Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL n. 84/99) apresentado pela Comissão de Constituição e Justiça e de Cidadania

Novembro, 2010

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Assinam esse documento:

Ronaldo Lemos, professor titular de direito, mestre em direito pela Universidade de Harvard, doutor em direito pela Universidade de São Paulo

Carlos Affonso Pereira de Souza, professor de direito, mestre e doutor em direito pela Universidade do Estado do Rio de Janeiro

Sérgio Branco, professor de direito, mestre e doutorando em direito pela Universidade do Estado do Rio de Janeiro

Pedro Nicoletti Mizukami, professor de direito, mestre em direito pela Pontifícia Universidade Católica de São Paulo

Marília Maciel, professora de direito e mestre em Integração Latino-americana pela Universidade Federal de Santa Maria – UFSM

Joana Varon Ferraz, professora de direito, bacharel em Relações Internacionais pela PUC-SP e mestre em Direito e Desenvolvimento pela FGV-SP

Bruno Magrani, professor de direito, mestre em direito pela universidade de Harvard.

Luiz Fernando Moncau, professor de direito, mestrando em direito constitucional pela PUC-RJ.

Danilo Doneda, professor, mestre e doutor em direito pela UERJ, pesquisador na Autoridade Garante para proteção de dados da Itália.

Pedro Francisco, professor de direito, pós-graduado em Direito do entretenimento pela Universidade do Estado do Rio de Janeiro

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Introdução

Como contribuição aos debates nacionais sobre regulação da Internet no Brasil, o Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas (CTS-FGV) vem, por este documento, apresentar sua análise do texto substitutivo do PL 84/99, redigido após a avaliação da Comissão de Constituição e Justiça e de Cidadania, com relatoria do Deputado Regis de Oliveira.

Ainda que se trate de uma 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, tanto o PL 84/99, como seu substitutivo, têm 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 incis o III do artigo 22.**

No que tange os problemas de abrangência, ainda que a intenção do projeto seja criminalizar somente condutas graves no âmbito da rede, seus dispositivos estendem-se para além da tipificação de condutas criminais, traçando obrigações de vigilância por parte dos provedores de acesso e de conteúdo e obrigações de disponibilização de dados sem que haja a necessidade de ordem judicial, o que representa uma **ameaça à garantia de direitos fundamentais dos usuários**, como, por exemplo, os direitos à **privacidade e ao devido processo legal**. Além disso, a imprecisão da redação dos artigos, por exemplo, ao tratar conceitos relacionados à proteção de dados com pouco rigor técnico, corrobora para aumentar ainda mais essa ameaça aos direitos fundamentais. Permite ainda que condutas triviais e cotidianas entre usuários da rede mundial de computadores encontrem-se abrangidas pelo tipo penal prescrito pelo projeto. Em outras

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

palavras, conforme será demonstrado a seguir, em análise pontual de cada artigo proposto, se aprovado da forma como está, o projeto levará à **criminalização potencial de um grande número de usuários pela prática de atos triviais,** que em sua maioria são legais ou que são regulados simplesmente como ilícitos civis, em função do seu menor potencial ofensivo.

Não obstante, cabe ainda ressaltar que o texto substitutivo, salvo pequenas alterações, apenas repete o texto do PL 84/99, que foi alvo de críticas contundentes por parte da sociedade civil e que, reconhecidas pelos órgãos de governo, em especial o Ministério da Justiça, ensejaram um processo democrático de elaboração de um Marco Civil para a Internet no Brasil, visando estabelecer princípios, garantias e direitos dos usuários de Internet e delimitar deveres e responsabilidades a serem exigidos dos prestadores de serviços. As críticas feitas ao PL 84/99 apontaram ainda que, considerando contexto atual em que se encontra a legislação nacional e a forma como se encontra redigido o Projeto, sua aprovação traria riscos consideráveis ao desenvolvimento pleno da Internet no Brasil. Esses riscos se traduzem tanto em um **desincentivo à existência de um ambiente propício à inovação**, **no qual os agentes empreendedores contam com previsibilidade jurídica e lidam com regras civis claras e pré-estabelecidas**, como também por representar uma **ameaça à garantia de direitos fundamentais dos usuários**.

Para incentivar a inovação, um país precisa contar com regras claras no sentido de estabelecer os limites à responsabilidade dos atores, que permitam segurança e previsibilidade nas iniciativas feitas na rede (tais como investimentos, manutenção de arquivos, bancos de dados, etc). As regras penais devem ser criadas apenas quando as regras civis se mostrem insuficientes, sob pena de se elevar o custo de investimento no setor e desestimular a criação de

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

iniciativas privadas, públicas e empresariais na área. É preciso ter especial atenção para que a legislação criminal a ser adotada não seja excessivamente ampla ou vaga, como é o caso do PL em questão. A excessiva indefinição de termos criminais gera incertezas, especialmente para regular um assunto complexo que demanda definições técnicas prévias, que ainda não foram pensadas legislativamente no país. Por esse motivo, o legislador precisa ser cauteloso ao regulamentar a questão, estabelecendo a precisão necessária para garantir os objetivos da lei, mas sem extrapolar limites ou basear-se em conceitos demasiadamente amplos. Além disso, qualquer medida de regulação que autorize o monitoramento de atividades online, inclusive a guarda de informações dos usuários, deve necessariamente contar com os necessários freios e contrapesos, que evitem abusos, o que não é o caso do projeto em questão.

