

Escola de Direito da Fundação Getulio Vargas
Centro de Tecnologia e Sociedade



Proposta de Alteração do PLC 84/99 / PLC 89/03 (Crimes Digitais) e
Estudo sobre História Legislativa e Marco Regulatório da Internet no
Brasil

Ronaldo Lemos

Mestre em direito pela Universidade Harvard

Doutor em direito pela USP

Professor titular de propriedade intelectual da Escola de Direito da FGV-RJ

Carlos Affonso Pereira de Sousa

Mestre e doutor em direito civil pela UERJ

Professor titular de responsabilidade civil da Escola de Direito da FGV-RJ

Sérgio Branco

Mestre em direito civil pela UERJ

Professor titular de direito civil da Escola de Direito da FGV-RJ

Pedro Mizukami

Mestre em direito constitucional pela PUC-SP

Luiz Moncau

Mestrando em direito constitucional pela PUC-RJ

Bruno Magrani

Mestrando em direito pela Universidade Harvard



1. Introdução¹

Durante o processo de privatizações na década de 90, o Brasil adotou um abrangente marco regulatório para o setor de telecomunicações. Apesar desse esforço, uma questão fundamental acabou sendo deixada de lado: a regulamentação da Internet. Ao contrário de outros países, que ao final dos anos 1990 e começo dos anos 2000 adotaram legislações específicas para regular o tema, o Brasil, passados mais de 15 anos do acesso público à rede, ainda não possui dispositivos legislativos específicos sobre a questão.

As conseqüências dessa lacuna são negativas e abrangentes. Em primeiro lugar, fica prejudicada a inovação nacional. Sem um estatuto legislativo que defina de forma clara e precisa os riscos e responsabilidades na rede, fica difícil a criação de um ambiente de empreendedorismo descentralizado, que envolva não apenas grandes iniciativas, mas a criação e experimentação de modelos, muitas vezes através de pequenos empreendimentos, que são a principal fonte de inovação na rede. São muitos os temas não regulamentados pela lei brasileira: privacidade, responsabilidade de provedores, relações de consumo online, proteção de dados, dentre vários outros. Trata-se de uma agenda ampla de temas, demandando um marco regulatório para as atividades civis e comerciais na rede.

Ao final da década de 90, vários projetos de lei preocupavam-se com a regulamentação destes temas de forma ampla, conforme detalhado abaixo. No entanto, nenhum desses projetos logrou êxito. Os temas fundamentais à estrutura da rede foram sendo progressivamente abandonados e substituídos por uma agenda exclusivamente criminal. A partir do começo dos anos 2000, praticamente desapareceu do Congresso Nacional qualquer proposta de regulamentação específica que pudesse abordar elementos fundamentais de um marco regulatório da internet. Em vez disso, passou a prevalecer uma agenda exclusiva no âmbito do direito criminal, com a tipificação de condutas e criação de penas.

2. Os riscos da regulamentação criminal

A iniciativa de se regular a Internet do ponto de vista criminal é louvável, especialmente para coibir condutas graves. No entanto, ela traz em si riscos consideráveis. O

¹ A concepção e revisão deste documento contou com importantes e substanciais contribuições de Marília Maciel e Koichi Kameda, do Centro de Tecnologia e Sociedade da FGV Direito Rio.

caminho natural de regulamentação da rede, seguido por todos os países desenvolvidos, é primeiramente estabelecer um marco regulatório civil, que defina claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições acessando a rede, para a partir daí definir uma regras criminais. O direito criminal deve ser visto como *ultima ratio*, isto é, o último recurso, que é adotado quando todas as demais formas de regulação falham. Nesse sentido, o caminho correto seria a partir do estabelecimento do marco civil, verificar o que teve efeito ou não de então adotar legislação criminal para regular a rede com base na experiência adquirida.

Para inovar, um país precisa ter regras civis claras, que permitam segurança e previsibilidade nas iniciativas feitas na rede (como investimentos, empresas, arquivos, bancos de dados, serviços etc.). As regras penais devem ser criadas a partir da experiência das regras civis, sob pena de se elevar o custo de investimento no setor e desestimula a criação de iniciativas privadas, públicas e empresariais na área.

É preciso ter especial atenção para que a legislação criminal a ser adotada não seja excessivamente ampla ou vaga. A excessiva indefinição de termos criminais gera incertezas, especialmente para regular um assunto complexo que demanda definições técnicas prévias, que ainda não foram pensadas legislativamente no País.

Prova disso é que a Convenção de Cibercrimes, que é citada como "inspiração" para o projeto de lei, não teve adesão de nenhum país latino-americano e nem pela maioria absoluta dos países em desenvolvimento (contam-se nos dedos os países pobres que aderiram à convenção). Os países que se comprometeram com a convenção são, principalmente, países ricos que já fizeram seu dever de casa de regulamentar a Internet do ponto de vista civil e, somente depois disso, estabeleceram parâmetros criminais para a rede. O Brasil agora segue a via inversa: está criando primeiro punições criminais, sem antes regulamentar técnica e civilmente a Internet.

Por esse motivo, precisa ser cauteloso ao regulamentar a questão, estabelecendo a precisão necessária para garantir os objetivos da lei, mas sem extrapolar limites ou basear-se em conceitos demasiadamente amplos.

Além disso, qualquer medida de regulação que autorize o monitoramento de atividades online, inclusive a guarda de informações dos usuários, deve necessariamente

contar com os necessários freios e contrapesos, que funcionem como garantia a direitos invioláveis como a privacidade e o devido processo legal.

3. Três objetivos: regulamentação criminal, criação de meios de investigação e proteção a direitos fundamentais

Existem três objetivos que devem ser atendidos simultaneamente. O primeiro é a regulamentação criminal dos delitos na internet, através de definições e termos precisos, diretamente relacionados às condutas específicas que se pretende coibir. O segundo é a criação de mecanismos legais para que as autoridades competentes possam proceder a investigação e formação de provas envolvendo esses delitos. O terceiro, igualmente importante, é que na regulamentação dos meios de investigação e de guarda de dados dos usuários sejam estabelecidas também garantias que protejam direitos constitucionais na rede, como a privacidade e o devido processo legal.

Nesse sentido, o presente estudo procura:

A) Fazer sugestões de modificações ao texto do projeto em tramitação mais avançada (PLC 89/03, na numeração do Senado – PLC 84/99, na numeração da Câmara), de modo a propor, na ausência de uma regulamentação mais abrangente da rede, uma legislação criminal que não gere danos colaterais excessivos à Internet brasileira.

Note-se que a proposta de modificação apresentada no presente estudo atende às preocupações de segurança na rede, como por exemplo, segurança bancária, clonagem de cartões de crédito, envio de vírus e cavalos-de-Tróia, bem como cria mecanismos para a identificação dos perpetradores de crimes online.

O texto apresentado através desse estudo, no entanto, toma cuidado de propor alterações que regulamentem de forma específica essas questões, sem danos colaterais, ao mesmo tempo em que estabelece as necessárias garantias processuais para que não haja desequilíbrio entre a possibilidade de execução criminal com outros direitos fundamentais.

B) Traçar um histórico detalhado dos projetos de regulamentação legislativa da internet no Brasil, terminando com uma análise da situação atual, que leva à conclusão da necessidade urgente da adoção de um marco regulatório civil no País.

A) PROPOSTA DE ALTERAÇÃO AO PLC 89/03 (PLC 84/99)

Em vista dos comentários acima, segue abaixo o exemplo de como deve ficar o texto final da legislação relativa aos crimes na Internet, com suas respectivas razões de alteração. A consolidação desses artigos no projeto ora apresentado busca representar, de maneira clara, a combinação dos artigos a serem mantidos do PLC 89/03 (PLC 84/99) com os novos artigos sugeridos e que deverão ser aprovados no Congresso. Conforme amplamente discutido alhures, o texto do projeto atualmente na Câmara encontra-se excessivamente amplo e vago, com o potencial de criar incertezas e danos colaterais à regulamentação da internet no Brasil. Essas incertezas, no entanto, são foco de alguns poucos artigos, os quais a proposta abaixo tem por objetivo substituir. Os artigos considerados problemáticos provocaram intensa manifestação por parte da sociedade civil, o que resultou em um abaixo assinado com mais de 140 mil assinaturas² e diversos atos públicos contrários à redação atual do projeto.

O texto aqui apresentado procura preservar os objetivos originais do projeto, no sentido de regulamentar as condutas de maior gravidade na rede. No entanto busca-se incorporar as sugestões efetuadas pela sociedade civil e pelo Ministério da Justiça, para que a redação fique mais precisa, específica e compatível com a experiência de outros países, estabelecendo-se, ainda, um regime de garantias como contrapartida à ampliação dos poderes de investigação das autoridades competentes.

Proposta de Alterações no PL de Crimes Eletrônicos
PROJETO DE LEI N° _____

O CONGRESSO NACIONAL decreta:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante o uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de

² <http://www.petitiononline.com/veto2008/petition.html>

comunicação ou sistemas informatizados e similares, e dá outras providências.

Art 2º O Título VIII da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do Capítulo IV, assim redigido:

“Capítulo IV

DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS

Invasão de rede de computadores, dispositivo de comunicação ou sistema informatizado

Artigo 285-A. Invadir rede de computadores, dispositivo de comunicação ou sistema informatizado sem autorização de seu titular com o fim de obter vantagem ilícita.

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

§ 1º – Na mesma pena incorre quem, valendo-se de privilégios de administração, acesso direto à rede de computadores, dispositivo de comunicação ou sistema informatizado, ou do uso de recurso técnicos de interceptação de dados, facilita a realização do crime previsto neste artigo.

§ 2º – Se da invasão resultar a obtenção de dados confidenciais, instalação de vulnerabilidades, destruição ou alteração de arquivos, controle remoto não-autorizado do dispositivo de comunicação, rede de computadores ou sistema informatizado invadido, a pena é aumentada de um terço.

Artigo 285-B. Nos crimes definidos neste Capítulo somente se procede mediante queixa, salvo se o crime é cometido contra a União, Estados, Distrito Federal, Municípios, empresas concessionárias de serviços públicos, agências reguladoras, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias.”

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

Art. 3º - 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:

“Inserção ou difusão de código malicioso

Artigo 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado sem a autorização de seu legítimo titular.

Pena – reclusão, de 1 (um) a 2 (dois) anos, e multa.

Parágrafo único – Se do crime resulta destruição, inutilização, deterioração, funcionamento defeituoso, ou controle remoto não-autorizado de dispositivo de comunicação, rede de computadores ou sistema informatizado:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.”

JUSTIFICATIVA: *O dispositivo que tratava de código malicioso no projeto original era excessivamente amplo e vago, com risco da criação*

de severos danos colaterais. Através da redação acima torna o tipo penal preciso. São mantidas as agravantes do projeto original pertinentes ao tipo, que não extrapolam seu objetivo. Além disso, a redação adicional outra conduta não prevista anteriormente na redação atual, com o intuito de coibir o controle remoto através de código malicioso (as chamadas “botnets”, compostas de computadores controlados à distância sem o conhecimento do seu respectivo usuário).

Art. 4º O *caput* do art. 163 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar com a seguinte redação:

“Dano

Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:

..... (NR)”

Art. 5º – Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate aos crimes definidos nesta lei.

Art 6º – 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 contra rede de computadores, dispositivo de comunicação ou sistema informatizado.

.....”

JUSTIFICATIVA: *Os artigos acima são de caráter permissivo e facultam à administração pública a criação de setores e equipes especializados nos crimes definidos pelo PLC 89/03. Além disso, a redação do Artigo 6º torna competência do Departamento de Polícia*

Federal do Ministério da Justiça os “delitos contra rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 7º O art. 265 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa 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, informação ou telecomunicação, ou qualquer outro de utilidade pública:

..... “(NR)

Art. 8.º O *caput* do art. 259 e o *caput* do art. 262 do Capítulo VII do Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

“Dano Simples

Art. 259. Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar.”(NR)

.....
.....

“Dano em material ou aparelhamento de guerra ou dado eletrônico

Art. 262. Praticar dano em material ou aparelhamento de guerra ou dado eletrônico de utilidade militar, ainda que em construção ou fabricação, ou em efeitos recolhidos a depósito, pertencentes ou não às forças armadas: (NR)”

Art. 9.º Os incisos II e III do art. 356 do Capítulo I do Título I do Livro II da Parte Especial do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passam a vigorar com a seguinte redação:

“CAPÍTULO I

DA TRAIÇÃO

Favor ao inimigo

Art. 356.

II - entregando ao inimigo ou expondo a perigo dessa consequência navio, aeronave, força ou posição, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar;

III - perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo de perda, destruição, inutilização ou deterioração, navio, aeronave, engenho de guerra motomecanizado, provisões, dado eletrônico ou qualquer outro elemento de ação militar.”(NR)

Art. 10. O provedor de acesso é obrigado a:

I – manter sob sigilo, em ambiente controlado e de segurança, para provimento de investigação pública formalizada, os *logs* de acesso de seus usuários pelo prazo de 6 (seis) meses, após o qual deverão ser descartados;

II – fornecer mediante autorização judicial e por requisição formal do Ministério Público ou da autoridade policial, para uso exclusivo e sigiloso destes, os *logs* de acesso referidos no inciso I, para fins de investigação criminal ou instrução processual penal;

III – manter registrados em separado e sigilosamente os dados cadastrais do usuário, limitados a nome completo, gênero, filiação, data de nascimento e número de registro de pessoa física ou jurídica, vinculando-os aos *logs* de acesso referidos no inciso I somente mediante autorização judicial e por requisição exclusiva do Ministério Público ou da autoridade policial, para fins de investigação criminal ou instrução processual penal;

IV – informar aos usuários, de forma adequada e clara, as medidas e procedimentos de segurança e sigilo dos *logs* de acesso e dados cadastrais coletados;

§ 1.º A interceptação, coleta, arquivamento, escuta e disponibilização de dados outros que não os *logs* de acesso será regulada pela lei que trata da interceptação de comunicação telefônica e dados telemáticos.

§ 2.º Caberá ao órgão público solicitante ressarcir os provedores de acesso dos custos inerentes ao armazenamento dos *logs*, na forma definida em regulamento.

§ 3.º Os procedimentos de segurança necessários à preservação do sigilo e da integridade dos dados referidos neste artigo serão definidos na forma do regulamento.

JUSTIFICATIVA: *Um dos temas que mais causaram controvérsia na redação atual do PLC 89/03 (PLC 84/99) foi o conteúdo do seu artigo 22, que trata do monitoramento de informações dos usuários e sua respectiva guarda por parte dos provedores da internet. A redação original foi criticada de forma contundente (com termos como “vigilantismo”, “vigilância privada” e outros). Com isso, o objetivo da proposta do artigo 10, que substitui o artigo 22 original, é o de ampliar os poderes de investigação e formação de provas concedidos às autoridades investigatórias e ao Poder Judiciário, sem no entanto extrapolar ou afetar direitos e garantias fundamentais, estando de acordo com a experiência de outros países. Com isso, a redação proposta obriga os provedores de serviço da internet à guarda dos chamados “logs de acesso” por 6 (seis) meses. Esse é o prazo adotado tipicamente, por exemplo, em países da União Européia (é importante mencionar que os Estados Unidos sequer autorizam a guarda dos logs de acesso). O prazo é também maior do que aquele estabelecido pela Convenção de Budapeste, de 90 dias (apesar de não contar com adesão do Brasil, a Convenção é frequentemente citada como inspiração para o PLC 89/03/PLC 84/99).*

Art. 11. A preservação e disponibilização de dados a que esta lei faz referência deve atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas nos fatos em apuração.

