A CONVENÇÃO DE BUDAPESTE E AS LEIS BRASILEIRAS[1]

Gills Lopes Macêdo Souza[2]
Dalliana Vilar Pereira[3]

A falta de legislação é o principal problema para a investigação e até mesmo para conseguir criminalizar algumas condutas.
Delegado Felipe T. Seixas (*apud* MAZENOTTI, 2009)

Em redes [de computadores], assim como em outras áreas, a única constante são as mudanças.
Matt Hayden (HAYDEN, 1999, p. XIX)

RESUMO

As redes de computadores e a *Internet* são tão impactantes na vida diária que, assim como as grandes transformações tecnológicas – desde o controle do fogo à era nuclear –, trazem consigo benefícios e mazelas. A tipificação dos crimes cometidos no ciberespaço é imprescindível para que os poderes públicos possam acompanhar a dinâmica de um mundo globalizado. O presente artigo pretende relatar o que é e qual a importância de um provável ingresso do Brasil à Convenção de Budapeste (Convenção sobre o Cibercrime, 2001), uma vez que, tornado-se membro da supracitada Convenção, ele adentraria num Regime Internacional de combate ao cibercrime, facilitando, assim, uma cooperação maior com outros países que sofrem das mesmas práticas ilícitas, mas que possuem leis diferentes. Todavia, este trabalho propõe ressalvas a um ingresso sem discussão com a sociedade e ao Projeto de Lei proposto pelo Senador Eduardo Azeredo, que tipifica as práticas do cibercrime, mas que fere também a liberdade do cidadão comum.

Palavras-chave: Cibercrime. Convenção de Budapeste. Legislação. Senador Eduardo Azeredo.

[1]Trabalho apresentado e aceito para publicação nos Anais do *1° Seminário Cibercrime e Cooperação Penal Internacional*, organizado pelo CCJ da UFPB e pela *Association Internacionale de Lutte Contra la Cybercriminalite* (França), João Pessoa/PB, maio de 2009.

[2] Graduando da turma pioneira de Relações Internacionais (UEPB), tecnolando em Redes de Computadores (IFPB), Coordenador de Produção da Integrativa.com.br, membro do grupo de pesquisa GEH@ETE (UEPB/CNPq) e Assessor de TI da Empresa Júnior de Relações Internacionais. Correio eletrônico: gills@gills.com.br.

[3] Graduanda em Direito (UFPB), cursou Relações Internacionais na UEPB até o quinto período. É monitora-bolsista da disciplina *Direito Constitucional* na UFPB. Correio eletrônico: dalliana.vilar@gmail.com.

1 INTRODUÇÃO

Com o surgimento da *Internet*, muitas possibilidades e oportunidades foram deslumbradas, sobretudo no que diz respeito ao *encurtamento* das distâncias e à obtenção, manipulação e armazenamento de informações. Com sua popularização, no final da década de 1990 e início dos anos 2000, surgia a necessidade de entender aquele espaço virtual, nascente e fecundo, sob prismas diversos: antropológico, econômico, social, linguístico, cultural e outros. A interdisciplinaridade se apresentava como uma poderosa arma para prover conhecimentos cada vez mais precisos e eficientes na obtenção de respostas[4]. Com isso, várias áreas distintas das Ciências Exatas – mais especificamente da Tecnologia da Informação (TI) – tiveram que se debruçar sobre um emaranhado de códigos binários e beber diretamente da fonte da Revolução Tecnológica.

Da popularização, ou seja, da imergência do indivíduo no novo espaço, se dá o que os autores deste trabalho chamam de *cibersocialização* do mesmo, ou seja, a imergência desse novo espaço no indivíduo. Surge, então, o *ciberespaço*, e, com ele, uma *cibercultura*.

Assim como o espaço real, o *ciberespaço* se constitui num ambiente de trocas sociais, econômicas, morais etc. e, ao mesmo tempo, de mudanças cada vez mais rápidas no *modus operandi* de comunicação, informação e interação. No último caso, não mais diretamente com humanos e, sim, através das máquinas, tais trocas se realizam por meios audiovisuais (*hardwares* e/ ou *softwares*) .

Para efeito de comparação com outro extraordinário invento tecnológico, que é o telefone, o *PhD* Lori Valigra (THING, 2003, XXI) ressalta, em sua mais famosa citação, que o telefone levou 75 anos para chegar à marca de 50 milhões de usuários, enquanto que a *Internet* levou apenas quatro para fazer o mesmo. Portanto, a *Internet* passa, desde os últimos anos do século XX, a fazer parte dos hábitos populares, de Ocidente a Oriente, de Norte a Sul. Como uma grande explosão, ela invade o lar, a academia e a indústria, e reivindica autonomia para se manter em constante expansão. Com isso, novos cenários surgem, novos atores se apresentam e novas perspectivas são postas para os contratos sociais. Emerge, dentre outros efeitos colaterais desta revolução técnico-social, o cibercrime e, com ele, indagações sobre como combatê-lo num espaço totalmente desfigurado daquele conhecido pelo Estado Moderno, o qual, por sua vez, foi engendrado essencialmente na base territorial.

