Resenha didática - tipificação e punição dos crimes de informática[1]

PLS 76/2000 (PLC 89 de 2003 e PLS 137 de 2000)

O Substitutivo apresentado pelo Senador Eduardo Azeredo aglutinou três projetos de lei que já tramitavam no Senado, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências (veja as razões em detalhe no Apêndice B).

O PLC 89, de 2003, de autoria do Deputado Luiz Piauhylino, altera:

- o **Código Penal**, Decreto-Lei nº 2.848, de 7 de dezembro de 1940;
- a **Lei de Interceptações Telefônicas**, Lei nº 9.296, de 24 de julho de 1996.

O PLS 76, de 2000, de autoria do Senador Renan Calheiros, nos termos do Substitutivo, altera as duas leis acima e mais:

- o **Código Penal Militar**, o Decreto-Lei nº 1.001, de 21 de outubro de 1969;
- o **Código do Processo Penal**, Decreto-Lei nº 3.689, de 3 de outubro de 1941;
- a **Lei da Repressão Uniforme**, a Lei nº 10.446, de 8 de maio de 2002;
- o **Código do Consumidor**, Lei nº 8.078, de 11 de setembro de 1990.

O PLS 137, de 2000, de autoria do Senador Leomar Quintanilha, determina:

- o aumento das penas ao triplo para delitos cometidos com o uso de informática.

A Convenção sobre o Cibercrime, do Conselho da Europa

A Convenção sobre o Cibercrime, celebrada em Budapest, Hungria, a 23 de novembro de 2001, pelo Conselho da Europa, teve como signatários 43 paises, europeus na sua maioria (veja lista detalhada no Apêndice A) e ainda Estados Unidos, Canadá e Japão. Cada Estado signatário deve ratificar as disposições constantes da Convenção no seu ordenamento jurídico interno.

Embora o Brasil ainda não seja signatário da Convenção sobre o Cibercrime, pode ser considerado um país em harmonia com suas deliberações, pois o presente Projeto de Lei já atende às recomendações do seu Preâmbulo, como, por exemplo, “a adoção de poderes suficientes para efetivamente combater as ofensas criminais e facilitar a sua detecção, investigação e persecução penal, nos níveis doméstico e internacional e provendo protocolos para uma rápida e confiável cooperação internacional”.

A harmonia é importante para otimizar a repressão dos crimes de informática, notadamente transnacionais. O presente Projeto de Lei coloca o Brasil em condições de poder tratar e acordar de maneira diferenciada, o que facilitará em muito a cooperação judiciária internacional e eventuais extradições, com os países signatários da Convenção de Budapest e outras, inclusive os EUA, país sede dos maiores provedores de acesso à rede mundial de computadores.

Em resumo a Convenção recomenda procedimentos processuais penais, a guarda criteriosa das informações trafegadas nos sistemas informatizados e sua liberação para as autoridades de forma a cumprir os objetivos relacionados no preâmbulo. Além disso, trata da necessária cooperação internacional, das questões de extradição, da assistência mútua entre os Estados, da denúncia espontânea e sugere procedimentos na ausência de acordos internacionais específicos, além da definição da confidencialidade e limitações de uso. Define também a admissão à Convenção de novos Estados por convite e a aprovação por maioria do Conselho.

Resenha didática - tipificação e punição dos crimes de informática[2]

PLS 76/2000 (PLC 89 de 2003 e PLS 137 de 2000)

A harmonia crescente da legislação brasileira com a Convenção sobre o Cibercrime

A legislação brasileira em vigor já tipifica alguns dos crimes identificados pela Convenção, como os crimes contra os direitos do autor e crimes de pedofilia, e, caso a caso, cuida de alguns outros já tipificados no Código Penal. Veja abaixo o que segundo a Convenção, a legislação penal em cada Estado signatário deve tratar e a sua correspondência na legislação brasileira:

As leis brasileiras e a Convenção de Budapest (CP – Código Penal CPM – Código Penal Militar)

