Comentários e Sugestões sobre o Projeto de Lei de Crimes Eletrônicos (PL n. 84/99)

Centro de Tecnologia e Sociedade

Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas

Agosto de 2008

Assinam este documento:

Ronaldo Lemos, professor titular de direito, mestre em direito pela universidade de Harvard, doutor em direito pela Universidade de São Paulo (rlemos@fgv.br);

Thiago Bottino, professor titular de direito penal da FGV Direito Rio, mestre pela PUC-Rio e doutor em direito pela Universidade Estadual do Rio de Janeiro (thiago.bottino@fgv.br);

Carlos Affonso Pereira de Souza, professor de direito, mestre e doutorando em direito pela Universidade do Estado do Rio de Janeiro (caf@fgv.br);

Sérgio Branco, professor de direito, mestre e doutorando em direito pela Universidade do Estado do Rio de Janeiro (sbranco@fgv.br);

Pedro Paranaguá, professor de direito, mestre em direito pela Universidade de Londres (pedro.paranagua@fgv.br);

Pedro Nicoletti Mizukami, professor de direito, mestre em direito pela Pontifícia Universidade Católica de São Paulo (pedro.mizukami@fgv.br);

Bruno Magrani, professor de direito, mestrando em propriedade intelectual pelo Instituto Nacional da Propriedade Industrial (bruno.magrani@fgv.br);

Luiz Fernando Moncau, professor de direito, bacharel em direito pela PUC-SP (luiz.moncau@fgv.br).

Membros do Centro de Tecnologia e Sociedade da Escola de Direito da Escola de Direito da Fundação Getulio Vargas.

O Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (CTS-FGV) vem pela presente apresentar sua contribuição no que diz respeito ao texto do PL 89/03. Trata-se de iniciativa importante, que tem entre os seus objetivos coibir a prática de crimes como a pedofilia, disseminação de vírus, dentre outras práticas aviltantes no âmbito da rede mundial de computadores.

É de se ressaltar, no entanto, que o texto atual do projeto apresenta problemas com relação a sua abrangência e imprecisão, que geram efeitos colaterais graves. Tais problemas ocorrem sobremaneira com relação aos artigos 285-A, 285-B, 163-A em seu parágrafo primeiro, inciso VII do artigo 6° e inciso III do artigo 22.

Ainda que a intenção do projeto seja a de criminalizar somente condutas graves como o roubo de senhas e a disseminação de vírus, a imprecisão da redação dos artigos referidos acima permite que condutas triviais e cotidianas entre usuários da rede mundial de computadores encontrem-se abrangidas pelo tipo penal prescrito pelo projeto. Em outras palavras, se aprovado da forma como está, o projeto leva à criminalização potencial de um grande número de usuários pela prática de atos que em sua maioria são legais ou que são regulados como ilícitos civis em função do seu menor potencial ofensivo.

Como exemplo, através do artigo 2° do Projeto de Lei, acrescenta-se ao Código Penal os artigos 285-A e 285-B. O primeiro, caracteriza como crime "acessar, mediante violação de segurança, de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso".

Com tal redação, além de criminalizar a invasão de sistemas ou o acesso a sistemas protegidos, o artigo proposto acaba também por abarcar a conduta daquele que desbloqueia um aparelho celular (considerado como "dispositivo de comunicação" de acordo com a definição do próprio projeto) ou um aparelho de DVD para assistir a um filme comprado no exterior.

Da mesma forma ocorre com o artigo 285-B, que acrescenta ao Código Penal o ato de "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". É importante mencionar que o projeto não qualifica o termo "expressa

restrição de acesso". Desse modo, essa expressão abrange tanto restrições legais, como contratuais ou tecnológicas. Todas são restrições "expressas" de acesso.

Da maneira como redigido, o artigo pode conduzir o juiz criminal à interpretação de que a transferência ou cópia de dados de um website cujos "termos de uso" vedam expressamente estas práticas, absolutamente corriqueiras, sejam penalizadas com até 3 anos de reclusão. Inúmeras outras condutas cotidianas encontram-se na mesma situação. Por exemplo, a extração de uma música de um tocador de mp3 (considerado como "dispositivo de comunicação" pela definição do próprio projeto) para o computador, contornando restrição tecnológica, passa a se configurar também como crime, mesmo que essa não seja a intenção do legislador. Mais que isso, a cópia de qualquer conteúdo conteúdo protegido por direito autoral de determinado website (considerado como "sistema informatizado" pela própria definição do projeto), cuja reprodução é vedada por "expressa restrição de acesso", no caso derivada da própria lei de direitos autorais, passa a ser tipificada como crime.

