Projeto de Lei de Cibercrimes: há outra alternativa para a internet brasileira?

*Luiz Moncau**
*Ronaldo Lemos***
*Thiago Bottino****

1. Introdução

No mundo todo, vive-se um momento de acelerado desenvolvimento tecnológico, que culminou no advento do que se convencionou chamar "sociedade da informação", ou seja, de uma sociedade na qual a informação e o conhecimento assumiram um papel crucial na produção de riqueza e de bem-estar para todos os indivíduos.

Essa sociedade caracteriza-se pela presença de tecnologias avançadas de informação e comunicação, que permitiram a redução dos custos de transações comerciais e o desenvolvimento do comércio eletrônico, bem como expandiram imensamente os horizontes do conhecimento para toda a humanidade.

O marco mais recente e central dessa sociedade da informação, certamente, é criação de um conglomerado de redes de computadores interligadas entre si de maneira completamente descentralizada e em escala mundial, batizada de internet. Essa rede mundial de computadores propiciou o acesso aos mais diversos

* Mestrando em teoria do Estado e direito constitucional pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio).
** Professor da FGV Direito Rio, mestre em direito pela Universidade de Harvard e doutor em direito pela Universidade de São Paulo (USP).
*** Professor da FGV Direito Rio e doutor pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) e membro da Comissão Permanente de Direito Penal do IAB.

tipos de informação, agilizando, barateando e simplificando a transferência de dados no mundo todo.

Por um lado, são claros os benefícios trazidos por tal evolução tecnológica. Por meio da internet, ampliou-se de maneira imensurável, para muitos cidadãos, o acesso à cultura, ao conhecimento e à informação. No campo das relações entre governo e cidadão, ficou extremamente mais fácil dar transparência e publicidade aos dados e ações do Estado, bem como obter o acesso a serviços públicos essenciais.

Mais do que isso, pelo acesso à rede mundial de computadores, é evidente a melhoria das condições para que cada cidadão exerça sua liberdade de expressão, já que a rede provê a todos os que estão conectados os meios para atingir um público antes alcançado só pelos historicamente concentrados meios de comunicação tradicionais. A partir dessas novas possibilidades de expressão asseguradas aos indivíduos, pode-se afirmar que há ganhos potenciais não só para a liberdade de expressão e manifestação, mas também para a democracia, fortalecendo o debate público e promovendo um diálogo mais aberto e robusto sobre os mais diversos temas, incluindo-se aqui aqueles que jamais tiveram espaço na mídia convencional.

Na mesma linha, não é exagerado afirmar que a evolução da tecnologia também criou inúmeras oportunidades de negócio, que vão desde a exploração de novas formas de distribuição do conteúdo, passando pelo comércio eletrônico e pelos inúmeros serviços online, entre tantas outras possibilidades.

Por outro lado, o uso da tecnologia (como o de qualquer outro invento humano) permite novas formas de provocar danos e amplia o potencial lesivo de ofensas à honra e à dignidade. Por meio do mau uso da tecnologia, velhos golpes ganham nova roupagem levando risco para o patrimônio dos indivíduos.

Nesse contexto, surgem diversas questões que o mundo todo busca resolver. Afinal, como permitir que a nova tecnologia se desenvolva maximizando o seu potencial de inclusão e progresso, mas com a efetiva coibição dos usos injustos e abusivos? Como municiar as autoridades para que persigam e reprimam a violação de direitos sem que, por outro lado, restrinja-se indevidamente os direitos fundamentais de liberdade e privacidade dos usuários da rede mundial de computadores? Como identificar condutas inadequadas e, mais que isso, como definir se tais condutas merecem ou não ser reprimidas por meio do direito penal? Em resumo: de que forma deve o Estado atuar para assegurar ou restringir as liberdades dos cidadãos diante do avanço tecnológico e, mais especificamente, como deve ser tal atuação no ambiente da rede mundial de computadores?

São inúmeras as iniciativas legislativas tentando responder a essas questões, algumas delas claramente exageradas. E não é preciso aprofundarmos as discussões sobre a regulação no âmbito da rede mundial de computadores para observarmos propostas de legislação que tratam o avanço tecnológico de maneira refratária. É possível encontrar iniciativas que preveem a proibição de máquinas

xerocopiadoras nos *campi* universitários, ignorando a existência do domínio público e das limitações e exceções ao direito de autor previstas na Lei de Direitos Autorais.[1]

Ainda que este não seja o objeto deste artigo, o exemplo é útil para demonstrar que as propostas legislativas podem apresentar-se, de antemão, avessas ao progresso tecnológico e que a regulação de fenômenos novos nem sempre vem acompanhada da necessária ponderação entre o interesse público e o privado.

Se a linha que divide a restrição indevida às liberdades individuais no caso exposto apresenta-se clara, em outros aparece de maneira muito mais tênue. Se parece óbvia a inadequação de medida que bane a cópia em universidades, o que dizer da proibição de jogos violentos ou da melhor forma de repressão do envio de Spam?

Muito embora esses pontos não sejam o foco deste artigo, todas essas discussões, em última análise, tocam-se num ponto fundamental: a forma como iremos nos posicionar diante do avanço da tecnologia.

Buscando trazer um pouco mais de equilíbrio a esta desafiadora discussão, este artigo analisa o projeto de lei do senador Eduardo Azeredo, aprovado no Senado Federal e em trâmite na Câmara dos Deputados sob o nº 84 de 1999, que busca tipificar como crime diversas condutas realizadas no âmbito da rede mundial de computadores.

Como se verá adiante, com o objetivo de municiar as autoridades para combater as condutas julgadas inadequadas, o legislador acabou por abarcar, por imprecisão técnica, diversas condutas triviais. Mais que isso, neste artigo será criticada a opção de recorrer diretamente ao direito penal como primeira alternativa para dissuadir as pessoas de práticas muitas vezes de pequeno potencial ofensivo, com consequências nefastas maiores do que os males que pretende combater.