Essa percepção foi amplamente demonstrada pelos vários agentes que se envolveram na discussão da regulação da internet no país, e que rechaçaram o PL 84/99, bem como por análises de casos internacionais, que deixam claro que o caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é, primeiramente, estabelecer um marco regulatório civil, que defina claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições no que diz respeito ao acesso à rede, para, a partir daí, se definir regras criminais. O **direito criminal deve ser visto como última *ratio***, isto é, o último recurso, que é adotado quando todas as demais formas de regulação falham. Assim sendo, o **texto substitutivo também é falho por não levar em conta todo esse processo de construção democrática do Marco Civil da Internet** e por não apreender com as discussões que se deram naquele âmbito, tratando da necessidade de se assegurar uma lei civil antes de partir para a regulação no âmbito criminal.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Essa não observância ao processo do Marco Civil, que inclusive tem sido estudado e bem avaliado entre acadêmicos e policy-makers dos países desenvolvidos (como, por exemplo, pelo Parlamento Europeu), é ainda mais crítica se observarmos que, desconsiderando as últimas tendências legislativas no país, as justificativas do texto substitutivo do PL 84/99 se baseiam, de maneira recorrente, no argumento de tentar harmonizar nossa legislação com a Convenção de Budapeste. Essa convenção, também denominada Convenção do Cybercrime, foi criada no âmbito do Conselho Europeu, visando estabelecer padrões de combate ao crime online. Aprovada em 23 de novembro de 2001, sem a participação do Brasil, entrando em vigor apenas em 2004, depois da ratificação de somente 5 países. Ainda que aberta para adesão de qualquer país do mundo, até hoje o texto foi ratificado por apenas mais 25 países, principalmente do leste europeu e parte da Europa central, o texto nunca foi aprovado pelo Brasil, mesmo depois de passar pela análise em diversas casas do governo (dentre elas; Ministério da Justiça; o Gabinete de Segurança Institucional da Presidência da República; Departamento de Polícia Federal; o Ministério de Ciência e Tecnologia, e o Ministério das Relações Exteriores), que consideraram o texto proposto à luz do ordenamento nacional. Portanto, não se pode tratar o texto da Convenção como referência para balizar nossa legislação. Os países que se comprometeram com essa Convenção são, principalmente, países que já cumpriram a tarefa de regulamentar a Internet do ponto de vista civil e somente depois disso, estabeleceram parâmetros criminais para a rede. Se tentarmos harmonizar nossa legislação com essa **Convenção que sequer foi aprovada pelo governo brasileiro,** corremos o risco de seguir a via inversa: criando primeiro punições criminais, sem antes regulamentar técnica e civilmente a Internet no país.

Diante do exposto, este estudo tem o objetivo de fazer uma análise dos artigos propostos no texto substitutivo ao PL 84/99, conforme apresentado pela Comissão de Constituição e Justiça e Cidadania (CCJC), ressaltando as pequenas

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

mudanças em relação ao texto anterior, e tecendo comentários mais detalhados no caso de artigos que apontamos como mais críticos tanto como ameaça à direitos fundamentais como ao desenvolvimento da internet no Brasil. Tal **análise será feita tanto por um viés pragmático como doutrinário,** ao se elencar os possíveis impactos sociais do texto proposto, ao criminalizar situações comuns no dia-a-dia do uso da rede, bem como ao levantar suas falhas no que diz respeito à técnica legislativa, razões pelas quais restará **justificada a desconsideração do referido projeto, ou, ao menos, a necessidade de supressão ou alteração dos artigos 285-A, 285-B (artigo 2° do Projeto), art. 1 63 (artigo 4° do projeto), o parágrafo primeiro do artigo 163- A (artigo 5° do Projeto), art. 171, inciso VII (art igo 6° do Projeto), art. 297 (art. 8° do projeto), art 298 (art. 9° do projeto) e o art. 22,** conforme o proposto a seguir:

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Análise comparativa dos artigos mais críticos do texto substitutivo e do texto do PL 84/99: avaliação de seus impactos

Art. 2: modifica Título VIII da parte Especial do Código Penal, acrescentando o 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

Projeto 84/99	Substitutivo Texto repete a redação original	Breves exemplos de impactos práticos negativos	Sugestão do CTS/FGV: Alteração da redação
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	**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	O **consumidor compra um tablet que foi vendido bloqueado** para uso de aplicativos que não sejam produzidos e/ou aprovados pelo fabricante **(ex.Ipad)**. Considerando a diversidade de aplicativos úteis que são lançados de maneira inovadora à margem da aprovação da fábrica, **decide desbloqueá-la**	**Artigo 285-A**. **Invadir** rede de computadores, dispositivo de comunicação ou sistema informatizado **sem autorização de seu titular com o fim de obter vantagem ilícita.** Pena – detenção, de 6 (seis) meses a 2 (dois) anos, e multa § 1°– Na mesma pena incorre quem, **valendo-se de privilégios** de

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.	utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.	para poder utilizar esses aplicativos a seu critério. Ao fazer isso **acessa**, mediante **violação de segurança**, **um dispositivo de comunicação** protegido por **expressa restrição de acesso**. Logo, está sujeito a pena 1 a 3 anos e multa.	administração, acesso direto à rede de computadores, dispositivo de comunicação ou sistema informatizado, ou do uso de recurso técnicos de interceptação de dados, **facilita a realização do crime** previsto neste artigo. § 2°– **Se da invasão resultar** a obtenção de dados confidenciais, instalação de vulnerabilidades, destruição ou alteração de arquivos, controle remoto não autorizado do dispositivo de comunicação, rede de computadores ou sistema informatizado invadido, a **pena é aumentada** de um terço.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação (Art 285-B)

PL 84/99	Substitutivo Altera a redação original	Breves exemplos de impactos práticos negativos	Sugestão de redação do CTS/FGV
Art. 285-B. Obter ou transferir, sem autorização ou em	**Art. 285-B.** Obter ou transferir, sem autorização ou em	Um garoto adquire músicas para seu iPod legalmente. Compra então um outro	Exclusão do Art. 285-B

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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.	desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos legalmente e com 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.	aparelho (como o Microsoft Zune). Decide retirar as músicas do iPod e transferir para o Zune. Com isso, **transferiu**, em **desconformidade com a autorização do legítimo titular** do **dispositivo de comunicação** protegido por **expressa restrição de acesso**, **dado** nele disponível. Logo, está sujeito a pena de 1 a 3 anos e multa. Da mesma maneira, 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.	

