

CRIMES INFORMÁTICOS: POSSIBILIDADES DE CONSTRUÇÃO DE UM MODELO NORMATIVO DE GOVERNANÇA DO CIBERESPAÇO

CYBERCRIMES: POSSIBILITIES ON BUILDING
A NORMATIVE MODEL OF CYBERSPACE
GOVERNANCE

*Salette Oro Boff

**Vinícius Borges Fortes

Resumo: Uma das marcas da evolução da humanidade se reflete na capacidade de transmitir informações. Junto a isso, o desenvolvimento tecnológico na área da informação e comunicação, facilitou o acesso ao conhecimento, nos mais diversos pontos do planeta. O ciberespaço, oferece novas e diferentes possibilidades de futuro, trazendo significativos desafios para o direito. Nesse contexto, a pesquisa investiga as contribuições apresentadas nos Relatórios e Resoluções da Seção Direito Penal Parte Geral, preparatória ao XIX Congresso Internacional de Direito Penal da AIDP – Associação Internacional de Direito Penal, que assinalam os principais pontos de convergência e divergência para a construção de um modelo normativo de governança e tutela penal do ciberespaço, a partir do mapeamento crítico. Assim, o trabalho tem como objetivos observar e mapear a interação legislativa no tocante ao tema dos crimes informáticos; e observar e mapear os resultados dos referidos relatórios e resoluções. O método utilizado no presente trabalho foi o dedutivo e a técnica da pesquisa bibliográfica.

Palavras-Chave: Ciberespaço, Sociedade da informação; Direito penal; Crimes informáticos.

Abstract: One of the hallmarks of human evolution is the ability to transmit information. Conjointly, technological development, in the area of information and communication, has facilitated access to knowledge in various parts of the world. Even though cyberspace offers new and different possibilities for the future, it can and does create considerable legal challenges. The many reports and resolutions of the Criminal Law Section – General Part, XIX International Congress of Criminal Law IAPL – International Association of Criminal Law, highlights important points, which converge and diverge, in the construction of a

* Pós-Doutora pela Universidade Federal de Santa Catarina (UFSC). Doutora em Direito pela Universidade do Vale do Rio dos Sinos – RS (UNISINOS). Professora e pesquisadora do Programa de Mestrado em Direito da Faculdade Meridional – RS (IMED). E-mail: salete.oro.boff@terra.com.br.

** Doutor em Direito pela Universidade Estácio de Sá – RJ (UNESA), Mestre em Direito pela Universidade Caxias do Sul – RS (UCS). Professor da Faculdade Meridional – RS (IMED). Pesquisador Membro do Grupo de Pesquisa em Direito e Desenvolvimento. Estudante vinculado ao GE-DAPI – Grupo de Estudo em Direito Ambiental e Propriedade Intelectual, certificado pela Universidade Federal Fluminense (UFF). E-mail: viniciusfortes@imed.edu.br.

normative model, based on critical mapping, for governance and criminal protection in cyberspace. Deductive reasoning and bibliographical research were the methods used in this study. Keywords: Amitai Etzioni. Communitarism. Condensed social right. Georges Gurvitch.

Keywords: Cyberspace; Information society; Criminal law; Cybercrimes.

Como citar: BOFF, Saete Oro; FORTES, Vinícius Borges. Crimes informáticos: possibilidades de construção de um modelo normativo de governança do ciberespaço. *Scientia Iuris*, Londrina, v. 20, n. 1, p. 59-78, abr. 2016. DOI: 10.5433/2178-8189.2016v20n1p59. ISSN: 2178-8189.

INTRODUÇÃO

O ciberespaço (espaço virtual), é um ambiente social, formado pelo fluxo de informações e mensagens transmitidas entre computadores, constituindo-se como uma rede aberta na qual qualquer pessoa pode ter acesso com a possibilidade de interagir, gerar dados, navegar e estabelecer relações na rede, por meio de provedores de acesso pelos quais se realizam várias atividades como o correio eletrônico; a computação de longa distância, o comércio eletrônico, o lazer, a pesquisa e outros.

No ambiente da rede, todos podem se comunicar com todos. Basta possuir um dispositivo de rede, que nos dias de hoje pode ser um computador, um tablet ou um smartphone. Ampliou-se a facilidade de acesso a informação armazenada em dispositivos, quer se trate de informações livremente disponíveis, quer se trate de informações e dados pessoais de ordem privada.

Nesse contexto, de inegável evolução das tecnologias, o avanço da Internet e a constituição do ciberespaço carecem de uma análise jurídica, normativa, sociológica, cultural e, até mesmo, psicológica. Com a evolução dos recursos da Internet, é oportuna a reflexão quanto aos insumos contributivos à cultura, acesso e democratização da informação, valorização da diversidade e o processo de inclusão digital.

Contudo, também é indispensável refletir sobre os problemas jurídicos decorrentes da massificação do uso da Internet. Assim, o estudo crítico no entorno do tema dos direitos à privacidade e à proteção aos dados pessoais é relevante para o meio jurídico, sobretudo quando se trata de uma reflexão frente aos marcos regulatórios do ciberespaço, indo de encontro com as premissas de criação da Internet, que pressupõem a não regulação.

No Brasil estudos se ocupam dos reflexos da Internet sobre os institutos de direito do consumidor e da necessidade de regulação da Internet em matéria penal, para fins de tratamento adequado aos denominados cibercrimes. Nesse sentido, o confronto entre a evolução tecnológica, o direito e os marcos regulatórios para o ciberespaço é inevitável para uma melhor compreensão da sociedade da informação, ou da sociedade em rede. Assim, a pesquisa se propõe a analisar o uso de tecnologias da informação e comunicação (TICs) com a finalidade de cometer crimes, denominados cibercrimes ou crimes informáticos.