A partir da avaliação dos problemas existentes nesse projeto de lei específico, este artigo extrairá algumas lições importantes sobre como proceder diante do avanço tecnológico, indicando um caminho sensato para procedermos à regulação da internet para garantir direitos, mas sem sufocar a inovação e as liberdades na internet.

Na segunda seção serão apresentadas algumas considerações sobre qual seria o melhor caminho a ser trilhado para promovermos a regulação da internet brasileira, atentando para fatores como a necessidade de se garantir um patamar mínimo de segurança jurídica para o empreendedorismo na rede e, em sentido oposto, sobre os riscos e a insegurança trazidos pela opção de responder à inovação diretamente com a utilização do direito penal.

---

[1] Projeto de Lei nº 1.197/2007.

Na terceira seção, teremos um breve histórico da proposta de lei hoje em debate para enfim proceder a uma avaliação detalhada dos pontos críticos trazidos pelo projeto. Na avaliação concreta dos dispositivos apresentados pelo projeto, buscaremos destacar sempre três planos de avaliação: o da técnica legislativa; da dogmática penal; e o plano pragmático.

A seção 4 esclarecerá algumas questões que rodeiam o debate legislativo sobre o processo, trazendo outras considerações sobre o projeto. Assim, almejamos deixar claro sobre o que efetivamente trata a proposta legislativa e o que não está nela contemplado. Eventualmente, será inescapável argumentar sobre matérias que não foram debatidas no Congresso de maneira aberta e sobre as quais não há qualquer consenso, mas que num olhar desatento podem acabar abrigadas na proposta legislativa em questão.

Por fim, na quinta e última seção apresentaremos algumas conclusões sobre as lições extraídas aqui, buscando apontar um sentido para futuras regulações para a rede mundial de computadores e, no que for aplicável, para o avanço das tecnologias de comunicação em geral.

2. Um projeto para a internet brasileira

Historicamente, o desenvolvimento de um país no setor das comunicações e das tecnologias de informação sempre foi considerado estratégico. Com o advento da sociedade da informação, entretanto, o desenvolvimento deste setor e, particularmente, da internet, ganhou muito em relevância em função da multiplicidade de temas a ele relacionado.

Com efeito, como já mencionado, ao tratarmos da rede mundial de computadores acabamos por abordar temas como: a ampliação do acesso à cultura e à informação; a necessidade de conexão para o desenvolvimento econômico e social; o incremento das possibilidades de participação popular e fiscalização dos governos; o aprofundamento ou a redução da desigualdade em função do provimento de acesso à rede em condições desiguais para as classes (ou países) de menor poder aquisitivo; as novas formas de interação cultural e produção de riqueza; entre tantos outros.

A forma indiscutível com que a internet afetou todos estes (e outros) campos da vida social conduz a um consenso: o país que não aprimorar sua infraestrutura e não avançar no sentido de ampliar o acesso e promover o desenvolvimento de regras claras que permitam o desenvolvimento da internet em seu território perderá vantagem competitiva no cenário internacional, em especial no que diz respeito ao mercado global de serviços digitais.

É neste ponto extremamente sensível que se insere a discussão acerca do Projeto de Lei nº 84/99. E a indagação que devemos fazer para avaliar a adequação dessa proposta legislativa é: qual deve ser o nosso projeto para a internet brasileira?

Não se trata de avaliar qual a melhor forma de vencer os desafios da inclusão digital, de promover a competição ou de baixar os custos de acesso à internet. Não se trata, igualmente, de discutir os graves problemas nas relações de consumo historicamente verificados na prestação dos serviços de telecomunicações.

Trata-se, por outro lado, de discutir qual é o modelo de regulação que, sem restringir de maneira precoce as liberdades existentes, será capaz de definir de maneira clara quais são as responsabilidades dos diversos agentes na rede (provedores, prestadores de serviço, usuários) e criar condições propícias para o empreendedorismo e a inovação.

Nesse sentido, questionamos: o primeiro marco legal para a internet brasileira deve ser um marco criminal?

Do ponto de vista da política legislativa, diversas razões apontam que não.

Com a possível aprovação do Projeto de Lei nº 84/99, a primeira legislação abrangente sobre internet no Brasil será criminal, não civil. Não há no Brasil, por exemplo, legislação que trate adequadamente de temas como a privacidade online, o regime de proteção aos dados pessoais, as salvaguardas e responsabilidades dos provedores de acesso e conteúdo, o comércio eletrônico e os serviços online.

Cumpre ressaltar, neste ponto, que o caminho natural é sempre o da regulamentação civil, devendo a lei penal ser adotada somente em casos excepcionais, nos casos realmente graves em que os bens jurídicos que se busca proteger (patrimônio, vida, integridade física) justificam a restrição à liberdade, bem consagrado em nossa Constituição Federal como um direito humano fundamental.

No Brasil, como se verá mais adiante na análise detalhada dos pontos mais graves do PL, propõe-se fazer o contrário: ao invés de se regular a internet no âmbito civil, a proposta legislativa em discussão opta por tratar de todos esses assuntos diretamente por meio do direito penal.

Com a ausência de regras claras no âmbito civil ou com regras que trazem sanções penais severas para, por exemplo, infrações à privacidade ou para o acesso não autorizado a dados protegidos, cria-se um verdadeiro *chilling effect* sobre a inovação.

Para esclarecer este ponto, tome-se como exemplo o empreendedor que deseja abrir um negócio qualquer, como um restaurante ou um estabelecimento de comércio. Ao iniciar o novo negócio, o empreendedor tentará calcular todos os riscos e oportunidades para sua empresa. Para tanto, além de uma análise de mercado, o empresário deverá avaliar quais são as exigências legais que deverá atender, quais são as salvaguardas jurídicas existentes, quais são os padrões de qualidade que deverá observar etc.

A análise de todos esses pontos traduz-se, ao final, numa noção razoavelmente clara dos custos e riscos existentes para o empreendimento.

