(ii)* intercepção ilegítima de dados informáticos, *(iii)* interferência em dados informáticos, *(iv)* interferência em sistema informático e *(v)* uso abusivo de dispositivo informático. Aparecem também previstos pela Decisão-quadro 2005/222/JAI do Conselho, nos artigos 2º (acesso ilegal aos sistemas de informação), 3º (interferência ilegal no sistema) e 4º (interferência ilegal nos dados).

O acerto ou não dessa classificação depende fundamentalmente do conteúdo material do injusto, daquilo que se entender como objeto de tutela da norma, o que, nesse contexto, não é tarefa fácil. O fato das conduta narradas recaírem sobre realidades especificamente informáticas, a exemplo do acesso a sistema informático ou interferência em dados informáticos, torna obscuro o bem jurídico tutelado e, assim, o âmbito de incidência do tipo. A título de mera ilustração, caso recepcionássemos o crime de interferência em dados informáticos (art. 4º da Convenção) como um delito de natureza exclusivamente patrimonial, semelhante ao tradicional delito de dano, teríamos que concluir que as condutas de "danificar, apagar, deteriorar, alterar ou eliminar dados informáticos" teriam relevo penal apenas quando tais dados tivessem valor econômico, deixando de fora todo o restante, como

---

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; 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.

dados de natureza pessoal e familiar (fotos, documentos pessoais, etc.).[30] Mas não só. A indefinição do bem jurídico torna a identificação e a mensuração do resultado igualmente incerta, inviabilizando, p. ex., a implementação de exigências típicas como o *dano grave* nos delito de interferência de dados, previsto pelo art. 4. 2. da Convenção, ou a *obstrução grave* no delito de interferência em sistemas, prevista no art. 5º da Convenção. A contrário senso, fica igualmente inviável o reconhecimento de um eventual *dano insignificante* ou *obstrução insignificante* incapaz de configurar o crime, dada a bagatelaridade dos seus efeitos.[31]

As propostas nesse âmbito são as mais variadas.

Há desde quem defenda a *segurança informática* como bem jurídico tutelado, argumentando no sentido de que, "na sociedade informatizada, a segurança no ciberespaço torna-se um importante valor, absolutamente merecedor e tutela jurídica" [32], como quem sustente uma ampla noção de "liberdade informática", isto é, a ideia de que os delitos informáticos seriam infrações "das distintas liberdades as que podem estender-se ao emprego dessas

[30] Nesse sentido, há quem defenda que os bens violados por um crime de informática não devem ser analisados pelo que eles representam economicamente, pelo seu valor patrimonial unicamente, mas, sim, analisados de acordo com o valor agregado à vida do indivíduo ou da sociedade empresarial que deles utilizem. Para Barros, por exemplo, o valor está inserido na utilidade agregada ao bem, no que ele representa na sua totalidade para a vida de quem o usufrui. (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). Assim também, no mesmo sentido, Zanellato, que expõe ser o valor de um bem informático a utilidade imanente desse mesmo objeto, não devendo ele ser valorado meramente de forma econômica (ZANELLATO, Marco Antonio. Condutas ilícitas na sociedade digital. *Revista de Direito do Consumidor*, vol. 44, p. 206, out. 2002).

[31] Ver dispositivo do relatório.

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

tecnologias". [33] Há ainda quem proponha o reconhecimento do bem jurídico na noção de *inviolabilidade das informações automatizadas* e, portanto, dos dados informáticos, compreendendo, assim, a tutela dos programas de computador, na medida em que também eles são dados.[34] E, em linha semelhante, quem defina o bem jurídico como o dado informático e o sistema informático.[35]

De pronto, é preciso ter em conta que a moderna teoria do crime como ofensa ao bem jurídico não é compatível com bens jurídicos vorazes, com bens de fronteiras fluidas e que a tudo compreende, como é o preciso caso da segurança e, também, nos contornos acima propostos, da alegada liberdade informática. Tais bens defraudam a necessária capacidade crítica do bem jurídico-penal.[36] Objeção semelhante pode ser também levantada contra as propostas do dado informático e do sistema informático. Por um lado, não nos parece que esses elementos possam constituir um valor em si mesmo, mas apenas na medida daquilo que informam (no caso do dado) ou daquilo que oferecem (no caso do sistema). Por outro, considerar o próprio dado e o sistema como bem jurídico equivale a uma espécie de sacralização de elementos informáticos, a permitir que qualquer contato venha a constituir crime. Constatação que inviabilizaria não só o caráter crítico da teoria, mas também a graduação do ilícito a partir dos efeitos produzidos a partir do ataque aos dados e ao sistema.