Para tanto, é indispensável refletir se a construção de um modelo normativo de governança do ciberespaço e tutela penal do ciberespaço são suficientes para resolver os conflitos cada vez mais frequentes que se originam desse espaço.

Ademais, é fundamental pensar no caso brasileiro, partindo-se da construção da Lei de Crimes Informáticos (Lei n.º 12.737/2012), bem como o Marco Civil da Internet (Lei n.º 12.965/2014), sobretudo em relação ao cumprimento das premissas de construção da Web, sem que ocorram rupturas paradigmáticas com a arquitetura de rede adotada com a sua constituição e constante adaptação que culminou na constituição da cibercultura e do ciberespaço.

A pesquisa desenvolve o método de análise do mapeamento crítico¹, analisando comparativamente a legislação brasileira relacionada aos crimes informáticos e as perspectivas sob o olhar do direito penal internacional. Assim, a pesquisa adota como paradigma de análise os Relatórios e Resoluções do XIX Congresso Internacional de Direito Penal da AIDP – Associação Internacional de Direito Penal, que se adotou o hodierno tema da “Sociedade da Informação e o Direito Penal”. O mapeamento crítico proposto nessa pesquisa leva em consideração a existência de recentes marcos regulatórios para a governança do ciberespaço e da tutela penal dos crimes informáticos no Brasil.

Com essas considerações, pretende-se buscar resposta a seguinte indagação: com a finalidade propor avanços no estudo da regulação e tutela dos crimes cometidos no ciberespaço, quais foram os principais pontos de convergência e divergência apresentados pelos relatórios e resoluções da Primeira Seção preparatória ao XIX Congresso Internacional de Direito Penal da AIDP – Associação Internacional de Direito Penal?

A pesquisa tem como objetivos: (i) observar e mapear a interação legislativa no tocante ao tema dos crimes informáticos; (ii) observar e mapear os resultados dos relatórios e resoluções da Primeira Seção preparatória ao XIX Congresso Internacional de Direito Penal da AIDP – Associação Internacional de Direito Penal.

Assim, a relevância do estudo concentra-se na evidência de que no contexto global mesmo com a evolução das tecnologias que contribuem para o avanço do ciberespaço, ainda não se conferiu suficientemente a devida relevância à análise jurídica, normativa, sociológica, cultural e até mesmo

¹ O termo mapeamento pode ser entendido como uma versão devidamente revista de uma análise analógica sem maiores questionamentos, efetuada rente à realidade, ou em outras palavras, a forma de análise jurídica não implica qualquer proposição transformadora para o direito. Mapeamento é a tentativa de descrever em detalhes a microestrutura juridicamente definida da sociedade com relação a seus ideais também articulados juridicamente. O segundo momento desta prática de análise deve ser chamado de crítica, isto é, uma versão revisada do que os juristas racionalistas desprezam como sendo a transformação da análise jurídica em conflito ideológico. Sua tarefa é explorar em detalhe as relações entre os arranjos institucionais da sociedade tais como representadas pelo direito, e os ideais ou programas professados por esses arranjos institucionais, na medida em que são frustrados ou cumpridos. (UNGER, 1996, p. 130).

psicológica, quanto à quanto à necessidade reflexão quanto à instituição de marcos regulatórios para a tutela dos crimes informáticos, ou seja, cometidos no ciberespaço.

E é justamente nesse contexto em que o estudo apresentado elucidará os conceitos fundamentais do ciberespaço, das perspectivas do direito penal brasileiro e do direito penal internacional, de modo a apresentar os resultados obtidos a partir dos relatórios e resoluções da Primeira Seção preparatória ao XIX Congresso Internacional de Direito Penal da AIDP – Associação Internacional de Direito Penal.

1 EM BUSCA DE UMA DEFINIÇÃO DO CIBERESPAÇO

A pesquisa tem diversas variáveis de natureza epistemológica, que perpassam necessariamente pela relativização da teoria do direito em virtude de um novo contexto global e social com o avanço da tecnologia da informação e comunicação. De acordo com Lessig (2006), um dos precursores do Cyberlaw na Stanford University, o conceito de ciberespaço varia rapidamente, sobretudo em razão da identidade evidenciada no tempo e no espaço de acordo com os objetivos de uso da rede pelos usuários.

O ciberespaço aqui referido corresponde ao espaço constituído por usuários e infraestrutura de rede na Internet. Como se sabe, a Internet trilhou suas primeiras experiências em 1969, a partir da criação do ARPANET – The Advanced Research Projects Agency Network, com a finalidade de atender demandas do Departamento de Defesa dos Estados Unidos da América, sobretudo em virtude das incertezas bélicas da Guerra Fria. A partir disso, as conexões em rede cresceram significativamente, até a criação no final da década de 1980 da World Wide Web (WWW), pelo físico Tim Berners-Lee e, no início da década de 1990, o desenvolvimento dos primeiros softwares para navegação em páginas da Internet (VASCONCELOS, 2003).

Com a evolução da tecnologia e dos recursos vinculados à rede mundial de computadores, a World Wide Web, ou Internet como ficou popularizada, é conveniente a reflexão quanto aos insumos contributivos à cultura, acesso e democratização da informação, valorização da diversidade e o processo de inclusão digital. Contudo, também é indispensável promover reflexões voltadas aos problemas jurídicos advindos da evolução tecnológica, sobretudo decorrentes da massificação do uso da Internet.