[4] Algo já visto durante a chamada *Revolução Behaviorista*.

2 O ciberespaço livre e anárquico[5]

> *(...) não há fronteiras demarcadas no ambiente cibernético. Isso derruba um dos principais pilares do chamado Estado Moderno.* MEDEIROS, 2002, p. 147.

No final dos anos 1980 e início dos 1990, o pesquisador britânico do CERN – *Conseil Européen pour la Recherche Nucléaire* (Conselho Europeu para a Pesquisa Nuclear), *Sir* Tim Berners-Lee, escreve[6] sobre uma possível e viável proposta de interconectar redes de computadores[7] numa única e gigantesca rede: a rede mundial de computadores. Surgia, assim, teórica e empiricamente, a *Internet*[8].

Também na década de 1980, o ex-programador do MIT, Richard Stallman, consolidava as instituições filosóficas, técnicas e jurídicas do *Movimento Software Livre*, as quais serviram de base para muitas das grandes invenções e programas que ajudariam a popularizar a *Internet* anos à frente: a Licença GNU, o sistema operacional GNU/Linux, o servidor *web* Apache, o navegador Firefox, dentre outros.[9]

Berners-Lee projetara a *Internet* para funcionar de forma descentralizada e o mais universal possível, afinal, os protocolos de transmissão e linguagens que a suportavam (*TCP/IP*[10], *HTTP*[11], *HTML*[12]) também eram/são livres e abertos à sociedade, acadêmica ou não. Logo, é possível acessar uma página HTML hospedada numa máquina X a partir de um terminal Y, não importando o tipo/marca deste. Uma espécie de *ciberisonomia* se constituíra.

---

[5] Esta parte é baseada no clássico das Relações Internacionais *A Sociedade Anárquica* (BULL, 2002) e nos discursos e escritos do programador estadunidense Richard Stallman, disponíveis em seu sítio pessoal, Stallman.org.

[6] Para ler proposta original, ver: LEE-BERNERS, Tim. **Information Management: A Proposal**. Disponível em: < http://www.w3.org/History/1989/proposal.html >. Acesso em: 13 maio 2009.

[7]Os quais, à época, se comunicavam isoladamente entre si,

[8] Ou *WWW* ou *World Wide Web* ou *Web.*

[9] Para melhor entendimento sobre o Movimento *Software* Livre e suas implicações sócio-econômico-políticas, no âmbito governamental e da inclusão social, vide SILVEIRA, Sérgio A.; CASSINO, João (Org.). ***Software* Livre e Inclusão Social**. São Paulo: Conrad, 2003.

[10] *Transmission Control Protocol/Internet Protocol*: linguagem básica de comunicação ou protocolo da rede mundial de computadores (THING, 2003, p. 853).

[11] *HyperText Transfer Protocol*: conjunto de regras para troca (permuta) de arquivos multimídia na rede mundial de computadores (THING, 2006, p. 407).

[12] *HyperText Markup Language*: conjunto de códigos inserido num arquivo destinado a uma página da rede mundial de computadores (THING, 2003, p. 401).

Stallman, por sua vez, proclama que todos os *softwares* devem ser *livres*, ou seja, ter seu código-fonte aberto para que qualquer pessoa possa acessá-lo, modificá-lo e redistribuí-lo sem implicações vindouras. Ele projeta uma *cibersociedade* mutuamente sustentada em princípios éticos e morais[13]. Essa anarquia facilitaria as relações entre os membros do *ciberespaço* e constituiria *micronações* e culturas engendradas dentro desse espaço, como é o caso dos *hackers, crackers, geeks* e das diversas redes de fóruns, por exemplo.

É conveniente ressaltar, nesse ínterim, que o conceito ontológico de anarquia possui alguns significados que, mal interpretados, podem levar à uma conclusão distinta da proposta pelos autores deste trabalho. Segundo o *Cambridge Dictionary*, anarquia significa a falta de organização e controle, especialmente na sociedade devido a uma ausência ou insuficiência de governo (*Cambridge University*, 2003, tradução nossa)[14].

Essa definição satisfaz completamente a perspectiva deste trabalho, uma vez que, ao contrário de *caos total* ou *terra de ninguém*, o conceito de anarquia, como vastamente aplicado ao sistema internacional, pelas Escolas de Relações Internacionais, torna a percepção do conceito de sistema como não-hierarquizado, ou seja, sem um ente centralizador das tomadas de decisões[15]. Fato este que produz constrangimentos e outras idiossincrasias aos atores, como a cooperação internacional.