A ausência de normas que estabeleçam de maneira inequívoca quais são as responsabilidades e salvaguardas dos provedores de conteúdo por violações praticadas por seus usuários (de direito autoral ou à honra de terceiros, por exemplo) não permite àquele que deseja criar um novo serviço digital saber quais são seus deveres diante da ocorrência de tais violações ou prever quais serão as consequências caso não adote as medidas necessárias e eficientes para preveni-las.

De maneira objetiva, não existe a obrigação de prevenir tais infrações ou mesmo diretrizes sobre as providências mínimas que um provedor deve adotar. Por outro lado, existe a possibilidade de que seja feita uma interpretação jurídica que conduza à sua responsabilização pelo conteúdo ilícito. Um exemplo que ilustra de maneira clara essa situação é o da decisão judicial que determinou o bloqueio do acesso dos internautas brasileiros ao YouTube em função da exposição de vídeo que violava a intimidade da apresentadora de televisão Daniela Cicarelli.

Assim, a consequência prática da incerteza sobre as obrigações que devem ser atendidas na oferta de um serviço de conteúdo gerado pelos usuários é o desestímulo à inovação. Afinal, quem de fato inovará sem nenhuma previsibilidade de suas obrigações?

O cenário piora quando, sem regras que definem a responsabilidade civil por infrações como essas, começam a surgir normas criminais que trazem penas rígidas ao responsável pelas violações. O empreendedor que já contava com o desestímulo da incerteza acerca da sua responsabilidade civil, passa a vislumbrar também a possibilidade de ser responsabilizado penalmente por tais infrações.

Sob essa ótica, o ideal seria a rejeição integral do projeto de lei (PL) e a discussão no Congresso de um novo projeto que regulasse as diversas atividades e serviços prestados via internet do ponto de vista exclusivamente civil. Entretanto, como se verá adiante, o atual estágio de tramitação do PL não permite essa mudança.

Dessa forma, avaliaremos na próxima seção os pontos mais críticos do projeto de lei, sugerindo a supressão de tais pontos para evitar outra consequência indesejável que decorre dessa opção legislativa para a internet brasileira, qual seja a inclusão nos tipos penais trazidos pelo projeto de condutas irrelevantes para o direito, ou cuja regulação deveria se dar apenas no âmbito civil em função do seu menor potencial ofensivo.

3. O projeto aprovado no Senado

O Projeto de Lei de Cibercrimes foi aprovado no Senado Federal no dia 9 de julho de 2008, na forma de um substitutivo apresentado pelo senador Eduardo Azeredo.

Em função do seu atual estágio de tramitação, somente é possível a aprovação do projeto tal como aceito pelo Senado, a supressão de alguns itens da proposta sem modificação na sua redação ou a aprovação integral do projeto tal como aprovado na Câmara.

A aprovação do projeto tal como aprovado na Câmara traria graves consequências para o desenvolvimento da internet no Brasil. Entre os equívocos da proposição aprovada naquela Casa, destaca-se a proposta de equiparação de dado à coisa para fins de configuração do crime de dano, previsto no art. 163 do Código Penal.

Referida proposta teria efeitos imprevisíveis no ordenamento jurídico brasileiro, dada a impossibilidade de tratar igualmente dois "objetos" de natureza completamente distinta. Com efeito, enquanto coisas são bens materiais e, portanto, "bens escassos", dados eletrônicos são bens "não escassos", ou seja, os dados possuem natureza fluida e o seu envio e aproveitamento por uma pessoa não impede sua utilização por outra.

Este não é o único problema do projeto tal como aprovado na Câmara. Entretanto, tendo em vista que muitos dos problemas contidos na proposta da Câmara mantiveram-se na versão final do substitutivo apresentado e aprovado no Senado, este artigo não procederá a uma análise detalhada dos outros pontos da proposição daquela Casa, sob pena de tornar-se demasiadamente extenso e repetitivo.

Assim, considerando a impossibilidade de promover a alteração da redação da proposição em seu atual estágio de tramitação e os problemas contidos na proposta originalmente aprovada na Câmara dos Deputados, apresentam-se para a sociedade brasileira duas alternativas: a supressão de alguns termos ou artigos do PL aprovado no Senado ou a aprovação do projeto tal como aprovado naquela Casa.

Como se demonstrará adiante numa análise dos principais problemas do projeto sob os pontos de vista pragmático, de técnica legislativa e de dogmática penal, é imprescindível a exclusão de pelo menos quatro dos seus artigos, evitando a criminalização de condutas triviais ou de menor potencial ofensivo, bem como a inviabilização de iniciativas de inclusão digital.

O art. 2º do projeto de lei

O art. 2º do projeto tal como aprovado no Senado acrescenta três artigos à parte especial do Código Penal, criando um capítulo dos crimes contra a segurança dos sistemas informatizados.

Todos os artigos propostos para o novo capítulo possuem problemas. Vejamos, artigo por artigo, a redação final aprovada no Senado e em debate na Câmara, apontando quais os potenciais problemas decorrentes da sua conversão em lei.

Art. 285-A

O artigo 2º do projeto de lei acresce ao Código Penal o seguinte capítulo:

Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado.[2]

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Comentários sobre o dispositivo

No plano da técnica legislativa

O princípio da tipicidade legal (não há crime sem lei anterior que o defina) pressupõe a taxatividade do texto legal, isto é, a utilização de conceitos sob os quais não haja possibilidade de atribuição de variadas interpretações. Evita-se ao máximo o uso de leis penais em branco (leis que dependem da integração de outra norma que lhe dê conteúdo) bem como a utilização de conceitos com diferentes sentidos.

Exemplificando, não há possibilidade de interpretações jurídicas distintas acerca do significado das expressões "ontem", "mãe" ou "fraude". Contudo, o atual tipo penal peca pelo uso de expressões passíveis de inúmeras interpretações. Os vocábulos "violação de segurança" e "expressa restrição de acesso" não têm

[2] O projeto define em seu art. 16, o que é rede de computadores, dispositivo de comunicação ou sistema informatizado. Para facilitar a compreensão das críticas aqui tecidas, traz-se abaixo a definição tal como trazida no PL:
I - dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;
II - sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;
III - rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações como dispositivo de comunicação "qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia". Pela definição, um CD, um DVD ou até mesmo um pedaço de papel pode ser considerado um dispositivo de comunicação.

definição legislativa e podem ser associados a uma pluralidade de situações cotidianas da internet que não são aquelas que se pretende punir criminalmente.

