# PROJETO DE LEI Nº , DE 2004

**(Do Sr. MARCOS ABRAMO)**

Altera a Lei nº 8.069, de 13 de julho de 1990, a Lei nº 9.296, de 24 de julho de 1996, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, e dá outras providências.

O Congresso Nacional decreta:

Art. 1º Esta lei altera a Lei nº 8.069, de 13 de julho de 1990, a Lei nº 9.296, de 24 de julho de 1996, e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, e dá outras providências.

Art. 2º Acrescente-se ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940, a seção V do Capítulo VI do Título I, com a seguinte redação:

**"SEÇÃO V**

**Dos crimes informáticos**

**Sabotagem informática**

**Art. 154-A. Impedir o funcionamento ou interferir na operação de um sistema informatizado por meio de invasão, introdução, transmissão, dano, apagamento, deterioração, alteração ou supressão de dados informáticos com**

**o objetivo de dificultar, embaraçar ou impedir o funcionamento do sistema informatizado.**

**Pena – detenção, de seis meses a um ano, e multa.**

**§ 1º Nas mesmas penas incorre quem cria, vende, produz, distribui, fornece a terceiro ou mantém a posse intencional de meio indevido de acesso a sistema informatizado.**

**§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Distrito Federal, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.**

**§ 3º Não constitui crime o impedimento ou interferência no funcionamento de sistema informatizado caso haja permissão expressa do responsável pelo sistema.**

**Falsidade informática**

**Art. 154-B. Danificar, alterar, apagar, introduzir ou suprimir dados informáticos de modo a obter ou produzir dados não autênticos para induzir terceiros a erro com a finalidade de obter, para si ou para outrem, vantagem indevida.**

**Pena – detenção, de seis meses a um ano, e multa.**

**§ 1º Nas mesmas penas incorre quem cria, vende, produz, distribui, fornece a terceiros ou mantém a posse intencional de meio indevido de falsificação de dados informáticos.**

**§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Distrito Federal, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.**

**§ 3º A conduta prevista no *caput* deste artigo constitui crime indiferentemente se os dados obtidos ou**

**produzidos estiverem ou não em forma diretamente legível ou inteligível.**

**Fraude informática**

**Art. 154-C. Causar a perda de coisa alheia com intenção fraudulenta de obter, para si ou para outrem, benefício econômico por meio de:**

**I – dano, alteração, apagamento, introdução ou supressão de dados informáticos; ou**

**II – interferência no funcionamento de um sistema informático.**

**Pena – detenção, de seis meses a um ano, e multa.**

**§ 1º Nas mesmas penas incorre quem cria, vende, produz, distribui, fornece a terceiros ou mantém a posse intencional de meio indevido que cause a perda de coisa alheia nos termos deste artigo.**

**§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Distrito Federal, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.**

**Sistema informatizado, dados informáticos, provedor de serviço, assinante, dados de tráfego, dados de conteúdo e informação de assinante**

**Art. 154-D Para efeitos penais, considera-se:**

**I - Sistema informatizado: qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais dentre eles executa o tratamento automatizado de dados;**

**II - Dados informáticos: qualquer representação de fatos, informações ou conceitos expressa sob**

**uma forma suscetível de processamento em um sistema informatizado, incluindo programas de computador aptos a fazer um sistema informatizado executar uma ou mais funções;**

**III - Provedor de serviço:**

**a) Qualquer entidade pública ou privada que faculte aos usuários dos seus serviços a possibilidade de se comunicar por meio de um sistema informatizado; ou**

**b) Qualquer outra entidade que processe ou armazene dados informáticos em nome de um serviço de comunicação ou dos usuários desse serviço;**

**IV - Assinante: usuário do serviço prestado pelo provedor de serviço;**

**V - Dados de tráfego: todos os dados informáticos relacionados a uma comunicação efetuada por meio de um sistema informatizado que forem gerados por esse sistema como elemento de uma cadeia de comunicação e que indicarem a origem, destino, trajeto, hora, data, tamanho, duração e tipo da comunicação;**