Recomendação da Convenção	Artigos das leis ou códigos
1 - do acesso ilegal ou não autorizado a sistemas informatizados	154-A e 155 § 4º,V do **CP** 339-A e 240 § 6º,V do **CPM**
2 - da interceptação ou interrupção de comunicações,	art. 16 do **Substitutivo**
3 - da interferência não autorizada sobre os dados armazenados	154-D, 163-A e 171-A do **CP** 339-D, 262-A e 281-A do **CPM**
4 - da falsificação em sistemas informatizados	163-A, 171-A, 298 e 298-A do **CP** 262-A e 281-A do **CPM**
5 - da quebra da integridade das informações	154-B do **CP** 339-B do **CPM**
6 - das fraudes em sistemas informatizados com ou sem ganho econômico	163-A e 171-A do **CP** 262-A e 281-A do **CPM**
7 - da pornografia infantil ou pedofilia	241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (**ECA**), alterado pela Lei 10.764, de 2003;
8 - da quebra dos direitos de autor	Lei 9.609, de 1998, (a **Lei do Software**), da Lei 9.610 de 1998, (a **Lei do Direito Autoral**) e da Lei 10.695 de 2003, (a **Lei Contra a Pirataria**);
9 - das tentativas ou ajudas a condutas criminosas	154-A § 1º do **CP** 339-A do **CPM**
10 - da responsabilidade de uma pessoa natural ou de uma organização	art. 21 do **Substitutivo**
11 - das penas de privação de liberdade e de sanções econômicas	penas de detenção, ou reclusão, e multa, com os respectivos agravantes e majorantes, das **Leis citadas** e dos artigos do **Substitutivo**.

A posição oficial do Brasil em relação à Convenção sobre o Cibercrime

Em dezembro de 2006 a Comissão de Relações Exteriores e Defesa Nacional do Senado Federal (CRE) aprovou Requerimento de Informações, de autoria do Senador Eduardo Azeredo, solicitando ao Ministério das Relações Exteriores qual o posicionamento oficial do Brasil em relação à Convenção, uma vez que ele ainda não é dela signatário.

Em fevereiro de 2007 o Senador Eduardo Azeredo foi recebido em audiência pelo Senhor Ministro das Relações Exteriores, Celso Amorim, tratando, entre outros assuntos, da Convenção sobre o Cibercrime e a posição do Brasil.

Resenha didática - tipificação e punição dos crimes de informática[3]

PLS 76/2000 (PLC 89 de 2003 e PLS 137 de 2000)

Em março de 2007 o Senador Eduardo Azeredo recebeu em audiência o Chefe de Cooperação Técnica, do Departamento de Problemas Criminais, da Secretaria Geral do Conselho da Europa. Ele sugeriu à Coordenadora Geral contra o Crime Transnacional do Ministério das Relações Exteriores, o envio de carta ao Conselho manifestando o interesse do Brasil à Convenção, após o que o Conselho ouvirá os seus Membros para que então o Brasil seja convidado a participar.

Os crimes ou delitos tipificados no Substitutivo são:

1 – Roubo de senha - Difusão de Código Malicioso – inclusão do art. 171-A – Fraude

É a tipificação do "phishing" com pena de reclusão, de um a três anos. Foi incluída a majorante de pena de uma sexta-parte se o autor se vale de nome falso ou da utilização da identidade de terceiros. Exclui o profissional que opera a defesa digital ou contra-ataque.

2 - Falsificação de cartão de crédito – inclusão de parágrafo único ao art. 298

Mantida a pena, passa a ser "Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico ou digital ou similar portátil de captura, processamento, armazenamento e transmissão de informações".

3 - Falsificação de telefone celular ou meio de acesso a sistema – inclusão do art. 298-A

Mantida a pena, passa a ser "Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado incluindo outros dispositivos falsificáveis".

4 - Calúnia, difamação e injúria - crimes contra a honra – inclusão do art. 141-A

Substitutivo inclui majorante de dois terços da pena para os casos em que os crimes do capítulo de "Crimes contra a Honra" – calúnia, difamação e injúria – são praticados mediante uso de informática.

5 - Difusão de Código Malicioso para causar dano – inclusão do art. 163 – A – "vírus"

O texto atualizou a redação dos projetos originais, colocando a difusão de código malicioso que cause dano, como, por exemplo, o "vírus", o "worm", o trojan", o "zumbi" etc. A pena prevista para quem comete esse crime foi alterada para reclusão. Exclui o profissional que opera a defesa digital ou contra-ataque.