3 A Convenção de Budapeste

> *O Estado não desaparece, porém. É apenas redimensionado na Era da Informação. Prolifera sob a forma de governos locais e regionais que se espalham pelo mundo com seus projetos, formam eleitorados e negociam com governos nacionais, empresas multinacionais e órgãos internacionais. (...) O que os governos locais e regionais não têm em termos de poder e recursos é compensado pela flexibilidade e atuação em redes.*
>
> CASTELLS, 2007.

[13] Algo que lembra o chamado "Primeiro debate das RI", onde, de um lado, estariam os chamados *idealistas* com suas visões de como o mundo *deveria ser*; e, do outro, os realistas, que viam na natureza hobbesiana dos Estados, ações que os faziam perceber como o mundo *realmente* era.

[14] *Lack of organization and control, especially in society because of an absence or failure of government.*

[15] Existe um consórcio de empresas, pesquisadores e colaboradores de todo o mundo chamado W3C (*World Wide Web Consortium*), do qual Berners-Lee faz parte, que propõe implementações e normas para tornar a *Internet* ainda mais acessível e universal. Tais normas, as *Web Standards*, não têm força de lei; são de caráter técnico e fortemente aconselhadas pelo W3C; nunca impostas.

Criada em 2001, na Hungria, pelo Conselho da Europa, e em vigor desde 2004, após a ratificação de cinco países, a Convenção de Budapeste, ou Convenção sobre o Cibercrime, engloba mais de 20 países (EDERLY, 2008) e tipifica os principais crimes cometidos na *Internet*.

Segundo seu Preâmbulo, a Convenção prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada". Ademais, ainda em seu escopo inicial, ressalta o obrigatório respeito: (i) à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa (1950); (ii) ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU (1966); à (iii) Convenção das Nações Unidas sobre os Direitos da Criança (1989); e (iv) à Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil (1999).

O Tratado de 2001 possui quatro Capítulos (Terminologia, Medidas a Tomar a Nível Nacional, Cooperação Internacional e Disposições Finais, respectivamente) e 48 artigos encorpados num texto de fácil compreensão, sobretudo porque não traz informações deveras técnicas.

O principal destaque da Convenção é que ela define (Capítulo I) os cibercrimes, tipificando-os como infrações contra sistemas e dados informáticos (Capítulo II, Título 1), infrações relacionadas com computadores (Capítulo II, Título 2), infrações relacionadas com o conteúdo, pornografia infantil (Capítulo II, Título 3), infrações relacionadas com a violação de direitos autorais (Capítulo II, Título 4). Todos dentro do Direito Penal Material.

Matérias do Direito Processual são as que se seguem: âmbito das disposições processuais, condições e salvaguardas, conservação expedita de dados informáticos armazenados, injunção, busca e apreensão de dados informáticos armazenados, recolha em tempo real de dados informáticos e interceptação de dados relativos ao conteúdo.

Competência e Cooperação Internacional são vistas no Artigo 22º, o qual aponta quando e como uma infração é cometida, além de deixar a critério das Partes a "jurisdição mais apropriada para o procedimento legal" (CONVENÇÃO SOBRE CIBERCRIME, p. 14).

Extradição é um assunto tratado no Artigo 24º, a qual "ficará sujeita às condições previstas pelo direito interno da Parte requerida ou pelos tratados de extradição aplicáveis" (*idem*, p. 15).

Tal acordo parte da premissa de que o combate ao cibercrime deve ser realizado através de um Regime Internacional[16]. Desse princípio, pode se partir para outro:

> *A prática do crime é tão antiga quanto a própria humanidade. Mas o crime global, a formação de redes entre poderosas organizações criminosas e seus associados, com atividades compartilhadas em todo o planeta, constitui um novo fenômeno que afeta profundamente a economia no âmbito internacional e nacional, a política, a segurança e, em última análise, as sociedades em geral.* CASTELLS, 2007, p. 203.

É notório que, com o fenômeno da globalização e da popularização da *Internet*, as fronteiras *indelimitáveis* do ciberespaço abrigaram não apenas criações em prol da cidadania e da participação universal (por exemplo: leitores de telas para cegos, teclados e aparelhos especiais para deficientes físicos, fóruns de discussão etc.), como também facilitaram que crimes, comumente praticados no "mundo real", se moldassem ao ciberespaço.