A situação neste caso específico é ainda mais grave quando consideramos que a ausência de um sentido legal para uma expressão como "expressa restrição de acesso" é passível de definição por um particular e não através da integração por outra norma, como ocorre no caso das leis penais em branco.

Com efeito, o que é uma "expressa restrição de acesso"? Muitas são as interpretações possíveis. A Lei de Direitos Autorais, por exemplo, pode configurar uma expressa restrição de acesso a conteúdo protegido por direito autoral, especialmente quando consideramos que, ainda que temporariamente, para acessarmos qualquer página ou informação através da rede mundial de computadores, precisamos executar uma cópia.

Além disso, pode-se interpretar como "expressa restrição de acesso" aquela imposta pela via contratual. Exemplo disso seria o do usuário que decide utilizar um programa de voz sobre IP (VoIP) para se comunicar. Utilizando-se da tecnologia VoIP (Skype, por exemplo), que usa a internet como plataforma, o usuário consegue comunicar-se a um custo infinitamente menor. Só que a companhia que lhe fornece o serviço de acesso à internet por banda larga é a mesma que explora comercialmente as linhas telefônicas e avisa em seu contrato de adesão que não permite o uso da tecnologia VoIP através da sua rede, instalando um programa que desabilita softwares dessa natureza. O usuário então instala um software que anula o bloqueio, utilizando-se do serviço de voz sobre IP.

Nesse caso, usuário praticou a conduta de utilizar o serviço de voz sobre IP (acessar), anulando o bloqueio imposto pela companhia (mediante violação de segurança), rede de computadores (rede do provedor) protegido por expressa restrição de acesso (restrição contratual feita pela companhia), punível com pena de um a três anos.

Por fim, ainda é possível a interpretação de que uma restrição tecnológica seja considerada expressa restrição de acesso. Como exemplo, tome-se a venda de CDs com mecanismo que impede o indivíduo que o comprou de transferir as músicas para um tocador de MP3. Caso o dono do CD insista e consiga superar o mecanismo anticópia, estará sujeito a uma pena de até três anos de prisão, maior do que a pena por atropelar uma pessoa (que é de dois anos) e próxima da pena para quem atropela e mata uma pessoa (que é de quatro anos). E o mais grave, a partir da definição por um particular do que é ou não crime para efeitos do art. 285-A.

Assim, em um breve exercício de interpretação do dispositivo proposto, tem-se que uma "expressa restrição de acesso" pode ser legal (Lei de Direitos Autorais, por exemplo), contratual ou tecnológica, sendo em dois de três casos um particular que dá conteúdo à norma penal.

Com esta redação o dispositivo proposto atinge não só as condutas que o legislador pretende evitar (como a invasão de sistemas) mas também provoca a

hiperinclusão de condutas destituídas de relevância penal. Ou seja, tipifica condutas que apesar de não serem materialmente criminosas, o serão formalmente e obrigarão o Estado a perseguir todos que as praticarem.

No plano da dogmática penal

O tipo penal está redigido como crime de perigo abstrato. Ou seja, não se exige para a configuração do crime nenhum dano (resultado lesivo a algum bem jurídico) nem mesmo um perigo concreto (criação de risco concreto, demonstrável, a algum bem jurídico). Essa espécie de legislação penal é apontada por alguns autores como inconstitucional e mesmo entre aqueles que defendem crimes cujo perigo é apenas presumido, a criminalização de tais condutas justifica-se apenas em hipóteses extremas. A conduta que não danifica, inutiliza nem afeta nenhum bem jurídico deve ser considerada atípica (não punível pelo direito penal), embora possa ser punida pelo direito civil ou administrativo por meio de multas, indenizações, interdições etc.

Tal tipo penal também atinge o princípio da proporcionalidade. Isso se dá porque a ativação do direito penal tem como consequência a privação da liberdade individual. Como a liberdade é um direito constitucional de grande relevância, sua afetação só é justificada se ocorre um dano (ou um perigo concreto de lesão) a outro bem jurídico igualmente relevante.

Com efeito, deve-se considerar como bem jurídico relevante aqueles valores que são protegidos pela Constituição, como a vida, a liberdade, o patrimônio, o meio ambiente, a honra, a intimidade, o sistema financeiro, a ordem tributária, a administração da justiça etc. No caso concreto, o bem jurídico protegido é a "segurança dos sistemas informatizados". Ora, a segurança do sistema não é um bem jurídico relevante; não é algo que mereça ser protegido por si só. A segurança do sistema informatizado só merece proteção penal se ela (a segurança do sistema) se presta a proteger um bem jurídico.

A lei, então, deveria prever a configuração de crime somente nos casos em que algum bem jurídico seja afetado. Nesse projeto, entretanto, não se adotou tal postura, de modo que se aprovado com tal redação os comportamentos mais inofensivos e corriqueiros serão criminalizados.

No plano pragmático

Uma vez abrangidas pela lei, as condutas inofensivas estarão sujeitas aos rigores do enquadramento como crime. E trata-se aí de um crime com uma pena alta, de um a três anos.

Disso decorre mais uma consequência que mereceria melhor ponderação do legislador. O fato de a pena máxima ser superior a dois anos não permite que o fato, mesmo que de pequeno potencial ofensivo, seja julgado por um Juizado Especial Criminal, onde os julgamentos são mais céleres e é possível a composição de acordos ou conciliações, filtrando os casos de menor relevância.

Com isso, dá-se a ativação do aparato estatal para a perseguição do infrator. De maneira bastante superficial, mas ilustrativa, impõe-se que o delegado instaure inquérito, realize uma investigação e remeta os autos ao Ministério Público. Ainda que o promotor ou procurador constate que a conduta é inofensiva, deverá oferecer denúncia, pois obedece ao princípio da obrigatoriedade da lei penal. E caso o promotor peça o arquivamento (alegando, por supor, o princípio da insignificância), o juiz de direito ainda deverá concordar com o pedido para que o arquivamento se efetive.