Art. 12 A fim de atender ao disposto no artigo 10, o provedor de acesso fica impedido de realizar o cruzamento dos *logs* de acesso com os dados cadastrais do usuário, salvo mediante ordem judicial que atenda aos requisitos previstos no referido artigo.

Art. 13. A requisição para disponibilização de *logs* de acesso e dados cadastrais deverá ser feita por escrito, endereçada ao juiz competente para o julgamento da infração apurada, e obrigatoriamente conter:

I – descrição pormenorizada de indícios razoáveis da ocorrência do crime;

II – relato motivado da imprescindibilidade dos *logs* solicitados, demonstrando-se a inviabilidade de produção probatória por outros meios;

III – motivação para que sejam fornecidos também os dados cadastrais do usuário;

IV – intervalo de tempo solicitado para o fornecimento dos *logs*, limitado ao prazo máximo dos últimos 6 (seis) meses da data de solicitação;

§ 1.º Desatendidos quaisquer dos requisitos indicados nos incisos deste artigo, a solicitação não será conhecida pelo juiz.

§ 2.º Não sendo necessária para fins da investigação a identificação dos dados cadastrais de usuário, o juiz competente deverá determinar a disponibilização apenas dos *logs* de acesso.

Art. 14. O juiz que solicitar *ex officio* para instrução probatória em processo-crime os dados referidos no artigo 7º deverá atender em decisão fundamentada os requisitos do artigo 10º.

Art. 15. As solicitações de que tratam os artigos 13 e 14 não serão deferidas na investigação de crimes punidos com pena privativa de

liberdade com pena máxima igual ou inferior a 2 (dois) anos, salvo com relação aos crimes definidos na presente lei.

Art. 16. O pedido de disponibilização de dados, uma vez deferido, deverá ser encaminhado ao provedor de acesso acompanhado da ordem judicial correspondente.

Parágrafo único. O provedor de acesso remeterá os dados solicitados exclusivamente à autoridade solicitante, que deverá mantê-los sob sigilo.

JUSTIFICATIVA: *Os artigos 11 a 16 definem as garantias substantivas e processuais em contrapartida à ampliação dos poderes de investigação e obrigação da guarda dos logs de acesso por parte dos provedores de serviço de internet. A principal garantia, derivada da Constituição Federal, é a necessidade de ordem judicial para a obtenção dos logs de acesso, bem como para o cruzamento destes dados com os dados cadastrais dos usuários. Outras garantias incluem o necessário regime de confidencialidade dos dados obtidos, bem como os requisitos processuais para sua requisição.*

Art. 17. Para os efeitos penais desta lei considera-se, dentre outros:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou digitais;

II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;

III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;

IV – código malicioso: programa desenvolvido especificamente para executar ações danosas, como vírus de computador, cavalos-de-tróia, *adware* e *spyware*, *backdoors*, *keyloggers*, *worms*, *bots*, *rootkits* e outros, que se propagam com ou sem a intervenção do usuário do dispositivo de comunicação ou sistema informatizado afetado.

V – provedor de acesso: qualquer pessoa jurídica, pública ou privada, que faculte aos usuários dos seus serviços a possibilidade de conexão à internet mediante atribuição ou validação de endereço IP;

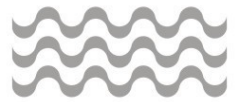
VI – dados cadastrais do usuário: dados fornecidos pelo usuário no momento da contratação do serviço de acesso à internet;

VII – *log* de acesso: informações referentes à hora, data, início, término, duração, endereço de Protocolo Internet (IP) utilizado e o terminal de origem da conexão;

Parágrafo único. Ficam excluídos do conceito de provedor de acesso os centros públicos de acesso gratuito ou não, as iniciativas de inclusão digital sem finalidade lucrativa e os empreendimentos que ofereçam acesso gratuito à Internet, quer quando promovidos pelo poder público, empresas públicas, sociedades de economia mista, fundações públicas ou por associações sem fins lucrativos.

JUSTIFICATIVA: *O Artigo 17 apresenta as definições dos termos utilizados no âmbito do projeto. É importante notar que são mantidas as principais definições do projeto original (dispositivo de comunicação, sistema informatizado e rede de computadores). Além disso, torna-se mais precisa a definição de código malicioso (que passa inclusive a exemplificar programas como vírus, cavalos de tróia, adware e spyware, backdoors, keyloggers, worms, bots, rootkits e outros congêneres que se propagam com ou sem a intervenção do usuário). Por fim, são definidos os termos “provedor de acesso”, “dados cadastrais” e “log de acesso”, especificando de forma precisa cada um deles.*

Art. 28. Esta lei entra em vigor cento e vinte dias após a data de sua publicação.



**B) HISTÓRIA LEGISLATIVA DA REGULAMENTAÇÃO DA
INTERNET NO BRASIL**

No esforço de contextualizar as mudanças propostas, o presente estudo apresenta um breve histórico da regulamentação da Internet no Brasil, abordando em mais detalhes, na sequência, o trâmite do PLC 84/99 / PLC 89/03. Em seguida, faz uma análise da situação jurídica atual da responsabilidade civil dos provedores de internet, concluindo pela necessidade de que, em paralelo aos esforços de regulamentação criminal da rede, retome-se a regulamentação civil da internet no Brasil.

1. Início dos esforços de regulamentação da Internet no Brasil

Pelo menos desde 1995 já existem, em nosso legislativo, tentativas de se regular o espaço da Internet. O PLC 1070/95, do Deputado Ildemar Kussler, e os oito outros projetos afins que a ele foram apensados, servem como um exemplo bastante ilustrativo da ansiedade regulatória provocada pela Internet. Responsabilidade dos provedores, comércio eletrônico, documentos e assinaturas digitais, pedofilia e crimes de acesso não-autorizado, temas até hoje controvertidos e objeto de projetos de lei ainda em tramitação, estão, desse modo, colocados em pauta no Brasil desde a abertura da Internet à iniciativa privada, com diferentes abordagens e configurações normativas. Quando se pensa, portanto, em regulamentação da Internet no Brasil, é de extrema importância realizar um recorte, identificando-se alguns projetos que têm importância histórica para o debate atual em torno da adequação do modelo de regulamentação para a Internet estabelecido pelo PLC 84/99 (ou PLC 89/03, na numeração do Senado), conhecido atualmente como o “Projeto Azeredo sobre Cibercrimes”, em razão do Senador que tem sido seu principal parecerista desde a remessa do texto ao Senado.

Pelo contraste que estabelece em relação à abordagem do Projeto Azeredo, cabe lembrar, especificamente, do PL 1589/99, posteriormente fundido com o texto de outro projeto de lei e apresentado como o PL 4906/01, pelo Deputado Júlio Semeghini. O texto do PL 1589/99 foi elaborado por uma comissão especial da OAB de São Paulo, à qual foi atribuída a tarefa de propor uma lei modelo regulando o comércio eletrônico, a ser apresentada ao Congresso Nacional, o que foi eventualmente levado a cabo pelo Deputado Luciano Pizzato.

O projeto em questão, no texto do PL 4906/01, abre capítulo especificamente voltado às obrigações e responsabilidades dos provedores, como normas dedicadas a problemas que o

Projeto Azeredo ignora ou regula de maneira que, como se verá, é pouco adequada ao espaço regulado. Cabe aqui reproduzir os artigos pertinentes:

“Capítulo IV

Das obrigações e responsabilidades dos provedores

Art. 34. Os provedores de acesso que assegurem a troca de documentos eletrônicos não podem tomar conhecimento de seu conteúdo, nem duplicá-los por qualquer meio ou ceder a terceiros qualquer informação, ainda que resumida ou por extrato, sobre a existência ou sobre o conteúdo desses documentos, salvo por indicação expressa do seu remetente.

§ 1º Igual sigilo recai sobre as informações que não se destinem ao conhecimento público armazenadas no provedor de serviços de armazenamento de dados.

§ 2º Somente mediante ordem do Poder Judiciário poderá o provedor dar acesso às informações acima referidas, sendo que as mesmas deverão ser mantidas, pelo respectivo juízo, em segredo de justiça.

Art. 35. O provedor que forneça ao ofertante serviços de conexão ou de transmissão de informações, ao ofertante ou adquirente, não será responsável pelo conteúdo das informações transmitidas.

Art. 36. O provedor que forneça ao ofertante serviço de armazenamento de arquivos e sistemas necessários para operacionalizar a oferta eletrônica de bens, serviços ou informações não será responsável pelo seu conteúdo, salvo, em ação regressiva do ofertante, se:

I – deixou de atualizar as informações objeto da oferta, tendo o ofertante tomado as medidas adequadas para efetivar as atualizações, conforme instruções do próprio provedor; ou

II – deixou de arquivar as informações ou, tendo-as arquivado, foram elas destruídas ou modificadas, tendo o ofertante tomado as medidas adequadas para seu arquivamento, segundo parâmetros estabelecidos pelo provedor.

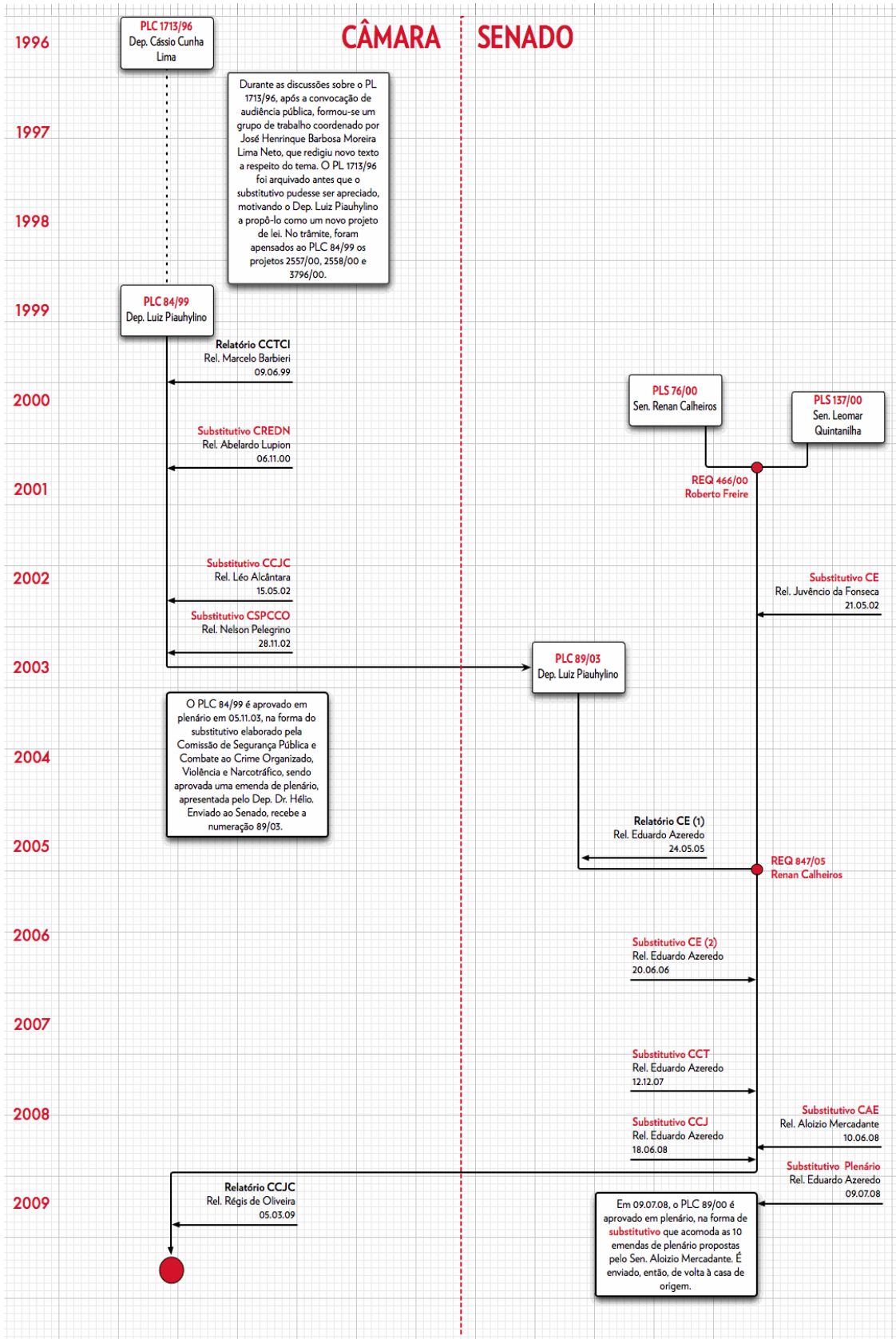
Art. 37. O provedor que forneça serviços de conexão ou de transmissão de informações, ao ofertante ou ao adquirente, não será obrigado a vigiar ou fiscalizar o conteúdo das informações transmitidas.

Art. 38. Responde civilmente por perdas e danos, e penalmente por co-autoria do delito praticado, o provedor de serviço de armazenamento de arquivos que, tendo conhecimento inequívoco de que a oferta de bens, serviços ou informações constitui crime ou contravenção penal, deixar de promover sua imediata suspensão ou interrupção de acesso por destinatários, competindo-lhe notificar, eletronicamente ou não, o ofertante, da medida adotada.”

É importante ter em mente, a partir das experiências pretéritas de regulação da Internet no Brasil, que o tema: **(a)** não é simples, e admite alternativas de regulação que devem ser sopesadas e avaliadas com cuidado, principalmente pelo risco sempre presente de se provocar danos colaterais irreversíveis ao desenvolvimento tecnológico e social do Brasil; **(b)** caso se opte começar a regulação pela via penal, apesar dos motivos aqui apresentados, é imperativo não extrapolar o âmbito regulatório que se atribui à legislação criminal, e sempre ter em

mente os danos colaterais referidos em “a”, que são comuns à regulação tanto pela via penal quanto pela via civil.

Feita essa observação, passamos agora a uma análise dos principais momentos que marcaram a tramitação do Projeto Azeredo, desde sua proposta original na Câmara e do antecedente do PLC 1713/96, indicando os pontos de “virada” em seu percurso: os pontos em que estratégias de regulação foram abandonadas em favor de outras, e os pontos em que alterações substanciais foram incluídas no projeto na forma dos substitutivos que foram apresentados após sua passagem por algumas das comissões da Câmara e do Senado. A linha do tempo na próxima página serve como orientação para os parágrafos que seguem.



A história do PLC 89/03 (ou PLC 84/99, na numeração original na Câmara dos Deputados) – o Projeto Azeredo sobre cibercrimes – começa em 1996, com projeto de lei apresentado na Câmara dos Deputados pelo Deputado Cássio Cunha Lima (PLC 1713/96), dispondo, conforme a ementa, sobre o “acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores”. Durante o trâmite do PLC 1713/96, foi convocada audiência pública para discutir o tema, com a subsequente composição de um grupo de trabalho para a elaboração de novo texto, a ser apresentado como substitutivo. O PLC 1713/96, entretanto, foi arquivado ao término da legislatura, o que motivou o Deputado Luiz Piauhyllino a propô-lo como novo projeto de lei, o PLC 84/99.³

O PLC 84/99 foi aprovado, sem modificações, na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI). Substitutivos foram apresentados na Comissão de Constituição, Justiça e Cidadania (CCJC) e na Comissão de Segurança Pública e Combate ao Crime Organizado (CSPCCO). **Na CSPCCO, normas referentes à privacidade, sigilo e direitos dos usuários, presentes desde a primeira versão do PLC 1713/96 (ver Tabela 7, Anexo), desapareceram, passando o projeto a versar estritamente a respeito de tipos penais, acrescido de algumas definições (ver Tabela 6, Anexo), e da problemática equiparação de “dado” e “senha” a “coisa”. A exclusão desses artigos ocorreu em razão de decisão, tomada na CSPCCO, de emendar o Código Penal ao invés de regular por lei esparsa os crimes em questão.**

Após passar pelas comissões, o projeto foi aprovado em plenário (com emenda proposta pelo Deputado Dr. Hélio), e enviado ao Senado Federal, onde passou a tramitar como PLC 89/03.