**VI - Dados de conteúdo: todos os dados informáticos relativos ao conteúdo de uma comunicação ou de uma mensagem; e**

**VII - Informação de assinante: qualquer informação referente ao assinante que esteja disponível na forma de dados informáticos ou em qualquer outra forma interpretável pelo provedor do serviço, excluindo dados de tráfego ou de conteúdo, que contenha dados relativos ao:**

**a) tipo do serviço de comunicação utilizado e período de prestação do serviço ao assinante;**

**b) identidade, endereço postal ou geográfico, telefone de contato e informações de faturamento e pagamento do assinante; e**

**c) qualquer outra informação sobre o local de instalação do equipamento de comunicação do assinante, se cabível.” (NR)**

Art. 3º Dê-se ao art. 7º da Lei nº 9.296, de 24 de julho de 1996, a seguinte redação:

**“Art. 7º Para os procedimentos de interceptação de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público e aos demais provedores de serviços de telecomunicações, de acesso à Internet e correlatos”. (NR)**

Art. 4º Acrescente-se ao § 1º do art. 241 da Lei nº 8.069, de 13 de julho de 1990, o inciso IV com a seguinte redação:

**“...**

**IV – intencionalmente armazena, guarda ou mantém a posse, em meio eletrônico, de fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.**

**...”.(NR)**

Art. 5º Os provedores de serviços de comunicações deverão manter cadastro de seus assinantes e registro dos acessos executados por eles.

§ 1º O cadastro deverá conter, no mínimo, as seguintes informações de assinante relativas a cada usuário:

I – nome ou razão social;

II – endereço com Código de Endereçamento Postal;

III – número telefônico de contato;

IV – número de registro do assinante no Cadastro de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Poder Executivo;

V – informações de faturamento e pagamento;

VI – tipo de serviço de comunicação utilizado;

VII – período de prestação do serviço ao assinante; e

VIII – local de instalação do equipamento de comunicação do assinante, se cabível.

§ 2º O registro dos acessos executados pelo assinante deverá conter, pelo menos, os seguintes dados de tráfego referentes a cada acesso:

I – identificação do usuário;

II – data e hora de conexão e desconexão;

III – endereço de rede do usuário na transação;

IV – código de acesso telefônico ou identificação do ponto de rede utilizado para executar a conexão; e

V – tipo do serviço utilizado.

§ 3º O provedor de serviço deverá preservar as informações de assinante relativas a cada usuário pelo prazo mínimo de cinco anos após a desvinculação entre as partes.

§ 4º Os dados de tráfego relativos aos acessos executados pelo assinante deverão ser preservados pelo provedor de serviço pelo prazo mínimo de cinco anos contados a partir da sua ocorrência.

§ 5º As informações de que trata este artigo somente poderão ser fornecidas às autoridades competentes mediante determinação judicial.

§ 6º O descumprimento ao disposto neste artigo sujeitará o provedor do serviço à multa de até dois mil reais a cada informação não registrada, acrescida de um terço em caso de reincidência.

§ 7º O provedor de serviço se obriga a armazenar o conteúdo de dados específicos hospedados por terceiros em seu sistema informático, bem como cooperar e ajudar as autoridades competentes na coleta ou armazenamento desses dados, desde que haja determinação judicial específica com essa intenção.

Art. 6º Para efeito da investigação criminal ou instrução processual penal dos crimes informáticos, é lícita a execução das seguintes medidas, desde que devidamente autorizadas por autoridade judicial competente:

I – provisão de segurança física e lógica a um sistema informático ou parte dele, ou a um meio de suporte ao armazenamento de dados informáticos;

II – elaboração ou retenção de cópia de dados informáticos;

III – preservação da integridade de dados informáticos armazenados;

IV – impedimento ao acesso ou remoção de dados informáticos de sistema informático;

V – revelação de informações de assinante ou de dados de tráfego específicos que estejam sob a guarda do provedor de serviço, segundo o disposto no art. 5º desta Lei; e

VI – busca e apreensão de dados informáticos armazenados ou dos meios de suporte a esses dados, estejam eles sob a guarda do provedor de serviço ou do assinante.