---

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

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

Por isso, andam bem melhor as tentativas de identificar o bem jurídico a partir do *valor que expressam* ou *resguardam* os elementos informáticos sobre os quais recaem a ação. Os dados informáticos e o sistema informático consistem, sem dúvida, no *objeto da ação* e podem corresponder, simultaneamente, ao *objeto do bem jurídico*, isto é, à materialização do valor que a norma busca tutelar, mas definitivamente não são, em si, o bem jurídico. A carta de amor, a foto de família, o vídeo erótico produzido pelo próprio casal são dados do mundo carregados de intimidade, ponto de materialização de valores como a intimidade, a privacidade e a livre disposição da própria imagem. E diferente não é quando tais realidades se expressam por meio de dados informáticos, na forma de um e-mail ou de uma foto ou vídeo digitais. Logo, tanto o acesso a esses dados, como a sua destruição, danificação, subtração, constituem crimes contra esses mesmos valores, corporificados nos referidos dados.

Em contrapartida, o resguardo de dados e sistemas informáticos de valor econômico, como os dados ou sistemas de uma empresa, são melhor localizados no capítulo dos crimes patrimoniais. Ataques reiterados a determinadas empresas virtuais que resultam no denominado *denial of service* (DoS), retirando a empresa do ar por algumas horas ou dias, são agressões de caráter fundamentalmente patrimonial e que podem gerar prejuízos gigantescos. E o mesmo parece ocorrer quando a ação de acesso ao sistema informático tem como objetivo, *v. g.*, alcançar um determinado segredo industrial. Embora haja um elemento de confidencialidade em jogo, é o valor econômico do segredo que se sobrepõe.

Em razão disso, andou bem o legislador espanhol ao dividir os problemas de acesso ao sistema, interceptação ilegítima e interferência em dados em títulos diversos, dedicado à intimidade e

à imagem (art. 197), por um lado, e ao patrimônio (art. 264), por outro. Embora possamos questionar se a totalidade dos elementos de valor estão devidamente cobertos, não há dúvida sobre definição do objeto de tutela, a permitir tanto a verificação da ofensa, como a graduação do injusto. O mesmo, contudo, não pode ser dito sobre a Convenção de Budapeste. É verdade que, ao definir, de forma genérica, os crimes informáticos como infrações contra a confidencialidade, a integridade e a disponibilidade de sistemas e dados informáticos,[37] ela alcança um largo espectro de cobertura e confere maior liberdade de configuração aos países signatários. Mas é igualmente verdade que, assim agindo, perdeu uma singular oportunidade de orientar materialmente as legislações nacionais, com importante repercussão para a harmonização legislativa em âmbito internacional.

A Convenção erra também, ao nosso sentir, quando avança na criminalização de atos meramente preparatórios. Em seu artigo sexto, intitulado de uso abusivo de dispositivos, é recomendada a criminalização da fabricação e comercialização de dispositivos maliciosos, isto é, dispositivos voltados à prática de crimes informáticos, bem como a simples posse dos referidos dispositivos. Trata-se, como é evidente, de atos preparatórios de crimes informáticos e, por isso, desprovidos de lesão ou perigo de lesão ao objeto de tutela da norma. Conquanto saibamos que não faltam exemplos de dispositivos semelhantes no que tange ao tráfico de drogas e ao terrorismo, é preciso ter em conta que a sua recepção defrauda a exigência de legitimidade material da teoria do crime como ofensa a um bem jurídico, equiparando o injusto penal à mera violação de dever, concepção essa, como se bem sabe, própria de modelos autoritários de Estado. Para tanto, basta lembrar da

[37] Cap. II, Seção 1, Título 1 da Convenção.

concepção de injusto defendida pela Escola de Kiel no período nacional-socialista.[38] Além disso, também sob a ótica da proporcionalidade, tal dispositivo enfrenta sérias dificuldades.[39] Crimes muitíssimo mais graves, como o homicídio, não contam com tamanho espectro punitivo.

Em sentido semelhante, outro excesso da Convenção pode ser encontrado no que tange à criminalização da pornografia infantil por meio informático. É indiscutível a dignidade e necessidade de tutela penal da infância contra a exploração sexual. Nesse aspecto foi muito feliz a Convenção, principalmente quando se tem em conta que o anonimato da internet associado aos aspectos espaciais do crime informático, já acima considerados, facilitaram em muito o mercado da pornografia infantil. O problema coloca-se especificamente quanto a fatos meramente simulados, isto é, quanto à criminalização de material pornográfico em que uma pessoa *aparenta* ser menor de idade, quando na realidade não o é, ou em que a imagem, denominada de realística, também não é real, mas sim metamorfoseada por computadores ou integralmente produzida por computador (art. 9.º 2 da Conv.).[40]