Mais uma vez se retoma Castells, quando este afirma, por exemplo, que a "internacionalização das atividades criminosas faz com que o crime organizado (...) estabeleça alianças estratégicas para cooperar com as transações pertinentes a cada organização, em vez de lutar entre si" (CASTELLS, 2007, p. 205). Hoje, há um leque de ferramentas *on-line* que, em sinergia e bem orquestrado, pode colocar em risco não apenas indivíduos específicos, mas também Estados. Por exemplo, uma organização terrorista pode planejar um atentado e, para tal, utilizar-se dos seguintes meios:

- troca de mensagens criptografadas via: bate-papos, correio eletrônico, mensageiros instantâneos, redes sociais etc.[17]

- escolha do local, através de programas GPS, mapas *on-line*, previsão meteorológica, tráfego da malha rodoviária através de câmeras ao vivo etc.

- obtenção/compra de artefatos através de sítios virtuais que vendam produtos de "segunda-mão" e/ou que não declaram impostos.

Sob esse prisma, a *Internet* parece ser um celeiro propício para a proliferação do que há de pior na humanidade. Porém, esses perigos reais são as grandes exceções do mundo virtual, que a

[16] Regime Internacional é entendido como um mecanismo que ajuda a estabilizar o sistema internacional, e que é definido como um conjunto de normas, regras e procedimentos que regulam as relações estatais numa área específica. Neste caso e em específico, no combate ao cibercrime.

[17] O leitor atente para o plural dos produtos/serviços.

Convenção ora em estudo visa a combater. O grande debate, que será melhor visto na próxima parte deste trabalho, diz respeito às liberdades e direitos das pessoas que não fazem parte dessa minoria criminosa. Elas também serão punidas? É nesse sentido que Castells afirma que "a pornografia infantil *on-line* é um dos principais argumentos favoráveis à criação de mecanismos de censura[18] na *Internet*." (CASTELLS, 2007, p. 185).

Tal afirmação remonta à CPI da Pedofilia, presidida pelo parlamentar Magno Malta, no ano de 2008, à qual uma grande empresa de tecnologia estava se negando a fornecer dados de supostos pedófilos, uma vez que, ao se cadastrar num de seus sítios virtuais, o internauta se assegura de que suas informações não são repassadas a terceiros. Após muitas negociações, depoimentos e intervenção do Ministério Público Federal, a empresa multinacional cooperou. Tal demora se deu pelo fato de que, apesar do suposto crime de pornografia infantil ter envolvido brasileiros, o servidor que hospedava as fotos se encontrava noutro Estado, portanto, noutra jurisdição, fora, portanto, do alcance das leis brasileiras.

Nesse caso, por exemplo, se o Brasil fosse membro da Convenção de Budapeste[19], provavelmente, a cooperação com autoridades estadunidenses teria acelerado o desenvolvimento da CPI, possibilitando uma repressão mais célere ao delito.

3.1 Possível ingresso brasileiro

Tendo em vista o relativismo da Convenção de Budapeste, bem como a flexibilidade do seu texto em, sobretudo, apontar caminhos e não propor soluções rígidas no que tange às controvérsias[20] e resolução de litígios, surgem, então, algumas dúvidas: por que o Brasil não adere à Convenção de Budapeste? O fato de o Brasil não fazer parte da Convenção o impede de criar suas próprias leis de combate ao cibercrime?

Como não foi um dos signatários do Tratado e como bem lembrou o Secretário-Geral do Ministério das Relações Exteriores/Itamaraty, Samuel Pinheiro Guimarães, o Brasil não pode

[18] Alertados pelo professor Alexandre Belo, durante a apresentação deste artigo, os autores tomaram precaução ao mencionar a palavra "censura" no mesmo. Ficam aqui os agradecimentos ao supracitado professor.

[19] Vide Título 3 do Capítulo 3, "Princípios Gerais relativos ao auxílio mútuo", e, sobretudo, o Título 4 do mesmo Capítulo, "Procedimentos relativos aos pedidos de auxílio mútuo na ausência de acordos internacionais aplicáveis".

[20] Controvérsia é definida por SOARES (1999, p. 20) como "qualquer diferença de qualificação e/ou avaliação de fatos, conjuntamente ou em separado da interpretação e/ou aplicação de normas internacionais".

simplesmente aderir à Convenção, e, sim, ser convidado pelo Comitê de Ministros do Conselho Europeu. No texto original, em seu Artigo 37º – Adesão à Convenção –, é possível se constatar o sobredito: "(...) O Comitê de Ministros do Conselho da Europa pode(...) convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção" (CONVENÇÃO SOBRE O CIBERCRIME, p. 23).

