

# **Seminário: A Lei Contra Cibercrimes**

## **TIPOS PENAIS**

24 de agosto de 2011

**Renato Opice Blum**

[renato@opiceblum.com.br](mailto:renato@opiceblum.com.br)

Copyright © 2011 – Todos os direitos reservados.

Joaquim Eugênio de Lima, 680 – 1º andar – São Paulo – SP – Brasil – 01403-000

Tel.: (55-11) 3253-0061- Fax: (55-11) 3285-5326

E-Mail: [contato@opiceblum.com.br](mailto:contato@opiceblum.com.br)

[www.opiceblum.com.br](http://www.opiceblum.com.br)

© 2000 Randy Glasbergen.  
www.glasbergen.com



"THE COMPUTER SAYS I NEED TO UPGRADE MY BRAIN  
TO BE COMPATIBLE WITH ITS NEW SOFTWARE."

Copyright 2006 by Randy Glasbergen.  
www.glasbergen.com



**“The identity I stole was a fake!  
Boy, you just can’t trust people these days!”**

**Art. 72.** Constituem crimes, puníveis com reclusão, de cinco a dez anos:

I - obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos;

II - desenvolver ou introduzir comando, instrução, ou programa de computador capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral;

III - causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.

## Violação de sigilo funcional

**Art. 325** - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:

Pena - detenção, de 6 (seis) meses a 2 (dois) anos, ou multa, se o fato não constitui crime mais grave.

§ 1º Nas mesmas penas deste artigo incorre quem: (Parágrafo acrescentado pela Lei nº 9.983, de 14.7.2000)

I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; (Alínea acrescentada pela Lei nº 9.983, de 14.7.2000)

II - se utiliza, indevidamente, do acesso restrito. (Alínea acrescentada pela Lei nº 9.983, de 14.7.2000)

§ 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem: (Parágrafo acrescentado pela Lei nº 9.983, de 14.7.2000)

Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.

# DISPOSITIVOS LEGAIS – LEI 11.829/2008

“Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.” (NR)

Art. 2º A Lei nº 8.069, de 13 de julho de 1990, passa a vigorar acrescida dos seguintes arts. 241-A, 241-B, 241-C, 241-D e 241-E:

“Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

§ 1º Nas mesmas penas incorre quem:

I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;

II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.

§ 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.

# DISPOSITIVOS LEGAIS – LEI 10.695/2003

Art. 184. Violar direitos de autor e os que lhe são conexos:  
Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.

§ 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:  
Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

§ 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, *nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.*" (NR)

## Artigo 168 – Prática de Atos Fraudulentos aos Credores

Praticar, antes ou depois da sentença que decretar a falência, conceder a recuperação judicial ou homologar a recuperação extra-judicial, ato fraudulento de que resulte ou possa resultar prejuízo aos credores, com o fim de obter ou assegurar vantagem indevida para si ou para outrem.

§ 1º A pena aumenta-se de 1/6 (um sexto) a 1/3 (um terço), se o agente:

III – destrói, apaga ou corrompe dados contábeis ou negociais armazenados em computador ou sistema informatizado (g.n.).

## Artigo 169 – Quebra de Sigilo Empresarial Indevido

Violar, explorar ou divulgar, sem justa causa, sigilo empresarial ou dados confidenciais sobre operações ou serviços, contribuindo para a condução do devedor a estado de inviabilidade econômica ou financeira.

## Supressão de documento

Art. 305 - Destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não podia dispor:

Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa, se o documento é público, e reclusão, de 1 (um) a 5 (cinco) anos, e multa, se o documento é particular.

## **Inserção de dados falsos em sistema de informações**

Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Artigo acrescentado pela Lei nº 9.983, de 14.7.2000)

Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.

## **Modificação ou alteração não autorizada de sistema de informações**

Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Artigo acrescentado pela Lei nº 9.983, de 14.7.2000)

Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.

Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (Parágrafo acrescentado pela Lei nº 9.983, de 14.7.2000)

# TERMO DE MÚTUA COOPERAÇÃO

CPI – Pedofilia (Senado Federal)

Manutenção e Guarda de IP's

Termo.pdf - Adobe Reader

Arquivo Editar Visualizar Documento Ferramentas Janela Ajuda

7 / 17 125% Localizar

III – a oferta do serviço for dirigida ao público brasileiro.