§ 1º Se no decorrer da investigação criminal ou da instrução processual penal forem detectados indícios relevantes de que os dados informáticos objeto da investigação ou instrução processual estão armazenados em outro sistema informático, as autoridades responsáveis pela investigação ou instrução processual poderão, de forma sumária, estender a medida executada ao outro sistema informático ou parte dele.

§ 2º Caso seja verificada a necessidade da preservação do sigilo na execução das medidas de que trata este artigo, os registros dessa execução deverão ser efetuados em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, de forma a preservar o sigilo das diligências.

§ 3º O pedido de execução das medidas de que trata este artigo conterá a demonstração de que a sua realização é necessária

para a apuração da infração penal, com indicação dos meios a serem empregados.

§ 4º Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a execução das medidas.

§ 5º O juiz, no prazo máximo de vinte e quatro horas, decidirá sobre o pedido de execução das medidas de que trata este artigo.

§ 6º Em caráter excepcional, os órgãos de investigação competentes terão a prerrogativa de requerer, enquanto aguardam determinação judicial, que o provedor de serviço ou o guardião dos dados informáticos sob investigação preservem a integridade ou mantenham confidenciais todos os dados, registros e informações solicitadas por esses órgãos que estejam relacionados com a investigação em questão.

§ 7º A decisão adotada pelo juiz deverá indicar a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual período uma vez comprovada a indispensabilidade do meio de prova.

§ 8º Deferido o pedido para execução das medidas de que trata este artigo, a autoridade policial conduzirá os procedimentos, dando ciência ao Ministério Público, que poderá acompanhar a sua realização.

§ 9º Para a execução das medidas de que trata este artigo, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público e aos demais provedores de serviços de telecomunicações, de acesso à Internet e correlatos.

§ 10. As medidas de que trata este artigo são aplicáveis inclusive para sistemas informáticos operados em benefício de um grupo fechado de usuários, mesmo que não empreguem redes de comunicações públicas ou que não estejam conectados a outro sistema informático, seja público ou privado.

Art. 7º O Poder Executivo designará um órgão para assistência mútua internacional que se portará como autoridade central responsável pelo contato com países estrangeiros para receber e enviar

solicitações de investigações relacionadas a sistemas e dados informáticos, ou para a coleta de evidências em forma eletrônica de infrações criminais.

§ 1º A autoridade central será responsável pela execução dos pedidos recebidos ou pela transmissão destes às autoridades competentes para a sua execução.

§ 2º A autoridade central poderá, em circunstâncias urgentes, enviar ou receber pedidos de assistência mútua por meios sumários de comunicação, inclusive fac-símile ou correio eletrônico, desde que tais meios ofereçam níveis apropriados de segurança e autenticação e confirmação formal.

§ 3º Em caso de urgência, os pedidos para assistência mútua formulados por países estrangeiros poderão ser recebidos por autoridades brasileiras distintas da autoridade central de que trata o *caput* deste artigo, desde que seja dada ciência imediata às autoridades centrais brasileira e do país de origem da solicitação.

§ 4º Em caso de urgência, os pedidos para assistência mútua formulados pelo Brasil poderão ser enviados por autoridades brasileiras distintas da autoridade central de que trata o *caput* deste artigo, desde que seja dada ciência imediata às autoridades centrais brasileira e do país destinatário da solicitação.

§ 5º A assistência mútua de que trata o *caput* deste artigo incluirá:

a) a provisão de aconselhamento técnico;

b) a adoção de medidas que permitam a execução sumária dos procedimentos previstos no art. 6º;

c) a coleta de evidências em forma eletrônica;

d) a provisão de informações legais; e

e) a localização de suspeitos.