Para exemplificar tal evolução e o reflexo das tecnologias sobre a

sociedade, Lessig (2006) menciona o discurso intitulado “Declaração de Independência para o Ciberespaço” proclamado logo após o rompimento da cultura bipolar com o fim da Guerra Fria pelo compositor do Grateful Dead, banda de Rock dos anos 1960, John Perry Barlow, que também é fundador da EFF – Eletronic Frontier Foundation, uma organização não-governamental que tem como escopo a defesa dos interesses dos usuários da Web, no qual pronuncia:

Governos da Era Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do ciberespaço, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não tem soberania onde nos reunimos (BARLOW, 2011).

A partir disso, é possível identificar uma constante mudança sobre a percepção do ciberespaço e das possibilidades de regulação e governança, sobretudo no que diz respeito ao alcance de instrumentos normativos que assegurem uma visão ampliada da tutela penal dos crimes informáticos, ou seja, cometidos no ciberespaço (BOFF; FORTES, 2014).

Portanto, o confronto entre a evolução tecnológica, o direito e os marcos regulatórios para o ciberespaço, em especial no contexto brasileiro, é inevitável para uma melhor compreensão da sociedade da informação, ou como refere Castells (2002), da sociedade em rede. Aliás, de acordo com o referido autor, na sociedade em rede há a predominância de um espaço dotado de fluxos informacionais, que se sobrepõem sobre os espaços físicos que constituíram as sociedades pré-modernas e, com isso, tem se tornado a manifestação espacial dominante nas sociedades atuais.

Nessa órbita, promover o estudo crítico no entorno do tema da tutela penal dos crimes informáticos cometidos no ciberespaço, sobretudo quando se trata de uma reflexão frente aos marcos regulatórios instituídos em escala global, com o objetivo de estabelecer parâmetros normativos que alcancem diferentes jurisdições no âmbito do ciberespaço.

No Brasil, como em outros Estados, a tutela penal dos crimes informáticos é tratada por legislações especiais que enfrentam temas como a invasão de dispositivo informático, a interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública e a falsificação de documento particular.

Ora, se há previsão normativa pátria, por que discutir tal tema? É a Lei a alternativa adequada a resolver problemas jurídicos identificados nessa pesquisa? Ao encontro das indagações apresentadas, e em reflexão sobre a solução de conflitos complexos na órbita jurídica, Streck (2011, p. 46) afirma que o Direito não atende a tais demandas

[...] não porque tal ‘complexidade’ não estaria prevista no sistema jurídico, mas, sim, porque há uma crise de modelo [...] que se instala justamente porque a dogmática jurídica, em plena sociedade transmoderna e repleta de conflitos transindividuais, continua trabalhando com a perspectiva de um direito cunhado para enfrentar conflitos interindividuais, bem nítidos em nossos Códigos [...].

Diante de tais premissas, pode-se afirmar que as camadas que compõem o sistema de comunicação da Internet e do meio digital são cada vez mais controladas. Entretanto, permanecem ainda dúvidas sobre quais são os fatores que deve-se considerar efetivos na regulação da Internet (LEMOS, 2005, p. 22). Nesse prisma, é relevante considerar o modelo de análise desenvolvido por Lessig (2006), que trata especificamente dos modos de regulação no que tange ao avanço da tecnologia. Para o doutrinador norte-americano, no início do século XIX o liberalismo dominante se preocupava com a manutenção e a garantia da liberdade e, diante disso, qualquer ameaça à liberdade provocaria o poder do Estado e a sua capacidade de gerar a Lei (LESSIG, 2006).

No contexto da tutela penal dos crimes informáticos, e sobretudo da garantia de direitos no ciberespaço, Lemos (2005) indaga sobre quais seriam os fatores que efetivamente ameaçam a liberdade. De acordo com o autor, no século XIX a resposta seria a Lei. Todavia, complementa o autor, no contexto da tecnologia dos tempos atuais, a Lei deixou de ser o único fator que contribui a limitação ou flexibilização da liberdade dos indivíduos, ou até mesmo para a regulação da sociedade em rede (LEMOS, 2005).

Nesse prisma, Lemos (2005) ressalta que o mesmo questionamento sobre quais fatores ameaçam a liberdade individual na sociedade da informação, é possível encontrar no mínimo quatro respostas: a Lei, as normas sociais, o mercado e a arquitetura ou código. Na concepção do autor, entende-se como lei “todo o conjunto normativo estatal, embasado constitucionalmente, em suas mais diversas naturezas e categorias hierárquicas”. As normas sociais,

incluem os usos e costumes e “qualquer postulação normativa compartilhada por comunidades ou inerente a determinadas situações e circunstâncias”. O contexto do mercado “é o outro fator relevante da regulação, por se tratar do mecanismo predominante de acesso aos bens econômicos”, somado à arquitetura, que é “a estrutura inerente de como as coisas são construídas e ocorrem.” (LEMOS, 2005).