---

[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] A ley especial contra los delitos informaticos en Venezuela, por exemplo, em seu artículo 10, prevê, com pena de três a seis anos de prisão, o crime de fabricação, distribuição ou venda de equipamentos destinados à vulnerar ou eliminar a segurança de qualquer sistema que utilize tecnologias da informação (VENEZUELA. Lei n. 48, de 30 de outubro de 2001. *Lei especial contra os delitos informáticos*. Gaceta Oficial n. 37.313, 30 out. 2001). Pena demasiadamente severa para um ato preparatório. A título de comparação, no mesmo país, a pena do crime de furto é de seis meses a três anos de prisão.

[40] No Brasil, em sentido semelhante, também, o Estatuto da Criança e do Adolescente que, em seu artigo 241-C, criminaliza a conduta de simulação de criança ou adolescente em sexo explícito ou pornográfico, por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra

Em ambos os casos, não há um menor envolvido. O bem jurídico não é lesado nem exposto a perigo, ainda que nos amplos limites de um crime de perigo abstrato. O que se tem aqui é a proibição de uma conduta meramente imoral, emanação de um nítido *direito penal de autor*, e, por isso, insuscetível de ser recepcionada nos quadros de um direito penal democrático. Meras imoralidades, desprovidas da mais ínfima periculosidade objetiva, não podem ser objeto de criminalização.[41] O argumento aduzido pelo Relatório Explicativo da Convenção, no sentido de que a pedofilia simulada poderia vir a seduzir crianças a participar de atos semelhantes[42] é absolutamente equivocado. Se o objetivo é criminalizar a sedução de menores, deve ser essa (seduzir), e não outra, a conduta a ser criminalizada. A presunção de efeitos – questionável presunção, diga-se – não pode substituir a criminalização direta da conduta que se deseja proibir. E, principalmente, quando a descrição típica é manifestamente desconectada da conduta (seduzir) e dos efeitos (risco de ser seduzido) que se desejam evitar. Observe-se que, em momento algum, o referido dispositivo menciona a alegada pretensão final, mencionada apenas no Relatório Explicativo. Tudo a indicar que, ao fim e ao cabo, o que verdadeiramente se tem aqui é, em realidade, uma proibição de cunho exclusivamente moral.

---

forma de representação visual. Aqui, não há a necessidade da prática, pela criança ou do adolescente, de qualquer das condutas descritas no tipo, basta que haja, apenas, a utilização de sua imagem, de forma simulada ou adulterada, para caracterizar o tipo penal.

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

42 COE, Introdução, n. 102.

4. A título de conclusão

Vinho velho em garrafa nova. Expressão que, conquanto bem ilustre a questão dos crimes informáticos, por vezes menospreza o impacto que a matéria de regulação e a sua expressão concreta pode vir a produzir em elementos tradicionais da dogmática penal.

A informática desconstrói as perspectivas tradicionais de tempo e espaço, reivindicando um novo olhar acerca das regras de competência da aplicação da lei penal e da sua coexistência em âmbito internacional. Regras essas que acabam por questionar, inclusive, a usual compreensão de figuras dogmáticas como os delitos de perigo abstrato. Isso por um lado. Por outro, o resgate da dimensão material do ilícito, normalmente descuidada em tempos como o nosso – tempos de entronização dos ideias de segurança e eficiência –, faz-se indispensável para reequilibrar a perene tensão entre liberdade e segurança. A teoria do crime como ofensa ao bem jurídico, a despeito da crítica que lhe é dirigida principalmente no âmbito do *Nebenstrafrecht*, ainda se faz absolutamente indispensável como elemento de identificação e compreensão do conteúdo material do injusto e, assim, também do âmbito do tipo dos crimes informáticos.

Esses são apenas alguns dos aspectos dogmáticos de particular relevo que colocam a denominada criminalidade informática e que, nos estreitos limites deste escrito, foram objeto da nossa reflexão. Reflexão essa, todavia, que parte de uma precisa premissa. A de que o inevitável avanço do direito penal a novos espaços de conflitualidade não significa e não deve significar a erosão de seus conceitos básicos e dos elementos que lhe confere identidade. Muito pelo contrário. A ideia desenvolvimento inerente a qualquer ciência, de modo a fazer frente aos desafios do seu

tempo, só faz sentido se respeitados os limites formais e materiais que lhe conferem forma e identidade. Esse é o verdadeiro desafio. Um desafio marcado pela responsabilidade e pelo equilíbrio, mas também, e fundamentalmente, pelo respeito aos direitos e garantias que conferem feição ao direito penal de qualquer tempo.

Referências

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.