**CLÁUSULA TERCEIRA – Da Manutenção e Guarda de Dados**

As empresas signatárias fornecedoras de serviço de telecomunicações e de acesso manterão, em ambiente controlado, os dados cadastrais dos usuários e os de conexão pelo prazo de três anos, e as fornecedoras de serviços de conteúdo ou interativo, pelo prazo de seis meses.

**Parágrafo único.** A empresa signatária que oferecer, simultaneamente, os serviços de telecomunicações, de acesso e de conteúdo ou interatividade respeitará os prazos a que se refere esta cláusula conforme a atividade.

208,2 x 292,7 mm

Folha Online - Informática - Ataques cibernéticos estão entre três maiores ameaças mundiais, di - Windows Internet Explorer for

http://www1.folha.uol.com.br/folha/informatica/ult124u487415.shtml

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

FOLHAONLINE  
www.folha.com.br  
Sexta-feira, 09 de janeiro de 2009

Notícias Especial Serviço Galeria Erramos Colunas Fale conosco Atendimento ao assinante Grupo Folha Assine Folha

Em cima da hora | Ambiente | Bichos | Brasil | Ciência e Saúde | Comida | Cotidiano | Dinheiro | Educação | Equilíbrio | Esporte | Ilustr

## informática

Comunicar erros Enviar -mail Imprimir

07/01/2009 - 18h17

### Ataques cibernéticos estão entre três maiores ameaças mundiais, diz FBI

da **France Presse**, em Nova York

Os ataques informatizados representam a maior ameaça para os Estados Unidos, depois da guerra nuclear e das armas de destruição em massa, e são cada vez mais difíceis de impedir, segundo especialistas da Polícia Federal norte-americana (FBI).

Durante uma conferência em Nova York nesta terça-feira (7), Shawn Henry, diretor adjunto da divisão informática do FBI, disse que esses ataques representam "o maior risco para a segurança

PUBLICIDADE

DESKTOP VOSTRO™ 200  
Processador Intel® Core™2 Duo

OFERTA IMPERDÍVEL!

Do more

Ligue agora para  
0800 722 3495  
e compre o seu!

busca

+tidas

1. Internet igno vendas
2. Polaroid lan sem tinta
3. Garotas de prostituição'
4. Microsoft lar na sexta
5. Sony aprese fashionistas

Internet 130%

# Wireless Door

How Credit-Card Data Went Out Wireless Door - WSJ.com - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço [http://online.wsj.com/article\\_email/SB117824446226991797-1MyQjAxMDE3NzA4NDIwNDQ0Wj.html](http://online.wsj.com/article_email/SB117824446226991797-1MyQjAxMDE3NzA4NDIwNDQ0Wj.html) Ir Links

**WSJ.com THE WALL STREET JOURNAL ONLINE**

Article Search   Quotes & Research

Advanced Search  Symbol(s)  Name

Free Dow Jones Sites As of Friday, May 4, 2007 Online Journal Subscribers LOG III

Home News Technology Markets Personal Journal Opinion Weekend & Leisure

**TODAY'S NEWSPAPER**  
**MY ONLINE JOURNAL**  
**FREE FEATURES**  
**MARKET DATA & TOOLS**  
**FIND A JOB**  
**FIND A HOME**  
**Special Offer**  
 Subscribe to the print Journal today and receive 8 weeks FREE! Click Here!

**THE WALL STREET JOURNAL DEALS & DEAL MAKERS CONFERENCE**  
 The country's top private equity investors, hedge fund managers, investment bankers, and economists

**PAGE ONE**  
**BREAKING THE CODE**  
**How Credit-Card Data Went Out Wireless Door**

Biggest Known Theft Came from Retailer With Old, Weak Security

By **JOSEPH PEREIRA**  
 May 4, 2007; Page A1

The biggest known theft of credit-card numbers in history began two summers ago outside a Marshalls discount clothing store near St. Paul, Minn.

There, investigators now believe, hackers pointed a telescope-shaped antenna toward the store and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers and the store's computers. That helped them hack into the central database of Marshalls' parent, TJX Cos. in Framingham, Mass., to repeatedly purloin information about customers.