Comentários sobre os dispositivos 285-A e 285-B:

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.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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 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 legalmente e com expressa restrição de acesso (PROIBIÇÃO FEITA NO CONTRATO COM A COMPANHIA)." Nesse caso, teríamos uma punição de até três anos de reclusão em presídio, com privação de liberdade para fatos absolutamente desprovidos de relevância penal.

O substitutivo inclui a expressão "protegidos legalmente", que não afasta todas as possibilidades de hiperinclusão de condutas inofensivas, pois é possível interpretar, por exemplo, que tudo que estiver disposto em contrato entre as partes – até mesmo, a princípio, em um contrato de adesão – encontra-se protegido legalmente.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

No plano pragmático: 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 é capaz de gerar uma forte pressão sobre as instituições (polícia, Ministério Público e Judiciário) que acabe por comprometer seu funcionamento eficaz.

Em suma, a redação original dos artigos 285A e 285B foi objeto de críticas contundentes por sua excessiva imprecisão e conseqüente potencial de gerar interpretações amplas que extrapolam o objetivo do tipo criminal. A redação sugerida para o 285-A torna o tipo penal preciso. Além disso, define de forma explícita agravantes para a conduta que não estavam previstas no projeto original (obtenção de dados confidenciais, instalação de vulnerabilidades, destruição ou alteração de arquivos, controle remoto não-autorizado). Com isso, não só o tipo penal fica bem definido, como passa a abranger as condutas que são hoje a principal fonte de preocupações para o sistema bancário e outros grandes administradores de redes, como a clonagem de cartão de crédito e a obtenção de dados de cadastro e senhas de forma não-autorizada.

Ação Penal
Art. 285-C

PL 84/99	Substitutivo Texto repete a redação original	Breves exemplos de impactos práticos negativos	Sugestão de redação do CTS/FGV: Alteração da redação
Art. 285-C. Nos	**Art. 285-C.** Nos crimes definidos	Diante da margem que os	**Artigo 285-B.**

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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.”	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.”	dispositivos anteriores abrem para tipificação de condutas triviais, o tipo de ação penal proposta acarretaria em uma explosão de processos.	Nos crimes definidos neste Capítulo somente se procede mediante queixa, salvo se o crime é cometido contra a União, Estados, Distrito Federal, Municípios, empresas concessionárias de serviços públicos, agências reguladoras, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias.”

Comentários sobre o dispositivo:

No plano da dogmática penal:

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

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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.

Art. 4º Modifica o caput do art. 163 do Código Penal

Dano
Art. 163.

PL 84/99	Substitutivo Texto repete a redação original	Breves exemplos de impactos práticos negativos	Sugestão de redação do CTS/FGV
Art. 163. Destruir, inutilizar ou deteriorar coisa alheia <u>ou dado eletrônico alheio:</u> Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.	Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio: Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.	Alguém acidentalmente apaga um e-mail no computador de outra pessoa (como um casal, amigos ou irmãos que compartilham o mesmo computador). Com isso **destruíram dado eletrônico alheio** e estão sujeitos a pena de 1 a 6 meses de detenção.	Supressão do dispositivo.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Comentários sobre o dispositivo:

No plano da técnica legislativa:
O conceito de "dado informático" presente no artigo 16 do PL 84/99 é demasiado amplo. Seria um e-mail, uma música, ou um banco de dados de uma grande empresa? Um arquivo digital de um acervo histórico? Um índice? Todos devariam ser tratados da mesma forma perante a lei? A indefinição do termo em uma lei penal é grave e pode levar a efeitos colaterais imprevisíveis. Nota-se ainda que uma confusão terminológica perpassa o texto do projeto, uma vez que nas definições e em outros artigos faz-se referência a "dados informáticos" e apenas no artigo 163 menciona-se "dado eletrônico".

No plano da dogmática penal:
Novamente, o texto traz definições amplas, como "dado eletrônico", o que acaba por criminalizar condutas triviais. Por exemplo, se alguém empresta um "pendrive" para um amigo, e essa pessoa acidentalmente apaga um arquivo nele pré-existente, teria cometido um crime, de acordo com o artigo.

Além disso, não se pode equiparar o dano de coisas materiais à destruição, inutilização ou deterioração de "dados eletrônicos", pois, independentemente da sua definição, esses dados circulam em plataformas digitais, e são facilmente deletados, alterados em sua formatação, o que pode levar à inutilização, etc. A pena de detenção, prevista para essas condutas não atende ao princípio da proporcionalidade.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Art. 5º: altera o Capítulo IV do Título II da Parte Especial do Código Penal, acrescentando o art. 163-A

Inserção ou difusão de código malicioso (art. 163-A)

PL 84/99	Substitutivo Altera o texto original	Breves exemplos de impactos práticos negativos	Sugestão de redação do CTS/FGV
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. **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.	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. **Inserção ou difusão de código malicioso seguido de dano** § 1º Produzir intencionalmente ou vender código malicioso destinado ao uso em dispositivo de comunicação, rede de computadores ou sistema informatizado. Pena – reclusão de 1 (um) a 3 (três) anos, e multa. § 2º Se do crime resulta	Um programador brasileiro disponibiliza na internet um programa que permite desbloquear um celular bloqueado. Com isso, **difundiu** código malicioso em **rede de computadores**, que **resulta no seu funcionamento desautorizado** pelo **legítimo titular do dispositivo de comunicação**. Está sujeito a pena de 2 a 4 anos e multa. Cabe ressaltar que nossa legislação autoriza não apenas essas práticas, como, no caso dos celulares, considera a faculdade de desbloqueio um direito do consumidor. A	Alteração do caput e supressão do parágrafo 1°. Artigo 163-A. Art 163-A Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado sem a autorização de seu legítimo titular. Pena – reclusão, de 1 (um) a 2 (dois) anos, e multa. Parágrafo único – Se do crime resulta destruição, inutilização,