6 - Acesso não autorizado – inclusão do art. 154-A

Aumenta a pena de uma sexta-parte, se o autor se vale de nome falso ou da utilização da identidade de terceiros. Exclui o profissional que opera a defesa digital ou contra-ataque.

7 – Obtenção não autorizada de informação e manutenção, transporte ou fornecimento indevido de informação obtida desautorizadamente – inclusão do art. 154–B

Foi incluída a conduta da utilização de informação além do prazo autorizado. A pena prevista é de detenção, de dois a quatro anos, e multa. Aumenta-se a pena de um terço se o dado ou informação obtida desautorizadamente é fornecida a terceiros pela rede de computadores,

dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa.

8 - Divulgação não autorizada de informações disponíveis em banco de dados - inclusão do art. 154–D

A pena é de detenção, de um a dois anos, e multa. Aumenta-se de pena se o autor se vale de nome falso ou da utilização da identidade de terceiros. Também aumenta a pena se o dado ou informação é fornecida indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa.

9 - Furto Qualificado por uso de informática – art. 155 - Furto – inclusão do § 4º, V

O Substitutivo tipificou o crime, mantendo a pena, a exemplo do tipo "o furto qualificado por uso de chave falsa".

10 - Atentado contra a segurança de serviço de utilidade pública – alteração do art. 265

Mantida a pena, incluído no tipo o serviço de "informação ou telecomunicação".

11 – Ataques a redes de computadores - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado – alteração do art. 266

Os novos serviços no tipo incluem os ataques a redes de computadores tipo DoS, DdoS etc.

Glossário – inclusão do art. 154-C

Para efeitos penais são definidos o que é "Dispositivo de Comunicação", "Sistema Informatizado", "Rede de Computadores", "Defesa Digital" e "Código Malicioso".

Equiparação à coisa – inclusão do art. 183-A

Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico, digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione o acesso a eles.

Sobre as obrigações do responsável por liberar acesso a uma rede de computadores ou prestar serviços mediante o seu uso:

- Guardar os dados aptos à identificação do usuário e das conexões por ele realizadas;
- Atendendo expressa autorização judicial, tornar disponíveis os dados à autoridade de auditoria técnica que será definida em regulamento;
- Atendendo expressa autorização judicial, fornecer os dados no curso de investigação;
- Atendendo expressa autorização judicial, preservar imediatamente os dados aptos à identificação do usuário e das conexões por ele realizadas no curso de investigação;
- Repassar à polícia as denúncias que receber de crimes cometidos na rede;
- Dar esclarecimentos aos usuários que estão sob a lei brasileira;
- Fazer campanhas de alerta quanto ao uso criminoso da rede de computadores;
- Divulgar boas práticas de segurança;

- Pagar multa variável, de R$2mil a R$100 mil, aplicada pela autoridade definida em regulamento, caso não atenda às obrigações de guarda e/ou fornecimento dos dados, independentemente de indenização à pessoa lesada.

APÊNDICE A
Países signatários da Convenção sobre os Cibercrimes de Budapest

Opening for signature

Place: Budapest
Date : 23/11/2001

Entry into force

Conditions: 5 Ratifications including at least 3 member States of the Council of Europe
Date : 1/7/2004

Status as of: 22/2/2007

Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra										
Armenia	23/11/2001	12/10/2006	1/2/2007							
Austria	23/11/2001									
Azerbaijan										
Belgium	23/11/2001									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X				
Croatia	23/11/2001	17/10/2002	1/7/2004							
Cyprus	23/11/2001	19/1/2005	1/5/2005							
Czech Republic	9/2/2005									
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001									
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia										
Germany	23/11/2001									
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001									
Latvia	5/5/2004									
Liechtenstein										

Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002									
Moldova	23/11/2001									
Monaco										
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001									
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005			55						
Slovakia	4/2/2005									
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001 r									
Sweden	23/11/2001									
Switzerland	23/11/2001									
the former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001									
Non-member States of the Council of Europestates	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Canada	23/11/2001									
Costa Rica										
Japan	23/11/2001									
Mexico										
Montenegro	7/4/2005			55						
South Africa	23/11/2001									
United States	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	24
Total number of ratifications/accessions:	19

Notes:(55) Date of signature by the state union of Serbia and Montenegro.
a: Accession - s: Signature without reservation as to ratification - su: Succession - r: Signature "ad referendum".
R.: Reservations - D.: Declarations - A.: Authorities - T.: Territorial Application - C.: Communication - O.: Objection.