The \$17.4-billion retailer's wireless network had less security than many people have on their home networks, and for 18 months the company -- which also owns T.J. Maxx, Home Goods and A.J. Wright -- had no idea what was going on. The hackers, who have not been found, downloaded at least 45.7 million credit- and debit-card numbers from about a year's worth of records, the company says. A person familiar with the firm's

EMAIL PRINT

Start a FREE trial of the Online Journal 

Subscribe to The Print Journal 

Free US Quotes:  
 Symbol  
 Name

Get FREE E-Mail by topic

Check Out our Mobile & Wireless Services

DIGEST OF EARNINGS  
 Details of the latest corporate earnings reported for FREE.

advertisement

**TATA CONSULTANCY SERVICES**

Internet

Iniciar Caixa de entra... Windows Live ... Jorge Henriqu... C:\Documents ... How Credit-Ca... FS@ ScreenCAP 09:13

# Jovem invade sistema 911 e faz Swat cair em trote

**Jovem invade sistema 911 e faz Swat cair em trote** - Terra - Vírus & Cia - Microsoft Internet Explorer fornecido por Opice Blum

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço <http://tecnologia.terra.com.br/interna/0,,OI2000670-EI4805,00.html> Ir Links >>

Fotos  
Celular & Wireless  
Cine & Foto  
Download  
Eletrônicos  
Games  
Hardware & Software  
Internet  
Negócios & TI  
Robôs  
Shopping  
Tecno Trash  
Tutoriais & Dicas  
vc repórter  
**Vírus & Cia**  
Correções

Convergência Digital  
InfomediaTV  
Mac+

Especiais  
Internet 10 anos

**Chat**  
A sua é encontrar alguém especial?

Quinta, 18 de outubro de 2007, 11h07

## Jovem invade sistema 911 e faz Swat cair em trote

Randall Ellis, hacker americano de 19 anos, deverá comparecer ao tribunal californiano de Orange County para responder pelas acusações de ter invadido o sistema de emergência policial americano, mais conhecido como 911. A Swat, atendendo o falso chamado, foi armada até a casa de uma família que nada tinha a ver com o caso.

» **Jovem quebra em 30 minutos filtro antipornografia do governo**  
 » **Garoto ataca ladrões de games a espadadas**  
 » **Polícia invade show de realidade online após trote**  
 » **Chat: tecle sobre a notícia**

Segundo o site The Register, Ellis invadiu o sistema telefônico e cadastrou um falso chamado sob um número de Orange County escolhido aleatoriamente. No chamado, alegava ser um usuário de drogas adolescente que havia sido baleado no ombro, e que estava na mira de bandidos que também ameaçavam a vida de sua irmã.

Como resultado, a equipe especial da Swat, armada com rifles, cães farejadores e até mesmo um helicóptero foi prontamente enviado ao local, segundo o jornal *The Orange County Register*.

A família moradora no endereço usado para o trote dormia quando a polícia chegou. E a situação poderia ter sido pior, caso a força policial tivesse disparado seus rifles contra um dos moradores que, assustado, saiu da casa armado com uma faca de cozinha. Ele e sua mulher chegaram a ser algemados até que o mal-entendido fosse desfeito, pouco depois.

Os métodos utilizados por Ellis não foram divulgados por questões de

**MAGNET**

Últimas de Vírus & Cia

- » Jovem invade sistema 911 e faz Swat cair em trote
- » Homens são presos por enviar emails com pornografia
- » Adobe Acrobat tem falha que permite invasão de PC
- » Microsoft corrige seis falhas com Patch Tuesday

Busca

Faça sua pesquisa na Internet:

BUSCAR

Inter Core Duo c/ Windows XP  
1GB de RAM - DVD-RW

12x R\$ 174,91 sem juros

extra.com.br

Internet

Iniciar Caixa de entrada - Mi... Tribunal Francês con... Aulas Jovem invade sistem...

12:19

# Invasão em e-mails

22/09/2008 - 21h31

## Piratas virtuais invadem e-mail do primeiro-ministro do Canadá

da Efe, em Toronto

Recomendar +1 0

Um grupo de piratas virtuais invadiu o e-mail do primeiro-ministro canadense, Stephen Harper. Na semana passada, o mesmo ocorreu com a [candidata republicana à vice-presidência](#) dos Estados Unidos, Sarah Palin.

No caso de Palin, os invasores tiveram acesso a uma conta pessoal no Yahoo!, enquanto no de Harper foi violado o correio oficial.

Chris Wattie/Reuters



Stephen Harper teve e-mail invadido por piratas virtuais, que enviaram mensagens

Nesta segunda-feira (22), o escritório do primeiro-ministro disse que pediu à agência canadense encarregada de contra-espionagem eletrônica que investigue a invasão no sistema de e-mail de Harper.

