PROJETO DE LEI Nº , DE 2012

Dispõe sobre o Estatuto da Internet no Brasil.

O Congresso Nacional decreta:

CAPÍTULO I

DOS PRINCÍPIOS FUNDAMENTAIS

Art. 1º Esta Lei dispõe sobre o Estatuto da Internet no Brasil.

Art. 2º Compete à União, nos termos das políticas estabelecidas pelos Poderes Executivo e Legislativo, estabelecer diretrizes e regulamentar o uso da Internet no Brasil.

Art. 3º O Poder Público tem o dever de:

I - garantir, a toda a população, o acesso à Internet, a preços razoáveis, em condições adequadas;

II - estimular a expansão do uso da Internet e de seus serviços de interesse público em benefício da população brasileira;

III - criar oportunidades de investimento e estimular o desenvolvimento tecnológico e industrial, em ambiente competitivo;

IV - criar condições para que o desenvolvimento do setor seja harmônico com as metas de desenvolvimento social do País.

Art. 4° O usuário de serviços de Internet tem direito:

I - de acesso aos serviços de Internet, com padrões de qualidade e regularidade adequados à sua natureza;

II - à informação adequada sobre as condições de prestação dos serviços;

III - à inviolabilidade e à confidencialidade de sua comunicação eletrônica, salvo nas hipóteses e condições constitucional e legalmente previstas;

IV - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pelos fornecedores de serviço.

Art. 5° O usuário de serviços de Internet tem o dever de:

I - utilizar adequadamente os serviços, equipamentos e redes de computadores;

II - respeitar os bens públicos e aqueles voltados à utilização do público em geral;

III - comunicar às autoridades irregularidades ocorridas e atos ilícitos cometidos por fornecedor de serviço de Internet e por outros usuários.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 6º Para os efeitos desta Lei, entende-se por:

I – meio eletrônico: o computador, o processador de dados, o disquete, o CD-ROM ou qualquer outro meio capaz de armazenar ou transmitir dados magnética, óptica ou eletronicamente;

II – sistema informático: qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais dentre eles executa o tratamento automatizado de dados;

III – 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 informático executar uma ou mais funções;

IV – 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;

V – assinante: usuário do serviço prestado pelo provedor de serviço;

VI – dados de tráfego: todos os dados informáticos relacionados a uma comunicação efetuada por meio de um sistema informático 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;

VII – dados de conteúdo: todos os dados informáticos relativos ao conteúdo de uma comunicação ou de uma mensagem;

VIII – informação de assinante: qualquer informação referente ao assinante que esteja disponível na forma de dados informáticos ou em qualquer outra forma interpretáveis pelo provedor do serviço, excluindo dados de tráfego ou de conteúdo, que contenha dados relativos:

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

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

c) a qualquer outra informação sobre o local de instalação do equipamento de comunicação do assinante, se cabível.

CAPÍTULO III

DOS REGISTROS DE DADOS DOS USUÁRIOS

Art. 7º 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 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, incluindo números de cartão de crédito ou número de identificação do cliente em bancos;

VI – tipo de serviço de comunicação utilizado;

VII – período de prestação do serviço ao assinante;

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 atribuído, definitiva ou temporariamente, pelo fornecedor de acesso ao cliente ou assinante para uma sessão particular;

IV – endereço de rede remoto que um cliente ou assinante usa ao se conectar ao sistema do fornecedor de acesso;

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

VI – registros locais e de interurbanos das conexões telefônicas;

VII – registros de tempos e de durações das sessões de conexão;

VIII – duração do serviço, incluindo a data de início e os tipos de serviço que utilizou;

XIX – número do telefone ou endereço eletrônico que permitam a identificação do assinante, incluindo os endereços de rede atribuídos temporariamente; e

X – tipo e 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 As informações de que trata este artigo poderão ser divulgadas sem a necessidade de determinação judicial:

I – com o prévio consentimento dos assinantes ou usuários do serviço;

II – por funcionário do provedor de serviço, desde que tal divulgação seja necessária ao restabelecimento das funcionalidades do serviço, proteção de seus direitos ou defesa de propriedade;

§7º O provedor de serviço deverá armazenar o conteúdo de dados específicos hospedados por terceiros em seu sistema informático,

bem como cooperar com as autoridades competentes na coleta ou armazenamento desses dados, se houver determinação judicial específica.

CAPÍTULO IV

DA COOPERAÇÃO INTERNACIONAL

Art. 8º O Poder Executivo deverá designar 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, 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 neste artigo;

c) a coleta de evidências em forma eletrônica;

d) a provisão de informações legais; e

e) a localização de suspeitos.

