



# SENADO FEDERAL

## PROJETO DE LEI DA CÂMARA Nº 35, DE 2012

(nº 2.793/2011, na Casa de origem, do Deputado Paulo Teixeira e outros)

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

“Invasão de dispositivo informático

Art. 154-A. Devassar dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, instalar vulnerabilidades ou obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos, se o fato não constituir crime mais grave.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação Penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266 .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública."(NR)

"Falsificação de documento particular

Art. 298 .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito."(NR)

Art. 4º Esta Lei entra em vigor 120 (cento e vinte) dias após a data de sua publicação oficial.

## **PROJETO DE LEI ORIGINAL Nº 2.793, DE 2011**

Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

O Congresso Nacional decreta:

Art. 1º. Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º. O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal fica acrescido dos seguintes arts. 154-A e 154-B:

### **Invasão de dispositivo informático**

Art. 154-A. Devassar dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, instalar vulnerabilidades ou obter vantagem ilícita:

Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais e industriais, informações sigilosas assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos, se o fato não constitui crime mais grave.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

- I – Presidente da República, governadores e prefeitos;
- II - Presidente do Supremo Tribunal Federal;
- III - Presidente da Câmara dos Deputados; do Senado Federal; de Assembléia Legislativa de Estado; da Câmara Legislativa do Distrito Federal ou de Câmara de Vereadores; ou
- IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

## **Ação Penal**

Art. 154-B. Nos crimes definidos no art. 154-A somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Art. 3º. Os artigos 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, passam a vigorar com a seguinte redação:

### **“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**

“Art. 266.....

.....  
§1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§2º Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública.” (NR)

### **“Falsificação de documento particular**

Art. 298.....

### **Falsificação de cartão**

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Art. 4º. Esta Lei entrará em vigor cento e vinte dias após a data de sua publicação.

## **JUSTIFICAÇÃO**

São inegáveis os avanços para a sociedade decorrentes do uso da Internet e das novas tecnologias. Estes avanços trazem a necessidade da regulamentação de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada em seus efeitos positivos e minimizada em seus impactos negativos. Nesta discussão, ganha relevo constante, sendo objeto de amplos debates sociais, a temática da repressão criminal a condutas indesejadas praticadas por estes meios.

Dentre os inúmeros projetos que abordam a matéria, encontra-se em estado avançado de tramitação neste Congresso Nacional um projeto de lei - o PL 84/99, de autoria do Deputado Luiz Piauhyllino - que tem por objeto a tipificação de “condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam

praticadas contra dispositivos de comunicação ou sistemas informatizados e similares”. Tal projeto, aprovado no Senado Federal em 2008, na forma de um substitutivo, encontra-se em tramitação final nesta Câmara dos Deputados.

A nosso ver, o PL 84/1999, em sua redação atual, traz propostas de criminalização demasiadamente abertas e desproporcionais, capazes de ensejar a tipificação criminal de condutas corriqueiras praticadas por grande parte da população na Internet. Ainda, fixa em um diploma penal matérias - como guarda e acesso a registros de conexão - que deveriam constar de uma regulamentação da Internet que fosse mais abrangente e mais atenta aos direitos e garantias do cidadão. Estas características indesejadas foram amplamente levantadas pela sociedade, por meio de manifestos públicos, movimentos virtuais e abaixo-assinados. Também foram apontadas pelos diversos especialistas que tiveram a oportunidade de apresentar suas contribuições e visões sobre a matéria nos seminários e audiências públicas organizados no âmbito da Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados.

Ocorre que, em seu atual estágio de tramitação, por conta de questões regimentais, o Projeto de Lei referido não pode mais ser emendado ou alterado. Apresentamos, portanto, nossa proposta alternativa de criação de tipos penais específicos para o ambiente da Internet. Esta redação que apresentamos, e que ainda é passível de aperfeiçoamentos e contribuições - sempre de forma a garantir os direitos do cidadão na Internet e evitar a criminalização de condutas legítimas e corriqueiras na Internet - é resultado, portanto, de um processo amplo de discussão, e que iniciou com a submissão de uma minuta preliminar e tentativa no portal e-Democracia, espaço de debate público e participação social por meios eletrônicos da Câmara dos Deputados. A proposta, em sua elaboração, contou também com a participação de órgãos do governo e de representantes da sociedade civil.