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

§ 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.”	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.	Resolução 477 da **Agência Nacional de Telecomunicações** (**Anatel**) determina que as empresas de telefonia celular serão obrigadas a desbloquear os aparelhos, se o usuário assim desejar, sem **nenhum tipo de cobrança**.	deterioração, funcionamento defeituoso, ou controle remoto não autorizado de 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. O resultado da redação de uma lei penal em branco é a hiperinclusão de condutas destituídas de relevância penal. Essa hiperinclusão é ainda maior se forem levados em consideração os parágrafos subseqüentes. O risco de punição de condutas destituídas de relevância penal é muito grande.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

No plano da dogmática penal:
Vejamos exemplos de reflexos negativos que essa hiperinclusão pode causar:

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.

No caso do § 1º, inserido no substitutivo, passa-se a punir não somente o efetivo uso do código malicioso, mas também os atos preparatórios, como sua mera produção e eventual venda. Esse dispositivo é problemático sob inúmeros aspectos. Primeiramente, institui uma barreira legal ao desenvolvimento de softwares e à livre produção de conhecimento nessa área. O processo de desenvolvimento de softwares – incluindo-se os testes feitos para averiguar sua segurança – leva à elaboração de códigos que podem ser entendidos como “código malicioso”. O termo "funcionamento desautorizado" constante do projeto também gera enorme incerteza jurídica no que tange ao desenvolvimento tecnológico, que depende 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

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

de aplicativos surgida em todo o mundo com o desbloqueio do iPhone, cuja existência seria impossível no Brasil, caso o projeto seja aprovado.

Assim, 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 de um produto para habilitar a utilização de aplicativos não autorizados pelo fabricante, utilizando-se para isso de software encontrado na internet. Isso poderia vir a impedir que um consumidor, que adquiriu o aparelho eletrônico legalmente, tenha condições de utilizá-lo em sua plenitude, fazendo uso de quaisque aplicativos que desejar, o que seria uma afronta aos direitos do consumidor.

Além disso, o artigo vai contra a tendência das legislações internacionais que consideram o uso de medidas tecnológicas de bloqueio como práticas de concorrência desleal. Os EUA aprovaram em julho de 2010 um conjunto de novas regras que possibilitam que o usuário efetue não apenas o desbloqueio de operadoras, como também contornem outras medidas de bloqueio tecnológico por processos como os de jailbraking.

Um segundo problema é que o uso dos chamados códigos maliciosos pode ser necessário para viabilizar o direito de acesso a conteúdos. No campo do direito autoral, tem-se identificado que uma das barreiras ao exercício das limitações e exceções previstas em lei (art. 46 da lei 9.610/98) e mesmo ao acesso a obras em domínio público é o uso indiscriminado de travas tecnológicas (TPMs ou DRMs). A introdução de TPMs em obras protegidas enseja um potencial conflito com o exercício das limitações e exceções, pois essas medidas visam a restringir o acesso a determinadas obras, ou ainda a prática de certas ações, como a cópia.

Esse diagnóstico levou à inclusão do art. 107 §2º no texto da proposta de reforma da lei de direito autoral. Se, por um lado, o art. 107 e seus incisos protegem as medidas tecnológicas (DRMs) contra alteração, supressão, modificação ou

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

inutilização, por outro lado, o §2º afirma que a proteção não se aplica quando essas condutas visarem permitir o exercício de limitações e exceções previstas no projeto de lei, ou quando a obra estiver em domínio público.[1] O art. 107 §2º da proposta de reforma da LDA traz uma disposição importante, pois impede que usos permitidos pelas limitações e exceções tornem-se inexequíveis em decorrência das medidas de proteção tecnológica. O dispositivo admite a utilização de ferramentas para burlar TPMs, desde que o objetivo seja permitir as utilizações previstas nos artigos 46 a 48.

Poderia-se pensar que a definição de "código malicioso" ajudaria a separar tipos de código que podem ou não ser produzidos, mas esse não é o caso. A definição de código malicioso (art. 16 IV do PL 84/99) não ajuda a solucionar o problema, pois a expressão "ações danosas" ou "obter informações de forma não autorizada" são de difícil delimitação prática. Por exemplo, segundo pode ser inferido pela regras dos três passos, presente na Convenção de Berna sobre a proteção de obras literárias, artísticas e científicas, o exercício das limitações e exceções pode trazer algum prejuízo ao autor, desde que o mesmo não seja injustificado.

Além disso, aquele que faz uso de dispositivo para burlar uma trava tecnológica (TPM), pode estar obtendo "informação de forma não autorizada" pelo detentor dos direitos autorais, mas agindo de acordo com os ditames constitucionais, que lhe garantem o direito a fruição de bens educacionais e culturais, e, caso a proposta de reforma da lei de direito autoral seja aprovada, pode estar agindo de acordo com a lei específica sobre o tema.

Por conseguinte, o art. 163-A § 1º do substitutivo vai contra os debates que estão sendo travados no âmbito da reforma da lei de direito autoral, pode vir a impedir o uso de "códigos" com finalidade legítima, e configura-se como uma barreira ao desenvolvimento do conhecimento na área de softwares.

[1] "§2º O disposto no caput não se aplica quando as condutas previstas nos incisos I, II e IV relativas aos sinais codificados e dispositivos técnicos forem realizadas para permitir as utilizações previstas nos arts. 46, 47 e 48 desta Lei ou quando findo o prazo dos direitos patrimoniais sobre a obra, interpretação, execução, fonograma ou emissão".