§ 6º 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.

§ 7º 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.

CAPÍTULO V

DOS CRIMES INFORMÁTICOS

Art. 9º O decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido da seguinte seção V do Capítulo VI do Título I:

“SEÇÃO V

DOS CRIMES INFORMÁTICOS

Acesso ilegítimo

Art. 154-A. Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informático:

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

§1º Nas mesmas penas incorre quem:

a) fornece a terceiro meio indevido ou não autorizado de acesso a meio eletrônico ou sistema informático;

b) transmite no país ou no estrangeiro qualquer informação que contenha qualquer ameaça a integridade de um meio eletrônico ou sistema informático.

§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.

Interceptação ilegítima

Art. 154-B. Interceptar, sem autorização, por meios técnicos, comunicação que se processo no interior de um sistema informático, a ele destinada ou dele proveniente:

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

§1º Nas mesmas penas incorre quem manufature, distribua, possua, divulgue, dissemine, venda ou produza dispositivo específico para a interceptação das comunicações.

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

Interferência ilícita em dados informáticos

Art. 154-C. Apagar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis dados ou programas informáticos alheios ou, por qualquer forma, lhes afetar a capacidade de uso, com o intuito de causar prejuízo a outrem ou obter benefício ilegítimo para si ou para terceiros:

Pena: detenção, de seis meses a 5 (cinco) anos, e multa.

§1º 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.

Interferência ilícita em sistema informático

Art. 154-D. Obstruir, sem autorização, o funcionamento de um sistema informático, por meio da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos:

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

§1º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Distrito Federal, Município, empresas concessionária de serviços públicos ou sociedade de economia mista.

Uso abusivo de dispositivos de interceptação

Art. 154-E. Manufaturar, distribuir, possuir ou fazer propaganda de dispositivos de interceptação de comunicações de qualquer tipo e transmitidas por qualquer meio.

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

§ 1º Nas mesmas penas incorre quem envia no País ou no estrangeiro dispositivos específicos para à interceptação de comunicações orais, telefônicas, por meio de fios ou eletrônicas;

§ 2º Não serão criminosas as condutas tipificadas neste artigo se praticada por:

a) funcionários de prestadores de serviço no curso normal de suas atribuições, desde que necessárias ao fornecimento do serviço;

b) funcionários a serviço do governo da República Federativa do Brasil, no curso normal de suas atribuições.

§ 3º 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.

Manipulação ilegítima de informação eletrônica

Art. 154-F. Manter ou fornecer, indevidamente ou sem autorização, dado ou informação obtida em meio eletrônico ou sistema informático:

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

§1º Nas mesmas penas incorre quem transporta, por qualquer meio, indevidamente ou sem autorização, dado ou informação obtida em meio eletrônico ou sistema informático.

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

Nomes de Domínios Enganadores

Art. 154-G. Usar nome de domínio falso ou enganador, com a intenção de iludir pessoas, para fornecer-lhes visão de materiais obscenos ou pornográficos:

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 facilite a consecução da conduta prevista no ***caput*** 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.

Falsidade informática

Art. 154-H. Danificar, alterar, apagar, introduzir ou suprimir dados informáticos de modo a obter ou produzir dados não autênticos para induzir terceiros a erro.

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.

Sabotagem informática

Art. 154-I. Impedir o funcionamento ou interferir na operação de um sistema informático por meio de invasão, introdução, transmissão, dano, deterioração, alteração ou supressão de dados informáticos com o objetivo de dificultar, embaraçar ou impedir o funcionamento do sistema informático.

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

§ 1º Nas mesmas penas incorre quem cria, manufatura, produz, distribui, fornece a terceiro, vende, faz propaganda, ou mantém a posse intencional de meio indevido de acesso a sistema informático ou meio eletrônico.

§ 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.

Fraude informática

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

I – dano, alteração, 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.”

Art. 10 O art. 163 do decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido dos §§ 2º a 4º com a redação abaixo, alterando-se a numeração do parágrafo único para §1º:

“Art. 163. .....

.....

Dano eletrônico

§2º Equipara-se à coisa:

I – o dado, a informação ou a base de dados presente em meio eletrônico ou sistema informatizado;

II – a senha ou qualquer meio de identificação que permita o acesso a meio eletrônico ou sistema informatizado.