Na percepção de Lessig (2006), na órbita do direito da tecnologia “o código é a Lei”. O que o professor da Stanford University pretende ao lançar tal assertiva é que as linguagens de programação de software alcançam muitas vezes relevância superior às estruturas normativas convencionais na órbita da Internet e da regulação tecnológica. Ao analisar as premissas inovadoras apresentadas por Lessig, Lemos (2005) ressalta que as categorias dogmáticas tradicionais não vislumbram a característica normativa contemporânea proclamada pelo autor, de que o “código é a Lei”. Nesse sentido, a partir da ruptura paradigmática na análise do direito por meio da evolução tecnológica, sobretudo no âmbito do ciberespaço, é possível que sejam rediscutidas controvérsias e posicionamentos pretéritos que se julgavam superados e que sejam propostas questões inéditas fundamentadas em aspectos sociológicos, políticos e econômicos, que “de tão interdisciplinares, põem em risco a própria especificidade do direito.” (LEMOS, 2005, p. 8).

Então tem-se presente que a tutela penal dos crimes informáticos é assunto latente e de fundamental importância na agenda dos Estados. É indispensável elucidar o caso brasileiro, conforme evidenciado na exposição de motivos do Projeto de Lei que propunha o Marco Civil da *Internet*², a Pesquisa Nacional por Amostra de Domicílios, realizada no ano 2009 pelo Instituto Brasileiro de Geografia e Estatística (IBGE), já sinalizava a existência de 68 milhões de usuários de Internet no Brasil, com taxa de crescimento de aproximadamente um milhão a cada três meses. A estatística apresentada representa oportunidades ao país, no entanto, também aponta uma série de riscos, que perpassam por diversos aspectos, dentre os quais estava elencada a carência de legislação específica para a regulação do ciberespaço e a tutela dos crimes informáticos (BRASIL, 2011).

Outrossim, a falta de definição legal específica diante da realidade enfrentada atualmente oportuniza que emanem do Poder Judiciário decisões conflitantes e contraditórias sobre temas que estão diretamente relacionados com o uso da Internet (BRASIL, 2011). De acordo com os elementos elencados na exposição de motivos do projeto de lei do Marco Civil da Internet, com a

ausência de normatização específica, o Brasil convive com diversos riscos, a saber:

- a) da aprovação desarticulada de propostas normativas especializadas, que gerem divergência e prejudiquem um tratamento harmônico da matéria;
- b) de prejuízos judiciais sensíveis, até que a jurisprudência se adeque às realidades da sociedade da informação;
- c) de desencontros ou mesmo omissões nas políticas públicas;
- e
- d) de violação progressiva de direitos dos usuários pelas práticas e contratos livremente firmados.

Observa-se, com isso, a relevância global conferida na atualidade para a tratativa normativa e regulatória para o ciberespaço, em especial no que diz respeito à tutela penal dos crimes informáticos, de modo a conjugar a defesa dos direitos humanos indispensáveis ao livre exercício da democracia que, nos tempos atuais, pressupõem o livre acesso à Internet como o um exercício regular de um direito inerente à condição humana, com a atribuição de sanções em face dos crimes cometidos nesse ambiente.

Aliás, cumpre ressaltar a natureza global da tutela dos crimes informáticos, sobretudo em razão do espaço onde a prática das condutas criminosas se efetivam, não havendo limitações geográficas. Nesse particular, Varella (2013, p. 41-42) explana que:

A internet, de forma específica, e a revolução tecnológica, de forma ampla, possibilitam um acoplamento entre espaços e tempos diferentes no campo do direito e da política. Cada Estado ou comunidade tem tempos próprios neste processo. A relação entre eles não é de maior ou menor evolução, porque trilham seus próprios caminhos. Ocorre um processo de influência mútua, ou irritação mútua, como preferem alguns autores, numa lógica de ampliação do contrato entre os sistemas sociais. Economia, política, ciência e direito possuem

² O Projeto de Lei n.º 2.126/2011 (BRASIL, 2011).

discursos comunicativos próprios que não são antagônicos, mas se complementam. Com a internet, ampliam-se as influências entre outras esferas de construção dos sistemas sociais, antes tipicamente nacionais e estrangeiros, fazendo interagir mais fortemente ideias nacionais, estrangeiras, internacionais, a partir do contato direto e imediato dos atores envolvidos interna e externamente.

Arnaud (2007) também corrobora com essa percepção ao afirmar que a dimensão de “fronteira”, e o que se denomina de “porosidade das fronteiras” esta diretamente ligado com os progressos tecnológicos. Assim, os Estados mantem sua soberania, entretanto com a erosão da autoridade, reduzindo substancialmente o controle de fluxos monetários e de informações transfronteiras.

Relevante destacar, ainda, o que Staffen (2015) refere como o direito global em nível de parceria, ou partnership, no caso da regulamentação e regulação da internet pela ICANN – Internet Corporation for Assigned Names and Numbers, que é uma instituição público-privada, que a partir de uma composição por organizações privadas, desenvolve funções públicas que geram impacto global, visto que a Internet corresponde a um bem jurídico global.

Diante disso, é fundamental observar as perspectivas regulatórias analisadas no âmbito da tutela dos crimes informáticos, o que passará a ser analisado a seguir.

2 DA ANÁLISE JURÍDICA DOS CRIMES INFORMÁTICOS A PARTIR DOS RELATÓRIOS E RESOLUÇÕES PREPARATÓRIAS AO XIX CONGRESSO INTERNACIONAL DE DIREITO PENAL DA AIDP – ASSOCIAÇÃO INTERNACIONAL DE DIREITO PENAL

A Associação Internacional de Direito Penal (AIDP) se constitui como a mais antiga organização mundial composta por especialistas das ciências criminais. A AIDP foi fundada em Paris no ano de 1924, como resultado da reorganização da União Internacional de Direito Penal. (ASSOCIAÇÃO INTERNACIONAL DE DIREITO PENAL, 2014).