§ 6º Deverá ser mantido sigilo sobre os procedimentos de assistência mútua executados desde que haja solicitação expressa por

parte do país requerente da assistência e que as leis brasileiras não exijam a sua publicidade.

§ 7º Serão recusados os pedidos de assistência mútua relacionados a condutas que não sejam consideradas infrações no Brasil ou aqueles em que a execução do pedido cause riscos à soberania, segurança ou ordem pública nacionais.

§ 8º O disposto neste artigo estará condicionado à existência de reciprocidade entre o Brasil e o país estrangeiro requerente ou recebedor do pedido de assistência mútua.

Art. 8º Fará parte da estrutura da autoridade central de que trata o art. 7º um órgão específico responsável pela assistência imediata e ininterrupta a países estrangeiros com a finalidade de prestar aconselhamento técnico, receber solicitações de apuração de infrações criminais relacionadas a sistemas e dados informáticos e coletar evidências em forma eletrônica de infrações criminais.

§ 1º O órgão de que trata o *caput* deste artigo deverá ter capacidade de se comunicar por meios sumários com órgãos similares estrangeiros, bem como de adotar as medidas necessárias para o rápido encaminhamento dos pedidos de preservação sumária de dados informáticos elaborados por países estrangeiros em conformidade com o art. 9º.

§ 2º O disposto neste artigo estará condicionado à existência de reciprocidade entre o Brasil e o país estrangeiro.

Art. 9º Os países estrangeiros poderão solicitar à autoridade central brasileira de que trata o art. 7º a preservação sumária de dados informáticos armazenados, devendo para isso especificar:

I – a identificação da autoridade que está requerendo a preservação de dados;

II – a infração que é alvo da investigação ou procedimento criminal;

III – breve resumo dos fatos relacionados;

IV – dados informáticos armazenados a serem preservados e sua relação com a infração;

V – qualquer informação disponível com a finalidade de identificar o guardião dos dados informáticos armazenados ou o local do sistema informático;

VI – a necessidade da preservação; e

VII – que o país requerente manifeste a intenção de submeter um pedido formal de assistência mútua para busca, apreensão ou diligência similar.

§ 1º Ao receber o pedido de preservação sumária de dados formulado por país estrangeiro, a autoridade central brasileira adotará todas as medidas apropriadas para preservar de forma sumária os dados especificados.

§ 2º A preservação de dados não deverá ser autorizada por período de tempo inferior a 60 (sessenta) dias, prazo no qual o país estrangeiro deverá submeter pedido formal de assistência mútua à autoridade central brasileira.

§ 3º Após o recebimento de um pedido de preservação de dados informáticos requerido em conformidade com o disposto neste artigo, eles deverão permanecer preservados até que as autoridades competentes brasileiras adotem uma decisão definitiva sobre o pedido de assistência mútua a ele relacionado.

§ 4º Serão recusados os pedidos de preservação de dados informáticos relacionados a condutas que não sejam consideradas infrações no Brasil ou aqueles em que a execução do pedido cause riscos à soberania, segurança ou ordem pública nacionais.

§ 5º O disposto neste artigo estará condicionado à existência de reciprocidade entre o Brasil e o país estrangeiro.

Art. 10. A interceptação em tempo real do fluxo de comunicações em sistemas informáticos relativo a dados de conteúdo e de tráfego é regulada pela Lei nº 9.296, de 24 de julho de 1996 e por esta Lei, no que couber.

Art. 11. Esta lei entrará em vigor na data da sua publicação.

# JUSTIFICAÇÃO

Nos últimos anos, a introdução das novas comodidades proporcionadas pelas tecnologias da informática tem sido acompanhada pela crescente ação dos piratas cibernéticos – os chamados *hackers*. Embora parte da população brasileira venha se habituando paulatinamente a utilizar os serviços prestados via Internet, o volume do comércio eletrônico no País ainda se encontra muito aquém do seu potencial de crescimento em decorrência da insegurança do cidadão em realizar transações comerciais por intermédio da rede mundial de computadores. Até mesmo instituições públicas de grande respeitabilidade perante a opinião pública, como o Banco do Brasil, o Banco Central e o Supremo Tribunal Federal, vêm sendo vítimas da ação criminosa dos *hackers*.