No domingo à noite, pouco depois que o escritório do primeiro-ministro enviou à imprensa em sua lista de contatos um comunicado no qual Harper condenava o atentado em Islamabad contra o hotel Marriott, os jornalistas receberam outras duas mensagens.

O título da primeira, "Por que não deveriam me temer", levantou suspeitas, já que, embora o país esteja em plena campanha eleitoral, é inusitado que o primeiro-ministro utilize seu e-mail institucional para enviar mensagens partidárias.

PUBLICIDADE

Passa o mouse e conheça uma nova computação.

PUBLICIDADE

COLEÇÃO FOLHA CINE EUROPEU DOMINGO nas bancas R\$ 15,90 cada livro

### as últimas que você não leu

- 0. Veja dicas e técnicas para fotografar melhor
- 0. Apple vale tanto quanto todos os bancos da zona do euro
- 0. Ribeirinhos esperam que exposição no Google atraia turistas
- 0. Brasileiro quer câmera avançada, mas mercado formal engatinha
- 0. Classe média impulsiona mercado de câmeras digitais no Brasil
- 0. Ação da HP despenca 20% por menor projeção e divisão de unidade
- 0. Gamescom consolida-se como feira de videogames além dos consoles

# Administrador de TI é preso por negar acesso a rede

**MERCADO**  
LEGISLAÇÃO

## Prefeito de São Francisco consegue recuperar senha da rede da cidade

Por IDG News Service/EUA  
Publicada em 23 de julho de 2008 às 09h26

E-mail Imprima Comente Erros? **aa** +7 0

[Tweet](#) 0 [Share](#) [Like](#)

**São Francisco - Prefeito conseguiu de volta a senha com o administrador da rede, que estava preso, acusado de negar acesso à rede.**

O prefeito de São Francisco, Gavin Newsom, se encontrou com o administrador de TI do município Terry Childs na segunda-feira (21/07) e o convenceu a entregar a senha de administração da rede multimilionária da cidade.

Childs foi preso na semana passado por se recusar a dar a senha dos switches e roteadores Cisco que compõem a rede FiberWAN da cidade, responsável por 60% do tráfego do governo municipal.

O administrador, que gerenciava a rede antes de ser preso, está na cadeia desde 13 de julho. Segundo registros do processo, ele é acusado de ter negado acesso à rede a outros servidores públicos.

Os registros mostram ainda que ele teria ligado equipamentos clandestinos à rede pública para poder monitorá-la de sua casa e implementado um protocolo que apagaria as configurações da rede se alguém além dele próprio tentasse acessar a rede

**Publicidade**

Descubra muitas razões para se conectar também.

[CONECTE-SE >](#) **FORD CONNECT**

**WHITE PAPERS**

Saiba mais sobre as 5 tecnologias essenciais para acompanhar as demandas de armazenamento de dados  
[> Download](#)

Semântica para SharePoint. Busca semântica utilizando ontologias.  
[> Download](#)

Conheça as soluções TOTVS para o segmento de Manufatura  
[> Download](#)

O novo perfil do consumidor mais exigente e informado tem sido um desafio às empresas varejistas. Conheça as soluções para o segmento  
[> Download](#)

Por conta das mudanças das relações econômicas geradas pela Web 2.0, o setor de Serviços precisa

**Quem leu esta notícia também leu:**

- [Brasil passa a controlar Orkut e presidente do Google Brasil assume AL](#)
- [Stand Center é condenado a pagar multa de R\\$ 7 bilhões à ABES](#)
- [Empresa de internet japonesa coloca Wikipedia em celulares](#)

Desenvolvido por: **upLexis**

**TOP 5 NOTÍCIAS | MAIS LIDAS DO DIA EM MERCADO**

**Dia** | **Semana** | **Mês**

- ["O efeito tablet é real", mas não para a HP, diz CEO](#)
- [Linux dominou os negócios em Wall Street](#)
- [O que as pessoas mais usam no smartphone?](#)

## (Substitutivo do Senado Federal)

Art. 2º O Título VIII da Parte Especial do Código Penal fica acrescido do Capítulo IV, assim redigido:

