

CRIMES CIBERNÉTICOS

PL 89/03

00 de 000000 de 2008

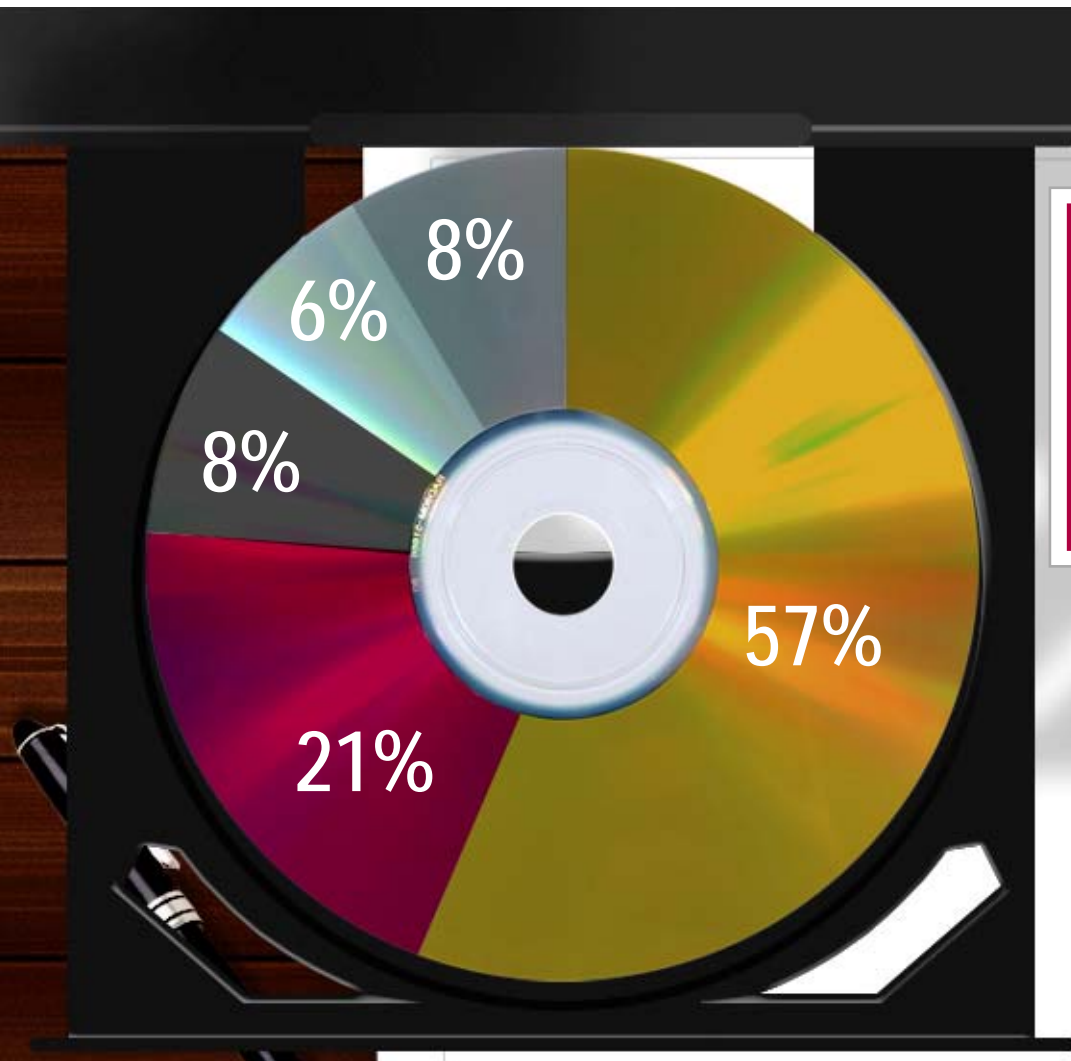


Missão da ABES

**SETOR
BRASILEIRO
DE SOFTWARE**



Perfil ABES



800 Associados

4,9 bilhões de dólares

73.000 postos de trabalho

Distribuição por Faturamento – US\$

- até 500 mil
- 500 mil a 1 milhão
- 1 milhão a 2 milhões
- 2 milhão a 5 milhões
- Acima de 5 milhões

ALTERAÇÕES LEGISLATIVAS PROPOSTAS

- ⇒ Decreto-Lei nº 2.848, de 07/12/1940 (**código penal**).
- ⇒ Decreto-Lei nº 1.001, de 21/10/1969 (**código penal militar**).
- ⇒ Lei nº 7.716, de 05/01/1989 (crimes de **preconceito** de raça ou de cor).
- ⇒ Lei nº 8.069, de 13/07/1990 (**ECA - Estatuto da Criança e do Adolescente**).
- ⇒ Lei nº 10.446, de 08/05/2002 (**infrações penais de repercussão interestadual ou internacional**).