A proposta da presente pesquisa reside na análise dos relatórios e resoluções propostas para o XIX Congresso Internacional de Direito Penal

da AIDP, realizado no ano 2014 no Brasil, tendo como temática a “Sociedade da Informação e o Direito Penal”. Cabe salientar, que os congressos da AIDP representam uma ocasião significativa para a discussão temas relevantes e que traduzem o posicionamento da AIDP em questões relacionadas ao direito penal e política criminal, de modo a repercutir para o desenvolvimento dos Estados. (ASSOCIAÇÃO INTERNACIONAL DE DIREITO PENAL, 2014).

A temática da 19ª edição do Congresso Internacional da AIDP é analisada sob quatro perspectivas habituais da Associação, quais sejam: direito penal parte geral, direito penal parte especial, direito processual penal e direito penal internacional. Destaca-se, ainda, que tais análises são desenvolvidas a partir de resoluções e relatórios oriundos dos quatro colóquios preparatórios realizados em Verona/Itália, Moscou/Rússia, Antália/Turquia e Helsinque/Finlândia. (CONGRESSO INTERNACIONAL DE DIREITO PENAL AIDP, 2014).

A seção direito penal parte geral, apresenta três documentos-base: questionário, relatório geral e resoluções. O questionário apresentado trata de temas relacionados à criminalização, técnica legislativa na tutela dos crimes informáticos, limites do anonimato e a internacionalização desses crimes. Em sua essência o questionário delimita o denominado “ciberdelito” como um termo de abrangência das condutas criminais que afetam interesses associados ao uso das tecnologias de informação e comunicação (TICs), tais como o funcionamento adequado de sistemas de computadores e Internet, a intimidade e integridade dos dados armazenados ou transferidos por meio de tais tecnologias ou a identidade virtual dos usuários da Internet. Refere, ainda, que um aspecto característico e comum de todas as figuras de ciberdelitos e da investigação destes reside na relação com sistemas, redes, dados de computadores de um lado e sistemas, redes e dados cibernéticos de outro. Nesse sentido, os ciberdelitos tem relação direta com os computadores em sentido tradicional e também com o ciberespaço e as bases de dados cibernéticas. (WEIGEND, 2014a).

É fundamental mencionar, nesse contexto, que os ciberdelitos, ou cibercrimes como referido por uma parte da doutrina penalista, é dotado de diferentes peculiaridades, que levam em conta níveis de oportunidade por tipo de crime, conforme apresentado por Wall (2003) na matriz abaixo observada:

Quadro 1 - The matrix of cybercrimes: level of opportunity by type of crime (with selected examples)

Crime Types ▶	<i>Crime against machines/ Integrity-related</i>	<i>Crime using machines/ Computer-related</i>	<i>Crimes in the machine/ Content - related</i>	<i>Crimes in the machine/ Content - related</i>
Opportunities ▼	/ Harmful /Trespass	Acquisition/ (Theft /Deception)	Obscenity	Violence
<u>Traditional crime using computers</u> More opportunities for traditional crime	* Phreaking * Chipping	* Frauds * Pyramid schemes	* Trading sexual materials	* Stalking * Harassment (personal)
<u>Hybrid cybercrime</u> New opportunities For traditional crime (e.g., organisation across boundaries)	* Cracking/ Hacking * Viruses * Hactivism	* Multiple large-scale frauds * 419 type fraud * Trade secret theft * ID Theft	* Online Sex trade / * Camgirl sites	* General Hate speech * Organised paedophile rings (Child abuse)
<u>True Cybercrime</u> New opportunities for new types of crime (Sui Generis)	* Spams (list construction and content) * Denial of Service * Information Warfare * Parasitic Computing	* Intellectual Property Piracy * Online Gambling *E-auction scams *Phishing	* Cyber-sex * Cyber-pimping	* Online Grooming * Organised Bomb talk /Drug talk * Targeted hate speech

Fonte: Wall (2003).

Ao encontro da complexidade identificada na matriz de Wall (2003), tornou-se cada vez mais indispensável a análise sobre o futuro da tutela penal dos crimes informáticos, cometidos no ciberespaço. Assim, a partir das respostas ao questionário proposto por Weigend (2014b), apresentadas por dezesseis sistemas jurídicos (Argentina, Bélgica, Brasil, Finlândia, França, Alemanha, Grécia, Hungria, Itália, Japão, Holanda, Polônia, Romênia, Espanha e Turquia), formulou-se um relatório geral tratando de elementos fundamentais para esses sistemas jurídicos, quais sejam: (a) a proteção dos bens jurídicos relacionados com as TICs e os desafios do ciberespaço; (b) a expansão das proibições penais, como por exemplo os atos preparatórios e a posse de materiais; (c) o problema do respeito ao princípio da legalidade, sobretudo a exigência de precisão das proibições penais; (d) as mudanças no conceito de autoria e responsabilidade acessória, em especial em relação aos provedores de acesso e aos provedores de hospedagem de conteúdo; (e) a função do direito penal em relação a outras formas de proteção dos bens jurídicos mediante mecanismos específicos de Internet, como o bloqueio de acesso ou a eliminação de websites; (f) as reações legislativas ao problema de que os usuários de Internet frequentemente permanecem no anonimato; (g) os esforços internacionais realizados para coordenar e harmonizar a legislação em uma área que, por definição, transcende as fronteiras nacionais. (WEIGEND, 2014b).