Difusão de vírus eletrônico

§3º Nas mesmas penas do §1º incorre quem cria, insere, difunde, transmite dado, informação, programa, código ou comando em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização ou que exceda os meios de acesso autorizados, com a finalidade de destruí-lo, inutilizá-lo, modificá-lo, causar-lhe danos ou dificultar-lhe o funcionamento.

§4º Nas mesmas penas do §1º incorre quem negligencia em uma ação por meio de computador que dê causa ou traga risco substancial de danos, perdas ou facilite condutas previstas neste artigo.”(NR)

Art. 11 O art. 167 do decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar com a seguinte redação:

“Art. 167. Nos casos do art. 163, §1º, inciso IV, quando o dado ou informação não tiver potencial de propagação ou alastramento, e do art. 164, somente se procede mediante queixa.”(NR)

Art. 12 O decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido do seguinte artigo:

“**Pornografia infantil**

Art. 218-A. Fotografar, publicar ou divulgar, por qualquer meio, cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de um a quatro anos, e multa.

§1º As penas são aumentadas de metade até dois terços se o crime é cometido por meio de rede de computadores ou outro meio de alta propagação.

§2º A ação penal é pública incondicionada.

§3º Nas mesmas penas incorre quem:

I – produz material pornográfico infantil com a finalidade de distribuí-lo por um sistema informático;

II – oferece ou torna disponível material pornográfico infantil por sistema informático;

III – distribui ou transmite material pornográfico infantil por um sistema informático;

IV – obtém, para si ou para outrem, material pornográfico infantil por um sistema informático;

V – detém a posse de material pornográfico infantil em um sistema informático ou em um meio de armazenamento de dados informáticos.

§4º Para os fins do parágrafo anterior, o termo “material pornográfico infantil” incluirá material pornográfico que visualmente descreva:

I - um menor envolvido em conduta sexualmente explícita;

II - uma pessoa que aparente ser um menor envolvido em conduta sexualmente explícita;

III – imagens realísticas que representem um menor envolvido em conduta sexualmente explícita;

IV – uma imagem, desenho ou representação produzida artificialmente, que represente um menor envolvido em conduta sexualmente explícita.”

Art. 13 Os artigos 265 e 266, ambos do Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passam a vigorar com a seguinte redação:

“**Atentado contra a segurança de serviço de utilidade pública**

Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor ou telecomunicação, ou qualquer outro de utilidade pública:” (NR)

“Interrupção ou perturbação de serviço telegráfico ou telefônico

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento: “(NR)

Art. 14 O art. 298 do Decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido do seguinte parágrafo único:

“Art. 298. .....

Falsificação de cartão de crédito

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito.”

Art. 15 O decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido do seguinte artigo:

“**Falsificação de telefone celular ou meio de acesso a sistema eletrônico**

Art. 298-A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de rádio-freqüência ou de telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado:

Pena – reclusão, de um a cinco anos, e multa.”

Art. 16 O art. 2º da lei n.º 9.296, de 24 de julho de 1996, passa a vigorar acrescido do §2º, renumerando-se o parágrafo único para §1º:

"Art. 2º. .....

.....

§2º O disposto no inciso III do *caput* não se aplica quando se tratar de interceptação do fluxo de comunicações em sistema de informática ou telemática."

Art. 17 O art. 138 do decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido do §4º, com a seguinte redação:

"

Calúnia

Art. 138.....

.....

§4º As penas aplicam-se cumulativamente e em dobro, quando a calúnia é veiculada, em todo ou em parte, em redes e sistemas informáticos, de acesso público ou privado."

Art. 18 O art. 139 do decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar com a renumeração do parágrafo único para §1º e acrescido do §2º com a seguinte redação:

"

Difamação

Art. 139.....

§2º As penas aplicam-se cumulativamente e em dobro, quando a calúnia é veiculada, em todo ou em parte, em redes e sistemas informáticos, de acesso público ou privado."

Art. 19 O art. 140 do decreto-lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido do §4º, com a seguinte redação:

“

Injúria

Art. 140.....

§4º As penas aplicam-se cumulativamente e em dobro, quando a calúnia é veiculada, em todo ou em parte, em redes e sistemas informáticos, de acesso público ou privado.”

Art. 20 Dê-se ao art. 7º da Lei n.º 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)

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 21 As multas previstas nesta Lei serão impostas judicialmente, mediante provocação da autoridade não atendida na solicitação.

Art. 22 Os recursos financeiros resultantes do recolhimento de multas estabelecidas nesta Lei serão destinados a Fundo Nacional de Segurança Pública, de que trata a Lei n.º 10.201, de 14 de fevereiro de 2001.