Paralelamente ao que ocorria na Câmara, em 2000, foram propostos dois projetos de lei a respeito do mesmo tema: o PLS 76/00 (Renan Calheiros) e o PLS 137/00 (Leomar Quintanilha). Ambos passaram a tramitar em conjunto em virtude do Requerimento 466/00 (Roberto Freire), e enfim foram apensados ao PLC 89/03, em atendimento ao Requerimento 847/05.

³ As diferenças mais marcantes entre os projetos – além daquelas referentes às condutas tipificadas (ver Tabelas 1 a 5, Anexo) – são: **(a)** a exclusão, no PLC 84/99, de normas que estabeleciam obrigações de controle de acesso, segurança e administração de dados pessoais a “administradores de rede” (legalmente constituídos, necessariamente) e “provedores de serviços de valor adicionado”; e **(b)** a técnica adotada pelo PLC 84/99 para os tipos qualificados. Ambos os projetos previam normas referentes à proteção da privacidade dos usuários da rede.

2. Alterações substanciais

As mudanças mais substanciais sofridas pelo PLC 89/03 no Senado ocorreram em dois momentos: **(1)** na segunda passagem pela Comissão de Educação, Cultura e Esporte (CE), quando apresentado o primeiro substitutivo do Senado; e **(2)** durante os debates na Comissão de Constituição, Justiça e Cidadania (CCJ), antes, todavia, que as discussões fossem sobrestadas para a remessa do projeto à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) e Comissão de Assuntos Econômicos (CAE).

2.1 Primeira passagem pela Comissão de Educação, Cultura e Esporte (CE)

Em 2005, o Senador Eduardo Azeredo foi designado relator do PLC 89/03 quando este passou pela Comissão de Educação, Cultura e Esporte (CE). Em seu parecer, votou pela aprovação do projeto tal como se encontrava, recusando emenda proposta pelo Senador Hélio Costa, com a justificativa de que o andamento do processo legislativo exigia celeridade, e que as demais questões deveriam ser objeto de outras leis a serem eventualmente aprovadas. Como os PLSs 76/00 e 137/00 foram enfim apensados ao PLC 89/03, o Senador Eduardo Azeredo optou por apresentar substitutivo drasticamente diferente ao oferecer seu segundo parecer na CE, com a inclusão de temas que não haviam sido contemplados anteriormente. Como relata o próprio Senador:

“[...] quando o projeto chegou à Comissão de Educação – e eu fui relator –, a minha primeira defesa foi no sentido de aprová-lo como ele tinha vindo da Câmara. Por quê? Por uma visão bem objetiva. Pensei: “*Vamos aprovar o projeto como está, porque ele já é bom, atende basicamente a 80% do que queríamos atender*”. É verdade que, com a velocidade da tecnologia, de lá para cá, algumas coisas mudaram. Mas vamos aprová-lo como está.

O Senador Hélio Costa, na época, ponderou que não, que já havia algumas coisas novas. Foi S.Exa., inclusive, que levantou essa questão do *fishing* [sic]. Mas, mesmo assim, foi aprovado num acordo. Aprovaríamos daquele jeito e faríamos um projeto complementar, uma PEC Paralela, aquela famosa PEC Paralela que nunca mais vingou. O problema é esse: a PEC Paralela não foi mais votada.

A idéia era essa, que aprovássemos como estava. E faríamos um projeto paralelo, para complementar o primeiro projeto.

Quando já corria o prazo no Senado, foi apresentado requerimento no sentido de apensar os projetos. Aí ele voltou para a Comissão de Educação. Como estava vencida aquela etapa que eu tinha defendido, pensei: *“Então, vamos agora fazer um projeto mais atualizado. E vamos complementá-lo com o que aconteceu da época da aprovação na Câmara até hoje”*.

Daí, então, é que o substitutivo foi feito. Foram fundidos, na verdade, vários projetos, o do Senador Renan Calheiros, do PMDB; o do Senador Leomar Quintanilha, do PC do B. Aproveitou-se a idéia do cadastramento, do Senador Delcídio Amaral, do PT de Mato Grosso do Sul.

Aí é que fizemos, então, este substitutivo que está em discussão, aprovado por unanimidade na Comissão de Educação e enviado para a Comissão de Constituição, Justiça e Cidadania, onde houve todo esse quiproquó, digamos assim”.⁴

Enviado à Comissão de Constituição, Justiça e Cidadania (CCJ), na qual também foi designado como relator o Senador Eduardo Azeredo, o projeto passou por outra rodada de alterações (o “quiproquó” a que se refere o Senador decorre de uma série de dispositivos polêmicos acrescentados ao projeto, conforme se verá no item 2.1). As discussões foram sobrestadas, todavia, por requerimentos solicitando que o projeto antes passasse pela Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática (CCT) e pela Comissão de Assuntos Econômicos (CAE). O Senador Eduardo Azeredo, relator do PLC 89/03 na CCT, apresentou junto ao seu parecer substitutivo fruto das discussões previamente ocorridas no âmbito da CCJ. Aprovado o parecer, o projeto foi remetido à CAE, sendo aprovado na forma de substitutivo apresentado pelo relator Senador Aloizio Mercadante, que fez uma série de alterações ao texto, mantendo, contudo, sua substância. Este texto foi enfim aprovado na CCJ, com alterações apenas nas disposições referentes aos crimes militares. Enviado ao plenário, dez emendas foram apresentadas pelo Senador Aloizio Mercadante, mantendo-se, ainda, a substância do texto. É esta a atual redação do projeto.

2.2 Segunda passagem Comissão de Educação, Cultura e Esporte

O texto legal anexado pelo Senador Eduardo Azeredo em seu segundo parecer na CE tem estrutura inteiramente tributária do PLC 89/03, de modo que o PLS 76/00, apensado, tem importância secundária, e serve mais como inspiração do que como fonte textual. O PLS

⁴ Senador Eduardo Azeredo, 14.11.2006, no seminário: “Liberdade de acesso à Internet e combate ao crime cibernético”, (Comissão de Direitos Humanos e Minorias). Notas taquigráficas disponíveis em: http://www.safernet.org.br/wiki/pub/SaferNet/PLSEduardoAzeredo/notas_taquigraficas-audiencia-publica-PLS-Azeredo-CDHM-14-11-2006.pdf. Citação constante da p. 16. Itálicos no original.

137/00, também apensado, previa apenas aumento de penas conforme o meio,⁵ de modo que o substitutivo apresentado é efetivamente uma nova versão do PLC 89/03.

Além de inserir modificações nos tipos penais que formavam, após a passagem pela CSPCCO da Câmara, o principal componente do projeto, o substitutivo inovou ao exigir o registro obrigatório de qualquer pessoa interessada em utilizar a Internet,⁶ com correspondente tipo penal criminalizando a violação desse dever. **O segundo relatório da CE e o substitutivo então apresentado marcam, portanto, uma virada no histórico de tramitação do PL 89/03: disposições referentes a cadastramento de dados, com o objetivo da identificação de eventuais criminosos, passaram a ser uma das principais demandas de alguns dos interessados na aprovação da lei:**

⁵ “O PLS n° 137, de 2000, de autoria do Senador Leomar Quintanilha, consiste em apenas um artigo, além da cláusula de vigência, e visa a aumentar em até o triplo as penas previstas para os crimes contra a pessoa, o patrimônio, a propriedade imaterial ou intelectual, os costumes, e a criança e o adolescente na hipótese de tais crimes serem cometidos por meio da utilização da tecnologia de informação e telecomunicações”. Segundo parecer apresentado na CE pelo Relator Eduardo Azeredo, p. 1.

⁶ “**Art. 14** Todo aquele que torna disponível o acesso a uma rede de computadores somente admitirá como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que for autenticado conforme validação positiva dos dados cadastrais previamente fornecidos pelo contratante de serviços. A contratação dar-se-á exclusivamente por meio formal, vedado o ajuste meramente consensual.

§1º O cadastro mantido por aquele que torna disponível o acesso a uma rede de computadores conterà obrigatoriamente as seguintes informações prestadas por meio presencial e com apresentação de documentação original: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas Físicas (CPF), mantido pelo Ministério da Fazenda ou o Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.

§ 2º O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei venha a determinar.

§ 3º A senha e o cadastro de identificação, a critério daquele que torna disponível o acesso, poderão ser substituídos por certificado digital emitido dentro das normas da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), conforme determina a MP 2.200-2 de 24 de agosto de 2001.

§ 4º O cadastro de identificação, a critério daquele que torna disponível o acesso, poderá ser obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma deste artigo.

§ 5º Para assegurar a identidade e a privacidade do usuário a senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.”

“Recentemente em Audiência Pública sobre o PLS nº 279 de 2003, do qual também sou relator, de autoria do nobre Senador Delcídio Amaral e que propõe a criação de um cadastro de titulares de correio eletrônico na internet, ficou evidente que, para fins de investigação, é necessário estabelecer um prazo legal de armazenamento dos dados de conexões e comunicações realizadas pelos equipamentos componentes da internet, o que será feito pelos seus provedores de acesso. Os serviços de telefonia e transmissão de dados mantêm por cinco anos os dados de conexões e chamadas realizadas por seus clientes para fins judiciais, mas na internet brasileira inexistente procedimento análogo.”⁷

As normas referentes ao cadastramento propriamente dito foram abrandadas durante os debates na CCJ, mas a obrigatoriedade de armazenamento de dados de conexão, sob responsabilidade dos provedores de acesso, para cruzamento com os dados de cadastro por eles mantidos, permaneceu no projeto até sua redação atual. O que se discute atualmente é o que exatamente implica a categoria “dados de conexão”, a conveniência da definição legal proposta, e o prazo de armazenamento (3 anos na redação atual, 5 anos no segundo substitutivo aprovado na CE).⁸ Preocupações extremamente discutíveis de índole procedimental, portanto, passaram a dominar o PLC 89/03, a despeito das tipificações ainda serem um ponto sensível.

No que diz respeito aos tipos penais propostos, a tentativa de se tipificar a violação de sistemas de DRM é nítida no substitutivo apresentado na segunda passagem do projeto pela CE. Incluiu-se no projeto, naquela oportunidade, a definição de “dispositivo de comunicação” em substituição à de “meio eletrônico”, em atenção a uma sugestão de Hélio Costa, recusada quando da primeira análise do projeto na CE.⁹ Observe-se que em versões pretéritas do projeto, a definição de “dispositivo de comunicação” era muito mais explícita do que a atual, e não deixava dúvidas a respeito das intenções que motivaram sua inclusão no PLC 89/03.

⁷ Senador Eduardo Azeredo, segundo parecer aprovado na CE, p. 13.

⁸ “**Art. 154-E.** Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.

Pena – detenção, de dois a seis meses, e multa.”

⁹ “Finalmente o Senador [Hélio Costa] sugeriu a mudança do termo “meio eletrônico” por “dispositivo de comunicação” no art. 154-C, à qual acatamos e no substitutivo promovemos sua atualização e complementação” (Segundo relatório aprovado na CE, p. 7).

Nas palavras do Senador Eduardo Azeredo, no oitavo parecer elaborado durante a passagem do PL 89/03 na CCJ (repetidas no relatório apresentado na CCT):

“— na definição de ‘Dispositivo de Comunicação’ incluímos a Expressão ‘os meios de captura de dados eletrônicos ou digitais ou similares’, substituímos [sic] a expressão ‘digitais’ por ‘eletrônicos ou digitais ou similares’ e incluímos a expressão ‘os receptores e os conversores de sinais de rádio ou televisão digital’, conhecidos como ‘*set-top box*’;”¹⁰

No substitutivo da CCT, a definição apresentada acrescentou, explicitamente, os telefones celulares:

“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;”

A definição, tal como redigida atualmente (após emenda na CAE), apesar de não ser explícita quanto ao que abarca, *continua incluindo*, por sua abrangência, os aparelhos mencionados acima:

I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;

Todos os tipos penais que fizerem, no projeto, referência a “dispositivo de comunicação” podem ser considerados, em diferentes medidas, como também criminalizando a violação de sistemas de DRM. O mesmo pode ser dito em relação às definições de “sistema informatizado” e “código malicioso” (definição incluída no substitutivo da CCT). A interação entre essas definições e os tipos penais podem dar margem, desta maneira, a interpretações que parecem pouco prováveis, a princípio, mas se encaixariam perfeitamente na *mens legis*. Outros problemas relativos aos tipos penais que aos poucos foram se formando durante a tramitação do projeto no Senado serão explicitados na próxima parte deste documento.

¹⁰ Oitava versão do parecer do Senador Eduardo Azeredo na CCJ, p. 8. Disponível em: http://www.safernet.org.br/twiki/pub/SaferNet/PLSEduardoAzeredo/PLS_Azeredo-CCJ-versao-de-19-04-2007.pdf.

2.3 As discussões na CCJ e o substitutivo da CCT

O segundo momento em que alterações substanciais foram acrescentadas ao PL 89/03 se deu quando da aprovação do parecer da CCT, relatado pelo Senador Eduardo Azeredo. O substitutivo apresentado na ocasião já era bastante diferente daquele aprovado na CE, incorporando modificações que resultaram de debates prévios na CCJ,¹¹ sobrestados em razão de requerimentos solicitando a discussão do PL 89/03 na CCT e na CAE.

Continuando a tendência, já observada no substitutivo da CE, de buscar a inclusão de normas que fortalecessem os procedimentos investigatórios e de instrução probatória para a persecução penal de “cibercrimes”, o substitutivo da CCT tem o objetivo claro de provocar alterações institucionais consideráveis para viabilizar tal propósito. Duas alterações merecem destaque:

- “p) acrescentar determinação para que a autoridade competente, nos termos de regulamento, estructure órgãos, setores e equipes de agentes especializados no combate à ação delituosa praticada em rede de computadores, dispositivo de comunicação ou sistema informatizado;
- q) alterar a Lei nº 10.446, de 8 de maio de 2002, a lei da repressão uniforme, para possibilitar a atuação da Polícia Federal na investigação dos crimes tratados no projeto de lei;”

Particularmente discutível é transferir atribuição da Polícia Federal, em suma, para a investigação de toda e qualquer infração ocorrida na Internet, independentemente de efetiva repercussão interestadual (presumida agora por determinação legal). O parecer menciona que a Polícia Federal atuará na investigação “dos crimes tratados no projeto de lei”, mas o texto enfim aprovado abre espaço a qualquer infração praticada via Internet. Não apenas é questionável que todo crime, a despeito da amplitude da rede, tenha repercussão interestadual (estelionato é um exemplo bastante óbvio, se ambos infrator e vítima estiverem no mesmo Estado da União), mas também se observa na modificação uma grave presunção, implícita, de que as polícias civis estaduais sejam incapazes de realizar investigações que envolvam a Internet.

Outras modificações extremamente controvertidas vieram, em bloco, na forma do art. 23 do substitutivo, **direcionadas a provedores de acesso**:

¹¹ Que resultaram, importante ressaltar, na eliminação de parte das normas referentes ao cadastramento obrigatório, e do instituto da igualmente polêmica “legítima defesa digital”.