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Justificativa da alteração proposta pelo CTS/FGV:

O dispositivo que tratava de código malicioso no projeto original era excessivamente amplo e vago, com risco da criação de severos danos colaterais. Através da redação acima torna o tipo penal preciso. São mantidas as agravantes do projeto original pertinentes ao tipo, que não extrapolam seu objetivo. A redação adiciona ainda outra conduta não prevista anteriormente na redação atual, com o intuito de coibir o controle remoto através de código malicioso (as chamadas "botnets", compostas de computadores controlados à distância sem o conhecimento do seu respectivo usuário). Por fim, não se encontra incorporada a proibição de produção ou venda de código malicioso, pelas razões apresentadas acima, segundo-se a exclusão do § 1º.

Art 6°. Acrescenta o inciso VII ao art. 171 do Códi go Penal
Estelionato Eletrônico (Art. 171, VII)

PL 84/99	Substitutivo Altera o texto original	Breves exemplos de impactos práticos negativos	Sugestão de redação do CTS/FGV
"Art. 171 ..... § 2º Nas mesmas penas incorre quem: ..... **Estelionato Eletrônico** VII – difunde, por qualquer meio, código malicioso com intuito de	"Art. 171 ..... § 2º Nas mesmas penas incorre quem: ..... **Estelionato Eletrônico** VII – difunde, por qualquer meio, código malicioso com intuito de devastar, copiar, alterar, destruir, facilitar	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	Exclusão integral do parágrafo 2º, inciso VII e do parágrafo 3º do artigo 171

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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 previsto no inciso VII do § 2º, a pena é aumentada de sexta parte.” (NR)	ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, visando o favorecimento econômico de si ou de terceiro em detrimento de outrem: § 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.”	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.	

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”, cujos problemas foram discutidos no comentário feito ao art 163-A. 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.

No plano da dogmática penal:
A introdução das mudanças é desnecessária, pois o estelionato já é punido independentemente da forma pela qual ele é praticado. 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).

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Sugere-se, por essas razões, a exclusão integral do parágrafo 2º, inciso VII e do parágrafo 3º do artigo 171

Art. 8º alteração do caput do art. 297 do Código Penal

Falsificação de dado eletrônico ou documento público
Art 297

PL 84/99	Substitutivo Altera o texto original	Breves exemplos de impactos práticos negativos	Sugestão de redação do CTS/FGV
Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro:	Art. 297. Falsificar ou alterar, no todo ou em parte, dado informático ou documento público verdadeiro:	A falta de clareza na redação do dispositivo, pode dificultar a alteração (e mesmo a elaboração colaborativa) de um amplo rol de conteúdos (músicas, textos, vídeos), disponibilizados por autarquias e fundações públicas, como universidades. Pode ainda dificultar a análise e a associação entre informações fornecidas pelo governo nos portais de transparência.	Supressão do artigo 297

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Comentários sobre o dispositivo:

No plano da técnica legislativa:
Tanto no PL 84/99 como no substitutivo, não fica claro se o adjetivo "público" se refere somente a documento ou se também se refere aos dados eletrônicos (ou informáticos). Essa falta de clareza pode levar à criminalização do simples ato de "alterar dado informático", inviabilizando a manipulação de qualquer informação "numa rede de computadores ou dispositivo de comunicação ou sistema informatizado" (PL 84/99, art 16, V) o que inviabilizaria alteração de um conteúdo em formato digital (um texto guardado no HD de um computador pessoal, por exemplo) e o funcionamento da própria internet.

Mesmo se o adjetivo "público" se aplicar a dados informáticos, subsistem problemas graves em relação a esse artigo. Em primeiro lugar, são muitos os tipos de conteúdo que podem ser incluídos no rol de dados informáticos públicos. O conceito de "dado informático", previsto no art 16, V do PL 84/99, é demasiado amplo. Seria um e-mail, um texto, uma música, ou um banco de dados? Um arquivo digital de um acervo histórico? Um índice? Toda essa informação, de natureza diversa, deveria receber igual tratamento na lei? A indefinição do termo presente em uma lei penal é grave e pode levar a efeitos colaterais imprevisíveis. Há ainda um segundo problema: os dados informáticos públicos seriam dados da Administração pública em sentido estrito, ou também das autarquias e fundações? No segundo caso, dados informáticos de universidades e bibliotecas, inclusive seus acervos, estariam abrangidos. Isso poderia criar um obstáculo à criação colaborativa de conhecimento e cultura no ambiente digital, mesmo no âmbito de instituições voltadas ao ensino e à pesquisa.

No plano da dogmática penal:
Primeiramente, é preciso destacar que a inclusão desse artigo é desnecessária, pois a prática de alteração ou falsificação de documento público, sem que se especifique o meio de difusão, se encontra presente no art. 297 do Código Penal.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

É extremamente danoso erigir um tipo penal em cima de um verbo como “alterar”, que não traz qualquer indício da intenção do agente ou do propósito da alteração. Uma das razões pelas quais informações são disponibilizadas em sites governamentais é o incentivo à transparência. Para que a sociedade possa fazer a análise e a associação entre informações fornecidas pelo governo de forma mais eficiente, é preciso que essa informação seja disponibilizada de maneira que possa ser lida tanto por seres humanos como por máquinas. A leitura por máquinas pode levar a alteração, mediante a associação de dados. Muitas vezes o formato no qual a informação se encontra disponibilizada é alterado nesse processo também. Os próprios agentes governamentais podem ter necessidade de alterar dados informáticos, seja para a sua correção ou atualização.