Nossa proposta observa, ainda, os direitos e garantias do cidadão que utiliza a Internet, nos termos propostos pelo já mencionado PL 2.126/2010, em tramitação nesta Câmara dos Deputados. Em nosso entendimento, a aprovação deste Projeto deve ser precedida da aprovação do Marco Civil da Internet. Não se deve admitir que legislações penais - infelizmente, um mal necessário em nossa sociedade - precedam o estabelecimento de direitos e garantias. A face repressiva do Estado não deve sobressair sobre seu papel como fiador máximo dos direitos do cidadão.

Em sua redação, buscamos evitar incorrer nos mesmos erros do PL 84/1999. O Projeto propõe, sim, a criação de tipos penais aplicáveis à condutas praticadas na Internet mas apenas aquelas estritamente necessárias à repressão daquelas atividades socialmente reconhecidas como ilegítimas e graves.

Vejamos algumas diferenças entre este Projeto e o PL 84/1999.

Em primeiro lugar, destaca-se que o presente projeto trata apenas de tipificações penais. Diferentemente do PL 84/99, não se abordam as questões relativas a guarda e fornecimento de registros, ou demais obrigações imputáveis a provedores de serviços de internet - questões que encontram lugar mais adequado numa regulamentação civil sobre a matéria.

Em segundo lugar, cabe notar que a presente proposta apresenta um número de tipos penais significativamente inferior àquele apresentado pelo PL 84/99. Norteamo-nos, nesta escolha, pela compreensão de que grande parte das condutas relativas praticadas por meios eletrônicos já se encontra passível de punição pelo ordenamento jurídico pátrio. Ainda, pautamo-nos pela visão de que não é a proliferação de tipos penais que levará à maior repressão de condutas.

Foram excluídas as definições pretensamente exaustivas do PL original, as quais não significavam ganho em precisão e clareza da legislação penal, dada a natureza muito ampla e indeterminada das respectivas redações. Buscou-se, a este respeito, a utilização de terminologias que já encerrasse de forma adequada as condutas que se pretende criminalizar, sem estendê-las indevidamente.

Ainda, com relação ao PL 84/99, nota-se que grande parte dos tipos penais ali propostos apresenta redação significativamente aberta, e muitas vezes sob a forma de tipos de mera conduta, cuja simples prática - independentemente do resultado obtido ou mesmo da específica caracterização da intenção do agente - já corresponderia à consecução da atividade criminosa. Tal estratégia redacional, típica de uma sociedade do risco e de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características. Exemplo disso é a criação de um capítulo com o objetivo de tutelar juridicamente, como bem jurídico protegido, a “segurança dos sistemas informatizados”. Tal estratégia, como já apontado, resulta na possibilidade de punição gravosa a meras condutas que, por sua natureza ou intenção, não mereceriam ensejar a repressão penal - como o acesso não autorizado a sistemas informáticos decorrentes de testes de segurança efetuados sem a prévia anuência dos titulares de sistemas informatizados.

Em contrapartida a esta tendência, o presente projeto de lei busca equilibrar as penas previstas segundo a gravidade das condutas, hierarquizando, a partir de um tipo principal, os patamares de penas aplicáveis a partir dos resultados danosos obtidos pela prática dos atos tipificados - e, obviamente, buscando harmonizar as penas previstas com as já existentes no ordenamento jurídico brasileiro. Busca, tanto quanto possível, orientar as tipificações a partir de um fim especial de agir, consistente na intenção consciente do agente em praticar determinada modalidade de atividade danosa a terceiro. Reinsere as condutas tipificadas na lógica atual dos bens jurídicos penalmente tutelados pelo ordenamento, evitando a expansão desnecessária da proteção penal para novas searas. Acrescenta como elementos básicos do tipo critérios de verificação - de modo, de meio, de finalidade - para que se verifique a conduta como efetivamente punível, buscando assim mitigar os efeitos indesejados de uma tipificação demasiadamente aberta sobre condutas sociais corriqueiras.