TIPIFICAR (Como Criminosas) **CONDUTAS REALIZADAS:**

- ⇒ mediante uso de sistema eletrônico, digital ou similares, ou
- ⇒ mediante uso de rede de computadores, ou
- ⇒ praticadas contra dispositivos de comunicação, ou
- ⇒ praticadas contra sistemas informatizados e similares

POR QUE TIPIFICAR CONDUTAS?

- ⇒ Ausência de um Penalista, puro (Marrey, Malheiros, JC Dias)
- ⇒ Com base no “Princípio de legalidade” que abarca o conceito de “Anterioridade da lei”, o ato que se pretende punir, deverá ter sido definido em lei, como crime, antes de ter sido praticado.
- ⇒ Não será considerado *crime*, a prática de um ato que não tenha sido previamente definido como ***tipo penal***, por lei (ou seja, que não tenha sido ***tipificado***).
- ⇒ Comentários ao evento RECIFE



POR QUE TIPIFICAR CONDUTAS?

1) Do art. 1º do Código Penal que diz:

“Não há crime sem lei anterior que o defina. Não há pena sem prévia COMINAÇÃO LEGAL.”

2) Do art. 1º do Código Penal Militar que diz

Art. 1º Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal

3) Do Art. 5º, inciso XXXIX, da Constituição Federal que estipula:

Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

4) Do Art. 5º, inciso XL da Constituição Federal que fixa:

A lei penal não retroagirá, salvo para beneficiar o réu.



DEFINIÇÕES DOS TERMOS TÉCNICOS

A própria conceituação suscita questionamentos:

Art. 16. Para os efeitos penais 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 qualquer outra tecnologia; (pager, Iphone, computador, celular, etc)

II. SISTEMA INFORMATIZADO: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados, eletrônica ou digitalmente, ou de forma equivalente; idem, etc.

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: o conjunto de instruções e tabelas de informações ou qualquer outro sistema DESENVOLVIDO PARA:

EXECUTAR AÇÕES DANOSAS ou OBTER DADOS OU INFORMAÇÕES DE FORMA INDEVIDA;

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;

Passará a ser considerado “**CRIME CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS**”

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

Reclusão, de 1 (um) a 3 (três) anos, e multa, agravada em 1/6 se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

Acessar, **MEDIANTE VIOLAÇÃO DE SEGURANÇA**, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso



285-B: Obtenção, transferência ou fornecimento não autorizado de dado ou informação:

Reclusão, de 1 (um) a 3 (três) anos, e multa, agravada em 1/3 se o dado ou informação obtida desautorizadamente é fornecida a terceiros

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**



Passa a ser tipificado no artigo **154-A** do código penal.

Trata-se de uma nova modalidade de “**VIOLAÇÃO DO SEGREDO PROFISSIONAL**” (art. 154), que apenas punia o ato de “Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem”.

A pena é de detenção, de 1 (um) a 2 (dois) anos, e multa, com agravo de 1/6 se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime

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 (Ex. Mail list – Abril)



INSERÇÃO OU DIFUSÃO DE CÓDIGO MALICIOSO

Será novo criado tipo penal, inserindo o art. **163-A** no CP: A pena será de reclusão, de 1 (um) a 3 (três) anos, e multa.

Nota: Há o crime, ainda que dele não resulte “dano”: basta inserir ou difundir o código malicioso

A pena será acrescida de 1/6 se o agente usa nome falso ou da utilização de identidade de terceiros

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.

Cabe indagar:

E se for sem querer? Alguém instala trojan na minha máquina e a mensagem se duplica para milhares?



INSERÇÃO OU DIFUSÃO DE CÓDIGO MALICIOSO SEGUIDO DE DANO

Os parágrafos ao novo art. **163-A** no CP tipifica e pune com maior severidade, a inserção de código malicioso, seguido de dano:

será de reclusão, de 2(dois) a 4 (quatro) anos, e multa, se da inserção ou difusão resultar dano.