Soma-se a isso a já mencionada hiperinclusão decorrente da abrangência da redação dada pelo legislador e teremos que, se convertido em lei, o dispositivo em discussão será capaz de gerar uma forte pressão sobre as instituições (polícia, Ministério Público e Judiciário), acabando por comprometer seu funcionamento eficaz.

Em tempos em que tanto se discute a morosidade do Poder Judiciário e a deficiência do Estado em distribuir a justiça, cabe indagar se a criminalização de condutas de pequeno potencial ofensivo não contribui para o agravamento deste quadro.

O art. 2º do projeto de lei acrescenta ao Código Penal, ainda, o art. 285-B, que padece de vícios de redação extremamente parecidos com os acima explicados.

Senão vejamos. Dispõe o art. 285-B do projeto de lei ora em análise, *in verbis*, o quanto segue:

> Obtenção, transferência ou fornecimento não autorizado de dado ou informação
> Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:
> Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Comentários sobre o dispositivo

No que diz respeito ao plano da técnica legislativa, todos os argumentos do artigo anterior (285-A) aplicam-se ao 285-B.

Com efeito, repete-se na redação o dilema da lei penal em branco: vocábulos "sem autorização ou em desconformidade com autorização", "legítimo titular da rede de computadores" (a internet é uma rede de computadores. Quem é seu legítimo titular?) e "expressa restrição de acesso" dão margem a múltiplas interpretações. O resultado da redação de uma lei penal em branco cujo preenchimento se realiza por particulares (que definem quais os termos de uma autorização ou impõem restrições de acesso tecnológicas/contratuais) é a hiperinclusão de condutas destituídas de relevância penal. Novamente, apesar de não serem materialmente criminosas, o serão formalmente, obrigando o Estado a perseguir todos que as praticarem.

No plano da dogmática penal repete-se o dilema do tipo penal de perigo abstrato, pois não se exige para a configuração do crime nenhum dano nem mesmo um perigo concreto a algum bem jurídico.

Esse tipo penal também atinge o princípio da proporcionalidade porque a transferência não autorizada não é necessariamente ruim ou danosa. Do contrário, muitas vezes ela pode ser benéfica, como nos casos de *cookies* (arquivos que transferem informações que permitem a um computador identificar o outro e configurar aquilo que será apresentado).

Diversos sítios da internet utilizam tal recurso. Quando alguém se conecta o *cookie* transfere informações sem pedido de autorização e o sítio que recebe as informações automaticamente reage e apresenta notícias relacionadas ao perfil do usuário (como notícias de um time ou sobre direito em primeiro plano, por exemplo). Além desse, entretanto, há outros inúmeros exemplos de hiperinclusão.

No plano pragmático repete-se o dilema da pressão sobre as instituições públicas, pois as penas impedem que o caso tenha o tratamento simplificado dos juizados especiais criminais e exige a instauração de inquérito e oferecimento de denúncia, ou manifestação do Ministério Público e do Judiciário, mesmo que em casos de pequeno potencial ofensivo, para que ocorra o arquivamento ou a transação penal.

Dispõe o art. 285-C, o quanto segue:

> Art. 285-C. Nos crimes definidos neste capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, estado, município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias.

Comentários sobre o dispositivo

Em primeiro lugar, cumpre destacar que esse artigo ficará prejudicado caso os dois anteriores sejam descartados. Em todo caso, carrega consigo um problema de ordem dogmática penal e outro de ordem pragmática.

No campo da dogmática penal isso se explica porque os delitos de pequena ou nenhuma ofensividade (e já vimos que os crimes tal como redigidos não exigem nenhum tipo de lesão ou risco concreto de lesão a nenhum bem jurídico relevante) são de ação privada. No caso, a proposta transforma esses delitos em crimes de ação pública condicionada. Ou seja, diante de uma representação da parte daquele que sofreu o crime, o Ministério Público (MP) estará obrigado a instaurar o processo. Não há nenhum ônus econômico para o particular (que nas ações privadas é obrigado a contratar advogado e pagar as custas do processo penal), o que permite presumir que haverá inúmeras provocações da ação do MP.

De fato, quando o crime é de ação privada, o particular pondera a relação de custo-benefício e só ajuíza a ação quando há expectativa de ganhar mais do que gastará com o processo. Aqui, o processo sai de graça para o particular, mas sobrecarrega o Estado. A polícia é obrigada a investigar e o MP deverá funcionar no polo ativo do processo, acusando o usuário de internet.

Na perspectiva pragmática, diante disso, é possível antever um crescimento de processos sem relevância que esse tipo penal tem o condão de gerar, sobrecarregando ainda mais o já moroso sistema judiciário brasileiro.

O art. 5º do projeto de lei

Através deste dispositivo, pretende-se acrescentar o art. 163-A e dois parágrafos ao Código Penal. Como se verá adiante, buscando combater a difusão de vírus de computador (chamados no projeto de "códigos maliciosos"), a proposta acaba por repetir o mesmo erro dos artigos já analisados, permitindo interpretações que abarcam condutas de pequeno ou nenhum potencial ofensivo, ou ainda, atingindo outras condutas que não as que se procura reprimir.

O art. 5º do PL tem a seguinte redação:

> Inserção ou difusão de código malicioso[3]
>
> Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.
> Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

[3] O projeto define em seu art. 16, o que é código malicioso. Para facilitar a compreensão das críticas aqui tecidas, traz-se abaixo a definição tal como trazida no PL:
IV - código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida.

> Inserção ou difusão de código malicioso seguido de dano
>
> § 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado.
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Art. 163-A, no plano da dogmática penal

Em primeiro lugar, repete-se aqui o dilema do tipo penal de perigo abstrato — não se exige para a configuração do crime nenhum dano nem mesmo um perigo concreto a algum bem jurídico.