Passando à análise específica dos tipos propostos, iniciemos pelo tipo de “invasão de dispositivo informático”, proposto como art. 154-A. O tipo insere-se no capítulo referente a crimes contra a liberdade individual, e na seção correspondente aos crimes contra a inviolabilidade de segredos. Apresenta como elemento nuclear o verbo “devassar”, representando assim um acesso indevido, e aproveitando-se da jurisprudência já consolidada a

respeito do tema quanto à violação de correspondência. Determina que o objeto da violação seja o “dispositivo informático alheio, conectado ou não a rede de computadores”. Evita-se, assim, a tipificação dos casos de violação ou devassa de um equipamento do próprio proprietário, como a remoção de medidas técnicas de proteção embutidas em sistemas operacionais de dispositivos informáticos. Estabelece como elemento necessário para a configuração do crime a violação indevida de mecanismo de segurança - evitando, assim, a criminalização do mero acesso a dispositivos desprotegidos, ou ainda a violação legítima a mecanismos de segurança, como a eliminação de uma medida técnica de proteção que inviabilize o acesso legítimo, em outro dispositivo informático, de uma CD ou DVD protegido, por exemplo. Por fim, estabelece a necessidade de intenção específica de “instalar vulnerabilidades, obter vantagem ilícita ou obter ou destruir dados ou informações não autorizados” - ou seja, pune-se apenas quando a conduta do agente estiver relacionada a determinado resultado danoso ou quando o objetivo do agente for efetivamente censurável e não se confundir com atividades legítimas da Internet, excluindo-se assim, mais uma vez, os casos de mero acesso a informações, ou os casos de obtenção de informações que, por sua natureza, não seriam passíveis de restrição de acesso. Quanto à pena, esta equipara-se à de violação de segredo profissional.

Pena semelhante é atribuída aos casos de produção, oferecimento, distribuição, venda ou difusão de programa de computador com o intuito específico de praticar as condutas definidas no caput. Busca-se, assim, sancionar a produção e difusão de vírus de computador e códigos maliciosos, como aqueles empregados para o roubo de senhas e demais atividades nocivas. Destaque-se, mais uma vez, a necessidade de que a finalidade específica do agente que produz, oferece, distribui, vende ou difunde tal programa de computador seja a de permitir que terceiros pratiquem as atividades nocivas anteriormente tipificadas. Afasta-se, assim, a tipificação da produção e distribuição de ferramentas que tenham por finalidade o mero teste de segurança de sistemas informáticos - e que, caso empregadas indevidamente, possam servir a finalidades nocivas. Isto porque faz-se necessário ao agente o dolo específico de permitir práticas criminosas.

Estabelecemos, ainda, penas proporcionalmente maiores ou causas de aumento de pena para quando a invasão apresentar resultados concretos revestidos de lesividade ainda maior. Isso ocorre, por exemplo, quando, como consequência da invasão, resulta prejuízo econômico para o proprietário do dispositivo invadido, ou quando da invasão resulta o controle remoto do dispositivo invadido, como nos casos da invasão de computadores de terceiros para a prática de atividades nocivas a partir deles.. Também se prevê pena maior - de seis meses a dois anos, e multa - para os casos em que, por meio da invasão, o criminoso obtém mensagens de email de terceiros - que são protegidas pelo direito à privacidade, ou informações expressamente reconhecidas como sigilosas em Lei. A pena cominada pode ainda ser aumentada se houver maior lesividade à privacidade - como nos casos em que houver divulgação, comercialização ou transmissão a terceiro dos dados ou informações sigilosos obtidos.