Também no caso do **§ 1º, do art. 163-A**, a pena será acrescida de 1/6 se o agente usa nome falso ou da utilização de identidade de terceiros.

Inserção ou difusão de código malicioso seguido de dano: § 1º SE DO CRIME RESULTA destruição, inutilização, deterioração, alteração, **DIFICULTAÇÃO DO FUNCIONAMENTO**, ou funcionamento desautorizado pelo 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.



MODIFICA TIPOS PENAIS JÁ EXISTENTES

O crime de dano passa a abranger “**Dano em DADO eletrônico**”. O **art. 163** do código penal passa a dizer:

Dano: Art. 163. Destruir, inutilizar ou DETERIORAR coisa alheia OU DADO ELETRÔNICO ALHEIO.

A pena no novo crime será idêntica (detenção, de um a seis meses, ou multa).

Há “dano qualificado” se há violência, ou o crime é praticado contra órgãos públicos, ou por motivo egoístico ou com “**prejuízo considerável à vítima**”, quando o a detenção será de 6 meses a 3 anos (Serpro, Dataprev, CAIXA, etc.)



ESTELIONATO ELETRÔNICO

O famoso tipo penal conhecido como “*Estelionato*”, ou simplesmente “**171**”, teve acrescida uma nova modalidade, qual seja “**ESTELIONATO ELETRÔNICO**” (nenhuma *ANALOGIA* com este Prédio...)

A nova modalidade de estelionato passa a ter idêntica penalidade (*reclusão, de um a cinco anos, e multa*).

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 a pena é aumentada de sexta parte.”



ESTELIONATO ELETRÔNICO

O tipo penal básico era: Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa. Exemplo: **vende**, permuta, dá em pagamento, em locação ou em garantia **coisa alheia** como própria; vende, permuta, dá em pagamento ou em garantia **coisa própria inalienável, gravada de ônus** ou litigiosa, ou imóvel que prometeu vender a terceiro; destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as conseqüências da lesão ou doença, com o intuito de haver indenização ou valor de **seguro**; emite **cheque, sem suficiente provisão de fundos** em poder do sacado, ou lhe frustra o pagamento.



ATENTADO CONTRA A SEGURANÇA DE SERVIÇO DE UTILIDADE PÚBLICA

Na descrição do crime ***“Atentado contra a segurança de serviço de utilidade pública”***, capitulado no art. ***“265”***, foram acrescentadas as hipóteses de atentados contra o funcionamento dos serviços de ***“informação ou telecomunicação”***

A nova modalidade de atentado terá idêntica penalidade (*reclusão, de um a cinco anos, e multa*). *Aumentar-se-á de 1/3 (um terço) até a metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços*). Ex. instalou vírus no servidor da Estação “3035” da Telefônica.

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: Pena - reclusão, de um a cinco anos, e multa (SPEED)



PERTURBAÇÃO DE SERVIÇO TELEFÔNICO

Na descrição do crime “*Interrupção ou perturbação de serviço telegráfico ou telefônico*”, capitulado no art. “**266**”, foram acrescentadas as expressões “**(SERVIÇO) INFORMÁTICO, DE DISPOSITIVO DE COMUNICAÇÃO, DE REDE DE COMPUTADORES, DE SISTEMA INFORMATIZADO OU DE TELECOMUNICAÇÃO**”

A nova modalidade delituosa terá idêntica penalidade (*detenção, de um a três anos, e multa*). Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública.

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.



FALSIFICAÇÃO DE DOCUMENTO PÚBLICO

Na descrição do crime “*Falsificação de documento público*”, capitulado no art. “**297**”, foram acrescentadas as expressões “*dado eletrônico*”. Com isso passa a ser tratado como falsificação documental, “falsificar *dado eletrônico público*” (ex. no site da receita, trocar a expressão “positiva” por “negativa” numa certidão).

A nova modalidade será igualmente punida (*reclusão, de dois a seis anos, e multa*). *Aumenta-se a pena em 1/6 se o agente é funcionário público, e comete o crime prevalecendo-se do cargo*

Falsificação de dado eletrônico ou documento público

Art. 297. FALSIFICAR, no todo ou em parte, DADO ELETRÔNICO ou documento público, ou alterar documento publico verdadeiro:

Exemplo: alterar o dado da Receita, a respeito das Certidões Negativas; ou sobre os saldos devedores ali existentes



FALSIFICAÇÃO DE DOCUMENTO PARTICULAR

Na descrição do crime “*Falsificação de documento particular*”, capitulado no art. “**298**”, foram acrescentadas as expressões “**dado eletrônico**”. Com isso passa a ser tratado como falsificação documental, “falsificar *dado eletrônico particular*” (ex. no site da Abes, o associado insere um novo programa, na lista dos programas listados numa certidão ABES).

