

SUBSTITUTIVO

(ao PLS 76/2000, PLS 137/2000 e PLC 89/2003)

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 9.296, de 24 de julho de 1996, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

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 9.296, de 24 de julho de 1996, Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei nº 10.446, de 8 de maio de 2002, e a Lei nº 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências.

Art. 2º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

“Dano por difusão de vírus eletrônico ou digital ou similar

Art. 163-A. Criar, inserir ou difundir vírus em dispositivo de comunicação, rede de computadores, ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo, deteriorá-lo, alterá-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 nome suposto ou da utilização de identidade de terceiros para a prática do crime.”

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

“Capítulo VII-A

DA VIOLAÇÃO DE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO

Acesso indevido a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 154-A. Acessar indevidamente, rede de computadores, dispositivo de comunicação ou sistema informatizado:

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

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

§ 2º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

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

§ 4º Nas mesmas penas incorre, o responsável pelo provedor de acesso à rede de computadores, dispositivo de comunicação ou sistema informatizado, que permite o acesso a usuário sem a devida identificação e autenticação ou que deixa de exigir, como condição de acesso, a necessária, identificação e regular cadastramento do usuário.

§ 5º No crime previsto no caput ou na hipótese do § 4º deste artigo, se o crime é culposo:

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

Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar

Art. 154-B. Obter indevidamente dado ou informação em rede de computadores, dispositivo de comunicação ou sistema informatizado:

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 indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado.

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

§ 3º Somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e suas subsidiárias.

Dispositivo de comunicação, sistema informatizado, rede de computadores, identificação de usuário, autenticação de usuário, provedor de acesso e provedor de serviço, dados de conexões realizadas

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

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

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

III – rede de computadores: os meios 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, este nível conhecido como internet, ou quanto ao proprietário, privado ou público;

IV – identificação de usuário: os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo e outros dados que sejam requeridos no momento do cadastramento de um novo usuário de rede de computadores, dispositivo de comunicação ou sistema informatizado;

V – autenticação de usuário: procedimentos de verificação e conferência da identificação do usuário, quando este tem acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado, realizado por quem torna disponível o acesso pelo usuário;

VI – provedor: o prestador de serviços de acesso à rede de computadores e o prestador de serviços relacionados a esse acesso;

VII – dados de conexões realizadas: aqueles dados aptos à identificação do usuário, os endereços eletrônicos de origem das conexões, a data, o horário de início e término e a referência GMT dos horários, relativos à cada conexão realizada pelos equipamentos de uma rede de computadores.

Violação ou divulgação indevida de informações depositadas em banco de dados

Art. 154-D. Violar, 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 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 por decisão da autoridade competente, ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

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

§ 3º Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de identificação de usuário, quando constatada qualquer conduta criminosa.

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

“**Art. 155.**

§ 4º

V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar.

.....”

Art. 5º O Código Penal passa a vigorar acrescido do seguinte art. 183-A:

“**Art. 183-A.** Para os efeitos penais equiparam-se à coisa o dado ou informação em meio eletrônico ou digital ou similar, o bit ou a menor quantidade de informação que pode ser entendida como tal, a base de dados armazenada, dispositivo de comunicação, a rede de computadores, o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos anteriormente citados.”

Art. 6º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

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

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

..... (NR)”

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

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

..... (NR)”

Art. 7º O Capítulo II do Título VIII do Código Penal passa a vigorar acrescido do seguinte artigo:

“Difusão maliciosa de código

Art. 266-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização, à rede de computadores, dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a três anos.

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

§ 2º É isento de pena o agente técnico ou o profissional habilitado que, a título de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação manipula código malicioso detectado, em proveito próprio ou de seu preponente e sem risco para terceiros.”

Art. 8º O art. 298 do Código Penal passa a vigorar acrescido do seguinte parágrafo único:

“Art. 298.

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

Parágrafo único. Equipara-se a documento particular o cartão de crédito ou débito ou qualquer outro dispositivo portátil capaz de capturar, processar, armazenar ou transmitir dados, utilizando-se de tecnologias

magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar.(NR)”

Art. 9º O Código Penal passa a vigorar acrescido do seguinte art.

298-A:

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

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

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

Art. 10. O Código Penal passa a vigorar acrescido do seguinte art.

141-A:

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

Art. 11. O Código Penal passa a vigorar acrescido do seguinte art.

356-A:

“Art. 356-A. Deixar de manter os dados de identificação de usuário e os dados de conexões realizadas por seus equipamentos, de valor probatório, aptos à identificação do usuário quando da ocorrência de crime, pelo prazo de três anos contados a partir da data de conexão, aquele que é o responsável pelo provedor de acesso à rede de computadores.”

Art. 12. O § 6º do art. 240 do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), passa a vigorar acrescido do seguinte inciso V:

“Art. 240.

.....

Furto qualificado

§ 6º

V - mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado ou similar.

.....”