Ainda no campo da invasão de dispositivos, a proposta traz, em seu parágrafo quinto, traz causa especial de aumento de pena quando o crime é cometido contra determinados sujeitos passivos que correspondam a altas autoridades públicas, por considerar que essas condutas terão lesividade ainda maior.

Quanto a estes crimes, destaca-se que, quando cometidos contra particular, deverão ser objeto de ação penal pública condicionada à apresentação de representação pelo interessado. Evita-se, assim, que haja repressão a condutas reputadas inofensivas pelos próprios ofendidos, com o conseqüente desperdício de recursos na ação estatal repressiva.

O projeto traz ainda duas alterações de artigos já existentes no Código Penal.

O primeiro diz respeito à tipificação da conduta de interrupção, impedimento ou dificuldade do restabelecimento de serviço telemático ou de serviço de informação de utilidade pública. Trata-se de ampliação do tipo atualmente previsto no art. 266 do Código Penal, que, atualmente, protege apenas os serviços telegráficos, radiotelegráficos ou telefônicos. É, portanto, mera “atualização tecnológica” da redação de dispositivo já existente. A esse respeito, destaque-se que um tipo análogo consta da redação da versão atualmente em tramitação do PL 84/1999. No entanto, no âmbito do PL 84/99, também consta como núcleo do tipo penal a mera “perturbação” de tais serviços, o que poderia abranger condutas inofensivas como o excesso de utilização de determinado serviço. O PL 84/99 também inseria como bens protegidos os serviços “telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação”. Destes, foram mantidos apenas o “telemático” e o “de informação de utilidade pública”. Assim, foram mantidos aqueles serviços que corresponderiam essencialmente a serviços públicos - uma vez que o tipo penal insere-se no Capítulo que trata “dos crimes contra a segurança dos meios de comunicação e transporte e outros serviços públicos” - e excluídos aqueles cuja natureza, eminentemente privada, não merecesse este nível de equiparação.

Por fim, incluiu-se a equiparação de cartões bancários eletrônicos, de crédito e débito, a documentos particulares, para permitir a tipificação no âmbito do crime de falsificação de documento particular. Trata-se de dispositivo não previsto no PL original e que preenche omissão hoje existente em nosso ordenamento. Dada a tipicidade estrita do direito penal, é preciso efetuar tal alteração para deixar claro que o crime de “falsificação” também ocorre quando o objeto é um cartão de crédito ou débito.

Espera-se, com este projeto, oferecer à sociedade uma alternativa equilibrada de repressão a condutas socialmente consideradas como indesejáveis, sem no entanto operar a criminalização excessiva e demasiado aberta que permitiria considerar todo e qualquer cidadão como um potencial criminoso em seu uso cotidiano da rede mundial de computadores. Conclamo, assim, os nobres Pares para juntos aprovarmos este projeto de lei e aperfeiçoá-lo durante a sua tramitação nesta Casa de Leis.

Sala das Sessões, em 29 de novembro de 2011

**Deputado Paulo Teixeira**  
**Deputado Luiza Erundina**  
**Deputado Manuela Dávila**  
**Deputado João Arruda**  
**Deputado Brizola Neto**  
**Deputado Emiliano José**

LEGISLAÇÃO CITADA ANEXADA PELA SECRETARIA-GERAL DA MESA

**DECRETO-LEI N° 2.848, DE 7 DE DEZEMBRO DE 1940.**

Código Penal.

.....  
Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:

Pena - detenção, de três meses a um ano, ou multa.

Parágrafo único - Somente se procede mediante representação.

.....  
Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública.

.....  
Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:

Pena - reclusão, de um a cinco anos, e multa.

.....  
*(Às Comissões de Ciência, Tecnologia, Inovação, Comunicação e Informática; e de Constituição, Justiça e Cidadania.)*

Publicado no **DSF**, em 18/05/2012.