“s) incluir artigo tratando das obrigações do responsável pelo provimento de acesso a uma rede de computadores, quais sejam:

- a. manter a obrigação da preservação de dados de conexões, retirando a expressão ‘e comunicações’, reduzindo a lista de informações a serem guardadas, e reduzindo o prazo de guarda de ‘cinco’ para ‘três’ anos;
- b. tornar disponíveis à autoridade competente e por autorização expressa da autoridade judicial os dados de conexão no curso de auditoria técnica a que forem submetidos;
- c. fornecer os dados de conexões realizadas quando solicitado pela autoridade competente no curso de investigação e por autorização expressa da autoridade judicial;
- d. preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de conexões realizadas, e outras informações solicitadas por aquela investigação, respondendo pela sua absoluta confidencialidade e inviolabilidade;
- e. informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, denúncia da qual tenha tomado conhecimento e que contenha indícios de prática de crime, sujeito a ação penal pública incondicionada, na rede de computadores, sob sua responsabilidade;
- f. informar ao usuário que aquela conexão de acesso à rede de computadores sob sua responsabilidade obedece às leis brasileiras, e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;
- g. alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;
- h. divulgar aos seus usuários, em local destacado, as boas práticas de segurança no uso de rede de computadores, dispositivo de comunicação e sistema informatizado;
- i. remeter para regulamento o detalhamento relativo à guarda de dados e outras obrigações;
- j. determinar o prazo de transição de cento e oitenta dias para que os dados e procedimentos requeridos estejam disponíveis;
- k. definir, respectivamente, a multa pelo descumprimento das obrigações e a destinação dos recursos financeiros resultantes da aplicação da multa;”

Essas modificações, no que persistiram no projeto final, serão discutidas na próxima parte deste documento. Cabe aqui, entretanto, mencionar o problema das definições de “dados de conexão” e “dados informáticos”, em associação às disposições indicadas acima, e na obrigação do item “d”, que equivale a uma **escuta telemática antecipada realizada sem a obtenção de ordem judicial**. Pouco importa que os dados sejam *comunicados* apenas após ordem judicial: já houve uma séria violação à privacidade e vida íntima. Outro ponto preocupante é a transferência a regulamento das normas relativas à guarda de dados e “outras obrigações”, e o sistema de delação automática, transformando-se os provedores de acesso em entidades de vigilância atuando *longa manus* dos órgãos oficiais de persecução.¹²

¹² É importante que se tenha em mente que o substitutivo da CCT também inovou com a seguinte disposição: “t) incluir artigo do substitutivo determinando que não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso e hospedagem quando constatada qualquer prática criminosa.”

Aprovado o substitutivo da CCT, o projeto foi encaminhado à CAE, apresentando o relator Deputado Aloizio Mercadante novo substitutivo. As alterações não foram substanciais, cuidando apenas de modificar a redação de alguns dispositivos sem alterar-lhes a essência, eliminando, ainda, normas irrelevantes como as dos arts. 16 e 17 do substitutivo.¹³ A alteração mais significativa talvez tenha sido o fim da equiparação entre “dado” e “coisa”.

De volta à CCJ, o parecer do Deputado Eduardo Azeredo foi aprovado, sendo apresentado um substitutivo que apenas se limitou a emendar a parte do projeto referente aos crimes militares. Em plenário, foram apresentadas dez emendas pelo Senador Aloizio Mercadante, em nada alterando, novamente, a substância do projeto, sendo o texto aprovado o atual PLC 89/03, devolvido à Câmara dos Deputados.

3. Situação atual da regulamentação da Internet no Brasil

Analisado o percurso do PLC 89/03, cabe agora proceder a uma análise da situação atual da regulamentação da Internet no Brasil, a partir da legislação em vigor no País, e sua aplicação em decisões envolvendo a internet. Apresenta-se aqui também a experiência internacional sobre responsabilização na rede, com destaque para o sistema norte-americano, para contraste.

Concluímos, ao final, ser urgente a retomada da discussão sobre um marco civil da internet brasileira, com a preocupação de não se deixar em segundo plano (a) as salvaguardas necessárias para provedores de acesso e de conteúdo, e (b) o regime de privacidade aplicável aos dados online.

¹³ “[...] sugerimos a supressão dos arts. 16 e 17 do parecer da CCT. O art. 16 prevê exceção à regra determinada pelo art. 2º da Lei 9296/96, que exclui a possibilidade de interceptação de comunicação para os crimes apenados com detenção. Já a alteração do art. 313 do Código de Processo Penal acrescenta novo inciso V, prevendo a possibilidade de prisão preventiva para os crimes “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”, enquanto o inciso I do mesmo art. 313 já prevê essa possibilidade para os crimes punidos com reclusão. Ambos perdem o sentido, uma vez que todas as penas previstas nas emendas ora apresentadas são de reclusão”. Parecer CAE, p. 5.

3.1 Regime de responsabilização dos provedores

Duas principais questões podem ser apontadas na definição do regime de responsabilização dos provedores de serviços na Internet: a definição sobre a aplicação de uma responsabilidade subjetiva ou objetiva e a incidência das regras do Código de Defesa do Consumidor (CDC) nas relações estabelecidas na Internet.

3.1.1 Responsabilidade civil subjetiva ou objetiva

Toda ação indenizatória requer, por princípio, a prova de três elementos: o dano sofrido (material ou moral), a conduta culposa do agente do dano (dolo ou culpa) e a relação de causalidade entre a conduta do agente e o dano sofrido. Essa regra não se aplica, no entanto, aos chamados casos de responsabilidade objetiva do agente. A responsabilidade objetiva prescinde desses elementos, bastando que a vítima prove que sofreu um dano e que esse dano deriva da conduta do agente. A responsabilidade objetiva aparece em diversos textos jurídicos brasileiros, como por exemplo, no Código de Defesa do Consumidor (CDC), que cria responsabilidade objetiva para fornecedores de produtos e serviços com relação a seus consumidores.

Ocorre que passados mais de 15 anos de acesso público à internet no Brasil, ainda não existe no país uma legislação específica que trate da responsabilidade dos provedores da internet (de acesso ou de conteúdo). Com isso, prevalecem dúvidas sobre qual seria a espécie de responsabilidade dos provedores, se subjetiva (exigindo dano, de conduta culposa e causalidade) ou objetiva (exigindo apenas a prova do dano e da causalidade), havendo uma tendência tanto doutrinária quanto jurisprudencial de se aplicar a responsabilidade objetiva aos provedores da internet.

Essa aplicação da responsabilidade objetiva expõe os provedores a um regime demasiadamente amplo de responsabilização civil, o que não apenas aumenta custos, como gera incerteza jurídica e prejuízos à inovação. Novos serviços online surgidos no Brasil não

têm como avaliar com segurança a extensão do risco jurídico incorrido.

Nesse sentido, na ausência de uma legislação específica para a responsabilidade civil na Internet, os tribunais nacionais têm aplicado de forma majoritária o regime de responsabilidade objetiva aos provedores de serviços na Internet, seja com base no CDC, seja com base no artigo 927 § do Código Civil.¹⁴

A principal decisão sobre o assunto tomada pelo Superior Tribunal de Justiça condenou a Terra Networks S/A a indenizar em 200 (duzentos) salários mínimos uma pessoa que teve o seu nome inserido indevidamente em página de encontros administrada pelo provedor. A decisão confirma a aplicação do CDC mesmo para serviços pretensamente gratuitos, pois considera que no caso existe uma remuneração indireta com a possibilidade de se divulgar para o usuário “anúncios, eventos e assinaturas”.¹⁵

Com a edição do novo Código Civil, em 2002, a vítima de danos causados na Internet não mais precisaria provar, em ações indenizatórias contra provedores, a existência de relação

¹⁴Código Civil, art. 927. “Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. *Parágrafo único.* Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.”

¹⁵Essa é a ementa da decisão: “DIREITO DO CONSUMIDOR E RESPONSABILIDADE CIVIL - RECURSO ESPECIAL - INDENIZAÇÃO - ART. 159 DO CC/16 E ARTS. 6º, VI, E 14, DA LEI Nº 8.078/90 - DEFICIÊNCIA NA FUNDAMENTAÇÃO - SÚMULA 284/STF – PROVEDOR DA INTERNET - DIVULGAÇÃO DE MATÉRIA NÃO AUTORIZADA - RESPONSABILIDADE DA EMPRESA PRESTADORA DE SERVIÇO - RELAÇÃO DE CONSUMO - REMUNERAÇÃO INDIRETA - DANOS MORAIS - QUANTUM RAZOÁVEL - VALOR MANTIDO. 1 - Não tendo a recorrente explicitado de que forma o v. acórdão recorrido teria violado determinados dispositivos legais (art. 159 do Código Civil de 1916 e arts. 6º, VI, e 14, ambos da Lei nº 8.078/90), não se conhece do Recurso Especial, neste aspecto, porquanto deficiente a sua fundamentação. Incidência da Súmula 284/STF. 2 - Inexiste violação ao art. 3º, § 2º, do Código de Defesa do Consumidor, porquanto, para a caracterização da relação de consumo, o serviço pode ser prestado pelo fornecedor mediante remuneração obtida de forma indireta. 3 - Quanto ao dissídio jurisprudencial, consideradas as peculiaridades do caso em questão, quais sejam, psicóloga, funcionária de empresa comercial de porte, inserida, equivocadamente e sem sua autorização, em site de encontros na internet, pertencente à empresa-recorrente, como “pessoa que se propõe a participar de programas de caráter afetivo e sexual”, inclusive com indicação de seu nome completo e número de telefone do trabalho, o valor fixado pelo Tribunal a quo a título de danos morais mostra-se razoável, limitando-se à compensação do sofrimento advindo do evento danoso. Valor indenizatório mantido em 200 (duzentos) salários mínimos, passível de correção monetária a contar desta data.” (STJ, Resp. 566468/RJ, j. em 23.11.2004).

de consumo para que fosse aplicado o regime de responsabilização objetiva (como ocorreu no caso acima). Atualmente existem diversas decisões que responsabilizam provedores de serviços na Internet apenas com base no artigo 927 § do Código Civil.¹⁶

Vale lembrar que a adoção do regime de responsabilização objetiva não implica automática condenação do provedor de serviços, podendo o mesmo se valer das chamadas excludentes de responsabilização, dentre as quais se podem mencionar: **(i)** a ocorrência de caso fortuito ou força maior que causa diretamente o dano; **(ii)** a existência de culpa exclusiva da vítima para o resultado danoso; **(iii)** um fato de terceiro; e até mesmo **(iv)** a afirmação de culpa concorrente entre vítima e agente do dano, reduzindo assim o valor a ser indenizado.

3.1.2 Aplicação do Código de Defesa do Consumidor

Além do comentado acima, alguns projetos de lei em apreciação no Congresso Nacional procuram consolidar a aplicação do CDC para o desenvolvimento de atividades típicas dos provedores. Nesse sentido, o PL nº 7093/02, de autoria do Deputado Ivan Paixão, que trata basicamente sobre o envio de mensagens eletrônicas em massa e não autorizadas (spam), afirma no seu artigo 11 que “aplicam-se as normas de defesa e proteção do consumidor vigente no País, naquilo que não conflitar com essa lei”.

¹⁶Esse foi o caso de uma decisão da 39ª Vara Cível do Foro Central de São Paulo que condenou uma lan-house a pagar danos morais por mensagem enviada por usuário de seus computadores. Segundo a decisão: “à ré cumpria, como estabelecimento origem da emissão da mensagem ofensiva, e portanto fornecedora de serviço de emissão de dados via internet, já que posto a disposição de seus clientes, produzir a prova de que o fato ocorreu pelo uso de sistema internet sem fio, e poderia ser constatado por perícia local. No entanto, entendeu por bem dispensar essa prova, deixando de considerar que na hipótese vigora a responsabilidade civil objetiva consoante prevista no art.927, § único, do Código Civil, em razão do desenvolvimento de atividade que por sua natureza implique em risco para o direito de outro, caso em que ao autorizar o reconhecimento do dever de indenizar não assume relevo a conduta dolosa ou culposa do agente já que basta a existência do dano e do nexó etiológico entre o fato e o dano. Nesse sentido, quem disponibiliza terminais de computadores ou rede sem fio para uso de internet assume o risco do uso indevido desse sistema para lesar direito de outrem, exemplo do que sucede no caso dos autos. Poder-se-ia cogitar das excludentes do caso fortuito força maior contudo cumpria à ré a prova, sendo que desse ônus descurando não há cogitar de sua incidência.” (Processo nº 583.00.2006.243439-5)

Vale mencionar que a aplicação do CDC às atividades desempenhadas pelos provedores de serviços na Internet possui muitos aspectos positivos. Por exemplo, no regramento de várias situações que não encontram o amparo devido em outros setores da legislação, como a proteção dos dados pessoais dos usuários e o próprio regime contratual aplicável.

Todavia, a aplicação de responsabilidade civil objetiva para as atividades desenvolvidas por provedores, fundamentada no risco criado, pode ser especialmente prejudicial: **(i)** para o grau de inovação empreendida por esses agentes em novos serviços e aplicações; **(ii)** para o aumento de custos de provedores representado pelo decorrente de ações judiciais e precauções jurídicas conexas; e **(iii)** para o desenvolvimento de aplicações colaborativas (“web 2.0” e outras). Com base na percepção de que os provedores de conteúdo e de acesso possuem uma posição vulnerável com relação a demandas jurídicas, a legislação de vários países (incluindo a norte-americana) adota uma série de salvaguardas para os provedores, conforme se verá abaixo. A razão para isso é a necessidade de haver um equilíbrio entre a responsabilidade dos provedores da internet e outros valores jurídicos igualmente importantes, como proporcionalidade, privacidade, acesso, isonomia, dentre outros.

3.1.3 Responsabilidade subjetiva - notificação da vítima para retirada de conteúdo

Entre as concepções de que o provedor de serviços na Internet não é responsável pelas informações disponibilizadas por seus usuários e aquela que defende a responsabilidade objetiva pelo risco, a responsabilidade subjetiva dos provedores pode ser fundamentada: (i) na impossibilidade do provedor monitorar todo o conteúdo gerado por seus usuários; e justamente por isso (ii) na possibilidade de que a pretensa vítima de um dano venha a dar conhecimento ao provedor do fato danoso (a vítima é, do ponto de vista econômico, o chamado *cheapest cost-avoider*).

É curioso verificar que esses princípios estiveram presentes desde o final da década de 90 em diversos projetos de lei apresentados ao Congresso Nacional, que não tiveram continuidade no seu trâmite. Nesse sentido, projetos como o apresentado pela Ordem dos Advogados de São Paulo e seu substitutivo (Projeto de Lei nº 4906/01), já tentavam criar

salvaguardas para os provedores ao disciplinar a matéria, equilibrando sua posição jurídica:

Art. 35. O provedor que forneça serviços de conexão ou de transmissão de informações, ao ofertante ou ao adquirente, não será obrigado a vigiar ou fiscalizar o conteúdo das informações transmitidas

Art. 36. Responde civilmente por perdas e danos, e penalmente por co-autoria do delito praticado, o provedor de serviço de armazenamento de arquivos que, tendo conhecimento inequívoco de que a oferta de bens, serviços ou informações constitui crime ou contravenção penal, deixar de promover sua imediata suspensão ou interrupção de acesso por destinatários, competindo-lhe notificar, eletronicamente ou não, o ofertante, da medida adotada.

Apesar disso, nenhuma legislação até o momento foi adotada, de modo que a responsabilidade dos provedores continua a ser regulada por regras gerais, com predominância da aplicação da responsabilidade objetiva.

3.2 Privacidade e dados pessoais

3.2.1 Armazenamento de dados pessoais

O armazenamento de dados pessoais e registros de navegação para que possam instruir eventuais e futuras ações indenizatórias é um tema presente em vários projetos de lei. O tempo de armazenamento desses dados varia bastante de acordo com o projeto focado. A atual redação do substitutivo sobre crimes na Internet aprovada no plenário do Senado, de autoria do Senador Eduardo Azeredo, chega a prever 3 anos como prazo de armazenamento.