Em segundo lugar, esse novo crime é desnecessário, justamente em função da nova redação sugerida para o crime de dano (art. 163) no art. 4º do próprio projeto de lei.

Esta nova redação para o crime de dano é suficiente para punir quem destrói dados eletrônicos (arquivos de computador), algo que não existe hoje. Com efeito, o art. 163 ficaria com a seguinte redação, se aprovada a proposta contida no art. 4º do próprio projeto de lei:

> Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio.
> A pena prevista para o crime é a mesma já prevista no Código Penal, qual seja a detenção de 1 (um) a 6 (seis) meses, ou multa.

Dessa forma, com a alteração proposta no art. 4º, o crime de dano de dado eletrônico ser punível, não importando se isso é feito por meio de vírus (ou de código malicioso) ou se alguém vai até o computador da mesa ao lado e apaga todos os arquivos do disco rígido.

Cumpre destacar que com a alteração do art. 4º, mesmo que a pessoa mal-intencionada que enviou o vírus não tenha sucesso (porque bloqueado o dano pela ação de um antivírus, por exemplo), terá realizado a conduta prevista no art. 163 do Código Penal. Isso porque o crime de dano admite a modalidade tentada (a tentativa de crime de dano é punida com a mesma pena do dano, reduzida de um a dois terços, na forma do atual art. 14 do Código Penal).

Por outro lado, caso o art. 5º do PL seja aprovado, será instaurado um absurdo jurídico. Afinal, o crime de danificar os arquivos de computador (deletando o disco rígido do colega) tem pena de um a seis meses; já o crime de enviar o vírus (mesmo que nenhum arquivo seja deletado ou danificado) tem pena de 12 a 36

meses. O perigo abstrato será punido com pena de 12 a seis vezes maior do que o dano efetivo. Essa situação, por óbvio, viola o princípio da proporcionalidade.

No plano pragmático

Repete-se o dilema da pressão sobre as instituições públicas porque as penas impedem que o caso tenha o tratamento simplificado dos juizados especiais criminais e exige a instauração de inquérito e oferecimento de denúncia, ou manifestação do Ministério Público e do Judiciário para que ocorra o arquivamento.

Art. 163-A, § 1º, no plano da técnica legislativa

Inicialmente, como esse parágrafo refere-se ao art. 163-A, todas as críticas tecidas naquele artigo aqui se aplicam. É importante frisar que a hiperinclusão nesses casos é muito acentuada. O risco de punição de condutas destituídas de relevância penal é muito grande.

Como exemplo, temos que a utilização de um código que promova o funcionamento não autorizado de um celular ou contorne uma restrição tecnológica qualquer (para acessar conteúdo protegido por direito autoral, por exemplo), acaba punível com pena de dois a quatro anos.

O ato de digitar (inserir) um código (malicioso) no controle remoto para promover o desbloqueio de um aparelho de DVD (dispositivo de comunicação) com o intuito de que ele fique habilitado a exibir o conteúdo de um disco comprado no exterior, por exemplo, também se enquadraria nesse tipo penal, por promover o funcionamento desautorizado do aparelho.

Ainda que se argumente que o legítimo titular do dispositivo de comunicação é o próprio usuário que o desbloqueou, mantém-se o problema quando consideramos que tais aparelhos trazem softwares embarcados (instalados) para seu funcionamento. Nesses casos, o usuário do software não é o seu legítimo titular, mas apenas licenciado para seu uso.

Se levarmos em consideração esse raciocínio, temos que o desbloqueio de um aparelho de celular para executar funções desabilitadas (como o funcionamento em outra operadora ou a instalação de programas antes incompatíveis) ou o próprio desbloqueio do DVD, provocaria o funcionamento não autorizado do software (sistema informatizado) embarcado nesses aparelhos, caracterizando a violação prevista no tipo penal.

Como se vê, repete-se aqui o mesmo problema já mencionado para os outros artigos do projeto de lei, permitindo-se que um particular defina o que é funcionamento autorizado ou não, com a possibilidade de que a lei alcance condutas triviais ou sem qualquer potencial ofensivo.

O art. 6º do projeto de lei

O referido dispositivo do projeto acrescenta o inciso VII ao § 2º do art. 171 do Código Penal, estabelecendo que incorre na mesma pena do estelionato quem praticar a conduta de estelionato eletrônico, definida da seguinte forma:

> Estelionato eletrônico
>
> VII - difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado.

Comentários sobre o dispositivo

No plano da dogmática penal

Esse crime é absolutamente desnecessário. O estelionato já é punido independentemente da forma pela qual ele é praticado. Prever um meio específico para a prática do crime ocasiona o absurdo da possibilidade de descriminalização de determinadas condutas que com o texto atual do projeto de lei seriam consideradas típicas. Aliás, já há várias operações policiais bem-sucedidas que identificaram estelionatários e fraudadores que se utilizavam da internet e que não se valiam, necessariamente, de códigos maliciosos.

Cumpre ressaltar, ainda, que da forma como redigido o artigo pode atingir condutas com baixíssimo ou nenhum potencial ofensivo. Com efeito, aproveitando o exemplo da crítica tecida ao artigo anterior, diversas comunidades e fóruns de discussão na rede mundial de computadores discutem a forma de contornar restrições tecnológicas. Basta uma simples procura na rede para, por exemplo, identificar usuários que ensinam como contornar a restrição utilizada nos aparelhos de DVDs.

Tal conduta, considerando-se a redação da presente proposta, seria punível com pena prevista para o crime de estelionato, qual seja, de reclusão de um a cinco anos e multa.

Com efeito, o ato de postar numa página de discussão o código que deve ser digitado para desbloquear o aparelho, representa o ato de difundir (postar) código malicioso (código a ser digitado) com o intuito de facilitar ou permitir o acesso indevido ao aparelho (dispositivo de comunicação) ou seu software (ou sistema informatizado).

Ainda que um magistrado ponderado afaste o crime num caso como esse, repete-se aqui o dilema da pressão sobre as instituições públicas.