Problemas igualmente graves podem ser observados nos artigos 5° e 6°, que acrescentam ao Código Penal o artigo 163-A e inserem, em seu artigo 171, o inciso VII. Apesar da intenção do legislador ser coibir a disseminação de vírus, a definição de "vírus" trazida pelo projeto é por demasiado ampla e criminalizam atividades não só lícitas, mas também necessários à pesquisa e desenvolvimento em pesquisa no país.

Nesse sentido, o Artigo 163-A pode ser considerado como o mais problemático de todo o projeto (Art. 163-A - Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores ou sistema informatizado. Parágrafo 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 de 2 a 4 anos e multa.)

Esse artigo, feito para combater a questão dos vírus do computador, foi muito além do conceito de "vírus". Ele diz respeito a qualquer programa que resulte na "alteração", "dificultação do funcionamento" ou "funcionamento desautorizado pelo legítimo titular". Por exemplo, o artigo torna atividade criminosa punível com pena de 2 a 4 anos de reclusão o desbloqueio do produto "iPhone" utilizando-se para isso de software encontrado na internet. Tal conduta é tipificada como "inserir código malicioso em

dispositivo de comunicação que resulta em funcionamento desautorizado pelo legítimo titular". O termos "funcionamento desautorizado" constante do projeto, dessa forma, gera enorme incerteza jurídica no que tange ao desenvolvimento tecnológico, que dependem sobremaneira de atividades que pesquisem formas não previstas (e muitas vezes não autorizadas) para o funcionamento de dispositivos tecnológicos. Um exemplo disso é a imensa indústria de programação de aplicativos surgida em todo o mundo com o desbloqueio do iPhone, que seria impossível de ter lugar no Brasil caso o projeto seja aprovado.

O inciso VII do artigo 6º também traz problemas importantes (VII - difundir, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatização). Dada a definição de "código malicioso" do artigo 163-A, parágrafo 1º, essa definição vai muito além dos "vírus" de computador. Vale notar que diferente de todas as outras hipóteses de estelionato do Código Penal, esse tipo criminaliza os chamados "atos preparatórios", ou seja, independente de alguém efetivamente receber ou utilizar o "código malicioso", causando dano efetivo, sua mera "difusão" já passa a ser considerada crime. E nesse sentido, por "código malicioso" entende-se qualquer programa de computador que provoque o "funcionamento não autorizado pelo legítimo titular", termo por demais abrangente e incerto.

Por fim, traz também grande preocupação a redação do artigo 22, inciso III do Projeto de Lei n° 84 de 1999. Referido artigo impõe aos provedores de acesso o dever de informar sigilosamente à autoridade competente denúncias que tenha recebido e que contenha indícios de prática de crime. Com tal medida, o provedor investe-se de de prerrogativas atribuídas somente a autoridades detentoras de poder de polícia, estas sim competentes para receber denúncias. Cria-se assim uma obrigação de vigilância por parte de entidade privada, em desatenção aos princípios constitucionais, inclusive que regem o direito penal, como a presunção de inocência, a privacidade e o devido processo legal.

Diante disso, vimos pela presente solicitar que sejam suprimidos do texto final do projeto os artigos 285-A, 285-B (artigo 2° do Projeto), o parágrafo primeiro do artigo 163-A (artigo 5° do Projeto), 171, inciso VII (artigo 6° do Projeto) e o inciso III do artigo 22 do Projeto.

Além dos aspectos apontados acima, cabe também um análise específica no âmbito da dogmática penal, que se segue abaixo.

CONSIDERAÇÕES ATINENTES À SISTEMÁTICA DO DIREITO PENAL

Art. 2º O Título VIII da Parte Especial do Código Penal fica acrescido do Capítulo IV, assim redigido:

"Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

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

O resultado da redação de uma lei penal em branco é a hiperinclusão de condutas destituídas de relevância penal. Ou seja, apesar de não serem materialmente criminosas, serão formalmente criminosas 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 é justificada 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 (multas, interdições etc.).