3.2.2 Informação de dados pessoais para terceiros

A regra geral do ordenamento jurídico brasileiro é de que dados pessoais e demais informações que possam levar à identificação de certo usuário somente podem ser

disponibilizadas pelos provedores mediante ordem judicial. Embora exista controvérsia se a simples solicitação por parte da força policial seria suficiente para obrigar os provedores a disponibilizar esses dados, o Superior Tribunal de Justiça (STJ) já decidiu, no Habeas Corpus nº 8493/99, que as empresas apenas são obrigadas a revelar dados pessoais de seus clientes mediante ordem judicial. O Supremo Tribunal Federal (STF) também decidiu no mesmo sentido recentemente, conforme abaixo:

A jurisprudência deste Tribunal é de que o sigilo da comunicação de dados somente pode ser violado por ordem judicial, para fins de investigação criminal ou instrução processual penal (art. 5º, XII, CF), ou pelas Comissões Parlamentares de Inquérito, que possuem poderes de investigação próprios das autoridades judiciais (art. 58, §3º, CF). Nesse sentido, os seguintes precedentes: RE 461.366/DF, Rel. Marco Aurélio, Primeira Turma, DJe nº 182, de 29.8.2008; MS 22.801/DF, Rel. Menezes Direito, Pleno, DJe nº 47, de 14.3.2008; Inq 2.245/MG, Rel. Joaquim Barbosa, Pleno, DJ 9.11.2007; RE-AgR 318.136/RJ, Rel. Cezar Peluso, Segunda Turma, DJ 6.10.2006; RE 418416/SC, Rel. Sepúlveda Pertence, Pleno, DJ 19.2.2006; HC 86.094/PE, Rel. Marco Aurélio, Primeira Turma, DJ 11.11.2005.

Voto do Ministro Celso de Mello no julgamento do MS 22.801/DF:

Tenho insistentemente salientado, em decisões várias que já proferi nesta Suprema corte, que a tutela jurídica da intimidade constitui – qualquer que seja a dimensão em que se projete – uma das expressões mais significativas em que se pluralizam os direitos da personalidade. Trata-se de valor constitucionalmente assegurado (CF, art. 5º, X), cuja proteção normativa busca erigir e reservar, sempre em favor do indivíduo – e contra a ação expansiva do arbítrio do Poder Público – uma esfera de autonomia intangível e indevassável pela atividade desenvolvida pelo aparelho de Estado.

Apesar de a privacidade ser protegida em âmbito da Constituição Federal, aumentam as pressões atualmente no sentido de se criar a obrigação por parte de provedores tanto da preservação de dados trafegados quanto da quebra do sigilo de usuários mediante requisição administrativa, sem ordem judicial, ou até mesmo a pedido de instituições privadas. Por essa razão, o tema da privacidade e o regime de proteção de dados trafegados e dados pessoais é outro assunto não regulado pela legislação brasileira e que agora demanda regulamentação civil mais específica no Brasil, a exemplo do que fizeram outros países.

4. Experiências internacionais

4.1 Estados Unidos

Nos Estados Unidos, a responsabilidade de provedores é regulada pelo US Code, em seu Título 17, § 512, conforme modificações inseridas pelo Digital Millenium Copyright Act (DMCA), de 1998, especial para os casos de infração ao direito autoral, bem como por meio do Communications Decency Act (CDA), lei aprovada no final de 1995.

O referido § 512 do DMCA estipula em que circunstâncias os provedores não deverão ser responsabilizados pelos atos praticados pelos seus usuários. Dessa forma, a lei norte-americana cria circunstâncias específicas, chamadas de salvaguardas (*safe harbors*) ao definir hipóteses em que há limitação à responsabilidade. Igualmente, o CDA também prevê, em seu artigo 230, limitação à responsabilidade dos provedores.

O DMCA, em seu artigo 512, cria definições específicas sob as quais os provedores ficam isentos de responsabilidade civil, havendo para isso a classificação dos provedores nas seguintes categorias:

- i) serviços de comunicação transitória (512 (a));
- ii) sistema de *cache* (512 (b));
- iii) hospedagem (512 (c)); e
- iv) ferramentas de localização de informações (512 (d)).

(i) serviços de comunicação transitória

Pelo artigo 512(a), define-se este serviço como aquele capaz de transmitir, rotear, fornecer conexões, através de um sistema ou de uma rede controlada ou operada pelo provedor de serviço, ou por razão da intermediação ou do armazenamento transitório de dados no curso dessa transmissão, desse roteamento ou desse fornecimento de conexões.

De modo geral, esta seção limita a responsabilidade do provedor em circunstâncias em que o provedor apenas atua como transmissor de dados, transmitindo informação digital de um ponto a outro, mediante solicitação. A limitação cobre atos de transmissão, roteamento ou fornecimento de conexão para outra informação, bem como de cópias intermediárias que são feitas automaticamente na operação da rede.

Para que haja limitação de responsabilidade por parte dos provedores definidos como de comunicação transitória, é necessário que sejam respeitadas as seguintes hipóteses: (1) a transmissão do material tenha sido iniciada ou solicitada por pessoa outra que o próprio provedor do serviço; (2) a transmissão, o roteamento, o fornecimento de conexões ou o armazenamento sejam feitos por meio de um processo técnico automático sem qualquer seleção de material pelo provedor de serviço; (3) o provedor de serviços não tenha selecionado os destinatários dos materiais transmitidos, exceto pela resposta automática do pedido do usuário; (4) nenhuma cópia do material que tenha sido feita pelo provedor de serviço no curso de eventual intermediação ou armazenamento provisório das informações seja mantida no sistema ou na rede de maneira ordinariamente acessível a qualquer outra pessoa, e nenhuma cópia seja mantida no sistema ou na rede de maneira acessível a qualquer usuário por um período maior do que o necessário para a transmissão, o roteamento ou o fornecimento de uma conexão; e (5) o material seja transmitido através do sistema ou da rede sem qualquer modificação de seu conteúdo.

(ii) sistema de *cache*

Por sistema de cache entende-se, nos termos do artigo 512 (b) do DMCA, o serviço destinado a intermediar e armazenar provisoriamente dados em um sistema ou em uma rede controlada ou operada pelo provedor de serviço.

De acordo com o U.S. Copyright Office Summary,¹⁷ o artigo 512(b) limita a responsabilidade de provedores de serviços pela prática de reter cópias, por tempo limitado,

¹⁷Cf. <http://www.copyright.gov/legislation/dmca.pdf>. Acesso em 23 de abril de 2009.

de material que tenha sido disponibilizado por terceiro e então transmitido pelo provedor. Neste caso, o provedor retém o material de modo que pedidos subsequentes para o mesmo material podem ser atendidos por meio do acesso à cópia em vez da busca pelo material em sua fonte original na rede.

Ainda em conformidade com o documento disponibilizado, essa prática conta com a vantagem de requerer menor capacidade de conexão e redução no tempo de espera para acesso à mesma informação. Por outro lado, pode resultar no acesso à informação não atualizada além de privar os operadores de website de verificarem com precisão o número de acesso a determinado website, o que pode ser importante no caso de remuneração por acesso a peça publicitária. Por tal razão, aquele que disponibiliza material online pode estabelecer regras sobre sua atualização e pode se valer de medidas tecnológicas para verificar o número de acessos.

Para haver limitação de responsabilidade pelo uso de sistema de *cache*, devem estar presentes as seguintes condições: (1) o conteúdo do material retido não pode ter sido modificado; (2) o provedor precisa cumprir as regras sobre atualização do material, substituindo as cópias retidas pelo material original, quando especificado de acordo com os padrões normalmente aceitos; (3) o provedor não pode interferir na tecnologia que informa o número de acesso àquele que disponibilizou o material, sempre que tal tecnologia cumprir com determinados requisitos; (4) o provedor tem que limitar o acesso dos usuários a determinado material de acordo com as condições de acesso (como senha, por exemplo) impostas por aquele que disponibilizou o material; e (5) qualquer material que tenha sido disponibilizado sem autorização do titular dos direitos autorais deverá ser removido ou bloqueado tão logo seja o provedor notificado que o material foi removido ou bloqueado ou tenha sido solicitada sua remoção ou bloqueio em seu *website* de origem.

(iii) hospedagem

Entende-se por provedor de hospedagem aquele que, nos termos do artigo 512(c), permite armazenar, conforme instruções do usuário, o material que reside em um sistema ou em uma rede controlada ou operada pelo provedor de serviço.

Nesta hipótese, a limitação de responsabilidade se dará nos seguintes casos: (1) (A) [o provedor] não possui conhecimento de que o material ou a atividade viola direitos; (B) na ausência de tal conhecimento, não conhece fatos ou circunstâncias pelos quais a atividade que viola direitos se tornaria evidente; (C) tão logo obtenha conhecimento ou ciência, aja imediatamente para remover ou desabilitar o acesso a este material; (2) os provedores não recebem qualquer benefício financeiro diretamente atribuível à atividade que viola direitos, caso os provedores tenham o direito e a habilidade de controlar tal atividade; e (3) se notificados de uma suposta atividade que viole direitos conforme descrita pela subseção (c) (3), os provedores responderem imediatamente para remover ou desabilitar o acesso ao material que alega-se como violando direitos.

Além das condições acima, o provedor deverá apontar um procurador (por exemplo, um correio eletrônico ou página *web* específica) para receber as notificações das violações alegadas. A lei ainda indica quais os elementos devem constar da notificação a ser endereçada ao procurador para que seja considerada válida.

A fim de evitar notificações abusivas ou equivocadas, a própria lei prevê o procedimento de contra-notificação no artigo 512 (g). Assim, uma vez que o provedor notifique o usuário de que o material por este disponibilizado foi removido em razão de denúncia de terceiro, poderá o usuário responder por meio de contra-notificação, a ser entregue ao terceiro denunciante. Neste caso, o provedor comunica o terceiro da contra-notificação e informa que voltará a disponibilizar o material controverso em 10 (dez) dias úteis.

A partir daí, o provedor poderá disponibilizar o material em não menos do que 10 (dez) e não mais do que 14 (quatorze) dias úteis, exceto se seu procurador for informado de ação proposta pelo denunciante com o objetivo de buscar ordem judicial para impedir o usuário de disponibilizar o material objeto da disputa.

(iv) ferramentas de localização de informações

Conforme definição do artigo 512(d), são ferramentas de localização de informações aquelas disponibilizadas por provedor com o objetivo de mostrar referências ou *links* para usuários de uma localidade *online*, incluindo diretórios, índices, referências, apontadores, ou *links* de hipertexto.

Nesta hipótese, a limitação de responsabilidade se dará em casos muito semelhantes ao do item anterior: **(1)(A)** os provedores não possuem conhecimento de que o material ou a atividade viola direitos; **(B)** na ausência de tal conhecimento, os provedores não conhecem fatos ou circunstâncias pelos quais a atividade que viola direitos se tornaria evidente; **(C)** tão logo os provedores obtenham conhecimento ou ciência, ajam para remover ou desabilitar o acesso a esse material; **(2)** os provedores não receberem qualquer benefício financeiro diretamente atribuível à atividade que viola direitos, caso os provedores tenham o direito e a habilidade de controlar tal atividade; e **(3)** se notificados de uma suposta atividade que viole direitos conforme descrita pela subseção (c)(3), os provedores responderem imediatamente para remover ou desabilitar o acesso ao material que alega-se estar violando direitos.

Embora o artigo 512 (d) não preveja a figura do procurador, os tribunais norte-americanos têm entendido que se aplicam a este artigo as mesmas previsões do artigo anterior, já que também no artigo 512 (d) faz-se menção à política de notificação para retirada de conteúdo considerado violador de direitos autorais.¹⁸

Já no CDA o regime de responsabilização adota critérios diferenciados. O CDA alterou o Communications Act de 1934 para nele fazer constar o artigo 230, que limita a responsabilidade dos provedores. Uma vez considerados intermediários, não haveria responsabilidade por conta de materiais publicados por terceiros.

¹⁸BELLIA, Patrícia L., BERMAN, Paul Schiff e POST, David G. *Cyberlaw – Problems of Policy and Jurisprudence in the Information Age*. St.Paul: Thomson/West, 2007. p. 524.

De acordo com o artigo 230 (c), “nenhum provedor ou usuário de serviço de computação interativo [*interactive computer service*] será considerado editor ou difusor de qualquer informação fornecida por outro provedor de conteúdo [*information content provider*]”,¹⁹ sendo que “provedor de conteúdo” [*information content provider*], neste caso, deve ser entendido como “qualquer pessoa ou entidade que seja responsável, no todo ou em parte, pela criação ou desenvolvimento de informação fornecida pela internet ou qualquer outro serviço de computação interativo” [*interactive computer service*].

Nos últimos anos, diversas têm sido as decisões judiciais favoráveis à não responsabilização dos provedores por conta de disponibilização, por seus usuários, de material considerado violador de direitos. A partir de um universo bastante vasto, apresentamos, a título de exemplo, apenas algumas das decisões que foram julgadas com base no DMCA ou no CDA.

i) Blumenthal v. Drudge (1998)²⁰

Matt Drudge mantinha coluna de fofocas no website AOL. Em uma de suas colunas, publicou matérias difamatórias contra Sidney Blumenthal, que processou tanto Drudge quanto AOL. A Corte competente julgou que, nos termos do artigo 230 do CDA, a AOL estava isenta de responsabilidade, mesmo sendo o colunista remunerado.

ii) Jane Doe v. America Online, Inc. (2001)²¹

Em uma de suas salas de bate-papo, um usuário da AOL disse estar interessado na aquisição de material pedófilo. Ofendida com a solicitação postada, uma usuária propôs ação judicial contra a AOL alegando que esta deveria se certificar de que seu serviço não facilitaria a distribuição de pornografia infantil. A Corte competente entendeu que a AOL estava isenta de responsabilidade nos termos do artigo 230 do CDA.

¹⁹No original: “(c) Protection for “Good Samaritan” blocking and screening of offensive material - (1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”

²⁰Cf. [http://smallbusiness.findlaw.com/copyright/copyright-realworld/internet-isp-liability\(1\).html](http://smallbusiness.findlaw.com/copyright/copyright-realworld/internet-isp-liability(1).html). Acesso em 05 de maio de 2009.

²¹Cf. [http://smallbusiness.findlaw.com/copyright/copyright-realworld/internet-isp-liability\(1\).html](http://smallbusiness.findlaw.com/copyright/copyright-realworld/internet-isp-liability(1).html). Acesso em 05 de maio de 2009.

iii) Corbis Corporation v. Amazon.com, Inc., et al. (2004)²²

O autor processou a Amazon por permitir que terceiros vendessem fotos protegidas por direitos autorais. Com base no DMCA, artigo 521 (c), a Corte competente julgou que a Amazon não poderia ser responsabilizada por atos de terceiro, uma vez que havia cumprido com todas as exigências previstas no DMCA para isenção de responsabilidade dos provedores.

iv) Robert Hendrickson v. Ebay, Inc., et al. (2004)²³

O autor propôs ação judicial contra o website Ebay por permitir que terceiros expusessem à venda cópias não autorizadas de determinado documentário. A Corte competente entendeu que o website não poderia ser responsabilizado por atos de terceiros com base no disposto no artigo 512 (c) do DMCA.

v) Doe vs. Bates (dezembro de 2006)²⁴

O autor propôs ação judicial alegando que o site Yahoo! havia hospedado fotos com pornografia infantil em um determinado grupo de discussão. O usuário que havia inserido as fotos foi preso. A Corte do Texas entendeu que o responsável era apenas aquele que havia inserido as fotos na internet, ou seja, o usuário, não havendo responsabilidade por parte do provedor, nos termos do que determina o artigo 230 do CDA.

vi) Barrett v. Rosenthal (2006)²⁵

A autora da ação denunciou fraudes no sistema de saúde. Os réus eram responsáveis por um grupo de discussão na internet onde foram distribuídas mensagens eletrônicas e declarações

²²Cf. http://www.internetlibrary.com/internetlib_subject.cfm?TopicID=19. Acesso em 05 de maio de 2009.