O art. 22 do projeto de lei

O art. 22 do projeto de lei cuida da guarda dos dados necessária à investigação criminal. Dispõe referido artigo, *in verbis*, o seguinte:

> Art. 22. O responsável pelo provimento de acesso a rede de computadores é obrigado a:
> I - manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e por esta gerados, e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;
> II - preservar imediatamente, após requisição judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações requisitadas por aquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
> III - informar, de maneira sigilosa, à autoridade competente, denúncia da qual tenha tomado conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.
> § 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria serão definidos nos termos de regulamento.
> § 2º O responsável citado no *caput* deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R$ 2.000,00 (dois mil reais) a R$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.
> § 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.

Comentários sobre o dispositivo

O artigo em exame contém graves problemas.

Em seu inciso I, cria-se a obrigação de que os provedores de acesso guardem pelo período de três anos todos os dados referentes à conexão de seus usuários a qualquer rede de computadores.

Isso significa, não somente a guarda desses dados por parte dos grandes provedores de acesso à internet, tal como as companhias telefônicas ou de TV a cabo, mas também por parte de todos aqueles que de certa forma provêm o acesso a qualquer tipo de rede (não só à internet), como prefeituras, universidades, escolas, bibliotecas, cafés, restaurantes e quaisquer outros estabelecimentos comerciais.

Já no inciso II, cria-se a obrigação de que todos esses provedores de acesso tenham condições de preservar não só os dados de endereçamento eletrônico da mensagem, mas também "outras informações requisitadas", no que é possível ler qualquer tipo de informação. Dessa forma, impõe-se aos provedores o ônus do monitoramento como prática recorrente, e aos usuários da rede (não só a internet) constantes violações ao seu direito constitucional à privacidade e ao sigilo de correspondência (art. 5º, incisos X e XII).

No inciso III, ato contínuo, o projeto demanda que tais provedores recebam denúncias e que encaminhem de maneira sigilosa tais denúncias à autoridade competente. Tal exigência faria algum sentido se estivéssemos tratando aqui de provedores de conteúdo que, ao receberem uma denúncia de racismo ou de difamação nos comentários de uma notícia, por exemplo, repassariam-na ao órgão governamental responsável. Ainda aqui, seria estranha a obrigação legal imposta aos provedores de receber denúncias e encaminhá-las sigilosamente.

Mas aqui se trata de provedores de acesso à rede, não de provedores de conteúdo. E, assim, não se pode compreender qual o propósito em obrigá-los a receber e encaminhar denúncias sigilosamente. Considerando-se ainda a imposição de multa no desatendimento da autoridade judicial, é inescapável concluir que a aprovação do projeto representaria a criação de sistema indutor da invasão da privacidade dos usuários por parte dos provedores de acesso.

Com efeito, para evitar não atender a autoridade que requisitou dados e minimizar o risco de punição com multa, o provedor tomará todas as medidas para se certificar de que, ao encaminhar denúncias ou atender tais requisições, municiará a investigação com o maior número possível de dados sobre a conduta investigada.

Em outras palavras, tem-se que o art. 22 tal como redigido prevê um sistema de delação a que os provedores estariam sujeitos, na medida em que são incumbidos de informar à autoridade competente qualquer denúncia da qual tenham tomado conhecimento e que contenha indícios da prática de crime. Caberia aos provedores, portanto, informar os casos em que — de acordo com as informações do denunciante e de suas próprias convicções — haveria indício de prática de crime. Como bem se vê, não só há violação evidente de direitos de privacidade, como também a instituição de um verdadeiro sistema de vigilância privada.

Por fim, cumpre ressaltar que a guarda de todos os dados mencionados estará, ainda, sujeita a condições estabelecidas em regulamento (tal como a guarda

em sala-cofre ou condições similares) e a auditoria. Mais que isso, essas condições aplicar-se-ão não só aos grandes provedores, mas a todas as iniciativas de inclusão digital, às redes *wi-fi* e *wi-max*, às universidades, bibliotecas, cafés, e assim sucessivamente. O projeto não prevê exceções.

Ou seja, ainda que a intenção do projeto fosse a de determinar a preservação dos dados para fins de investigação policial e de criar a obrigação de que os provedores de acesso à internet colaborem com a investigação, a verdadeira confusão de termos pode ter efeitos colaterais muito maiores do que o mal que se pretende combater.

É importante frisar que tais disposições afrontam diretamente a proteção constitucional à privacidade, uma vez que obrigam provedores de acesso à rede a possuírem condições de registrar, e efetivamente registrarem, sempre que solicitados, todos os dados que trafegam por seus sistemas. Considerando-se que na internet trafegam dados de naturezas diversas (por exemplo, chamadas telefônicas feitas pelo serviço de voz sobre IP, correspondências pessoais, comunicações de voz, documentos privados ou públicos, entre outros) todos estarão sujeitos a armazenamento e vigilância por parte de provedores.

A situação torna-se ainda mais grave quando se considera a convergência de todas as redes de telecomunicação para a internet, que absorve progressivamente suas funcionalidades. Com isso, a exorbitância do dispositivo proposto afetará qualquer comunicação no país, revogando na prática os dispositivos legais e constitucionais que garantem a inviolabilidade das comunicações e da privacidade. Tal dispositivo dá margem a toda sorte de abusos, e coloca em risco princípios basilares do Estado democrático de direito.

Com a aprovação de tal artigo, portanto, seria revogada na prática a proteção à privacidade e à inviolabilidade que resguardam as comunicações no Brasil. Um dispositivo como esse permitiria que comunicações eletrônicas realizadas em todo o país fossem devassadas sem maiores controles públicos, sob o manto do "segredo" exigido, inconstitucionalmente, pelo próprio projeto de lei.

4. Outras considerações sobre o projeto

O projeto de lei em discussão busca criminalizar diversas condutas no âmbito da rede mundial de computadores. Entre as que procura reprimir, está o envio de vírus de computador, a invasão de servidores de rede e o estelionato, entre outros.