Esse tipo penal também atinge o princípio da proporcionalidade. Tal se dá porque a ativação do direito penal tem como conseqüência 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. Considera-se 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; não é algo que mereça ser protegido por si só. A segurança do sistema informatizado só merece proteção penal se ela (segurança do sistema) se presta a proteger um bem jurídico.

A lei, então, deve prever que só haverá crime caso algum bem jurídico seja afetado. Se não for assim, mesmo os comportamentos mais inofensivos e corriqueiros serão criminalizados. Vejamos:

Um pai compra um celular e ativa a opção de bloquear o uso com uma senha. O filho vê o celular do pai em cima da mesa e resolve ligar para sua mãe mesmo sem a autorização do pai. O filho então testa algumas opções de senha e acaba por desbloquear o celular e liga para a mãe. Apesar da conduta ser inofensiva, pela redação do tipo penal sugerido haveria crime! Veja-se:

"Acessar (**O FILHO ACESSOU**), mediante violação de segurança (**VIOLANDO A SENHA DE USO PESSOAL**), rede de computadores, dispositivo de comunicação (**UM TELEFONE CELULAR**) ou sistema informatizado, protegidos por expressa restrição de acesso (**BLOQUEADO PELO PAI**)."

Outro exemplo:

Uma empresa limita o acesso dos empregados à internet visando à otimização do trabalho. Proíbe gerentes e pessoal administrativo de acessar a internet, limitando o acesso à intranet. Porém, o protocolo de segurança da rede interna da empresa faculta acesso à internet para diretores e presidente. Um empregado resolve utilizar a senha do chefe, sem o conhecimento deste, para acessar o ORKUT. Trata-se de um comportamento errado, justificaria até uma demissão por justa causa. Mas precisa ser criminalizado? Vejamos:

"Acessar (**O EMPREGADO ACESSOU**), mediante violação de segurança (**VIOLANDO A SENHA DE USO PESSOAL**), rede de computadores (**REDE INTERNA PARA USO DE REDE EXTERNA**), dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso (**A RESTRIÇÃO DECORRE DA PROIBIÇÃO FEITA PELA EMPRESA**)."

Mais um exemplo:

Um usuário de internet decide conversar com uma prima que mora em outro estado. Ao invés de usar o telefone, decide conversar por meio da internet (cujo custo é infinitamente menor) e instala um programa do tipo Skype. Ocorre que a companhia que 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 sua rede para transferência de voz (o chamado voice IP). Para certificar-se de que o usuário será obrigado a pagar pelo serviço mais caro, instala um programa no provedor que não permite a instalação de programas tipo Skype. Mas o usuário não quer se submeter a esse tratamento. Instala um programa que desabilita o bloqueador de Skype e mata as saudades da prima conversando por três horas (ao preço de R$ 0,50; cinqüenta centavos de real). Houve crime?

"Acessar (**O USUÁRIO ACESSOU**), mediante violação de segurança (**DESABILITANDO O BLOQUEADOR**), rede de computadores (**REDE DO PROVEDOR**), dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso (**PROIBIÇÃO FEITA PELA COMPANHIA**)."

Em todos esses casos, teríamos uma punição de até três anos de reclusão em presídio, com privação de liberdade para fatos absolutamente desprovidos de relevância penal. É evidente que não são esses os objetivos da lei penal, mas do jeito que está, abrange-se uma infinidade de condutas inofensivas. É novamente o fenômeno da hiperinclusão.

No plano pragmático:

Há quem sustente que absurdos como o narrado acima nunca acontecerão. Todavia, a história brasileira prova a cada dia que polícia, Ministério Público e Judiciário podem ser integrados por pessoas infinitamente menos razoáveis e ponderadas que o Congresso. Basta, para provar isso, ver como se repetem os

casos de pessoas presas durante meses por furtar balas, manteiga, shampoo, ou mesmo porque urinaram na rua.

Uma vez abrangida pela lei, a conduta inofensiva está sujeita aos rigores do enquadramento como crime. E crime com pena alta, de 1 a 3 anos. O fato da pena ser alta não permite que o fato seja julgado por um Juizado Especial Criminal (onde os julgamentos são céleres e pode-se fazer acordos ou conciliações, filtrando os casos de menor relevância). Isso obriga que o delegado instaure inquérito, realize uma investigação e remeta os autos ao Ministério Público. Mesmo que o promotor ou procurador constate que a conduta é inofensiva, deverá oferecer denúncia pois vigora o princípio da obrigatoriedade da lei penal. E caso o promotor peça o arquivamento (pode alegar o princípio da insignificância, que não é lei mas o judiciário aceita), o juiz deverá concordar com o pedido.