²³Cf. http://www.internetlibrary.com/internetlib_subject.cfm?TopicID=19. Acesso em 05 de maio de 2009.

²⁴Conforme informações disponíveis em <http://technology.findlaw.com/articles/00006/010615.html>. Acesso em 05 de maio de 2009.

²⁵Conforme informações disponíveis em <http://technology.findlaw.com/articles/00006/010536.html>. Acesso em 05 de maio de 2009.

difamatórias contra a autora. A Suprema Corte da Califórnia decidiu, com base no art. 230 do CDA, que os provedores não são responsáveis por conteúdo postado por terceiros.

vii) Sharon Fehrs v. Stubhub, Inc., and eBay, Inc. (2008)²⁶

A autora da ação processou Stubhub e eBay por permitirem a venda em seus websites, por parte de terceiros, de ingressos para o show do músico Bruce Springsteen a preço muito mais alto do que o praticado pelo site oficial, o que viola a lei da cidade de Portland. Com base no artigo 230 do CDA, o tribunal competente julgou que os réus apenas serviam de plataforma para busca de ingressos e a conseqüente transação de compra e venda, não sendo responsáveis por ato ilegal praticado por terceiros.

4.2 França

Recentemente, por pressão do presidente Nicholas Sarkozy e da então ministra da cultura Christine Albanel, a França promulgou legislativamente um sistema de responsabilidade civil específico para os casos de violação de direitos autorais denominado de resposta gradual (ou *three strikes*). Esse projeto de lei (chamado de lei Création et Internet) foi aprovado pela Assembléia Nacional francesa com pequena margem de votos (53% de votos favoráveis).

O modelo da resposta gradual baseia-se na suspensão do acesso à Internet após o envio de três notificações a usuários sobre a suspeita de violação de direitos autorais no ambiente online. As sanções e julgamento dos processos de advertência e desligamento ficariam por conta de um órgão administrativo a ser criado, a HADOPI (Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet). Aos usuários com acesso eventualmente bloqueado, seria aplicada uma dupla pena: além do desligamento, a continuidade do pagamento das mensalidades durante a suspensão por um mínimo de 1 ano.

Ocorre que o modelo foi considerado parcialmente inconstitucional pelo Conselho Constitucional francês. O Hadopi pode notificar supostos infratores, mas não terá o poder de

²⁶ Conforme informações disponíveis em <http://technology.findlaw.com/articles/00006/011209.html>. Acesso em 05 de maio de 2009.

cercear o acesso dos usuários à Internet. O Conselho Constitucional entendeu que o acesso à internet é direito fundamental (o que já havia sido definido pelo Parlamento Europeu no âmbito da União Européia). Entendeu também que o projeto violava garantias constitucionais como a privacidade dos usuários, a presunção de inocência, o devido processo legal e sobretudo a inafastabilidade do poder judiciário.

5. Conclusão

Com base no estudo acima, a sugestão é que sejam implementadas as modificações propostas para o PLC 89/03, conforme as razões expostas na introdução e nas seções subsequentes.

Além disso é possível verificar que a legislação brasileira encontra-se omissa no que tange à regulamentação da responsabilidade civil de provedores da internet e de questões relativas à privacidade, em vista dos regimes jurídicos adotados em outros países.

Diante disso, sugere-se o debate e a implementação de um marco regulatório civil para a internet brasileira, conforme a experiência de outros países. Esse marco regulatório civil deverá tratar, dentre outros temas, de salvaguardas para provedores de acesso e conteúdo, revertendo a tendência atual de aplicação generalizada da responsabilidade objetiva. Deve, ainda, possibilitar a definição de um regime de proteção a dados pessoais e dados trafegados, consolidando legislativamente o entendimento do Supremo Tribunal Federal e estabelecer critérios de proporcionalidade para os casos em que a violação de sigilo e monitoramento de informações trafegadas for inevitável.



ANEXO

Tabela 1 – Crimes de acesso: histórico

	PLC 1713/06	PLC 84/99 (original)	PLC 84/99 (CSPCCO)	PLC 89/03 (CE 2)	PLC 89/03 (CCT)	PLC 89/03 (CAE)	PLC 89/03 (Plenário)
Texto	<p>Acesso indevido</p> <p>Art. 18. Obter acesso, indevidamente, a um sistema de computador ou a uma rede integrada de computadores: Pena – detenção, de 3 (três) meses a 6 (seis) meses, ou multa. § 1º Se o acesso se faz por uso indevido de senha ou de processo de identificação magnética de terceiro; Pena – detenção de 1 (um) a 2 (dois) anos, e multa. § 2º Se, além disso, resulta prejuízo econômico para titular: Pena – detenção, de 1 (um) a 3 (três) anos, e multa. § 3º Se o acesso tem por escopo causar dando a outrem ou obter vantagem indevida; Pena – detenção, 2 (dois) a 4 (quatro) anos, e multa. § 4º Se o sistema ou rede integrada de computadores pertence a pessoa jurídica de direito</p>	<p>Acesso indevido ou não autorizado</p> <p>Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores. Pena – detenção, de seis meses a um ano em multa. § 1º Na mesma pena incorre quem, sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores. § 2º Se o crime é cometido: I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos; II – com considerável prejuízo para a vítima; III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de</p>	<p>Acesso indevido a meio eletrônico</p> <p>Art. 154-A. Acessar, indevidamente ou sem autorização, meio eletrônico ou sistema informatizado: Pena – detenção, de três meses a um ano, e multa. § 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a meio eletrônico 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 ou sociedade de economia mista.</p>	<p>Acesso indevido a dispositivo de comunicação</p> <p>Art. 154-A. Acessar indevidamente, ou sem autorização, dispositivo de comunicação ou sistema informatizado: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 1º Nas mesmas penas incorre quem fornece a terceiro meio indevido ou não autorizado de acesso a 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</p>	<p>Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado</p> <p>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</p>	<p>Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado</p> <p>Art. 285-A. Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.</p>	<p>Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado</p> <p>Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.</p>

	<p>público interno, autarquias, empresas públicas, sociedades de economia mista, fundações instituídas ou mantidas pelo Poder Público e serviços sociais autônomos, a pena é agravada em um terço.</p> <p>Art. 23. Obter acesso a sistema ou a rede integrada de computadores, com o intuito de disseminar informações fraudulentas: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.</p> <p>Art. 28. Obter acesso a sistemas de dados ou rede integrada de computadores com o objetivo de transferir, para si ou para outrem, dinheiros, fundos, créditos e aplicações de terceiros. Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.</p> <p>Art. 29. Obter acesso ilícito a sistema de computador ou a rede integrada de computadores, com o intuito de apropriar-se de informações confidenciais ligadas à segurança</p>	<p>terceiro. IV – com abuso de confiança. V – por motivo fútil; VI – com o uso indevido de senha ou processo de identificação de terceiro; ou VII – com a utilização de qualquer outro meio fraudulento. Pena – detenção, de um a dois anos e multa.</p>		<p>anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.</p>	<p>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.</p>		
--	--	---	--	---	--	--	--

	nacional. Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.						
Ação penal	Art. 18, <i>caput</i> e §§ 1-3, pública condicionada Art. 18, § 4º, pública incondicionada Art. 23, pública condicionada Art. 28, pública condicionada. Art. 29: pública incondicionada	Ação penal pública condicionada, salvo em relação ao acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos.	Art. 154-A ... § 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.	Art. 154-A. ... § 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.	Art. 154-A. ... § 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.	Ação penal pública condicionada, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias, conforme art. 285-C, também inserido pelo PL.	Ação penal pública condicionada, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias, conforme art. 285-C, também inserido pelo PL.

Tabela 2 – Crimes de obtenção/manipulação de dados: histórico

	PLC 1713/06	PLC 84/99 (original)	PLC 84/99 (CSPCCO)	PLC 89/03 (CE 2)	PLC 89/03 (CCT)	PLC 89/03 (CAE)	PLC 89/03 (Plenário)
Texto	<p>Art. 19. Apropriar-se indevidamente de valores, de que tem a posse ou detenção, através da manipulação de qualquer sistema de processamento de dados, obtendo assim vantagem econômica para si ou para outrem: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.</p> <p>Art. 20. Obter segredos empresariais ou informações de caráter confidencial em sistema ou rede integrada de computadores, com o intuito de causar danos financeiros ou obter vantagem econômica para si ou para outrem: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.</p> <p>Parágrafo único. Aumentam-se em um terço as penas se as informações são copiadas ou transferidas a outrem.</p> <p>Art.. 26. Obter, de forma não autorizada,</p>	<p>Obtenção indevida ou não autorizada de dado ou instrução de computador</p> <p>Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador. Pena: detenção, de três meses a um ano e multa.</p> <p>Parágrafo único. Se o crime é cometido: I – com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos; II – com considerável prejuízo para a vítima; III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro; IV – com abuso de confiança; V – por motivo fútil; VI – com o uso indevido de senha ou processo de</p>	<p>Manipulação indevida de informação eletrônica</p> <p>Art. 154-B. Manter ou fornecer, indevidamente ou sem autorização, dado ou informação presente em ou obtida de meio eletrônico ou sistema informatizado: Pena – detenção, de seis meses a um ano, e multa. § 1º Nas mesmas penas incorre quem transporta, indevidamente ou em autorização presente em ou obtida de meio eletrônico ou sistema informatizado através de ou para qualquer outro meio, eletrônico ou não; § 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.</p>	<p>Manipulação indevida de informação eletrônica</p> <p>Art. 154-B. Manter consigo, transportar ou fornecer indevidamente ou sem autorização, dado ou informação obtida em dispositivo de comunicação ou sistema informatizado: Pena – detenção, de 2 (dois) a 4 (quatro) anos, e multa. Parágrafo único – 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.</p>	<p>Obtenção, manutenção, transporte ou fornecimento não autorizado de informação eletrônica ou digital ou similar</p> <p>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 além do prazo definido e autorizado. § 2º Se o dado ou informação obtida desautorizadamente é fornecida a terceiros pela rede de computadores, dispositivo de</p>	<p>Obtenção, transferência ou fornecimento não autorizado de dado ou informação</p> <p>Art.. 285-B. Obter ou transferir dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização ou em desconformidade à autorização, do legítimo titular, quando exigida: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.</p>	<p>Obtenção, transferência ou fornecimento não autorizado de dado ou informação</p> <p>Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.</p>

	<p>informações confidenciais ou pessoais do indivíduo em sistema ou rede integrada de computadores:</p> <p>Pena – detenção, de 6 (seis) meses a 1(um) ano, e multa.</p> <p>Parágrafo único. Se resulta prejuízo econômico, a pena é aumentada até a metade.</p>	<p>identificação de terceiro; ou</p> <p>VII – com a utilização de qualquer outro meio fraudulento.</p> <p>Pena – detenção de um a dois anos e multa.</p>			<p>comunicação ou sistema informatizado, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.</p> <p>§ 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.</p>		
Ação penal	Ação penal pública condicionada.	Ação penal pública condicionada, salvo no caso de acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos	<p>Art. 154-B.</p> <p>...</p> <p>§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista.</p>	<p>Art. 154-B.</p> <p>...</p> <p>Parágrafo único – 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.</p>	<p>Art. 154-B.</p> <p>...</p> <p>§ 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.</p>	Ação penal pública condicionada, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias, conforme art. 285-C, também inserido pelo PL.	Ação penal pública condicionada, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias, conforme art. 285-C, também inserido pelo PL.

Tabela 3 – Crimes de divulgação/utilização indevida de informações pessoais: histórico

	PLC 1713/06	PLC 84/99 (original)	PLC 84/99 (CSPCCO)	PLC 89/03 (CE 2)	PLC 89/03 (CCT)	PLC 89/03 (CAE)	PLC 89/03 (Plenário)
Texto	<p>Art. 27. Deixar de informar ou de retificar dados pessoais contidos em rede integrada de computadores, quando requerido pelo interessado:</p> <p>Pena – detenção, de 3 a 9 meses, e multa.</p> <p>Parágrafo único. Na mesma pena incorre quem:</p> <p>I – transfere dados pessoais contidos em um sistema de computador, sem a permissão do interessado, a pessoa não autorizada com finalidade diversa daquela à qual a informação foi obtida;</p> <p>II – transfere, sem a permissão do interessado, dados pessoais para fora do país.</p>	N/A	N/A	<p>Divulgação de informações depositadas em banco de dados</p> <p>Art. 154-D. Divulgar, ou tornar disponíveis, para finalidade distinta daquela que motivou a estruturação do banco de dados, informações privadas referentes, direta ou indiretamente, a dados econômicos de pessoas físicas ou jurídicas, ou a dados de pessoas físicas 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 por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.</p> <p>Pena – detenção, de um a dois anos, e multa.</p> <p>Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale</p>	<p>Divulgação ou utilização indevida de informações contidas em banco de dados</p> <p>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.</p> <p>Pena – detenção, de um a dois anos, e multa.</p>	<p>Divulgação ou utilização indevida de informações e dados pessoais</p> <p>154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.</p> <p>Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.</p> <p>Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.</p>	<p>Divulgação ou utilização indevida de informações e dados pessoais</p> <p>Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:</p> <p>Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.</p> <p>Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.</p>

				de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de divulgação.	<p>§ 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.</p> <p>§ 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.</p>		
Ação penal	Ação penal pública condicionada.	N/A	N/A	Ação penal pública incondicionada.	Ação penal pública incondicionada.	Ação penal pública incondicionada.	Ação penal pública incondicionada.