Source : Treaty Office on http://conventions.coe.int

Resenha didática - tipificação e punição dos crimes de informática[7]

PLS 76/2000 (PLC 89 de 2003 e PLS 137 de 2000)

APÊNDICE B

Por que é preciso tipificar os crimes de informática ou cibercrimes:

Porque a Constituição Federal diz em seu art. 5º, do Título I, Capítulo I,dos Direitos e Garantias Fundamentais, no inciso XXXIX, que:
"XXXIX – não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal;"

No Direito Penal não se admite a analogia para prejudicar o réu; ou seja, a conduta deve estar claramente definida no texto da lei. Assim, algumas condutas criminosas mediante o uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, devem estar claramente definidas na lei.

Por que é preciso alterar o Código Penal:

Porque a Constituição Federal em seu art. 59, parágrafo único, diz que "Lei complementar disporá sobre a elaboração, redação, alteração e consolidação das leis." Esta lei é a Lei Complementar nº 95, de 26 de fevereiro de 1998, que no seu art. 7º, inciso IV, diz que:
"IV – o mesmo assunto não poderá ser disciplinado por mais de uma lei, exceto quando a subseqüente se destine a complementar lei considerada básica, vinculando-se a esta por remissão expressa.".

No nosso caso, a lei básica é o Código Penal, que está sendo alterado com mudanças de redação ou inclusão de novos artigos, parágrafos, incisos etc., em complemento à lei existente.

Considerações Gerais sobre Direito Penal

O Direito Penal é um dos ramos do Direito Público que define as infrações que devem ser punidas com mais rigor pelo Estado, e suas respectivas penas, estando a maior parte delas previstas no Código Penal. Inclui os crimes punidos com privação da liberdade, restrição de direitos e, também, multa. Inclui também as contravenções, definidas na Lei de Contravenções Penais e punidas com prisão simples, com a possibilidade de aplicação isolada de multa.

Em regra, para que exista a responsabilidade penal de uma pessoa em relação a um crime é necessário que ela tenha agido, ou se omitido, com intenção ou vontade, ou seja, com dolo.

Quando expressamente previsto na lei penal, é possível responsabilizar penalmente uma pessoa que age ou se omite por negligência, imprudência ou imperícia, ou seja, com culpa.

O Código Penal

O Código Penal está dividido em duas partes: a Parte Geral (arts. 1º a 120) e a Parte Especial (arts. 121 a 361). Cada parte é dividida em Títulos, estes em Capítulos e estes em Seções, de acordo com o bem jurídico que se quer proteger (como a vida, o patrimônio etc.). A essa divisão dá-se o nome de topologia, ou localização dos crimes dentro do código.

A Parte Geral trata da Aplicação da Lei Penal (arts 1º a 12), do Crime (arts. 13 a 24), da Imputabilidade Penal (arts. 26 a 28), do Concurso de Pessoas (arts. 29 a 31), das Penas (arts.

32 a 95), das Medidas de Segurança (arts. 96 a 99), da Ação Penal (arts. 100 a 106), da Extinção da Punibilidade (arts.107 a 120).

A Parte Especial trata dos Crimes contra a Pessoa (arts. 121 a 154), dos Crimes contra o Patrimônio (arts. 155 a 183), dos Crimes contra a Propriedade Imaterial (arts. 184 a 196), dos Crimes contra a Organização do Trabalho (arts. 197 a 207), dos Crimes contra o Sentimento Religioso e contra o Respeito aos Mortos (arts. 208 a 212), dos Crimes contra os Costumes (arts. 213 a 234), dos Crimes contra a Família (arts. 235 a 249), dos Crimes Contra a Incolumidade Pública (arts. 250 a 285), dos Crimes contra a Paz Pública (arts. 286 a 288), dos Crimes contra a Fé Pública (arts. 289 a 311), dos Crimes contra a Administração Pública (arts. 312 a 359) e Disposições Finais (arts. 360 e 361).