Apesar de a adesão ter de ser unânime entre os Estados membros, e como as relações multilaterais entre o Brasil e os principais países europeus não estão desgastadas (vide, principalmente, o Ano da França no Brasil), é praticamente certa uma provável aceitação ao ingresso brasileiro. Porém, o fato de ele ainda não ser membro, não exclui – respondendo à segunda questão – a possibilidade de se criar legislação própria para tipificar e combater o cibercrime. Todavia, os Projetos de Lei em tramitação, há aproximadamente 10 anos, mostram certa falta de diálogo com a sociedade, principal fomentadora do ciberespaço, conforme exposto a seguir.

4 O PLS[21] do Senador Eduardo Azeredo face à Convenção de Budapeste: implicações e perspectivas na luta contra o cibercrime

Tramita no Legislativo Nacional, dentre outros de mesma índole, um polêmico projeto de lei que visa a combater cibercrimes, o qual é proposto pelo Senador Eduardo Azeredo em substituição aos antecessores projetos 89/2003, 76/2000 e 137/2000.

Conforme seu proponente, o Senador citado, o mesmo visa a tipificar determinadas condutas cibernéticas, em consonância com as recomendações da Convenção de Budapeste, estando, nesse sentido, em harmonia com a mesma. No entanto, face ao desrespeito evidente aos direitos fundamentais e às liberdades civis que aquele acarreta, é explícita a dissonância entre esses instrumentos normativos, bem como a inconstitucionalidade de dispositivos do projeto em análise.

Nesse sentido, a Convenção mencionada, eminentemente flexível e respeitosa à soberania dos Estados Parte, incumbe-os, consoante explicitado, de estabelecer leis internas de combate ao cibercrime, recomendando que as infrações tipificadas relacionem-se a condutas em que se rompam, intencionalmente, medidas de segurança, com vistas à usurpação de dados, instituindo, assim, o elemento subjetivo do dolo específico[22], o qual restringe a abrangência do tipo penal. Ao

[21] Projeto de Lei do Senado.

[22] Segundo DAMÁSIO (2008, pp. 291-292), o dolo específico, que pressupõe o genérico, compreenderia, para a doutrina que adere a tal classificação, a vontade de praticar o fato e produzir um fim especial ou específico, que se

contrário, o PLS em questão impõe tal prática como infração indiscriminadamente, sem definir, como ressalta Corrêa, se a modalidade do tipo seria dolosa ou não, recaindo em imprecisão legislativa e podendo criminalizar muitos usuários honestos.

No §4º do art. 154-A do projeto, o legislador permite ao agente que atua a título de defesa digital praticar a conduta descrita no *caput* do mesmo artigo, desrespeitando o princípio da igualdade de todos perante a lei, positivado no art. 5º, caput, da Constituição Federal. Essa ressalva, pois, implica em flagrante inconstitucionalidade, concedendo a agentes com conhecimento técnico e a profissionais, possivelmente de empresas privadas transnacionais, o poder de invadir os dados alheios, estabelecendo, em certos termos, uma tecnocracia e tolhendo, assim, a soberania interna, face à perspectiva de que essa invasão consentida, no mundo real, equivaleria a permitir que essas empresas invadissem residências para verificar se seus residentes haviam praticado atos contrários a seus interesses, não estando o poder de polícia adstrito, portanto, ao Estado.

Ao fazê-lo, estaria-se instituindo, em verdade, um grampo privado no Brasil, sem necessidade de ordem judicial. Se quanto às escutas telefônicas de autoridades, estabelecidas, mediante investigações em curso, sem prévia ordem judicial, gerou-se a "CPI dos grampos" em que o direito à privacidade foi assaz ressaltado, por que a usurpação e invasão por técnicos dos dados individuais de usuários seriam legítimas? Ainda, instituir esse sistema equivaleria a adotar um posicionamento, *mutatis mutandis*, similar ao tido pelos Estados Unidos da América (EUA) face ao Iraque no pós-11 de setembro, qual seja: pelo fato de os criminosos poderem lhes atacar a qualquer momento, os EUA estariam atacando, indiscriminada e previamente, a todos os usuários.

Em contraposição a tal perspectiva, a Convenção, em seu Preâmbulo e em vários dispositivos, nomeadamente no art. 15, evoca a obrigatória consonância das medidas adotadas com os direitos fundamentais historicamente estabelecidos em diversos Documentos, entre os quais se inclui o direito de ir e vir ou de movimentar-se, o qual, transmutado ao mundo virtual, deveria implicar na possibilidade de os usuários compartilharem dados e arquivos, o que é tolhido no presente PLS. Neste, pelos §§ 1º e 2º do art. 154-B, estariam os usuários da rede mundial de computadores, em suas atividades corriqueiras, sendo punidos com excessivo rigor, criminalizando cidadãos comuns pelo simples fato de transportarem informações e arquivos em *CD*, *DVD* ou *MP3 player*, pressupondo-se, nesse caso, que a polícia brasileira, em tese, poderia revistar tais

encontraria fora do fato material – a saber: conduta, resultado e nexo de causalidade.

dispositivos eletrônicos em busca dessas informações, de forma a macular generalizadamente sua privacidade.