Esse fato somado à hiperinclusão decorrente dos três itens anteriores é capaz de gerar uma forte pressão sobre as instituições (polícia, Ministério Público e Judiciário) que acabe por comprometer seu funcionamento eficaz.

Sugestão: Exclusão integral do artigo 285-A.

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:

Todos os argumentos do artigo anterior (285-A) aplicam-se ao 285-B.

No plano da técnica legislativa:

Repete-se 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*". O resultado da redação de uma lei penal em branco é a hiperinclusão de condutas destituídas de relevância penal. Ou seja, apesar de não serem materialmente criminosas, serão formalmente criminosas e obrigarão o Estado a perseguir todos que as praticarem.

No plano da dogmática penal:

Repete-se 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).

Esse tipo penal também atinge o princípio da proporcionalidade porque a transferência não autorizada não é necessariamente ruim ou danosa. Ao contrário, às vezes ela é 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 este 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 (com notícias do Flamengo e notícias sobre Direito em primeiro plano, por exemplo). Há outros inúmeros possíveis exemplos de hiperinclusão.

No plano pragmático:

Repete-se o dilema da pressão 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.

Sugestão: Exclusão integral do artigo 285-B.

Ação Penal

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:

Esse artigo ficará prejudicado caso os dois anteriores sejam descartados para futuro aperfeiçoamento na redação.

Em todo caso, carrega consigo um problema de ordem dogmática penal e outro de ordem pragmática. No campo 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 notificação da parte daquele que sofreu o crime (a companhia telefônica do exemplo anterior) o Ministério Público estará obrigado a instaurar o processo. Não há nenhum ônus para o particular, o que permite presumir que haverá inúmeras provocações da ação do MP.

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. A polícia é obrigada a investigar de graça e o MP deverá funcionar no processo processando o usuário de internet de graça. Já se antevê, na perspectiva pragmática, a explosão de processos sem relevância que esse tipo penal têm o condão de gerar.

Sugestão: Exclusão integral do artigo 285-C.

Art. 4º O caput do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

"Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio: ....."(NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

"Inserção ou difusão de código malicioso

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.

Comentários sobre o dispositivo:

No plano da técnica legislativa:

Repete-se o dilema da lei penal em branco. Esse crime do 163-A pretende criminalizar a divulgação do chamado "vírus". Porém, o crime está todo calcado no conceito de código malicioso. Ora, hoje não há uma definição jurídica do que seja código malicioso. É verdade que o projeto atual prevê a aprovação de uma definição de código malicioso. Mas se ela for suprimida? E se ela for vetada no momento de sancionar o projeto? Ademais, mesmo que ela seja aprovada, a dinâmica da tecnologia é muito veloz e em breve poderá haver vírus que não se possa subsumir ao conceito de código malicioso. Por fim, o resultado da redação de uma lei penal em branco é a hiperinclusão de condutas destituídas de relevância penal. Ou seja, apesar de não serem materialmente criminosas, serão formalmente criminosas e obrigarão o Estado a perseguir todos que as praticarem.

No plano da dogmática penal:

Em primeiro lugar, repete-se 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. A nova redação sugerida para o crime de dano (art. 163) é suficiente para punir quem destrói dados eletrônicos (arquivos de computador), algo que não existe hoje. A nova redação para o crime de dano (art. 163) é "Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio", 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. E mesmo que a pessoa mal-intencionada que enviou o vírus não tenha sucesso (porque bloqueado o dano pela ação de um anti-vírus) ainda assim pode-se punir a pessoa mal-intencionada 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 1 a 2 terços, na forma do atual art. 14, do Código Penal).

Por outro lado, caso esse artigo seja aprovado e vire lei, será instaurado um absurdo jurídico. Afinal, o crime de danificar os arquivos de computador (deletando o disco rígido do colega) tem pena de 1 a 6 meses; já o crime de enviar o vírus (mesmo que nenhum arquivo seja deletado) tem pena de 12 a 36 meses! **Veja-se que o perigo abstrato será punido com pena de 12 a 6 vezes maior do que o dano efetivo**. Essa situação 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.