Art. 9º Modifica o caput do art. 298 do Código Penal

Falsificação de dado eletrônico ou documento particular
Art. 298

PL 84/99	Substitutivo Altera o texto original	Breves exemplos de impactos práticos	Sugestão de redação do CTS/FGV
Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular ou alterar documento particular verdadeiro:	Art. 298. Falsificar ou alterar, no todo ou em parte, dado informático ou documento particular verdadeiro:	Se alguém empresta um “pendrive” para um amigo, e essa pessoa altera um arquivo nele pré-existente, teria cometido um crime, de acordo com o artigo.	Supressão do art. 298

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Comentários sobre o dispositivo:

No plano da técnica legislativa:
Todos os comentários feitos em relação ao artigo 297 aplicam-se aqui. Na verdade, acentua-se nesse artigo o problema já apontado a respeito dos diferentes tipos de conteúdo que podem ser entendidos como "dado informático particular". O conceito de "dado informático", previsto no art 16, V do PL 84/99, é demasiado amplo. Seria um e-mail, um texto, uma música, ou um banco de dados? Um arquivo digital? A aprovação de um artigo como esse poderia lançar na ilegalidade uma cultura de construção colaborativa de conteúdos que floresce atualmente na rede. Por exemplo, alguém que fizesse melhorias e correções a um texto disponível na rede poderia ser enquadrado no crime do art. 298: falsificar ou alterar (O INDIVÍDUO ALTEROU), no todo ou em parte, dado informático (ARQUIVO DE TEXTO) ou documento particular verdadeiro.

É preciso destacar que a inclusão desse artigo é desnecessária, pois a prática de alteração ou falsificação de documento particular, sem que se especifique o meio de difusão, se encontra presente no art. 298 do Código Penal.

Art 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público, bem como os prestadores de serviço de conteúdo, são obrigados a :

PL 84/99	Substitutivo Altera o texto original	Breves exemplos de impactos práticos	Sugestão de redação do CTS/FGV
Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial	Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou	O artigo transforma os provedores de acesso em polícia privada. Passam a	Exclusão integral do artigo 22, a matéria deve ser regulada na esfera civil

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

ou do setor público é obrigado a: I – manter em ambiente controlado e de segurança, pelo prazo de 3 (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 fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial; II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade; III – informar, de maneira sigilosa, à autoridade	do setor público, bem como os prestadores de serviço de conteúdo, são obrigados 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, destino, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória e o Ministério Público mediante requisição; II – preservar imediatamente, após requisição, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade; III – informar, de maneira sigilosa, à autoridade policial ou judicial, informação em seu poder ou que tenha conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal, cuja prática haja ocorrido no âmbito da rede de	ter a obrigação de vigiar os usuários, mesmo aqueles que não estão cometendo nenhum ilícito, e de denunciar "**indícios da prática de crime**" às autoridades	

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

competente, denúncia que tenha recebido 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	computadores sob sua responsabilidade, ressalvada a responsabilização administrativa, civil e penal da pessoa jurídica, sem exclusão das pessoas físicas, autoras, co-autoras ou participes do mesmo fato; § 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a perícia à qual serão submetidos e a autoridade competente responsável por requisitar a perícia, bem como as condições para que sejam fornecidos e utilizados, serão definidos nos termos de regulamento, preservando-se sempre a agilidade na obtenção destas informações e o sigilo na sua manipulação § 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, considerando-se a natureza,		

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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.	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, assegurada à distribuição igualitária entre os Estados membros, na forma de regulamento		

Comentários sobre o dispositivo:

No plano da técnica legislativa:

A redação original do PL 84/99 já apresentava diversos problemas, apontados em estudos anteriores realizados pelo CTS/FGV. O substitutivo sob análise acentua essas deficiências na medida em que afasta o controle judicial, desconsidera conceitos já consolidados no âmbito da proteção de dados e ignora a realidade prática de funcionamento

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

dos provedores de acesso e de conteúdo. Isso traz conseqüências graves tanto para a proteção de direitos fundamentais, quanto para a possibilidade de inovação na rede.

Ao procurar relaxar a necessidade de ordem judicial para a obtenção de dados do usuário pela Autoridade Policial ou Ministério público junto aos provedores de acesso e conteúdo, desconsiderou-se toda uma diversidade de tipos de dados, enquadrando-os apenas como “dados de conexão”, no caso do inciso I, e “outras informações” .

Tanto os dados cadastrais como os demais dados tratados pelos provedores de acesso e conteúdo, sempre que relacionados a uma pessoa identificada ou identificável, são dados pessoais e, como tal, dignos de proteção. Esta proteção pode ser graduada, desde os dados cujo tratamento possa ser tolerado em determinadas circunstâncias até aqueles cuja tutela é elevada ao máximo (caso dos verdadeiros dados sensíveis). Porém todos merecem um mínimo de garantias, entre as quais está a de não poderem ser fornecidos sem que as devidas medidas de controle sejam colocadas em ação, ou seja, via requisição judicial.

Além destes expressivos equívocos ao tratar de dados, o texto também não leva em conta a diversidade que está por traz do conceito de provedores, especialmente dos provedores de serviços de conteúdo, o que pode acarretar em prejuízos significativos ao exercício da liberdade na rede e ao fomento de um ambiente jurídico procípio à inovação na Internet. Por exemplo, um programador, que seja um pequeno empreendedor tentando desenvolver usos criativos em uma determinada plataforma web, muitas vezes com poucos recursos de pesquisa e desenvolvimento, ficará obrigado a criar toda uma estrutura de armazenamento de dados daqueles que acessam sua plataforma, sob pena de multa, antes mesmo de começar a se beneficiar de eventuais lucros da mesma, o que pode, de antemão, inviabilizar sua empreitada.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Com um tipo de previsão como essa, seria inviável, por exemplo, que uma plataforma como o Facebook, pela da maneira orgânica como se deu sua criação (o que é a praxe nos experimentos desenvolvidos na rede), fosse inventada no pais.

No plano da dogmática penal:
Regular os direitos e deveres relativos aos vários tipos de dados gerados pelo usuário quando navega é uma tarefa crucial, uma vez em que há interesses conflitantes e legítimos envolvidos. De um lado, o interesse de privacidade dos usuários, assegurado pela Constituição Federal. E de outro, o interesse de estabelecer condições para a investigação de delitos. Equilibrá-los é tarefa difícil, mas necessária.