Art. 23 Esta lei entra em vigor no ato de sua publicação.

JUSTIFICAÇÃO

A Internet é uma tecnologia que se tornou indispensável na vida moderna. Entretanto, como acontece em todas as novas tecnologias, ela pode ser usada também para finalidades inadequadas, como meio para indivíduos possam obter vantagens ilícitas, em prejuízo alheio.

Esse aspecto fica evidente quando verificamos a expansão praticamente exponencial da criminalidade na rede mundial de computadores. Algumas estimativas dão conta de que os lucros auferidos com crimes praticados por meio da Internet já são maiores do que o oriundo do tráfico de entorpecentes.

Esse contexto deixa evidente a necessidade de estabelecermos um marco legal que tenha o intuito de criar as bases para o funcionamento de um ambiente virtual estável e seguro, onde os cidadãos, empresas e governos possam interagir sem estarem vulneráveis e expostos à cibercriminalidade.

A proposta desse marco legal para a Internet deve conter necessariamente obrigatoriedade de registros por parte dos provedores, tipificações penais específicas para condutas no ambiente digital, dispositivos processuais que visam agilizar os processos de investigação pelas autoridades públicas, definição de conceitos e a instituição do arcabouço legal que sustente a cooperação do Brasil em acordos internacionais de elucidação de crimes digitais, como é o caso da Convenção de Budapeste – tratado internacional que se propõe a promover a cooperação dos países no combate ao cibercrime.

O texto que apresentamos, portanto, aborda a questão de segurança da informação digital de forma ampla e sintonizada com os mais avançados dispositivos legais em vigência no mundo. Assim, o Capítulo I trata dos princípios fundamentais que devem nortear a expansão da Internet no Brasil, além de definir direitos e deveres tanto para usuários quanto para o Poder Público, notadamente os formuladores de políticas publicas – Poderes Executivo e Legislativo.

No Capítulo II introduzimos as definições dos aspectos que se relacionam à matéria, com o intuito de elevar os níveis de previsibilidade na interpretação da norma no âmbito judicial, objetivando o

aprimoramento da segurança jurídica, evitando, porém, tornar a lei vinculada ao estado atual do desenvolvimento tecnológico, o que nos levou a optar por definições genéricas e em consonância com legislações internacionais. Consideramos que, assim, conseguimos conferir perenidade à norma, evitando sua obsolescência ante a introdução de novas tecnologias.

A questão da obrigatoriedade de implementação de cadastros de usuários e seus registros transacionais é tratada no Capítulo III da nossa proposta, nos quais utilizamos as normas e conceitos emanados tanto da referida Convenção de Budapeste quanto legislações estrangeiras já plenamente assentadas no ordenamento jurídico de seus respectivos países.

Outro aspecto muito importante no combate ao crime digital é seu caráter transnacional, o que demanda a construção de mecanismos legislativos que permitam às autoridades públicas se relacionarem de forma ágil, eficiente e cooperativa com outros países.

Esses dispositivos que procuramos introduzir no Capítulo IV, visando a instituição de uma autoridade central responsável pelo contato com países estrangeiros no tratamento de delitos virtuais, a implantação da rede 24/7 proposta pela Convenção de Budapeste e a definição de procedimentos processuais referentes às solicitações internacionais de preservação sumária de dados informáticos.

Os mecanismos propostos são aderentes aos princípios emanados pela Convenção de Budapeste, o que permite ao Brasil, dessa forma, assinar acordos de cooperação com os países signatários daquele tratado.

As tipificações penais necessárias a imputação criminal são tratadas no Capítulo V, por meio de uma série de emendas ao Código Penal Brasileiro, abrangendo todas as condutas praticadas por criminosos digitais. Além disso, as modificações na Lei de Escuta - Lei n.º 9.296, de 24 de julho de 1996 - determinam 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 que facilitará a atuação das autoridades policiais.

Assim sendo, entendemos que o texto oferecido é um marco legal sintonizado com as legislações mais avançadas do mundo, absorvendo o que existe de mais moderno no tratamento da matéria ao incorporar os conceitos que emanaram da Convenção de Budapeste, o que permitirá ao País pleitear a assinatura de tal instrumento, mecanismo institucional de grande eficiência no combate aos crimes digitais no contexto global.

Diante do exposto, peço o apoio dos nobres parlamentares desta Casa para a aprovação deste Projeto de Lei.

Sala das Sessões, em de de 2012.

Deputado Edson Pimenta