Nesse ínterim, se adentraria numa sociedade em que todos são, *a priori*, suspeitos, e não presumidamente inocentes, em evidente desrespeito ao princípio do estado de inocência, estabelecido, segundo Damásio[23], a partir do art. 5º, LVII da Carta Magna. Romperia-se, ainda, com os direitos constitucionais de todos à privacidade e intimidade, de uma forma sem precedentes ou proporcionalidade, pois, no paradoxo entre monitoramento e privacidade, de que trata Assis Medeiros (MEDEIROS, 2002, p. 153), se supervalorizaria o primeiro em detrimento da segunda. Enfim, claramente se adotaria um posicionamento antidemocrático através desse policiamento cibernético indiscriminado, ao se privar a democratização da informação pela proibição do compartilhamento de arquivos entre usuários.

No sentido da decorrência de uma generalizada criminalização, no §2º do art. 163-A do PLS, é tipificada a conduta culposa[24] de difusão de código malicioso, diferentemente do disposto no relacionado Acordo Internacional, em que é exaustivamente recomendada a caracterização do dolo nas condutas ilícitas. De forma que, pelo primeiro, por exemplo, o cidadão que, desconhecendo a existência de vírus em seu computador, o transmitir, mediante uma conversa num mensageiro instantâneo, por exemplo, recairá em um ilícito, podendo ser punido com reclusão de três a cinco anos.

Tal configuração instauraria uma difundida insegurança entre os cidadãos virtuais, o que, nas palavras de Pedro Abramovay, Secretário de Assuntos Legislativos do Ministério da Justiça, entrevistado pela Folha Online[25], poderia gerar *vigilanismo*, ao se tratar todos os internautas como criminosos, em completo desrespeito ao preceito básico e fundador da *Internet*, qual seja, a liberdade por excelência.

Consoante exposto, apesar de ter sido moldado para estar em harmonia com a supracitada Convenção, o projeto analisado institui muitas obrigações naquela inexistentes, extrapolando os limites da razoabilidade e da proporcionalidade. De forma que, ainda, pelo inciso I do art. 21 do referido PLS, o provedor é obrigado a guardar dados aptos à identificação do usuário e dos

[23] DAMÁSIO, 2008, p. 11.

[24] Doutrina Welzel afirma que conduta culposa é toda aquela em que o sujeito não observa o cuidado necessário nas relações com os demais face a um resultado suscetível de constituir fato delituoso (*apud* DAMÁSIO, 2008, p. 296).

[25] Folha Online. Disponível em: < http://www1.folha.uol.com.br/folha/informatica/ utl124u565313.shtml >. Acesso em: 19 maio 2009.

endereços eletrônicos de origem, rastreando-se direta e indiscriminadamente o usuário, a despeito de sua liberdade de navegação cibernética. Por sua vez, pela Convenção, a qual presa pela razoabilidade e pelo respeito às liberdades dos internautas, rastreia-se o provedor e, indiretamente, através dele, quando necessário e com base em ordem judicial, chega-se ao usuário.

Segundo a mesma ótica, Corrêa (CORRÊA, 2008, p. 100-101) critica tal PLS, corroborando nossa argumentação ao dispor da falta de clareza na tipificação dos 11 crimes previstos, a qual traria imponderáveis prejuízos à aplicação do mesmo, e ao ressaltar a imprecisão técnica da linguagem adotada, a qual abre margens para dúvidas quanto à necessidade de elemento subjetivo ou não para a configuração do delito, ensejando dificuldades interpretativas.

De modo que o projeto analisado, a despeito de compreender uma importante iniciativa do Poder Legislativo para o combate aos crimes cibernéticos, especificamente aos crimes *de* computador – posto que os ditos crimes *no* computador já se encontram tipificados no Código Penal e Leis esparsas[26] –, demanda maiores discussões e amadurecimento, como indicam as manifestações crescentes de membros da sociedade civil, músicos, políticos, bem como de organizações como o Safernet e a Associação Software Livre, nas quais o PLS do Senador Azeredo vem sendo tachado de *AI-5 Digital*.

5 Considerações finais

> *No que tange ao Direito da Internet, de natureza e abrangência internacionais, "os estudos dos internacionalistas devem rumar para uma análise de quais instrumentos legais poderão ser aplicados ao caso concreto e se é possível promover a adoção de princípios básicos de democracia, soberania, leis e tratados internacionais.*
> VASCONCELOS, 2003, p. 52-53.