O presente artigo, porém, levou em conta apenas o interesse de averiguar a eventual prática de delitos, desconsiderando direitos de privacidade e o princípio do devido processo legal. O dispositivo cria um verdadeiro sistema de "vigilância privada", uma vez que estabelece a obrigação, por parte de provedores de acesso e de conteúdo, de manterem permanente vigilância sobre seus usuários. Além disso, exige que as denúncias feitas por esses provedores sejam “sigilosas”, ao arrepio da Constituição Federal e do devido processo legal (inciso III).

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

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

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.

Por outro lado, durante o processo do Marco Civil, buscou-se opiniões, e portanto, capacitação técnica para tratar dos diferentes tipos de dados que trafegam na rede e para entender as diferentes implicações dos diversos serviços de provisão de acesso e conteúdo. A idéia por trás do Marco Civil é de estabelecer os regimes de armazenamento destes dados, deixando claro, as obrigações, direitos e deveres das partes no âmbito civil. A necessidade de guarda de alguns dados é combinada com o respeito à privacidade e ao devido processo legal, com controle do judiciário. O Marco Civil elenca três espécies de registro:

1) Registro de conexão:
Trata-se dos dados referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP vinculado ao terminal para o recebimento de pacotes de dados, conforme definido pelo Artigo 4º, Inciso V do texto. São

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

os dados que um determinado provedor de acesso (como o Velox, o Speedy e outros) registra dos seus usuários quando eles estão acessando a rede.
Em outras palavras, os registros de conexão dizem quando determinado computador – ou conjunto de computadores, caso estejam usando o mesmo endereço IP – se conectou à Internet. É o registro mais básico que pode ser feito no contexto do Marco Civil, e todas as informações que constam em um registro de conexão são anônimas, isto é, apenas com os registros de conexão não é possível saber quem é o usuário por traz daquelas conexões.

De acordo com o texto da minuta, os registros de conexão deverão ser armazenados somente pelos provedores do serviço de conexão (Velox, Speedy etc.), por um prazo máximo de 6 (seis) meses. Além disso, os provedores de conexão estão impedidos de fiscalizar os pacotes de dados, isto é, utilizar ferramentas técnicas que permitam "enxergar" o tipo de conteúdo que está sendo trafegado.

O prazo de 6 (seis) meses está em concordância com grande parte dos países europeus. Outros projetos de lei que vieram antes do Marco Civil demandavam que esses dados fosse guardados por 3 (três) anos. O Marco Civil entende que esse prazo é muito longo e viola a esfera de expectativa de privacidade dos usuários da internet. Além disso, são poucos os países que praticam prazos de 3 anos, sobretudo aqueles com pendores mais autoritários e policialescos.

2) Registro de acesso a serviços de Internet:
Os registros de acesso, conforme definidos pelo Marco Civil, são os dados referentes à data e hora de uso de um determinado serviço de Internet, a partir de um determinado endereço IP. Em outras palavras, são os dados registrados quando um usuário acessa "serviços de internet", isto é, sites, blogs, sua conta de email, seu perfil em uma rede social etc.

Esses dados são armazenados pelo serviço de Internet (a rede social, o serviço de e-mail, o site, ou o blog). Assim como ocorre nos registros de conexão, esses dados são anônimos e sozinhos não conseguem identificar quem é o usuário.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Pelo texto do Marco Civil, os registros de acesso a serviços de Internet não possuem armazenamento obrigatório. Nenhum site, blog ou outros provedores de serviços de internet precisam armazená-los. Mas o provedor de serviços de Internet (sites, blogs, redes sociais, etc) que desejar fazê-lo, deve informar o usuário a esse respeito, que deve concordar a respeito desse armazenamento. Deve ser informado ao usuário também o período de conservação desses registros.

3) Dados cadastrais:

Dados cadastrais são as informações pessoais que o usuário fornece aos provedores de conexão e aos provedores de serviço de Internet. Essas informações podem incluir noem, endereço, CPF, identidade, idade etc. Em outras palavras, são as informações que são solicitadas do usuário toda vez que ele contrata a prestação de serviços de acesso à internet. Ou então, aquelas informações que o usuário fornece a um site na internet para acessar seus serviços (como a assinatura de um portal, a compra de um produto online, e outras, em que o usuário precisa se identificar para realizar a operação).

Pelo texto do Marco Civil, os dados cadastrais são protegidos e só poderão ser associadas aos registros de conexão ou aos registros de acesso a serviços de Internet mediante ordem judicial. Cabe ao juiz decidir, de acordo com as diretrizes estabelecidas pelo Marco Civil, quando a identidade do usuário pode ser conectadas às suas práticas de acesso online. Só lembrando, hoje no Brasil, com a ausência de regras, há muitos casos em que o usuário é “revelado” por mera requisição administrativa, sem uma ordem judicial. O Marco Civil é contrário a essa situação. Sua proposta é de que a identidade do usuário online só pode ser revelada mediante ordem judicial.

4) Dados de comunicações eletrônicas:

O quarto e último tipo de dados que o Marco Civil se refere são dos dados de comunicações eletrônicas. Tratam-se dos conteúdos trafegados pelos usuários, isto é, o e-mail enviado por ele, uma conversa online por Skype, uma foto enviada, um texto e assim por diante. Em suma, são as “comunicações” feitas pelo usuário através da internet.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

A inviolabilidade e o sigilo das comunicações pessoais são direitos protegidos pela Constituição Federal, derivados do direito à privacidade. Sendo assim, as comunicações eletrônicas feitas pela internet, ou seja, os dados de comunicações eletrônicas, também estão protegidos pela Constituição. O Marco Civil reforça essa questão, dispondo que nenhum usuário da Internet pode ter seu email violado por terceiros (nem qualquer outra comunicação eletrônica).