A respeito das questões observadas no questionário e no relatório geral, é possível identificar nas considerações de Koops (2011) de que a Internet merece

atenção especial por causa de várias características: (a) é global e permite conexões em tempo real entre as pessoas, independentemente da sua localização; (b) o tempo, a distância, e as fronteiras nacionais são muito menos importantes do que no crime tradicional; (c) a Internet, sendo uma rede digital, permite que os dados de processamento de informação e em formas automatizados, quase à velocidade da luz, e em uma escala sem precedentes. Logo, a complexidade dos ciberdelitos é diversa dos crimes cometidos em outros espaços e circunstâncias.

Diante das problemáticas apresentadas, a seção direito penal parte geral apresentou resoluções divididas em cinco grupos: (a) considerações gerais para a legislação penal; (b) alternativas à sanção penal; (c) o princípio da legalidade; (d) a ampliação das leis penais; e (e) a cooperação internacional. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

No que diz respeito ao primeiro grupo, no tocante às considerações gerais para a legislação penal, concluiu-se que as TICs e o ciberespaço criaram interesses específicos que devem ser respeitados e protegidos, a exemplo da integridade e privacidade dos sistemas de TICs e das identidades pessoais no ciberespaço. De acordo com essas considerações, os autores de alguns delitos tradicionais como a fraude, a falsidade e violações aos direitos de autor utilizam as redes TIC e o ciberespaço, o que potencializa a periculosidade da conduta, o que demanda uma aceitação e adaptação por parte dos legisladores, tribunais e sistemas de justiça penal. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

Além disso, dentro das considerações gerais da primeira resolução, concluiu-se que a integridade das redes de TIC e o ciberespaço são vitais para as sociedades modernas, inclusive em relação aos meios de comunicação, e que os comportamentos nocivos ou perigosos nestas áreas podem comprometer interesses fundamentais, e por essa razão é necessário que os Estados criem políticas eficientes sobre proteção das redes de TIC e os interesses atingidos. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

Por outro lado, a resolução pondera a necessidade de evitar o excesso de regulamentação e criminalização do ciberespaço, sob pena de comprometer a liberdade de comunicação que é uma característica própria e genuína do ciberespaço. Além disso, os legisladores devem estar conscientes de que a regulação do comportamento, a partir da criação de leis penais e a imposição de controles desproporcionais no ciberespaço pode interferir nos direitos fundamentais, especialmente a liberdade de expressão e a liberdade de coletar informações. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

Em relação ao segundo grupo, no tocante às alternativas à sanção penal, a

primeira resolução é taxativa ao concluir que é fundamental estimular os usuários de redes de TIC e os fornecedores de sistemas para criar mecanismos de proteção e segurança da rede, incluindo a autorregulação dos provedores. O descuido na tomada de medidas de segurança não deve conduzir à responsabilidade penal por parte dos usuários, exceto se punido pela violação de obrigações específicas para a manutenção da segurança dos dados impostas aos sujeitos responsáveis. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

No mesmo grupo, a primeira resolução pondera que as proibições penais são dotadas de forte reprovação moral e, por essa razão, pode estigmatizar criminosos. Diante disso, é dever dos Estados examinar cuidadosamente se as medidas não-criminais podem ser igualmente eficazes na prevenção de ataques a redes e abuso da liberdade das TICs e do ciberespaço. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

Diante disso, surgem as seguintes propostas: (a) como alternativas viáveis em relação às ordens judiciais, a compensação dos danos às vítimas de acordo com a lei civil, bem como a promoção de instrumentos de justiça restaurativa; (b) a imposição de medidas administrativas, tais como o bloqueio de acesso ou remoção de sites ofensivos, conjugando o efeito dissuasor sem recorrer a lei penal, no entanto, sem a ocorrência de atos desproporcionais que configurem a prática de censura pelas autoridades executivas; (c) de acordo com a necessidade, para efeitos de dissuasão, os legisladores podem também considerar a permissão do armazenamento de dados, sob controle judicial eficaz, para posterior identificação de usuários suspeitos de crimes graves. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

No terceiro grupo de resoluções, vinculado ao debate do princípio da legalidade, concluiu-se que este acaba por exigir das infrações no âmbito das TIC e do ciberespaço são definidos por lei. Refere, ainda, que isso vale também para a definição dos deveres e obrigações dos indivíduos combinados com o resultado de responsabilização penal. Nesse sentido, a resolução recomenda que a legislação empregue termos que definam a conduta proibida com a maior precisão possível, considerando ainda a necessidade de adaptação legal por conta das mudanças tecnológicas, não cabendo aos tribunais estender a interpretação sobre os termos das proibições para além do seu sentido usual. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

O quarto grupo de resoluções, comprometido com a discussão da expansão das leis penais, considerou que em muitas leis foram criminalizados meros atos preparatórios de ataques a interesses das TICs e do ciberespaço,

como a produção, distribuição e posse de malware. A expansão das leis penais é legítima na medida em que os atos preparatórios, como tais, criam um risco dano iminente. Logo, quando os atos preparatórios forem puníveis, a pena deve ser menor do que a prevista para o crime consumado. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

Outros aspectos considerados no quarto grupo estão vinculados à necessidade fazer diferenciações em relação à criminalização da posse de software, a qual não deve conduzir a restrições indevidas sobre o uso legítimo de software, e ao destaque de que a mera posse e exibição de dados pode ser punido somente quando se concretizarem de forma intencional e causem danos diretos e indiretos às pessoas. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