Observados e analisados os aspectos eminentemente jurídicos do *ciberespaço*, podemos afirmar que a criminalização das condutas imorais e ofensivas, ao mesmo correlatas, circunda dois

[26] José Anchieschi Gomes, especialista em criminalidade na rede de computadores, propõe a distinção entre crimes *de* computador – aqueles que afetam diretamente o funcionamento da rede, como a cópia ou interceptação de dados ou a invasão de *emails*, *homepages* e sistemas de rede – e crimes *no* computador – em que a máquina compreende um instrumento para a concretização da conduta típica de crimes já punidos pelo ordenamento penal, como a pedofilia ou os crimes contra a honra (*apud* Medeiros, 2002). Nesse sentido, os primeiros demandariam a iniciativa do Poder Legislativo para poderem ser combatidos, sob pena de se ferir o princípio da legalidade, positivado no art. 5º, XXXIX da Lex Legum; ao passo que os demais, deveriam ser reprimidos mediante as leis já estabelecidas, e não através de novas leis, visto a possibilidade de se recair em um *bis in idem*, ferindo o ordenamento constitucional.

binômios, a saber: de um lado, a liberdade de informação e a censura[27] e, de outro, a privacidade e o monitoramento.

A liberdade informática, decorrência direta da liberdade de informação, tutelada pelo art. 220 da Constituição Federal, compreende, consoante Paesani (PAESANI, 2002, p. 21-22), o aspecto ativo de informar e o aspecto passivo de ser informado, decorrendo, do equilíbrio entre esses dois âmbitos, a comunicação em uma sociedade pluralista. Face à ocorrência de abusos desse direito constitucionalmente assegurado, é evidenciada a necessidade de se impor limites ao mesmo, instaurando-se o controle estatal sobre a expressão intelectual, sob o jus do permissivo inserto no art. 221 do diploma supracitado.

Por sua vez, a privacidade, direito intrínseco aos indivíduos, apesar de realmente dever ser protegida, ao servir tanto para assegurar o ato honesto dos bons cidadãos quanto para esconder as atitudes abusivas dos criminosos, pode ser tolhida, configurando-se, nas palavras de Assis Medeiros, um paradoxo, qual seja: "*A monitoração é defendida para que se possa identificar os criminosos cibernéticos, mas, ao mesmo tempo, é uma espécie de crime contra as liberdades individuais"* (Medeiros, 2002, p. 153).

Nesse sentido, com vistas a promover uma repressão eficaz aos delitos cibernéticos, é necessária uma ponderação entre os interesses acima descritos, sob a perspectiva da razoabilidade, tanto no âmbito legislativo quanto no jurisdicional. De forma que, além de se considerar essas questões controversas, é preciso que se atente às peculiaridades do ambiente virtual, posto suas características de anarquia, individualidade e autonomia, por cuja manutenção, consoante outrora citado, atua o Movimento *Software* Livre.

Em detrimento das considerações acima, no entanto, o PLS do Senador Eduardo Azeredo, de maior evidência na regulamentação nacional dos crimes de computador, extrapola consideravelmente os limites da razoabilidade, sobrepondo a necessidade de combate às condutas ofensivas nesse âmbito aos direitos e liberdades individuais. Desse modo, a despeito de sua pretensão, emerge em desequilíbrio com as orientações da Convenção de Budapeste, pela qual, consoante exaustivamente dissertado, as conquistas históricas dos direitos dos cidadãos devem ser respeitadas, ainda no combate à criminalidade cibernética.

[27] É importante ressaltar que a censura aqui referenciada corresponde à ação de controle estatal sobre a liberdade de expressão ou movimentação dos internautas, não implicando no significado mais expressivo do termo, o qual o interliga aos anos de chumbo da história brasileira.

Apesar de suas limitações, o projeto analisado é de suma importância para a discussão dessas questões, posto que, na realidade das novas tecnologias e das novas ofensas aos direitos positivados, lacunas objetivas são estabelecidas na ordem jurídica, não podendo o Poder Judiciário utilizar-se apenas e por longo lapso temporal dos elementos integrativos da ordem jurídica (VASCONCELOS, 2003, p. 48), estabelecidos no art. 4º da LICC, sendo imprescindível a tipificação de novas condutas, conforme dispõem o PLS e a Convenção mencionados, sem, entretanto, macular sobremaneira os direitos e liberdades individuais.

Dessa forma, ao lado dos setores do poder estatal, aos quais cabem, através do direito, a compreensão e o acompanhamento dessas inovações com a finalidade de se garantir a pacificação social e o desenvolvimento sustentável dessas novas relações (CORRÊA, 2008, p. 3), devem se fazer ouvir os membros da sociedade civil, bem como os diretamente vinculados ao mundo cibernético, caso dos defensores do *Software* Livre e dos integrantes de ONGs – em relevo, o SaferNet –, os quais têm se manifestado, nas ruas e através de abaixo assinado – como o *Meganão* – em contraposição ao PLS em questão, por este compreender, em última análise, uma ruptura com a liberdade de expressão e uma criminalização em massa dos cidadãos internautas.