Tabela 4 – Crimes de dano/difusão de código malicioso/estelionato : histórico [em itálico: texto extraído do CP, não alterado pelos substitutivos]

	PLC 1713/06	PLC 84/99 (original)	PLC 84/99 (CSPCCO)	PLC 89/03 (CE 2)	PLC 89/03 (CCT)	PLC 89/03 (CAE)	PLC 89/03 (Plenário)
<p>Texto [Parte especial, Título II, Capítulo IV, CP – Patrimônio; Dano]</p>			<p>[Dano. Art. 163. Destruir, inutilizar ou deteriorar coisa alheia: <i>Pena – detenção, de um a seis meses, ou multa.</i></p> <p><i>Dano qualificado</i> Parágrafo único - Se o crime é cometido: I - com violência à pessoa ou grave ameaça; II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave III - contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista; IV - por motivo egoístico ou com prejuízo considerável para a vítima: <i>Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.]</i></p>	<p>Dano por Difusão de Vírus Eletrônico</p> <p>Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo ou dificultar-lhe o funcionamento. Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.</p>	<p>Dano por difusão de código malicioso eletrônico ou digital ou similar</p> <p>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.</p> <p>Dano qualificado por difusão de código malicioso eletrônico ou digital ou similar</p> <p>§ 1º Se o crime é cometido com finalidade de destruição, inutilização, deterioração, alteração, dificuldade 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</p>	<p>Dano Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio: (NR) <i>[Pena – detenção, de um a seis meses, ou multa.]</i></p> <p>Inserção ou difusão de código malicioso</p> <p>Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado. Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.</p> <p>Inserção ou difusão de código malicioso seguido de dano</p> <p>§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de</p>	<p>Dano Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio: (NR) <i>[Pena – detenção, de um a seis meses, ou multa.]</i></p> <p>Inserção ou difusão de código malicioso</p> <p>Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.</p> <p>Inserção ou difusão de código malicioso seguido de dano</p> <p>§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento desautorizado pelo</p>

			<p>Art. 163. Dano eletrônico</p> <p>§ 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.</p> <p>Difusão de vírus eletrônico</p> <p>§3º Nas mesmas penas do § 1º [Nota: antigo parágrafo único] incorre quem cria, insere ou difunde dado ou informação em meio eletrônico ou sistema informatizado, indevidamente ou sem autorização, com a finalidade de destruí-lo, inutilizá-lo, modificá-lo ou dificultar-lhe o funcionamento.</p>		<p>multa.</p> <p>Difusão de código malicioso eletrônico ou digital ou similar seguido de dano</p> <p>§ 2º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade 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.</p>	<p>dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.</p>	<p>legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.</p>
<p>Texto [Parte Especial, Título II,</p>					<p>Difusão de código malicioso</p> <p>Art. 171-A. Difundir, por qualquer meio, programa,</p>	<p>Art. 171 ... § 2º Nas mesmas penas incorre quem:</p>	<p>Art. 171. ... § 2º Nas mesmas penas incorre quem:</p>

<p>Capítulo VI, CP – Patrimônio; Estelionato e outras fraudes]</p>					<p>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.</p>	<p>Estelionato Eletrônico VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado: § 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime do inciso VII do § 2º deste artigo, a pena é aumentada de sexta parte.</p>	<p>Estelionato Eletrônico VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado. § 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte.</p>
<p>Texto [Parte especial, Título II, Capítulo VIII, CP – Patrimônio; Disposições gerais]</p>				<p>Art. 183-A. Equiparam-se à coisa o dado ou informação em meio eletrônico, a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos.</p>	<p>Art. 183-A. Para efeitos penais, equiparam-se à coisa o dado, 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</p>	<p>Excluído.</p>	

					proporcione acesso a eles.		
<p>Texto [Parte especial, Título VIII, Capítulo II, CP – Incolumidad e Pública; Segurança dos meios de comunicação e transporte e outros serviços públicos]</p>				<p>Difusão maliciosa de Código</p> <p>Art. 266-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, a dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:</p> <p>Pena – detenção de um a dois anos.</p> <p>Parágrafo único. A pena é aumentada de sexta parte, se o agente se vale de anonimato, de nome suposto ou da utilização de identidade de terceiros para a prática de acesso.</p>			

<p>Texto [tipificação em lei esparsa]</p>		<p>Dano a dado ou programa de computador Art. 8º. Apagar, destruir, modificar ou de qualquer forma inutilizar total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada. Pena – detenção, de um a três anos e multa. Parágrafo único. Se o crime é cometido: I – contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos; II – com considerável prejuízo para a vítima; III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro; IV – com abuso de confiança; V – por motivo fútil; VI – com o uso indevido de senha ou processo de identificação de terceiro; ou VII – com a utilização de qualquer outro meio fraudulento. Pena – detenção, de dois</p>					
--	--	--	--	--	--	--	--

		<p>a quatro anos e multa.</p> <p>Alteração de senha ou mecanismo de acesso a programa de computador ou dados</p> <p>Art. 10. Apagar destruir, alterar, ou de qualquer forma inutilizar senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.</p> <p>Pena – detenção de um a dois anos e multa.</p> <p>Criação, desenvolvimento ou inserção em computador de dados ou programas de computador com fins nocivos</p> <p>Art. 13 – Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou</p>					
--	--	---	--	--	--	--	--

		<p>impossibilita, total ou parcialmente, a utilização de computador ou rede de computadores.</p> <p>Pena – reclusão, de um a quatro anos e multa.</p> <p>Parágrafo único. Se o crime é cometido:</p> <p>I – contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;</p> <p>II – com considerável prejuízo para a vítima;</p> <p>III – com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;</p> <p>IV – com abuso de confiança;</p> <p>V – por motivo fútil;</p> <p>VI – com o uso indevido de senha ou processo de identificação de terceiro;</p> <p>ou</p> <p>VII – com a utilização de qualquer outro meio fraudulento.</p> <p>Pena – reclusão, de dois a seis anos e multa.</p>					
--	--	--	--	--	--	--	--

<p>Ação penal</p>		<p>Ação penal pública condicionada, salvo se conduta é cometida contra o interesse da União, Estado, DF, Município, órgão ou entidade da administração direta ou indireta, empresa concessionária de serviços públicos, fundações instituídas ou mantidas pelo poder público, serviços sociais autônomos, instituições financeiras ou empresas que explorem ramo de atividade controlada pelo poder público.</p>	<p><i>[Art. 167 - Nos casos do art. 163, do inciso IV do seu parágrafo e do art. 164, somente se procede mediante queixa.]</i></p> <p>Restante dos tipos que não o de dano simples: ação penal pública incondicionada.</p>	<p>Ação penal pública incondicionada.</p>	<p>Ação penal pública incondicionada.</p>	<p><i>[Art. 167 - Nos casos do art. 163, do inciso IV do seu parágrafo e do art. 164, somente se procede mediante queixa.]</i></p> <p>Restante dos tipos que não o de dano simples: ação penal pública incondicionada</p>	<p><i>[Art. 167 - Nos casos do art. 163, do inciso IV do seu parágrafo e do art. 164, somente se procede mediante queixa.]</i></p> <p>Restante dos tipos que não o de dano simples: ação penal pública incondicionada</p>
--------------------------	--	--	--	---	---	---	---

Tabela 5 – Outros crimes [em itálico: texto extraído do CP, não alterado pelos substitutivos, exceto nos casos em que é feita ressalva em contrário]

	PLC 1713/06	PLC 84/99 (original)	PLC 84/99 (CSPCCO)	PLC 89/03 (CE 2)	PLC 89/03 (CCT)	PLC 89/03 (CAE)	PLC 89/03 (Plenário)
Texto [Falsificação]	<p>Art. 24. Falsificar, alterar ou apagar documentos através de sistema ou rede integrada de computadores e seus periféricos:</p> <p>Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.</p> <p>§ 1º Nas mesmas penas incorre quem, sabendo ser falso, utiliza-se de documento obtido através de sistema ou rede integrada de computadores;</p> <p>§ 2º Considera-se documento o dado constante no sistema de computador e suporte físico como disquete, disco compacto, <i>cd-rom</i>, ou qualquer outro aparelho usado para o armazenamento de informação, por meio mecânico, ótico ou eletrônico.</p>	N/A	<p><i>[Falsificação de documento particular</i></p> <p><i>Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:]</i></p> <p>Falsificação de cartão de crédito</p> <p>Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito.</p> <p>Falsificação de telefone celular ou meio de acesso a sistema eletrônico</p> <p>Art. 298-A. Criar ou copiar, indevidamente ou sem autorização, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de radiofrequência ou de telefonia celular ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado:</p>	<p><i>[Falsificação de documento particular</i></p> <p><i>Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:]</i></p> <p>Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento e processamento de informações</p> <p>Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de armazenamento ou processamento de informações. (NR)</p> <p>Falsificação de telefone celular ou meio de acesso a sistema eletrônico</p> <p>Art. 298-A. Criar ou</p>	<p><i>[Falsificação de documento particular</i></p> <p><i>Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:]</i></p> <p>Falsificação de cartão de crédito ou débito ou qualquer dispositivo eletrônico portátil de captura, processamento, armazenamento e transmissão de informações.</p> <p>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)</p> <p>Falsificação de telefone</p>	<p>Falsificação de dado eletrônico ou documento público</p> <p>Art. 297. Falsificar ou alterar, no todo ou em parte, dado eletrônico ou documento público verdadeiro: (NR) <i>[Pena - reclusão, de dois a seis anos, e multa.]</i></p> <p>Falsificação de dado eletrônico ou documento particular</p> <p>Art. 298. Falsificar ou alterar, no todo ou em parte, dado eletrônico ou documento particular verdadeiro: (NR) <i>[Pena - reclusão, de um a cinco anos, e multa.]</i></p>	<p>Falsificação de dado eletrônico ou documento público</p> <p>Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público verdadeiro: (NR) <i>[Pena - reclusão, de dois a seis anos, e multa.]</i></p> <p>Falsificação de dado eletrônico ou documento particular</p> <p>Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento particular verdadeiro: (NR) <i>[Pena - reclusão, de um a cinco anos, e multa.]</i></p>

			<p>Pena – reclusão de um a cinco anos, e multa.</p>	<p>copiar, indevidamente ou sem autorização, ou falsificar código; seqüência alfanumérica; cartão inteligente; transmissor ou receptor de radiofrequência ou de telefonia celular; ou qualquer instrumento que permita o acesso a meio eletrônico ou sistema informatizado;</p> <p>Pena – reclusão de um a cinco anos, e multa.</p>	<p>celular ou meio de acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado</p> <p>Art. 298-A. Criar ou copiar, indevidamente, ou falsificar código, seqüência alfanumérica, cartão inteligente, transmissor ou receptor de rádio frequência ou telefonia celular, ou qualquer instrumento que permita o acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado;</p> <p>Pena – reclusão, de um a cinco anos, e multa.</p>		
<p>Texto [Serviços]</p>	<p>Art. 22. Obstruir o funcionamento da rede integrada de computadores ou provocar-lhe distúrbios: Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.</p> <p>Parágrafo único. Se resulta obstrução permanente ou distúrbio grave:</p> <p>Pena – reclusão de 4 a 6 anos, e multa.</p>	N/A	<p>Atentado contra a segurança de serviço de utilidade pública</p> <p>Art. 265. Atentar contra a segurança ou o funcionamento de água, luz, força, calor ou telecomunicação, ou qualquer outro de utilidade pública: (NR) [Pena - reclusão, de um a cinco anos, e multa. Parágrafo único - Aumentar-se-á a pena de 1/3 (um terço) até a</p>	<p>Atentado contra a segurança de serviço de utilidade pública</p> <p>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) [Pena - reclusão, de um a cinco anos, e multa. Parágrafo único - Aumentar-se-á a pena de</p>	<p>Atentado contra a segurança de serviço de utilidade pública</p> <p>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) [Pena - reclusão, de um a cinco anos, e multa. Parágrafo único - Aumentar-se-á a pena de</p>	<p>Atentado contra a segurança de serviço de utilidade pública</p> <p>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) [Pena - reclusão, de um a cinco anos, e multa. Parágrafo único - Aumentar-se-á a pena de</p>	<p>Atentado contra a segurança de serviço de utilidade pública</p> <p>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) [Pena - reclusão, de um a cinco anos, e multa. Parágrafo único -</p>

			<p>metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços.]</p> <p>Interrupção ou perturbação de serviço telegráfico ou telefônico</p> <p>Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento: (NR) [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.]</p>	<p>1/3 (um terço) até a metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços.]</p> <p>Interrupção ou perturbação de serviço telegráfico ou telefônico</p> <p>Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático ou de telecomunicação, impedir ou dificultar-lhe o restabelecimento: (NR) [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.]</p>	<p>1/3 (um terço) até a metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços.]</p> <p>Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado</p> <p>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) [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.]</p>	<p>1/3 (um terço) até a metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços.]</p> <p>Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado</p> <p>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) [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.]</p>	<p>Aumentar-se-á a pena de 1/3 (um terço) até a metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços.]</p> <p>Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado</p> <p>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) [Pena – detenção, de um a três anos, e multa. Parágrafo único – Aplicam-se as penas em dobro, se o crime é cometido por ocasião</p>
--	--	--	---	--	--	--	--

							<i>de calamidade pública.]</i>
Texto [Pornografia infantil]		N/A	<i>[Inclusão no Código Penal]</i> 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 2/3 (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.	N/A	<i>[Alteração de redação – Lei 8069/90]</i> Art. 241. Apresentar, produzir, vender, fornecer, divulgar, publicar ou manter consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: (NR) <i>[Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.]</i>	<i>[Alteração de redação – Lei 8069/90]</i> Art. 241. Apresentar, produzir, vender, receptor, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: (NR) <i>[Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.]</i>	<i>[Alteração de redação – Lei 8069/90]</i> Art. 241. Apresentar, produzir, vender, receptor, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente: (NR) <i>[Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.]</i>
Ação penal	Ação penal pública condicionada.	N/A	Ação penal pública incondicionada.	Ação penal pública incondicionada.	Ação penal pública incondicionada.	Ação penal pública incondicionada.	Ação penal pública incondicionada.

Tabela 6 Definições legais

PLC 1713/96	PLC 84/99 (original)	PLC 84/99 (CSPCCO)	PLC 89/03 (CE 2)	PLC 89/03 (CCT)	PLC 89/03 (CAE)	PLC 89/03 (Plenário)
<p>Art. 2.º Considera-se, para efeitos desta lei:</p> <p>a) Rede integrada de computadores - qualquer sistema, ou conjunto de sistemas, destinado à interligação de computadores ou demais equipamentos de tratamento eletrônico, opto-eletrônico ou ótico de dados, com o fim de oferecer, em caráter público ou privado, informações e serviços a usuários que conectem seus equipamentos ao sistema.</p> <p>b) Administrador de rede integrada de computadores - entidade responsável pelo funcionamento de rede de computadores, ou de parte de uma rede de computadores, e pela continuidade dos respectivos serviços de rede.</p> <p>c) Infra-estrutura de rede - conjunto dos recursos ou serviços de telecomunicações ou de conexão de outra natureza que viabilizem o funcionamento de rede de computadores.</p> <p>d) Serviços de rede -</p>	<p>Art. 3º: Para fins desta lei, entende-se por Informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável</p>	<p>Art. 154-C. Para os efeitos penais, considera-se:</p> <p>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.</p> <p>II – sistema informatizado: a rede de computadores, a base de dados, o programa de computador ou qualquer outro sistema capaz de armazenar ou transmitir dados eletronicamente.</p>	<p>Art. 154-C. Para os efeitos penais, considera-se:</p> <p>I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados digitais, ou qualquer outro meio capaz de processar, armazenar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia digital.</p> <p>II – sistema informatizado: a rede de computadores, 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, armazenar ou transmitir dados eletronicamente.</p> <p>III – identificação de usuário: os dados de nome de acesso, senha criteriosa, nome completo, filiação,</p>	<p>Art. 154-C. Para os efeitos penais considera-se:</p> <p>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;</p> <p>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</p>	<p>Art. 14. Para os efeitos penais considera-se, dentre outros:</p> <p>I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;</p> <p>II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;</p> <p>III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;</p> <p>IV – código malicioso: o conjunto de instruções e</p>	<p>Art. 16. Para os efeitos penais considera-se, dentre outros:</p> <p>I – dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia;</p> <p>II – sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;</p> <p>III – rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações;</p> <p>IV – código malicioso: o conjunto de instruções e</p>

<p>serviços essenciais ao funcionamento de rede integrada de computadores, providos pelo administrador de rede, inclusive serviços de controle de acesso, segurança das informações, controle do tráfego e catalogação de usuários e provedores de serviços de valor adicionado.</p> <p>e) Serviços de valor adicionado - serviços oferecidos aos usuários da rede integrada de computadores que criam novas utilidades específicas, ou novas atividades, relacionadas com o uso da rede.</p> <p>f) Serviço de informação - serviço de valor adicionado caracterizado pela disseminação de informações, limitada ou não, através de rede integrada de computadores.</p> <p>g) Serviço de acesso a bases de dados - serviço de valor adicionado caracterizado pela coleta, armazenamento de disponibilidade para consulta de informações em bases de dados.</p> <p>h) Transferência eletrônica de fundos (TEF) - serviço de valor adicionado caracterizado pelo intercâmbio de ordens de crédito ou débito entre</p>			<p>endereço completo, data de nascimento, numero da carteira de identidade ou equivalente legal, que sejam requeridos no momento do cadastramento de um novo usuário de dispositivo de comunicação ou sistema informatizado.</p> <p>IV – autenticação de usuário: procedimentos de validação e conferência da identificação do usuário, quando este tem acesso ao dispositivo de comunicação ou sistema informatizado, realizados por quem os torna disponíveis ao usuário.</p>	<p>digitalmente ou de forma equivalente;</p> <p>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;</p> <p>IV - 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;</p> <p>V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob uma forma suscetível de processamento</p>	<p>tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;</p> <p>V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;</p> <p>VI – 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.</p>	<p>tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;</p> <p>V – dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado;</p> <p>VI – 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.</p>
---	--	--	---	---	---	---

<p>usuários de uma rede integrada de computadores, ou por operações cuja finalidade e efeito sejam a transferência de fundos de um patrimônio a outro sem movimentação efetiva de moeda, através de instruções eletrônicas.</p> <p>i) Base de dados - coleção de informações, armazenada em meio eletrônico, opto-eletrônico ou ótico, que permita a busca das mesmas por procedimentos manuais ou automatizadas de qualquer natureza.</p> <p>j) Provedor de serviços - entidade responsável pela oferta de serviços de valor adicionado.</p> <p>l) Provedor de informações - entidade responsável pela oferta de serviços de informação ou de acesso a bases de dados</p> <p>m) Usuário de rede - pessoa física ou jurídica que utiliza os serviços oferecidos pela rede integrada de computadores ou pelos provedores de serviços ou de informações através dessa rede, ou que possa, legitimamente, receber ou ter acesso a informações transportadas pela rede de computadores.</p> <p>n) Controle de acesso à rede - conjunto de procedimentos</p>				<p>numa rede de computadores ou dispositivo de comunicação ou sistema informatizado, incluindo um programa, apto a fazer um sistema informatizado executar uma função;</p> <p>VI – 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.</p>		
--	--	--	--	--	--	--

de segurança, estabelecidos pelo administrador da rede, a serem executados pelo usuário para ter acesso aos serviços da rede.