Por que é preciso criar medidas administrativas como, por exemplo, a guarda de dados:

Porque a Constituição Federal diz em seu art. 5º, do Título I, Capítulo I, dos Direitos e Garantias Fundamentais, no inciso II, que:
"II – ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;"

E a Lei Complementar nº 95, de 26 de fevereiro de 1998, que no seu art. 3º, inciso III, prescreve que:
"Art. 3º A lei será estruturada em três partes básicas:
.....
III – parte final, compreendendo as disposições pertinentes às medidas necessárias à implementação das normas de conteúdo substantivo [...]."

No nosso caso, como acontece hoje, se a autoridade judicial requerer as informações de conexões informáticas, a parte responsável pela conexão pode alegar que não é obrigado por lei a guardar e muito menos a fornecer as informações.

APÊNDICE C
Sugestões encaminhadas para a Consultoria Legislativa

Art. 2º O Capítulo V do Título I da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do seguinte art. 141-A:

"**Art. 141-A.** As penas neste Capítulo aumentam-se de dois terços caso os crimes sejam cometidos por intermédio de rede de computadores, dispositivo de comunicação ou sistema informatizado."

Art. 3º O Título I da Parte Especial do Código Penal fica acrescido do Capítulo VI-A, assim redigido:

"Capítulo VI-A

DOS CRIMES CONTRA REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

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

Art. 154-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Nas mesmas penas incorre quem, permite, facilita ou fornece a terceiro meio não autorizado de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 2º 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 suas subsidiárias.

§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de acesso.

§ 4º Não há crime quando o agente acessa a título de defesa digital, excetuado o desvio de finalidade ou o excesso.

Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar

Art. 154-B. Obter dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:

Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa.

§ 1º Nas mesmas penas incorre quem mantém consigo, transporta ou fornece dado ou informação obtida nas mesmas circunstâncias do "caput", ou desses se utiliza alem do prazo definido e autorizado.

§ 2º Se o dado ou informação obtida desautorizadamente é fornecida a terceiros pela rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

§ 3º 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 suas subsidiárias.

Dispositivo de comunicação, sistema informatizado, rede de computadores e defesa digital

Art. 154-C. Para os efeitos penais considera-se:

I – dispositivo de comunicação: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, os receptores e os conversores de sinais de rádio ou televisão digital ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

II – sistema informatizado: o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: os instrumentos físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial;

IV – defesa digital: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação;

V - código malicioso: o conjunto de instruções e tabelas de informações ou programa de computador ou qualquer outro sistema capaz de executar uma seqüência de operações que resultem em ação de dano ou de obtenção indevida de informações contra terceiro, de maneira dissimulada ou oculta, transparecendo tratar-se de ação de curso normal;

VI – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado, incluindo um programa, apto a fazer um sistema informatizado executar uma função;

VII – dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

Divulgação ou utilização indevida de informações contidas em banco de dados

Art. 154-D Divulgar, utilizar, comercializar ou disponibilizar informações contidas em banco de dados com finalidade distinta da que motivou o registro das mesmas, incluindo-se informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas naturais ou jurídicas, ou a dados de pessoas naturais referentes a raça, opinião política, religiosa, crença, ideologia, saúde física ou mental, orientação sexual, registros policiais, assuntos familiares ou profissionais, além de outras de caráter sigiloso, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

Pena – detenção, de um a dois anos, e multa.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 2º Se o crime ocorre em rede de computadores, dispositivo de comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.“

Art. 4º O § 4º do art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte inciso V:

“**Art. 155.** .....
.....

§ 4º .....
.....

V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar, ou contra rede de computadores, dispositivos de comunicação ou sistemas informatizados e similares".

..... (NR) "

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

"**Dano por difusão de código malicioso eletrônico ou digital ou similar**

Art. 163-A. Criar, 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.

Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar

§ 1º Se o crime é cometido com finalidade de destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

Difusão de código malicioso eletrônico ou digital ou similar seguido de dano

§ 2º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado, e as circunstâncias demonstram que o agente não quis o resultado, nem assumiu o risco de produzi-lo:

Pena – reclusão, de 3 (dois) a 5 (cinco) anos, e multa.

§ 3º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

§ 4º Não há crime quando a ação do agente é a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

Art. 6º O Capitulo VI do Título II do Código Penal passa a vigorar acrescido do seguinte artigo:

"**Difusão de código malicioso**

Art. 171-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por

qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, com obtenção de vantagem ilícita, em prejuízo alheio:

Pena – reclusão, de um a três anos.