Ainda, em relação à proposta de expansão das leis penais, os provedores de serviços de TIC não deveriam ser obrigados a censurar o conteúdo por eles processado. A responsabilidade penal a esse respeito deve ser limitada a casos que os provedores são alertados, de modo confiável e específico, quanto à existência de conteúdo proibido no seu domínio, e em não havendo medidas razoáveis e imediatas para a restauração da legalidade. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

O quinto e último grupo de resoluções diz respeito à cooperação internacional, que é tema recorrente no debate relacionado aos crimes informáticos. De acordo com a proposta desse grupo, devem ser harmonizadas as políticas globais relacionadas com a justiça criminal para a proteção das redes TIC e os interesses do ciberespaço e do usuário, a fim de assegurar uma proteção eficaz, evitar discrepâncias entre os regulamentos da matéria, melhorar a cooperação internacional e evitar os conflitos de jurisdição. (PROPUESTA DE RESOLUCIÓN AIDP, 2014).

Observa-se, diante disso, que o compromisso assumido pela Associação Internacional de Direito Penal em discutir com propriedade, seriedade e responsabilidade temas hodiernos, como é o caso do direito penal na sociedade da informação, se confirma a partir dos resultados identificados no questionário, no relatório geral e nas resoluções apontadas nos colóquios preparatórios. Ademais, o conteúdo gerado a partir do debate proporcionado em tais oportunidades contribui de forma significativa para a reformulação conceitual do direito penal e a sua relação com os crimes informáticos, sobretudo pela dinâmica de evolução e transformação das condutas delituosas e dos meios aplicados para o cometimento dos crimes dessa natureza.

CONSIDERAÇÕES FINAIS

Há pouco mais de uma década, quando a Internet ainda ensaiava os primeiros passos em território brasileiro, o compositor brasileiro e defensor da liberdade dos direitos no ciberespaço, Gilberto Gil (ROHTER, 2007) referenciou na música “Pela Internet” uma das primeiras impressões do que a rede representava na vida dos usuários: “ Eu quero entrar na rede, Promover um debate, Juntar via Internet, Um grupo de tientes de Connecticut, [...] Eu quero entrar na rede para contatar, Os lares do Nepal e os bares do Gabão”.

Definitivamente vive-se num tempo em que a simultaneidade proporcionada pela Internet oportuniza a vivência de uma experiência revolucionária da comunicação, do relacionamento social e do consumo. No sentido apresentado por Gil, vive-se na era dos websites e a transcendência dos gigabytes nas “nuvens” com a cloud computing. Diante disso, é inegável que as relações estabelecidas no ambiente virtual carecem da análise do direito sob os prismas sociológico, hermenêutico, jurisdicional e do *modus operandi* que a tecnologia instiga a investigar.

O consumidor moderno cada vez mais procura a Internet para realizar transações comerciais, e isso ocorre por diversos fatores, como por exemplo, a otimização do tempo disponível, a tentativa de manutenção da privacidade, a amplitude na realização de pesquisas de preços.

Figura-se uma geração de indivíduos cada vez mais familiarizados com o ato de “googlear”. Sim, “googlear”, da tradução do verbo “to google”, inserido no vocabulário do inglês estadunidense após a transformação do buscador Google em uma das maiores potências em comunicação e informação do Planeta. A Internet e, sobretudo o ato de “Googlear”, trouxeram repercussões das mais diversas na vida individual e em sociedade, colocando em xeque diversos paradigmas da vida pós-moderna: o consumo, as relações sociais, a comunicação e a informação jamais serão as mesmas.

E diante de tais mudanças, é fundamental o desenvolvimento de pesquisas no âmbito do direito penal e a sociedade da informação, de modo a estabelecer um novo olhar sobre os crimes cuja origem se deu no ciberespaço ou sobre ele repercutirão os efeitos nefastos da violação de direitos. Com o estudo desenvolvido foi possível identificar uma série de vulnerabilidades latentes, desencadeadas pelo uso de tecnologias que objetivam a difusão da informação e do conhecimento a partir das TICs, que na análise proposta pela presente pesquisa reside na transformação inerente ao direito penal.

Nesse sentido, a imprecisão jurídica oferecida pelo ordenamento jurídico em escala global, sobretudo em relação à regulação do ciberespaço e à tutela penal dos crimes informáticos, acaba por sujeitar as partes e os conflitos com os quais estão envolvidas à mercê da “consciência” jurisdicional, observando-se uma distância longa do que Streck (2011) defende há tempos, como a busca por uma resposta correta e adequada à Constituição dos Estados.

Diante disso, cabe retomar a problematização da pesquisa a partir da indagação: com a finalidade propor avanços no estudo da regulação e tutela dos crimes cometidos no ciberespaço, quais foram os principais pontos de convergência e divergência apresentados pelos relatórios e resoluções da Primeira Seção preparatória ao XIX Congresso Internacional de Direito Penal da AIDP – Associação Internacional de Direito Penal? Com isso a pesquisa ora desenvolvida, houve um aprofundamento da análise que considerou elementos inseridos na prática dos crimes informáticos em escala global e as iniciativas necessárias que representem uma possibilidade de resposta para as problemáticas apresentadas na Primeira Seção preparatória ao XIX Congresso Internacional de Direito Penal da AIDP.

Portanto, o ciberespaço, de um modo geral, oferece novas e diferentes perspectivas e expectativas do futuro. Há um tempo, quando se assistia a um filme de ficção científica, imaginava-se o futuro que estava por vir. Agora, tem-se impressão que se aproxima da certeza de que o futuro é agora, e nesse futuro presente, indubitavelmente, é necessário promover uma imersão conceitual do Direito no ciberespaço, preservando acima de tudo os direitos fundamentais de todos os partícipes das relações estabelecidas nesse espaço.