Art. 13. O 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) fica acrescido do art. 262-A, assim redigido:

“Dano por difusão de vírus eletrônico ou digital ou similar

Art. 262-A. Criar, inserir ou difundir vírus em rede de computadores, dispositivo de comunicação ou sistema informatizado, com a finalidade de destruí-lo, inutilizá-lo, deteriorá-lo, alterá-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 nome suposto ou da utilização de identidade de terceiros para a prática de acesso.”

Art. 14. O Título VII da Parte Especial do Livro I do Código Penal Militar, Decreto-Lei, nº 1.001, de 21 de outubro de 1969, fica acrescido do Capítulo VII-A, assim redigido:

“Capítulo VII-A**DA VIOLAÇÃO DE REDE DE COMPUTADORES,
DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA
INFORMATIZADO****Acesso indevido a rede de computadores, dispositivo de
comunicação ou sistema informatizado**

Art. 339-A. Acessar indevidamente rede de computadores, dispositivo de comunicação ou sistema informatizado:

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

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

§ 2º 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 do crime.

§ 3º Nas mesmas penas incorre, o responsável pelo provedor de acesso à rede de computadores, dispositivo de comunicação ou sistema informatizado, que permite o acesso a usuário sem a devida identificação e autenticação ou que deixa de exigir, como condição de acesso, a necessária, identificação e regular cadastramento do usuário.

§ 4º No crime previsto no caput ou na hipótese do § 3º deste artigo, se o crime é culposo:

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

Obtenção, manutenção, transporte ou fornecimento indevido de informação eletrônica ou digital ou similar

Art. 339-B. Obter indevidamente dado ou informação em rede de computadores, dispositivo de comunicação ou sistema informatizado.

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 indevidamente em rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 2º Se o dado ou informação obtida indevidamente é fornecida pela rede de computadores, ou em qualquer outro meio de divulgação em massa, a pena é aumentada de um terço.

Dispositivo de comunicação, sistema informatizado, rede de computadores, identificação de usuário, autenticação de usuário e provedor

Art. 339-C. Para os efeitos penais considera-se:

I – dispositivo de comunicação: o computador, o computador de mão, o telefone celular, o processador de dados, os meios de armazenamento de dados eletrônicos ou digitais ou similares, os meios de captura de dados, ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias

magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;

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

III – rede de computadores: os meios 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, este nível conhecido como internet, ou quanto ao proprietário, privado ou público;

IV – identificação de usuário: os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento e endereço completo e outros dados que sejam requeridos no momento do cadastramento de um novo usuário de rede de computadores, dispositivo de comunicação ou sistema informatizado;

V – autenticação de usuário: procedimentos de verificação e conferência da identificação do usuário, quando este tem acesso a rede de computadores, dispositivo de comunicação ou sistema informatizado, realizado por quem torna disponível o acesso pelo usuário;

VI – provedor: o prestador de serviços de acesso à rede de computadores e o prestador de serviços relacionados a esse acesso;

VII – dados de conexões realizadas: aqueles dados aptos à identificação do usuário, os endereços eletrônicos de origem das conexões, a data, o horário de início e término e a referência GMT dos horários, relativos à cada conexão realizada pelos equipamentos de uma rede de computadores.

Violação, divulgação de informações depositadas em banco de dados

Art. 339-D. Violar, 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 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 por decisão da autoridade competente, ou

mediante expressa anuência da pessoa a que se referem, ou de seu representante legal.

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

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

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

§ 3º Não constitui violação do dever de sigilo a comunicação, às autoridades competentes, de prática de ilícitos penais, abrangendo o fornecimento de informações de acesso, hospedagem e dados de identificação de usuário, quando constatada qualquer prática criminosa.”

Art. 15. O Título V da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do Capítulo VIII-A, assim redigido:

“Capítulo VIII-A

DISPOSIÇÕES GERAIS

Art. 267-A. Para os efeitos penais equiparam-se à coisa o dado ou informação em meio eletrônico ou digital ou similar, o bit ou a menor quantidade de informação que pode ser entendida como tal, a base de dados armazenada, a rede de computadores, o dispositivo de comunicação e o sistema informatizado, a senha ou similar ou qualquer meio que proporcione acesso aos mesmos.”

Art. 16. O Capítulo I do Título VI da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 281-A, assim redigido:

“Difusão maliciosa de código

Art. 281-A. Difundir, por qualquer meio, programa, conjunto de instruções ou sistema informatizado com o propósito de levar a erro ou, por qualquer forma indevida, induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que

facilitem ou permitam o acesso indevido ou sem autorização, a rede de computadores, dispositivo de comunicação ou a sistema informatizado, ou a obtenção de qualquer vantagem ilícita:

Pena – reclusão de um a três anos.

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

§ 2º É isento de pena o agente técnico ou o profissional habilitado que, em proveito próprio ou de seu preponente e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, atua a título de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação e manipula, sem desvio de finalidade ou excesso, código malicioso detectado.”