O quadro que se delineia não se observa somente no Brasil, mas principalmente nos países desenvolvidos, onde têm ocorrido intensas discussões sobre a viabilidade da adoção de mecanismos legais com o objetivo de conter a proliferação dos crimes digitais. Fruto desses debates, a Comunidade Européia aprovou, em 23 de novembro de 2001, a Convenção em Cibercrime. O instrumento proposto tipifica como crime diversas condutas praticadas no mundo das tecnologias da informação, além de prever dispositivos específicos com o intuito de agilizar a apuração desses delitos e promover a cooperação entre as nações signatárias da Convenção na sua investigação.

No Brasil, a ausência de um arcabouço jurídico que permita às autoridades judiciárias nacionais enfrentar e punir com rapidez os responsáveis pelas fraudes informáticas estimulou a Câmara dos Deputados a aprofundar o debate legislativo acerca da matéria. A discussão travada sobre o assunto nesta Casa culminou com a aprovação, no ano de 2003, do Projeto de Lei nº 84, de 1999, de autoria do Deputado Luiz Piauhylino, que dispõe sobre os crimes cibernéticos e impõe penalidades para uma série de condutas ilícitas específicas cometidas no ambiente virtual. Atualmente, a proposição se encontra tramitando na Comissão de Educação do Senado Federal, onde já recebeu parecer favorável do Relator no Órgão, Senador Eduardo Azeredo.

Em nosso entendimento, para que o País possa expandir o segmento do comércio eletrônico, é necessário que o nosso ordenamento jurídico esteja sintonizado com a legislação internacional acerca da matéria. Nesse sentido, a intenção do Projeto de Lei de nossa autoria consiste em complementar o PL nº 84, de 1999, na forma em que foi remetido pela Câmara dos Deputados ao Senado Federal, de sorte a adequar as leis brasileiras – vigentes e futuras – ao que estabelece a Convenção Européia.

De forma simplificada, a Convenção em Cibercrime proposta pela Comunidade Européia foi segmentada em quatro partes principais. A primeira delas trata da definição da terminologia relativa aos crimes virtuais e da tipificação dos delitos. Dentre eles, os crimes de acesso ilegal, dano informático, uso indevido de dispositivos informáticos e pornografia infantil já são previstos, no todo ou em parte, no PL aprovado na Câmara dos Deputados. Da mesma forma, o crime de interceptação ilegal já é tipificado na Lei da Escuta – Lei nº 9.296, de 24 de julho de 1996, enquanto que as infrações relacionadas a violações a direitos autorais e conexos já são tratadas na Lei nº 9.610, de 19 de fevereiro de 1998, na Lei nº 9.609, de 19 de fevereiro de 1998, e no art. 184 do Código Penal – Decreto-Lei nº 2.848, de 7 de dezembro de 1940.

Não obstante, os crimes de sabotagem informática, falsidade informática e fraude informática, embora recebam menção expressa na Convenção, não são prescritos nem na legislação vigente nem no Projeto de Lei em apreciação no Senado Federal. Por esse motivo, em nossa proposição, optamos por propor que essas infrações sejam introduzidas ao Código Penal brasileiro. Além disso, no art. 2º de nosso Projeto também adequamos a terminologia utilizada no Código ao disposto na Convenção Européia.

Ademais, o art. 3º de nossa proposta modifica a Lei da Escuta de modo a determinar que não apenas as concessionárias de serviços públicos sejam obrigadas a prestar auxílio ao Poder Público na interceptação de dados informáticos em investigações criminais, mas também os provedores de acesso à Internet e demais empresas prestadoras de serviços correlatos. O dispositivo facilitará sobremaneira a atuação das autoridades policiais, que hoje se vêem limitadas na sua ação contra os *hackers*.