Da forma como redigido o projeto, outras questões acabam abarcadas pelas possíveis interpretações de seus dispositivos, como o enrijecimento das regras de propriedade intelectual, questão sobre a qual há hoje um grande debate e pouco

consenso, em especial quando tratamos de uma opção criminalizadora para combater violações de direito de autor.

Importante ressaltar o que se afirma aqui: não é que seria ilegítimo um debate sobre tal questão no Congresso. Pelo contrário, tal debate é de extrema importância, desde que se dê em foro adequado e de maneira ampla e clara.

Em sentido contrário, temos que o presente projeto não deve ser encarado como a proposta que irá municiar nossas autoridades com a infraestrutura legal necessária para combater crimes como a pedofilia. Com efeito, apesar de tratar dessa questão de maneira superficial, uma das bandeiras que conduziu à aprovação da proposta no Senado foi justamente a do combate à pornografia infantil.

Necessário notar, entretanto, que durante o trâmite do projeto em questão, outro projeto de lei, este sim promovendo um grande avanço no combate aos crimes de pedofilia, foi aprovado no Congresso sancionado pelo presidente da República. Trata-se do PL nº 3.773/08, criado a partir de ampla discussão com a sociedade civil no curso da CPI da Pedofilia, que teve lugar no Senado Federal.

Por fim, é importante esclarecer que o Brasil não assinou o tratado internacional de cibercrimes, denominado Convenção de Budapeste. Referido acordo internacional, com efeito, não contou com a participação brasileira em sua elaboração e foi aprovado no auge do clamor por repressão pós 11 de setembro.

Cumpre destacar que mesmo nos EUA, onde a política nos anos de governo Bush orientou-se de maneira inequívoca para a repressão e criminalização de condutas, foram listadas 13 ressalvas[4] à Convenção de Budapeste. Se por si só tal deveria servir como um alerta, demonstrando que mesmo nos locais mais afeitos à repressão pela via criminal existem ressalvas importantes a serem feitas, é ainda mais relevante e de suma importância frisar que naquele país existem leis civis para a internet desde meados dos anos 1990.

5. Conclusão

Apesar de o atual estágio de tramitação não mais permitir a rejeição do projeto, ainda é possível suprimir os pontos mais graves da proposta.

Para os autores deste artigo, é a medida mais acertada neste momento, pois em primeiro lugar, o direito penal deveria ser utilizado como *ultima ratio,* não como primeira opção de legislação para um setor em desenvolvimento.

Como demonstramos, ainda que se optasse por uma legislação criminal para a questão, a proposta em debate certamente não traz em seu bojo a melhor redação

[4] Council of Europe. Disponível em: <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=26/04/05&CL=ENG&VL=1>. Acesso em: 31 jan. 2009.

para evitar a prática das condutas que o legislador tenta impedir. Da forma como redigida, acaba por abarcar diversas condutas triviais, sem potencial ofensivo e que não colocam em perigo bens jurídicos relevantes.

Outro ponto que merece destaque é a necessidade do preparo de um ambiente regulatório que possibilite o pleno desenvolvimento da internet brasileira. Nesse sentido, imperativa é a criação de uma lei civil definindo responsabilidades e obrigações dos diversos agentes que interagem na rede.

Entre os temas que carecem de regulamentação e que podem ser abordados do ponto de vista civil, destacam-se o da responsabilidade dos provedores de conteúdo por materiais que violam direitos de terceiros, o comércio eletrônico, o Spam, a proteção de dados pessoais dos usuários e seus direitos ante os provedores de acesso e conteúdo.

Apesar dos esforços nessa direção, é evidente a existência de uma tendência criminalizadora e repressiva em diversas legislações, decisões judiciais ou projetos de lei país afora. Exemplos claros são encontrados em propostas como a de proibir as máquinas copiadoras nas universidades, nas rígidas regras impostas às *lan houses*[5] ou na forma como se acaba por impedir os discursos e a expressão contidos em jogos eletrônicos.

Lição importante da experiência legislativa em questão, entretanto, é a de que em ambientes naturalmente ligados à inovação, regras punitivas e estanques retardam o amadurecimento da tecnologia e de novos modelos de negócio, sendo prejudiciais para o desenvolvimento do setor. Mais do que isso, afetam liberdades e desestimulam a experimentação por parte de novos empreendedores.

Quando se trata de tecnologia, cumpre também ressaltar a importância da participação da comunidade técnica ligada ao objeto da regulação. No caso do projeto em debate, a partir da manifestação de movimentos diretamente ligados à questão, foram identificados alguns dos graves problemas técnicos explanados acima.

Isso não significa, outrossim, que tais discussões devam ser delegadas exclusivamente aos operadores do direito e aos técnicos do setor regulado. No caso do projeto em debate, foi a partir da tradução dos conceitos técnicos utilizados para uma linguagem mais acessível que se evidenciou o repúdio de uma grande quantidade de pessoas[6] a uma lei criminal tal como proposta e abriu-se espaço para um verdadeiro debate público sobre a questão.

---

[5] Centros públicos de acesso pago à internet, que congregam outros serviços como a impressão de currículos, jogos eletrônicos etc. No Rio de Janeiro, as *lan houses* devem manter distância mínima de 1.000 metros de estabelecimentos de ensino, de acordo com a Lei nº 4.782/2006.

[6] Em 31 de janeiro de 2009, a petição online organizada contra o projeto contava com 135.876 assinaturas. PETITION ONLINE. Pelo veto ao projeto de cibercrimes – Em defesa da liberdade e do progresso do conhecimento na internet brasileira. Disponível em: <www.petitiononline.com/mod_perl/signed.cgi?veto2008> Acesso em: 31 jan. 2009.

Por fim, e talvez o mais importante, é necessário sempre lembrar que ao tratarmos de projetos em uma seara que ampliou de maneira inequívoca a liberdade de expressão e o acesso a serviços essenciais, ao conhecimento e à informação, é indispensável o exercício de ponderação entre a repressão a condutas inadequadas e os efeitos nocivos dessa política sobre as liberdades e outros direitos fundamentais assegurados em nossa Constituição.