Comunicações eletrônicas, assim como qualquer outra forma de comunicação pessoal, só podem ser violadas mediante ordem judicial, para fins específicos de investigação criminal ou instrução processual penal. Essas medidas estão previstas e reguladas na Lei 9296/96, que regula as interceptações das comunicações telefônicas, informáticas e telemáticas. O Marco Civil reforça que qualquer forma de violar as comunicações pessoais devem obrigatoriamente seguir os requisitos da Lei 9296/96.

Percebe-se, portanto, um cuidado bem mais significativo do Marco Civil em propor uma categorização dos dados que trafegam na rede, o que decorre em diferentes obrigações por parte dos provedores, mas sempre sob a égide da preservação da privacidade. Todo o cuidado e busca de referências técnicas que foram levados à cabo para que se pudesse elaborar uma legislação civil deveriam ser ainda maiores para uma lei que visa ao estabelecimento de sanções criminais.

Considerando-se que o presente artigo do substitutivo não atende à necessidades de categorizações técnicas sobre os diversos tipos de dados que trafegam na internet, de forma a violar diretamente a Constituição Federal, criando até mesmo um sistema de vigilância privada, não há alternativa possível de ser proposta. Por sua infração direta a princípios basilares do Estado Democrático de Direito, o dispositivo deve ser repudiado na íntegra.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

Considerações finais:

Como se sabe, nas discussões sobre o PL 84/99 o Governo chegou à conclusão que um Marco Civil deveria existir, tratando de direitos e obrigações na rede. A Secretaria de Assuntos Legislativos do Ministério da Justiça (SAL-MJ) e o Centro de Tecnologia e Sociedade da Fundação Getulio Vargas (CTS-FGV) criaram uma plataforma no *site* Cultura Digital[2] para receber comentários sobre a iniciativa.

O processo de consulta pública foi dividido em duas fases. Na primeira, que teve início em outubro de 2009 e durou pouco mais de 45 dias, foi submetido à apreciação da sociedade um texto que continha princípios gerais para a regulação da rede. Os participantes poderiam detalhar esses princípios e propor novos temas a serem abarcados em uma futura legislação.

Durante essa primeira fase de consulta foram recebidos mais de 800 comentários, que foram sistematizados e traduziram-se no texto do anteprojeto posto em consulta pública na plataforma *online* por, inicialmente, mais 45 dias. Atendendo a pedidos diversos, essa segunda etapa foi prorrogada por uma semana e encerrou-se no dia 30 de maio de 2010.

Na última fase houve aproximadamente 1.200 comentários ao texto. Além de indivíduos e organizações da sociedade civil, participaram também empresas e associações ligadas à indústria de conteúdo, tanto nacionais como estrangeiras, o que aumentou a diversidade de opiniões.

Além dos comentários na plataforma de discussão online, o processo de debate público do Marco Civil aproveitou a atividade intensa em outros canais da rede, como as manifestações feitas em blogs e no Twitter. Uma busca pela *hashtag* #marcocivil ofereceu, durante o período da consulta, um bom termômetro da intensidade da participação.

Todos os *tweets* realizados utilizando essa *hashtag* foram considerados como uma forma auxiliar de contribuição. A consulta foi povoada por vários *tweets* do perfil oficial (@marcocivil), provocando a discussão sobre pontos específicos

[2] http://culturadigital.br/marcocivil/

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459

dos três eixos. Todas essas provocações eram prontamente replicadas por vários seguidores. Contou-se também com a participação de pessoas que divulgavam links interessantes, fossem eles artigos sobre o Marco Civil na imprensa ou temas que se relacionavam com o debate e que serviam para enriquecer a discussão. Muitas entidades, empresas e organizações, bem como alguns indivíduos, enviaram suas contribuições através do email de contato do processo. Esses documentos, em sua maioria documentos extensos que analisavam toda a minuta sob consulta, foram submetidos ao público e abertos também à discussão na plataforma online. Tal medida reforçou o aspecto transparente e aberto do debate.

A ferramenta conhecida como *trackback*, que permite aos autores de blogs rastrear links ao seu texto na rede, também foi amplamente utilizada no debate. Desta forma, comentários, opiniões e posições sobre o processo de construção do Marco Civil da internet apresentadas na blogosfera que fizeram links diretos à consulta também foram utilizadas como forma de contribuição. Os debates presenciais, organizados pela equipe da SAL-MJ ou de forma independente, bem como as audiências públicas realizadas ao longo das duas fases do processo, em vários pontos do país, tiveram um papel importantíssimo. Com o término do debate público, coube à equipe do Marco Civil, reunindo representantes da SAL-MJ e do CTS/FGV, compilar todos os comentários, identificar as opiniões prevalecentes e fazer as alterações porventura devidas para finalmente apresentar à comunidade o texto a ser encaminhado ao Congresso Nacional, o que deve acontecer em breve.

A existência desse processo democrático de discussão com a sociedade não podem ser ignorados pelo legislador. É preciso que se leve em consideração o esforço, não só da sociedade, mas do próprio Governo, para tornar o processo de regulação da rede trasparente e participativo. Assim, além de todas as deficiências de técnica legislativa e doutrina criminal do PL 84/99 e seu substitutivo, o fato do presente substitutivo ter sido introduzido às vésperas da apresentação do texto final do Marco Civil ao Congresso e em um período eleitoral é extremamente negativo. Além de inviabilizar o debate público, não dá o devido valor à experiêcia de democracia participativa no âmbito de construção do Marco Civil, que caminha para resultar em um texto com maior precisão técnica e que segue valores previamente pactuados pela sociedade.

FGV DIREITO RIO
Praia de Botafogo, 190 13º andar 22250-900 Rio de Janeiro RJ Brasil
Tel: (55 21) 2559 6065 Fax: (55 21) 2559-5459