O art. 4º, por sua vez, transforma em crime a posse intencional em meio eletrônico de imagens pornográficas envolvendo crianças ou adolescentes. Por meio desse mecanismo, será legalmente possível enquadrar como criminosos aqueles usuários que detêm em seu poder grande volume de imagens digitalizadas com conteúdo relacionado a atos de pedofilia e que não foram flagrados pelos órgãos de investigação competentes durante a transmissão ou recepção dessas fotos pela rede.

A segunda parte da Convenção Européia trata de providências atinentes à execução processual e à apuração dos crimes cibernéticos. Dentre elas, destaca-se o dispositivo instituído com o objetivo de obrigar os provedores de acesso à Internet a registrar a identidade de seus assinantes e as conexões efetuadas por eles. Além disso, a Convenção impõe aos provedores o encargo de preservar, de forma sumária, dados de assinantes que estejam sob investigação, tais como páginas pessoais hospedadas no provedor que façam apologia a práticas consideradas ilegais no Brasil. Adicionalmente, são previstas medidas com o intuito de tornar mais céleres as diligências relacionadas aos crimes digitais.

Nesse sentido, o art. 5º de nossa proposição prescreve obrigações para os provedores em conformidade com o disposto na Convenção. Ademais, o art. 6º estabelece procedimentos processuais com a intenção de tornar mais desembaraçada a atuação das autoridades policiais e do Ministério Público na apuração das infrações informáticas.

A terceira parte da Convenção dispõe sobre instrumentos de cooperação internacional no combate ao cibercrime. Com esse objetivo, prevê a instituição de mecanismos de assistência mútua entre as nações, assim como a instalação de uma rede de funcionamento 24/7 – vinte e quatro horas por dia e sete dias por semana – para prestação de assistência imediata entre países na investigação de crimes informáticos. Além disso, possui dispositivo que permite a uma nação solicitar a outra a preservação sumária de dados pré-determinados, de modo que sejam reduzidos os riscos de comprometimento na apuração dessa modalidade de crime.

O art. 7º do Projeto de Lei de nossa lavra propõe a instituição de uma autoridade central responsável pelo contato com países estrangeiros no tratamento de delitos virtuais. Por sua vez, o art. 8º prevê a

implantação da rede 24/7 proposta pela Convenção Européia, que hoje já opera no Brasil de maneira informal. Em adição, o art. 9º estabelece procedimentos processuais referentes às solicitações internacionais de preservação sumária de dados informáticos.

Por fim, a quarta e última parte da Convenção apresenta as suas disposições gerais. Nesse capítulo, é prevista a adesão de países não pertencentes à União Européia, desde que haja o convite por parte do Conselho Europeu e a nação interessada consinta com os termos do instrumento.

Acreditamos que, por meio do disposto no Projeto de Lei oferecido, se completará o processo de modernização da legislação brasileira no que diz respeito aos crimes informáticos, iniciado nesta Casa por ocasião da discussão do PL nº 84, de 1999, e de outras proposições que o antecederam.

Além de estabelecer mecanismos essenciais para a agilização da apuração dos delitos digitais, a adaptação da nossa lei aos preceitos da Convenção Européia em Cibercrime permitirá ao País pleitear a assinatura de tal instrumento. Ao se tornar seu signatário, o Brasil estará se equiparando à grande parte das nações desenvolvidas do planeta no que tange ao combate aos crimes dessa natureza.

Ademais, a aprovação do Projeto de Lei apresentado representa uma oportunidade singular para que o Brasil expanda o mercado local de comércio eletrônico e ao mesmo tempo cumpra o desafio de afastar o estigma que ostenta no cenário internacional de abrigar um paraíso de impunidade para os piratas cibernéticos.

Dessa forma, face à relevância da proposição para a nossa sociedade, contamos com o apoio dos ilustres Pares para aprovar a presente iniciativa.

Sala das Sessões, em de de 2004.

Deputado MARCOS ABRAMO