§ 1º A pena é aumentada de sexta parte, se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de difusão de código malicioso.

§ 2º Não há crime quando a difusão ocorrer a título de defesa digital, excetuado o desvio de finalidade ou o excesso."

Art. 7º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

"**Art. 183-A.** Para efeitos penais, equiparam-se à coisa o dado, informação ou unidade de informação em meio eletrônico ou digital ou similar, a base de dados armazenada, o dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer instrumento que proporcione acesso a eles."

Art. 8º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

"**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, informação ou telecomunicação, ou qualquer outro de utilidade pública:

..... (NR)"

"**Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado**

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:

..... (NR)"

Art. 9º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

"**Art. 298**. .....

.....

Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico ou digital ou similar portátil de captura, processamento, armazenamento e transmissão de informações.

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer outro dispositivo portátil capaz de capturar, processar, armazenar ou transmitir dados, utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar.(NR)"

Art. 10. O Código Penal passa a vigorar acrescido do seguinte art. 298-A:

"**Falsificação de telefone celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado**

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

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

Art. 11. a **Art. 15 –** Alterações equivalentes do Código Penal Militar

Art. 16. O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do seguinte § 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 rede de computadores, dispositivo de comunicação ou sistema informatizado." (NR)

Art. 17. O art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código do Processo Penal (CPP), passa a vigorar acrescido do seguinte inciso IV:

> "**Art. 313.** .....
> .....
>
> IV – punidos com detenção, se tiverem sido praticados contra rede de computadores, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado, nos termos da lei penal.(NR)"

Art. 18. Os órgãos da polícia judiciária, nos termos de regulamento, estruturarão setores e equipes de agentes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 19. O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

> "**Art. 1º** .....
> .....
>
> V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado. (NR)"

Art. 20. O art. 9º da Lei nº 8.078, de 11 de setembro de 1990 passa a vigorar com a seguinte redação:

> "Art. 9º .....
> .....
>
> *Parágrafo único.* O disposto neste artigo se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso do produto ou serviço e para a proteção dos dados trafegados, quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso a rede de computadores ou provimento de serviço por meio dela.(NR)"

Art. 21. O responsável pelo provimento de acesso a rede de computadores é obrigado a:

I – manter em ambiente controlado e de segurança os dados de conexões realizadas por seus equipamentos, aptos à identificação do usuário e dos endereços eletrônicos de origem, da data, do horário de início e término e referência GMT, das conexões, pelo prazo de três anos, para prover os elementos probatórios essenciais de identificação da autoria das conexões na rede de computadores;

II – tornar disponíveis à autoridade competente, por expressa autorização judicial, os dados e informações mencionados no inciso I no curso de auditoria técnica a que forem

submetidos;

III – fornecer, por expressa autorização judicial, no curso de investigação, os dados de conexões realizadas e os dados de identificação de usuário;

IV – preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, os dados de identificação de usuário e as comunicações realizadas daquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

V – informar, de maneira sigilosa, à autoridade policial competente, denúncia da qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade;

VI – informar ao seu usuário que o uso da rede sob sua responsabilidade obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;

VII – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;

VIII – divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivo de comunicação e sistema informatizado.

§ 1º Os dados de conexões realizadas em rede de computadores, aptos à identificação do usuário, as condições de segurança de sua guarda, a auditoria à qual serão submetidos, a autoridade competente responsável pela auditoria e o texto a ser informado aos usuários de rede de computadores serão definidos nos termos de regulamento.

§ 2º Os dados e procedimentos de que cuida o inciso I deste artigo deverão estar aptos a atender ao disposto nos incisos II , III e IV no prazo de cento e oitenta dias, a partir da promulgação desta Lei.

§ 3º O responsável citado no *caput* deste artigo que não cumprir o disposto no § 2º, 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 verificação ou solicitação, aplicada em dobro em caso de reincidência, que será imposta mediante procedimento administrativo, pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração.

§ 4º 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.

Art. 22. Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de identificação de usuário, quando constatada qualquer conduta criminosa.

Art. 23. Esta Lei entrará em vigor sessenta dias após a data de sua publicação.