A nova modalidade será igualmente punida (*reclusão, de um a cinco anos, e multa.*). Nesse caso, não há o agravante em 1/6.

Falsificação de dado eletrônico ou documento particular

Art. 298. *FALSIFICAR, no todo ou em parte, DADO ELETRÔNICO ou documento particular ou alterar documento particular verdadeiro.*

Exemplo: alterar o Saldo Bancário (credor ou devedor) de um correntista.



MODIFICAÇÕES NO CÓDIGO PENAL MILITAR – DL 1.001/69

Conceito de “**CRIME MILITAR**”: Art. 9º Consideram-se crimes militares, em tempo de paz:

Os crimes de que trata este Código, quando definidos de modo diverso na lei penal comum, ou nela não previstos, qualquer que seja o agente (**inclusive civil**), salvo disposição especial;

OS CRIMES previstos neste Código, embora também o sejam com igual definição na lei penal comum, **QUANDO PRATICADOS POR MILITAR** (Exemplo: comete lesão Corporal c/ civil)

- ⇒ Contra militar na mesma situação ou assemelhado;
 - ⇒ Em lugar sujeito à administração militar, contra militar da reserva, ou reformado, ou assemelhado, ou civil;
 - ⇒ Ainda que fora do lugar sujeito à administração militar contra militar da reserva, ou reformado, ou civil;
 - ⇒ durante o período de manobras ou exercício, contra militar da reserva, ou reformado, ou assemelhado, ou civil;
 - ⇒ contra o patrimônio sob a administração militar, ou a ordem administrativa militar.



“Art. 251, inciso VI - Estelionato Eletrônico

VI - DIFUNDE, por qualquer meio, CÓDIGO MALICIOSO com o intuito de facilitar ou permitir o acesso indevido a rede de computadores, dispositivo de comunicação ou a sistema informatizado, EM PREJUÍZO DA ADMINISTRAÇÃO MILITAR

Haverá aumento da pena em 1/6 Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime.

Trata-se de tipo penal novo, antes não previsto em lei.

É o mesmo novo crime previsto no inciso VII, do art. 171, do código penal (se aprovado for o atual PL), acrescido da expressão “em prejuízo da administração militar”



ARTIGO 259 = CÓDIGO PENAL MILITAR

Art. 259 - Dano Simples

Destruir, inutilizar, deteriorar ou fazer desaparecer coisa alheia ou dado eletrônico alheio, desde que este esteja sob administração militar:

A parte final em negrito e sublinhado constitui-se em acréscimo à redação atual.



ARTIGO 262 = CÓDIGO PENAL MILITAR

“Art. 262 - Dano em material ou aparelhamento de guerra

“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”

A pena continuará igual (reclusão, até seis anos).

A modificação se resume no acréscimo da expressão “ou dado eletrônico”



ARTIGO 262 – A = CÓDIGO PENAL MILITAR

Art. 262-A Inserção ou difusão de CÓDIGO MALICIOSO

Art. 262-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado, DESDE QUE O FATO ATENTE CONTRA A ADMINISTRAÇÃO MILITAR:

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

Nota: Corresponderá ao novo art. 163-A, que o PL propõe seja acrescido ao Código Penal



ARTIGO 262 – A (PARÁGRAFOS) CP Militar

Art. 262-A (parágrafos)

Para os crimes de que trata o Art. 262-A (inserção ou difusão de CÓDIGO MALICIOSO), o projeto prevê dois agravantes:

Inserção ou difusão código malicioso SEGUIDO DE DANO

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento não autorizado pelo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Nesse caso, a pena será de reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

Mediante uso de nome falso ou identidade de terceiros:

§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime

hipótese em que pena é aumentada da sexta parte



Artigo 339 – A = CÓDIGO PENAL MILITAR

Art. 339-A DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS (MILITARES)

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

Art. 339-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, **DESDE QUE O FATO ATENTE CONTRA A ADMINISTRAÇÃO MILITAR:**

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.