REFERÊNCIAS

ARNAUD, André-Jean. **Governar sem fronteiras: entre globalização e pós-globalização**. Rio de Janeiro: Lumen Juris, 2007. v. 2.

ASSOCIAÇÃO INTERNACIONAL DE DIREITO PENAL. **Historia de la asociación internacional de derecho penal**. Disponível em: <http://www.penal.org/?page=mainaidp&id_rubrique=18&lang=es>. Acesso em: 25 abr. 2014.

BARLOW, John Perry. A Declaration of the independence of cyberspace. Disponível em: <<https://projects.eff.org/~barlow/Declaration-Final.html>>. Acesso em: 23 fev. 2011.

BOFF, Salete Oro; FORTES, Vinícius Borges. A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. **Sequência**, Florianópolis, v. 35, n. 68, p. 109-127, 2014.

BRASIL. **Exposição de motivos ao projeto de Lei n.º 2.126/2011**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm>. Acesso em: 24 dez. 2012.

CASTELLS, Manuel. **A sociedade em rede: a era da informação: economia, sociedade e cultura**. São Paulo: Paz e Terra, 2002. v. 1.

CONGRESSO INTERNACIONAL DE DIREITO PENAL AIDP. **Mensagem do presidente da associação internacional de direito penal**. Disponível em: <<http://aidp2014.org/>>. Acesso em: 25 abr. 2014.

KOOPS, Bert-Jaap. The internet and its opportunities for cybercrime. **Tilburg Law School Legal Studies Research Paper Series**, n. 9, 2011. Disponível em: <<http://ssrn.com/abstract=1738223>>. Acesso em: 23 abr. 2014.

LEMONS, Ronaldo. **Direito, tecnologia e cultura**. Rio de Janeiro: FGV, 2005. Disponível em: <http://books.google.com/books?hl=en&lr=&id=xG-2W7YnTfUC&oi=fnd&pg=PA7&dq=DIREITO,+TECNOLOGIA+E+CULTURA&ots=PXCUp6AS7u&sig=2dkpHEIZXv_3UBOaPkho2wMKO58>. Acesso em: 15 jan. 2013.

LESSIG, Lawrence. **Code v2**. New York: Basic Books, 2006.

PROPUESTA DE RESOLUCIÓN AIDP. **Sección I – derecho penal parte general**. In: CONGRESO INTERNACIONAL DE DERECHO PENAL. “SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL” AIDP-IAPL, 19., 2014, Rio de Janeiro. **Anais...** Rio de Janeiro, 2014. Disponível em: <<http://www.penal.org/spip/IMG/SECTION%201%20Resolutions%20ESP.pdf>>. Acesso em: 25 abr. 2014.

ROHTER, Larry. Gilberto Gil hears the future, some rights reserved. **The New**

York Times, New York, 11 Mar. 2007. Disponível em: http://www.nytimes.com/2007/03/11/arts/music/11roht.html?pagewanted=all&_r=0. Acesso em: 29 ago. 2011.

STAFFEN, Márcio Ricardo. **Interfaces do direito global**. Rio de Janeiro: Lumen Juris, 2015.

STRECK, Lenio Luiz. **Hermenêutica jurídica e(m) crise: uma exploração hermenêutica da construção do Direito**. 10. ed. Porto Alegre: Livraria do Advogado, 2011.

UNGER, Roberto Mangabeira. **What should legal analysis become?** New York: Verso, 1996.

VARELLA, M. D. **Internacionalização do direito: direito internacional, globalização e complexidade**. Brasília: UniCEUB, 2013.

VASCONCELOS, Fernando Antonio. **Internet: a responsabilidade do provedor pelos danos praticados**. Curitiba: Juruá, 2003.

WALL, D. S. Mapping out cybercrimes in a cyberspatial surveillant assemblage. In: WEBSTER, K.; BALL, K. (Org.). **The intensification of surveillance: crime, terrorism, and welfare in the information age**. Londres: Pluto, 2003. p. 112-136.

WEIGEND, Thomas. Cuestionario sección I – parte general. In: CONGRESO INTERNACIONAL DE DERECHO PENAL. “SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL” AIDP-IAPL, 19., 2014, Rio de Janeiro. **Anais...** Rio de Janeiro, 2014. Disponível em: <http://www.penal.org/IMG/pdf/Seccion_1_Esp.pdf>. Acesso em: 25 abr. 2014a.

WEIGEND, Thomas. Relación general sección i – parte general. In: CONGRESO INTERNACIONAL DE DERECHO PENAL. “SOCIEDAD DE LA INFORMACIÓN Y DERECHO PENAL” AIDP-IAPL, 19., 2014, Rio de Janeiro. **Anais...** Rio de Janeiro, 2014. Disponível em: <<http://www.penal.org/spip/IMG/SECTION%20I%20General%20Report%20ESP.pdf>>. Acesso em: 25 abr. 2014b.

Como citar: BOFF, Salete Oro; FORTES, Vinícius Borges. Crimes informáticos: possibilidades de construção de um modelo normativo de governança do ciberespaço. *Scientia Iuris*, Londrina, v. 20, n. 1, p. 59-78, abr. 2016. DOI: 10.5433/2178-8189.2016v20n1p59. ISSN: 2178-8189.

Submetido em 29/03/2015

Aprovado em 28/08/2015