Sugestão: Exclusão integral do artigo 163-A.

> **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

Comentários sobre o dispositivo:

No plano da técnica legislativa:

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

Um advogado compra um telefone celular da marca iPhone, importado. Esse telefone está bloqueado para funcionar somente com os serviços de uma determinada companhia telefônica. Se o advogado desbloquear o celular (o desbloqueio não é físico, é feito pelo uso de um software que pode ser enquadrado na definição de código malicioso) ele poderá ser punido com quatro anos de prisão. Afinal, sua conduta encaixa-se no tipo:

Art. 163-A. Inserir ou difundir código malicioso **(ELE INSERIU UM SOFTWARE)** em dispositivo de comunicação **(TELEFONE CELULAR IPHONE)**, rede de computadores, ou sistema informatizado.

Se do crime resulta destruição, inutilização, deterioração, alteração **(RESULTOU ALTERAÇÃO NO FUNCIONAMENTO)**, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular **(O FABRICANTE EXPRESSAMENTE DESAUTORIZOU O USO PARA OUTRA COMPANHIA TELEFÔNICA)**, de dispositivo de comunicação **(TELEFONE CELULAR IPHONE)**, de rede de computadores, ou de sistema informatizado

Seria possível enumerar inúmeros outros exemplos de condutas que não se pretenderia punir, mas que estariam passíveis de criminalização.

Sugestão: Exclusão integral dos parágrafos 1º e 2º do artigo 163-A.

Art. 6º O art. 171 do Código Penal passa a vigorar acrescido dos seguintes dispositivos:

"**Art. 171** .....

§ 2º Nas mesmas penas incorre quem:

.....

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:

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte."

Comentários sobre o dispositivo:

No plano da técnica legislativa:

Repete-se o dilema da lei penal em branco, pois novamente há referência ao conceito de "código malicioso".

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 da 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).

Sugestão: Exclusão integral do parágrafo 2º, inciso VII e do parágrafo 3º do artigo 171.

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.

§ 1° 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.

§ 2° 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.

§ 3° Os recursos financeiros resultantes do recolhimento das multas estabelecidas

Comentários sobre o dispositivo:

O artigo em exame cria um verdadeiro sistema de "vigilância privada", uma vez que estabelece a obrigação, por parte de provedores de acesso à internet, de manterem permanente vigilância sobre seus usuários. Além disso, exige que as denúncias sejam "sigilosas", ao arrepio da Constituição Federal e do devido processo legal. Tais disposições afrontam diretamente a proteção constitucional à privacidade, uma vez que obrigam provedores de acesso à internet a registrarem 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, dentre outros) ***todos*** estarão sujeitos a armazenamento e vigilância por parte de provedores. O art. 22, inciso I, depois de uma leitura preliminar pode não causar muito alarme: observe-se, todavia, que o art. 22, inciso II, também faz referência a "outras informações requisitadas", no que é possível ler *qualquer tipo de informação*, impondo-se aos provedores o ônus do monitoramento indiscriminado como prática recorrente, e aos usuários da internet constantes violações ao seu direito constitucional à privacidade e ao sigilo de correspondência (art. 5º, incisos X e XII), desrespeitando-se igualmente o princípio da dignidade da pessoa humana (art. 1º, inciso III da CF).

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 a privacidade. Tal dispositivo dá margem a toda sorte de abusos, e coloca em risco princípios basilares do Estado Democrático de Direito.

Na verdade, o art. 22 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 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 ***vigilância privada*** no âmbito da internet. Igualmente grave é o fato de o projeto de lei em comento atribuir à esfera administrativa a definição dos "tipos de dados a serem armazenados", suas condições de segurança e regime de auditoria, bem como a "autoridade competente" por ela responsável.

Considerando-se que o presente artigo viola diretamente a Constituição Federal, criando até mesmo um sistema de vigilância privada, não há alternativa possível de ser proposta. Por sua natureza de infração direta a princípios basilares do Estado Democrático de Direito, o dispositivo deve ser repudiado na íntegra.

Na prática, tal artigo simplesmente revoga a proteção à privacidade e à inviolabilidade que resguarda 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 lei.

Sugestão: Exclusão integral do artigo 22. Caso isso não for possível, ao menos o inciso III deve ser suprimido.