NOTA: corresponde ao novo 285-A, proposto ao CP, pelo PL



ARTIGO 339-B = CÓDIGO PENAL MILITAR

NOVO TIPO PENAL MILITAR – Art. 339-B:

OBTENÇÃO, TRANSFERÊNCIA OU FORNECIMENTO NÃO AUTORIZADO DE DADO OU INFORMAÇÃO

Art. 339-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, *DESDE QUE O FATO ATENTE CONTRA A ADMINISTRAÇÃO MILITAR:*

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.

NOTA: corresponde ao novo 285-B, proposto ao CP, pelo PL



ARTIGO 339-C = Código Penal Militar

DIVULGAÇÃO OU UTILIZAÇÃO INDEVIDA DE INFORMAÇÕES E DADOS PESSOAIS

Art. 339-C Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em SISTEMA INFORMATIZADO SOB ADMINISTRAÇÃO MILITAR 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. Pena – detenção, de um a dois anos, e multa.

Parágrafo único - Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática de crime, a pena é aumentada da sexta parte.”.

NOTA: corresponde ao novo 154-A, proposto ao CP, pelo PL



FALSIFICAÇÃO DE DOCUMENTO

Art. 311. Falsificar, no todo ou em parte, documento público ou particular, ou dado eletrônico ou alterar documento verdadeiro, DESDE QUE O FATO ATENTE CONTRA A ADMINISTRAÇÃO OU O SERVIÇO MILITAR:”

NOTA: corresponde ao novo 297, proposto ao CP, pelo PL



ARTIGO 356 = CÓDIGO PENAL MILITAR

Art. 356. DA TRAIÇÃO - FAVOR AO INIMIGO

II - Entregando ao inimigo ou expondo a perigo dessa consequência navio, aeronave, fôrça 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):”

NOTA: a NOVIDADE ESTÁ NA INCLUSÃO DO ELEMENTO “DADO ELETRÔNICO”, como modalidade de traição.



ARTIGO 1º, INCISO V DA LEI 10.446/2002

- ⇒ *MODIFICAÇÕES na lei sobre infrações penais de repercussão interestadual ou internacional*
- ⇒ Novo inciso V, ao art. 1º, da lei 10.446/2002, autoriza o Departamento de **Polícia** Federal do Ministério da Justiça, Polícias Militares e Cíveis dos Estados a **proceder à investigação, quando houver crime com repercussão interestadual ou internacional que exija repressão uniforme, PRATICADOS CONTRA OU MEDIANTE REDE DE COMPUTADORES, DISPOSITIVO DE COMUNICAÇÃO OU SISTEMA INFORMATIZADO.**

CRIMES de PRECONCEITO DE RAÇA OU DE COR

⇒ MODIFICAÇÕES NA LEI QUE DEFINE OS CRIMES RESULTANTES DE PRECONCEITO DE RAÇA OU DE COR

- **Altera o inciso II do § 3º do art. 20 da Lei nº 7.716, de 05/01/89, acrescentando os termos “ELETRÔNICAS, OU DA PUBLICAÇÃO POR QUALQUER MEIO”**
- **II – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.**

⇒ O artigo ao qual se incorpora o inciso alterado pune com RECLUSÃO DE UM A TRÊS ANOS e multa, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional, fixando que “o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência, “a cessação das transmissões” acima referidas.



ESTATUTO DA CRIANÇA E DO ADOLESCENTE:

⇒ (Altera o caput do art. 241 da Lei nº 8.069, de 13/07/90), acrescentando os termos “*RECEPTAR*” E “*ARMAZENAR CONSIGO*”

“ **Art. 241.** Apresentar, produzir, vender, *RECEPTAR*, 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:

⇒ A pena não foi alterada (reclusão de 2 (dois) a 6 (seis) anos, e multa).



Acrescentando os termos “RECEPTAR” E “ARMAZENAR CONSIGO”

Mantém a previsão que determina que: *“incorre na mesma pena quem:*

II - ASSEGURA OS MEIOS OU SERVIÇOS PARA O ARMAZENAMENTO das fotografias, cenas ou imagens produzidas na forma do caput deste artigo (DataCenters, Google, ML)

III - ASSEGURA, por qualquer meio, O ACESSO, NA REDE MUNDIAL de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo.