Isso posto, os autores deste entendem que, até o momento, o ingresso do Brasil à Convenção de Budapeste seja a mais correta atitude a ser tomada, face à necessária uniformização do combate transnacional aos crimes cibernéticos, evidentemente desterritorializados, e ao respeito aos direitos e liberdades individuais por ela impostos. Paralela à qual, este trabalho defende, ainda, a eminente necessidade de se estabelecer, no âmbito nacional, um diálogo entre os distintos polos intrinsecamente interessados na repressão a tais crimes e na preservação dos direitos historicamente positivados, fazendo-se prevalecer os princípios da democracia e do Estado Democrático de Direito.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. In: ANGHER, Anne Joyce (Org.). **Vade Mecum acadêmico de direito**. 6ª ed. São Paulo: Rideel, 2008.

BRASIL. MINISTÉRIO PÚBLICO FEDERAL. *Cibercrime: CCJI sugere adesão do Brasil à Convenção de Budapeste.* Disponível em: < http://ccji.pgr.mpf.gov.br/institucional/informes/ cibercrime-ccji-sugere-adesao-do-brasil-a-convencao-de-budapeste >. Acesso em: 20 maio 2009.

BULL, Hedley. **A Sociedade Anárquica**. Brasília: Universidade de Brasília, 2002.

CAMBRIDGE UNIVERSITY. *Cambridge Advanced Leaner's Dictionary*. Cambridge: Cambridge University Press, 2003. 1 CD-ROM.

CASTELLS, Manuel. **Fim do Milênio**. 4. ed. Tradução de Klauss Brandini Gerhardt e Roneide Venancio Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura; v. 3).

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: < http://ccji.pgr.mpf.gov.br/documentos /docs_documentos/convencao_cibercrime.pdf >. Acesso em: 09 maio 2009.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 4. ed. São Paulo: Saraiva, 2008.

ERDELY, Maria Fernanda. *Itamaraty ainda estuda adesão à Convenção de Budapeste.* Disponível em: < http://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao convencao_budapeste >. Acesso em: 18 maio 2009.

Folha de São Paulo. *Projeto quer controlar acesso à internet.* Disponível em: < http://www1.folha. uol.com.br/folha/informática/utl124u20908.shtml >. Acesso em: 19 maio 2009.

Folha Online. *Ato contra "Lei Azeredo" reúne militantes, Suplicy e fãs de Teatro Mágico em SP*. Disponível em: < http://www1.folha.uol.com.br/folha/informática/utl124u566083.shtml >. Acesso em: 19 maio 2009.

Folha Online. *Ministério da Justiça critica lei sobre crimes na internet e quer veto a artigos***.** Disponível em: < http://www1.folha.uol.com.br/folha/ informática/utl124u565313.shtml >. Acesso em: 19 maio 2009.

HAYDEN, Matt. **Aprenda em 24 horas Redes**. Tradução de Marcos Pinto. Rio de Janeiro: Campus, 1999.

JESUS, Damásio E. de. **Direito Penal**. 29. ed. São Paulo: Saraiva, 2008. v. 1.

MAZENOTTI, Priscilla. *Convenção de Budapeste contra pedofilia pode ser exemplo para o Brasil, diz delegado.* Disponível em: <http://www.mndh.org.br/index.php?option=com_content&task=view&id469&Itemid=56>. Acesso em: 20 maio 2009. Reportagem vinculada à Agência Brasil.

MEDEIROS, Assis. **Hackers: entre a ética e a criminalização**. Florianópolis: Visual Books, 2002.

MEGANÃO. Disponível em: < http://meganao.wordpress.com/o-mega-não/o-que-combatemos/ >. Acesso em: 19 maio 2009.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2002.

SAFERNET. *Brasil não pode aderir a Convenção de Budapeste sobre o Cibercrime.* Disponível em: < http://www.safernet.org.br/twiki/bin/view/ SaferNet/Noticia20070528221656 >. Acesso em: 15 maio 2009.

SOARES, Guido F.S. *Solução e Prevenção de Litígios Internacionais: tipologias e características atuais*. In: MERCADANTE, Aramita de A.; MAGALHÃES, José Carlos (Coord.). **Solução e prevenção de litígios internacionais**. Porto Alegre: Livraria do Advogado, 1999. p. 11-64.

THING, Lowell (Ed.). **Dicionário de Tecnologia *Whatis.com***. São Paulo: Futura, 2003.

W3C. Disponível em: < http://www.w3.org/ >. Acesso em: 14 maio 2009.

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