Art. 17. O Capítulo VII do Título VII da Parte Especial do Livro I do Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), fica acrescido do art. 352-A, assim redigido:

“**Art. 352-A.** Deixar de manter os dados de identificação de usuário e os dados de conexões realizadas por seus equipamentos, de valor probatório, aptos à identificação do usuário quando da ocorrência de crime, pelo prazo de três anos contados a partir da data de conexão, aquele que é o responsável pelo provedor de acesso à rede de computadores.”

Art. 18. O art. 2º da Lei nº 9.296, de 24 de julho de 1996, passa a vigorar acrescido do seguinte § 2º, renumerando-se o parágrafo único para § 1º:

“**Art. 2º**

.....

§ 2º O disposto no inciso III do *caput* não se aplica quando se tratar de interceptação do fluxo de comunicações em rede de computadores, dispositivo de comunicação ou sistema informatizado.” (NR)

Art. 19. O art. 313 do Decreto-Lei nº 3.689, de 3 de outubro de 1941, Código do Processo Penal (CPP), passa a vigorar acrescido do seguinte inciso IV:

“**Art. 313.**.....

IV – punidos com detenção, se tiverem sido praticados contra rede de computadores, dispositivo de comunicação ou sistema informatizado, ou se tiverem sido praticados mediante uso de rede de computadores, dispositivo de comunicação ou sistema informatizado.(NR)”

Art. 20. Todo aquele que acessar uma rede de computadores, local, regional, nacional ou mundial, deverá identificar-se e cadastrar-se naquele provedor que torna 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 revisarem sua identificação e cadastro junto ao provedor que torna disponível o acesso.

Art. 21. Todo provedor de acesso a uma rede de computadores sob sua responsabilidade somente admitirá como usuário pessoa natural, dispositivo de comunicação ou sistema informatizado que for autenticado por meio hábil e legal à verificação positiva da identificação de usuário, ficando facultado o uso de tecnologia que garanta a autenticidade e integridade dos dados e informações digitais ou o uso de outras entidades de dados de identificação de usuário já existentes que tenham sido constituidas de maneira presencial, de forma a prover a autenticidade das conexões, a integridade dos dados e informações e a segurança das comunicações e transações na rede de computadores, dispositivo de comunicação e sistema informatizado.

Parágrafo único. A identificação do usuário de rede de computadores poderá ser definida nos termos de regulamento, sendo obrigatórios para a pessoa natural os dados de identificador de acesso, senha ou similar, nome completo, data de nascimento, um número de documento hábil e legal de identidade e endereço completo, sendo obrigatória para o provedor de acesso a uma rede de computadores, para o dispositivo de comunicação e para o sistema informatizado a indicação de uma pessoa natural responsável.

Art. 22. Todo provedor de acesso a uma rede de computadores é obrigado a:

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

II – tornar disponíveis à autoridade competente os dados e informações elencados no inciso I no curso de auditoria técnica a que forem submetidos;

III – fornecer, quando solicitado pela autoridade competente no curso de investigação, os dados de conexões realizadas e os dados de identificação de usuário;

IV – informar, de maneira sigilosa, à autoridade competente à qual está jurisdicionado, fato do qual tenha tomado conhecimento e que contenha indícios de conduta delituosa na rede de computadores sob sua responsabilidade;

V – informar ao usuário, quando da requisição da sua identificação e autenticação, que aquela conexão obedece às leis brasileiras e que toda comunicação ali realizada será de exclusiva responsabilidade do usuário, perante as leis brasileiras, para prover os elementos essenciais para fazer prova da autenticidade da autoria das conexões na rede de computadores;

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

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

Parágrafo único. Os dados de conexões realizadas em rede de computadores, as condições de alta segurança de sua guarda, a auditoria à qual serão submetidas, a autoridade competente responsável pela auditoria e o texto a ser informado aos usuários de rede de computadores, serão definidos nos termos de regulamento em prazo não superior a noventa dias a partir da data de

publicação desta lei, sendo obrigatórios aqueles dados de conexão realizadas definidos neste artigo.

Art. 23. A autoridade competente, nos termos de regulamento, estruturará órgãos, setores e equipes de agentes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 24. O art. 1º da Lei nº 10.446, de 8 de maio de 2002 passa a vigorar com a seguinte redação:

“**Art. 1º**

 V – os delitos praticados contra ou mediante rede de computadores, dispositivo de comunicação ou sistema informatizado. (NR)”

Art. 25. O art. 9º da Lei nº 8.078, de 11 de setembro de 1990 passa a vigorar com a seguinte redação:

“**Art. 9º**

Parágrafo único. – o mesmo se aplica à segurança digital do consumidor, mediante a informação da necessidade do uso de senhas ou similar para a proteção do uso do produto ou serviço e para a proteção dos dados trafegados, quando se tratar de dispositivo de comunicação, sistema informatizado ou provimento de acesso a rede de computadores ou provimento de serviço mediante o uso dela.(NR)”

Art. 26. Esta Lei entra em vigor sessenta dias após a data de sua publicação.

Sala da Comissão,

, Presidente

, Relator