- Lans Houses; Provedores de acesso; Net, Telefônica
- INSTALAÇÕES PRÓPRIAS DAS EMPRESAS

PENALIDADES PECUNIÁRIAS AO PROVEDOR DE ACESSO

“Obrigações dos provedores de acesso”: O PL propõe MULTA PECUNIÁRIA (art. 22)

Art. 22. O RESPONSÁVEL PELO PROVIMENTO DE ACESSO a rede de computadores mundial, comercial ou do setor público é obrigado a:

Quem é o Responsável? O datacenter? O ASP? O presidente?

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 fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;

Basta mensurar o espaço exigido para armazenar tantos dados..



PENALIDADES PECUNIÁRIAS AO PROVEDOR DE ACESSO

II – PRESERVAR imediatamente, após requisição judicial, OUTRAS INFORMAÇÕES REQUISITADAS em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

Quais “outras” informações? O CPF do infrator? Sua descrição física?

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.

Denúncias recebidas de quem? Como identifico se há indícios?

Se for uma “denúncia vazia” de conteúdo?

Pirataria de Software é público ou privada?



PENALIDADES PECUNIÁRIAS AO PROVEDOR DE ACESSO

§ 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 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.

2K até 100K POR REQUISIÇÃO!

E se forem 100 mil usuários do ML?

Pode dobrar!



Atividades Institucionais

§ 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.**

Regulamentar Lei Penal (embora a pena seja de caráter pecuniário)?

§ 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.

Para depois ser contingenciados? Porque não ao MP?



REESTRUTURAÇÃO DA POLÍCIA JUDICIÁRIA

O **Art. 18** do PL contém simples comando absolutamente desnecessário e de eficácia duvidosa:

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

O que acontece para quem não obedecer

Com quais recursos financeiros esses órgãos atenderão a esse comando?



*Associação Software Livre é contra o fim da privacidade
na Internet Convergência Digital (RJ - Carreira - 20/08/2008)*

A Associação Software Livre (ASL) participou nesta terça-feira (19), do Meeting de Tecnologia, que aconteceu na Federasul, em Porto Alegre (RS), com a presença do Senador Eduardo Azeredo (PSDB-MG), onde foi abordado o Projeto de Lei sobre crimes eletrônicos. Estiveram presentes Sady Jacques, Coordenador Geral da ASL, e Mário Teza, também membro do Comitê Gestor da Internet no Brasil. O Coordenador Geral da ASL, Sady Jacques, entregou em mãos ao senador, documentos com o objetivo de esclarecer a preocupação da ASL com a liberdade no uso da internet. O processo está invertido. Estão criando uma lei que imputa penas, podendo paralisar a Internet, explica Jacques. A aprovação do Projeto de Lei iniciado na Câmara (PLC) 89/2003, representa uma ameaça a direitos fundamentais e traz regras que criminalizam o acesso legítimo a conteúdos digitais, na avaliação da entidade.



O substitutivo de autoria do Senador Eduardo Azeredo (PSDB-MG) foi votado em 9 de julho pelo Senado Federal e agora segue para a Câmara dos Deputados. A Associação Software Livre entende que o Projeto de Lei pode tornar puníveis homens e mulheres de bem a partir de uma distorção gravíssima da lei, que deve servir à sociedade como um todo e não à sistemas em particular, seja ele social, econômico ou financeiro, além de dever presumir inocência e não culpa. Para a Associação Software Livre, o tema deveria ser mais discutido entre a sociedade, antes de entrar em vigor. Deveria haver um debate maior sobre o assunto, orientando à construção de um marco regulatório adequado ao exercício das liberdades na rede, completa Jacques. Conforme mostra a Petição On Line, que já conta com 108.000 assinaturas, os brasileiros estão preocupados com a discussão e esperam maior atenção para com o futuro da liberdade da Internet



DEFINIÇÕES DOS TERMOS TÉCNICOS

Art. 16. Para os efeitos penais 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 qualquer outra tecnologia;
- 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: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida;



DEFINIÇÕES DOS TERMOS TÉCNICOS

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;

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.

Art. 17. Para efeitos penais consideram-se também como bens protegidos o dado, o dispositivo de comunicação, a rede de computadores, o sistema informatizado.



Obrigado!

Desenvolver, Promover, Informar, Proteger.

MANOEL ANTONIO DOS SANTOS
OAB-SP Nº 73.537

Associação Brasileira das Empresas de Software
Av. Ibirapuera, 2907 – 8º andar Cj. 811
04029-200 – São Paulo SP –
fone: + 55 11 5044-7900 fax: + 55 11 5044-7901
www.abes.org.br