Art. 11. São consideradas pessoais as informações que permitam, sob qualquer forma, direta ou indiretamente, a identificação de pessoas físicas às quais elas se refiram ou se apliquem.

Art. 24. ...

§ 2º Considera-se documento o dado constante no sistema de computador e suporte físico como disquete, disco compacto, cd-rom ou qualquer outro aparelho usado para o armazenamento de informação, por meio mecânico, ótico ou eletrônico.

--	--	--	--	--	--	--

Tabela 7 Informações, privacidade, provedores de acesso

	PLC 1713/06	PLC 84/99 (original)	PLC 84/99 (CSPCCO)	PLC 89/03 (CE 2)	PLC 89/03 (CCT)	PLC 89/03 (CAE)	PLC 89/03 (Plenário)
Texto	<p>Capítulo I</p> <p>I – Dos princípios que regulam a prestação de serviço por redes de computadores</p> <p>Art. 1.º O acesso, o tratamento e a disseminação de informações através das redes integradas de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos, da privacidade das informações pessoais e da garantia de acesso às informações disseminadas pelos serviços da rede.</p>	<p>Capítulo I</p> <p>Dos princípios que regulam a prestação de serviço por redes de computadores</p> <p>Art. 1.º O acesso, o processamento e a disseminação de informações através das redes de computadores devem estar a serviço do cidadão e da sociedade, respeitados os critérios de garantia dos direitos individuais e coletivos e de privacidade e segurança de pessoas físicas e jurídicas e da garantia de acesso às informações disseminadas pelos serviços da rede.</p> <p>Art. 2.º É livre a estruturação e o funcionamento das redes de computadores e seus serviços, ressalvadas as disposições específicas</p>	N/A	<p><i>[Inclusões ao CP]</i></p> <p>Dados de conexões e comunicações realizadas</p> <p>Art. 154-E. Deixar de manter, aquele que torna disponível o acesso a rede de computadores, os dados de conexões e comunicações realizadas por seus equipamentos, aptas à identificação do usuário, endereços eletrônicos de origem e destino no transporte dos registros de dados e informações, data e horário de início e término da conexão, incluindo protocolo de internet ou mecanismo de identificação equivalente, pelo prazo de cinco anos.</p> <p>Pena – detenção, de dois a seis meses, e multa.</p> <p>Permitir acesso por usuário não identificado e não autenticado</p>	<p>Art. 23. O responsável pelo provimento de acesso a rede de computadores é obrigado a:</p> <p>I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o estrito objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e por esta gerados, cujo fornecimento será feito exclusivamente à autoridade investigatória e dependerá de prévia e expressa autorização judicial;</p> <p>II – tornar disponíveis à autoridade competente, por expressa autorização judicial, os dados e informações mencionados</p>	<p>Art. 19. O responsável pelo provimento de acesso a rede de computadores é obrigado a:</p> <p>I – manter em ambiente controlado e de segurança, pelo prazo de três anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e por esta gerados, e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;</p> <p>II – preservar imediatamente, após requisição judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações</p>	<p>Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:</p> <p>I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;</p> <p>II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de</p>

<p>...</p> <p>Art. 3.º É livre a estruturação e o funcionamento de redes integradas de computadores e seus serviços, nos termos desta Lei, ressalvadas as disposições específicas aplicáveis à sua infra-estrutura.</p> <p>II – Do controle de acesso às redes de computadores</p> <p>Art. 4.º Toda rede de computadores cujo acesso é oferecido ao público, ou a uma comunidade restrita, gratuitamente ou mediante remuneração de qualquer natureza, deverá ter um administrador de rede legalmente constituído.</p> <p>Art. 5.º O administrador de rede é responsável pelos serviços de</p>	<p>reguladas em lei.</p> <p>Capítulo II Do uso de informações disponíveis em computadores ou redes de computadores</p> <p>Art. 3.º Para fins desta lei, entende-se por informações privadas aquelas relativas a pessoa física ou jurídica identificada ou identificável. Parágrafo único. É identificável a pessoa cuja individualização não envolva custos ou prazos desproporcionados.</p> <p>Art. 4.º Ninguém será obrigado a fornecer informações sobre sua pessoa ou de terceiros, salvo nos casos previstos em lei.</p> <p>Art. 5.º A coleta, o processamento e a distribuição, com finalidades comerciais, de informações privadas ficam sujeitas à prévia aquiescência da pessoa a que se referem, que poderá ser tornada sem efeito a qualquer</p>		<p>Art. 154-F. Permitir, aquele que torna disponível o acesso a rede de computadores, a usuário, sem a devida identificação e autenticação, qualquer tipo de acesso ou uso pela rede de computadores. Pena – detenção, de um a dois anos, e multa. Parágrafo único. Na mesma pena incorre, o responsável por provedor de acesso a rede de computadores, que deixa de exigir, como condição de acesso a rede, a necessária, identificação e regular cadastramento do usuário.</p> <p>...</p> <p><i>[No corpo da lei:]</i></p> <p>Art. 13. Todo aquele que desejar acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele que torne disponível este acesso. Parágrafo único. Os atuais usuários terão prazo de cento e vinte dias após a entrada em vigor desta Lei para providenciarem ou</p>	<p>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 que cuida o inciso I deste artigo; IV – preservar imediatamente, após a solicitação expressa da autoridade judicial, no curso de investigação, os dados de que cuida o inciso I deste artigo e outras informações solicitadas por aquela 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 da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade; VI – informar ao seu usuário que o uso da rede sob sua responsabilidade</p>	<p>requisitadas por aquela investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade; III – informar, de maneira sigilosa, à autoridade competente, denúncia da qual tenha tomado conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade. § 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento. § 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R\$ 2.000,00 (dois mil reais) a R\$ 100.000,00 (cem mil</p>	<p>investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade; III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade. § 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento. § 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R\$ 2.000,00</p>
--	--	--	--	--	--	--

	<p>rede e pela segurança do controle de acesso, nos termos contratuais estabelecidos com o usuário, respeitadas as disposições da Lei n.º 8.078, de 11 de setembro de 1990, que “dispõe sobre a proteção do consumidor e dá outras providências”.</p> <p>Art. 6.º O usuário deverá empenhar-se em preservar a segurança e o segredo de suas senhas, cartões, chaves ou outras formas de acesso à rede de computadores.</p> <p>Art. 7.º O provedor de serviços de valor adicionado poderão estabelecer procedimentos adicionais de controle de acesso a seus serviços, bases de dados ou informações.</p> <p>III – Da segurança</p>	<p>momento, ressalvando-se o pagamento de indenizações a terceiros, quando couberem.</p> <p>§ 1º A toda pessoa cadastrada dar-se-á conhecimento das informações privadas armazenadas e das respectivas fontes.</p> <p>§ 2º Fica assegurado o direito à retificação de qualquer informação privada incorreta.</p> <p>§ 3º Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação privada será mantida à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.</p> <p>§ 4º Qualquer pessoa, física ou jurídica, tem o direito de interpelar o proprietário de rede de computadores ou provedor de serviço para saber se mantém informações a seu respeito, e o respectivo teor.</p> <p>Art. 6.º Os serviços de informações ou de acesso a bancos de dados não distribuirão informações privadas referentes, direta ou indiretamente, a</p>		<p>revisarem sua identificação e cadastro junto a quem, de sua preferência, torne disponível o acesso aqui definido.</p> <p>Art. 14. Todo aquele que torna disponível o acesso a uma rede de computadores somente admitirá como usuário pessoa ou dispositivo de comunicação ou sistema informatizado que for autenticado conforme validação positiva dos dados cadastrais previamente fornecidos pelo contratante de serviços. A contratação dar-se-á exclusivamente por meio formal, vedado o ajuste meramente consensual.</p> <p>§1º O cadastro mantido por aquele que torna disponível o acesso a uma rede de computadores conterà obrigatoriamente as seguintes informações prestadas por meio presencial e com apresentação de documentação original: nome de acesso; senha de acesso ou mecanismo similar; nome completo; endereço completo com</p>	<p>obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras;</p> <p>VII – alertar aos seus usuários, em campanhas periódicas, quanto ao uso criminoso de rede de computadores, dispositivo de comunicação e sistema informatizado;</p> <p>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.</p> <p>§ 1º Os dados de que cuida o inciso I deste artigo, 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.</p> <p>§ 2º Os dados e procedimentos de que cuida o inciso I deste artigo deverão estar aptos a atender ao disposto nos</p>	<p>reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.</p> <p>§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.</p> <p>Excluído o art. 24 do substitutivo da CCT..</p>	<p>(dois mil reais) a R\$ 100.000,00 (cem mil reais) a cada requisição, aplicada em dobro em caso de reincidência, que será imposta pela autoridade judicial desatendida, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.</p> <p>§ 3º Os recursos financeiros resultantes do recolhimento das multas estabelecidas neste artigo serão destinados ao Fundo Nacional de Segurança Pública, de que trata a Lei nº 10.201, de 14 de fevereiro de 2001.</p>
--	---	--	--	---	---	--	--

<p>dos serviços e das informações nas redes de computadores</p> <p>Art. 8º O administrador de rede e o provedor de cada serviço são solidariamente responsáveis, nos termos de suas atribuições específicas, pela segurança, integridade e sigilo das informações armazenadas em bases de dados ou disponíveis à consulta e manuseio por usuários da rede.</p> <p>Art. 9º O provedor de informações está sujeito às determinações estabelecidas na legislação vigente para a atividade de agência de notícias.</p> <p>Art. 10. As disposições relativas aos serviços de transferência eletrônica de fundos serão regulamentadas por disposição</p>	<p>origem racial, opinião política, filosófica, religiosa ou de orientação sexual, e de filiação a qualquer entidade, pública ou privada, salvo autorização expressa do interessado.</p> <p>Art. 7.º O acesso de terceiros, não autorizados pelos respectivos interessados, a informações privadas mantidas em redes de computadores dependerá de prévia autorização judicial.</p>		<p>logradouro, número, complemento, código de endereçamento postal, cidade e estado da federação; número de registro junto aos serviços ou institutos de identificação das Secretarias de Segurança Pública Estaduais ou conselhos de registro profissional; número de inscrição no Cadastro de Pessoas Físicas (CPF), mantido pelo Ministério da Fazenda ou o Número de Identificação do Trabalhador (NIT), mantido pelo Ministério da Previdência Social.</p> <p>§ 2º O cadastro somente poderá ser fornecido a terceiros mediante expressa autorização da autoridade competente ou em casos que a Lei venha a determinar.</p> <p>§ 3º A senha e o cadastro de identificação, a critério daquele que torna disponível o acesso, poderão ser substituídos por certificado digital emitido dentro das normas da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), conforme determina a MP 2.200-2 de 24 de agosto de 2001.</p>	<p>incisos II, III e IV no prazo de cento e oitenta dias, a partir da promulgação desta Lei.</p> <p>§ 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.</p> <p>§ 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.</p> <p>Art. 24. Não constitui violação do dever de</p>		
--	---	--	--	---	--	--

	<p>específica, atendidos os direitos e obrigações estabelecidos nesta Lei.</p> <p>IV – Do uso de informações disponíveis em redes de computadores ou bases de dados</p> <p>Art. 11. São consideradas pessoais as informações que permitam, sob qualquer forma, direta ou indiretamente, a identificação de pessoas físicas às quais elas se refiram ou se apliquem.</p> <p>Art. 12. Ninguém será obrigado a fornecer informações e dados sobre sua pessoa ou a de terceiros, salvo nos casos previstos em lei.</p> <p>Art. 13. A coleta, o processamento e a distribuição, com</p>			<p>§ 4º O cadastro de identificação, a critério daquele que torna disponível o acesso, poderá ser obtido mediante instrumento público de convênio de cooperação ou colaboração com aqueles que já o tenham constituído na forma deste artigo.</p> <p>§ 5º Para assegurar a identidade e a privacidade do usuário a senha de acesso poderá ser armazenada criptografada por algoritmo não reversível.</p>	<p>sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de conexões realizadas, quando constatada qualquer conduta criminosa.</p>		
--	--	--	--	--	--	--	--

<p>finalidades comerciais, de informações pessoais ficam sujeitas à prévia aquiescência da pessoa a que se referem.</p> <p>§ 1º À toda pessoa cadastrada dar-se-á conhecimento das informações pessoais armazenadas e das respectivas fontes.</p> <p>§ 2º É assegurado ao indivíduo o direito de retificar qualquer informação pessoal que julgar incorreta.</p> <p>§ 3º Salvo por disposição legal ou determinação judicial em contrário, nenhuma informação pessoal será conservada à revelia da pessoa a que se refere ou além do tempo previsto para a sua validade.</p> <p>§ 4º Qualquer pessoa, identificando-se, tem o direito de interpelar o prestador de serviço de informação ou de acesso a bases de</p>						
--	--	--	--	--	--	--

<p>dados para saber se estes dispõem de informações pessoais a seu respeito.</p> <p>Art. 14. É proibida a coleta de dados por meios fraudulentos, desleais ou ilícitos.</p> <p>Art. 15. Os serviços de informação ou de acesso a base de dados não distribuirão informações pessoais que revelem, direta ou indiretamente, as origens raciais, as opiniões políticas, filosóficas, religiosas ou sexuais e a filiação a qualquer entidade, salvo autorização expressa do interessado.</p> <p>Art. 16. Nenhuma decisão administrativa ou judicial poderá basear-se, para a definição do perfil do acusado ou da parte, apenas em dados obtidos mediante o</p>							
---	--	--	--	--	--	--	--

	<p>cruzamento de informações automatizadas.</p> <p>Art. 17. Somente por ordem judicial e observado [sic] os procedimentos e a legislação cabíveis, poderá haver cruzamento de informações automatizadas com vistas à obtenção de dados sigilosos.</p>						
--	--	--	--	--	--	--	--