### **Capítulo IV DOS CRIMES CONTRA A SEGURANÇA DOS SISTEMAS INFORMATIZADOS**

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

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.*

Internet | Gizmodo Brasil - Windows Internet Explorer

http://www.gizmodo.com.br/categorias/internet?page=2

Arquivo Editar Exibir Favoritos Fragmentas Ajuda

Google  Go  Bookmarks 49 blocked Check AutoLink AutoFill Send to Settings

Internet | Gizmodo Brasil Ferramentas

INTERNET

## Pendrive com movimentações de tropas britânicas é encontrado em chão de boate



Parece que o Ministro da Defesa do Reino Unido está prestes a escutar o cottado responsável por deixar um pendrive carregado com movimentações da tropas no chão da boate "The Beach", em

# Confidencial - Google

Firefox | confidencial "do not distribute" - Pesqui... | +

http://www.google.com.br/search?q=confidencial "do not distribute"&ie=utf-8&oe=utf-8&aq=t&rls=org.r | Google

traduzidas 29 Oct 2006 – Follow-up Measurement About Google Searching for **Confidential Do Not Distribute** As communicators, every day we try to keep up on the latest ...

Mais ferramentas

[PDF] [BBY CONFIDENTIAL - DO NOT DISTRIBUTE Best Buy Employee News](#) - [ Traduzir esta página ]  
[www.iabc.com/education/pdf/BarryJohnson-CaseStudy1\\_printcolor.pdf](http://www.iabc.com/education/pdf/BarryJohnson-CaseStudy1_printcolor.pdf)  
 Formato do arquivo: PDF/Adobe Acrobat - [Visualização rápida](#)  
 BBY **CONFIDENTIAL - DO NOT. DISTRIBUTE.** Best Buy Employee News. Intranet News Delivery at Best Buy. Barry Johnson. Director, News Team. June 25, 2008 ...

[PDF] [CONFIDENTIAL \(PLEASE DO NOT DISTRIBUTE WITHOUT REMOVING THE INFO ...](#) - [ Traduzir esta página ]  
[www.ebri.org/pdf/programs/policyforums/dec2002/SpeakerBios-1202.pdf](http://www.ebri.org/pdf/programs/policyforums/dec2002/SpeakerBios-1202.pdf)  
 Formato do arquivo: PDF/Adobe Acrobat - [Visualização rápida](#)  
 1. Will Today's Workers Retire With Adequate Income? And, How Are. Today's Retirees Surviving From A Financial Perspective? An EBRI-ERF Policy Forum ...

[PDF] [MARS Confidential – Do Not Distribute](#) - [ Traduzir esta página ]  
[www.rogerssupply.com/pdf/evergreen.pdf](http://www.rogerssupply.com/pdf/evergreen.pdf)  
 Formato do arquivo: PDF/Adobe Acrobat - [Visualização rápida](#)  
 MARS **Confidential – Do Not Distribute.** What is Evergreen? ➤ World's first ECM aftermarket indoor blower motor for nearly all standard ...

[PDF] [Confidential. Do not distribute. Pre-embargo material. Lack of ...](#) - [ Traduzir esta página ]  
[info.med.yale.edu/chldstdy/autism/resources/pdf/citalopram.pdf](http://info.med.yale.edu/chldstdy/autism/resources/pdf/citalopram.pdf)  
 Formato do arquivo: PDF/Adobe Acrobat  
 de BH King - 2009 - [Citado por 44 - Artigos relacionados](#)  
**Confidential. Do not distribute.** Pre-embargo material. ORIGINAL ARTICLE. Lack of Efficacy of Citalopram in Children. With Autism Spectrum Disorders and ...

[Confidential. Do not distribute. Pre-embargo material.](#) - [ Traduzir esta página ]  
[www.slideshare.net/.../confidential-do-not-d...](http://www.slideshare.net/.../confidential-do-not-d...) - Estados Unidos - Em cache  
**Confidential. Do not distribute.** Pre-embargo material. ORIGINAL ARTICLE Thyroid Cancer Survival in the Un.

[PDF] [Confidential. Do not distribute. Pre-embargo material. Effects of ...](#) - [ Traduzir esta página ]

# Malware sequestra arquivos e cobra resgate para devolvê-los

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

## Malware seqüestra - e não devolve mesmo

Autor do cavalo-de-tróia que seqüestra arquivos faz novas ameaças.

Dias atrás, o Plantão INFO noticiou sobre o Gpcode, um cavalo-de-tróia que invade a máquina e criptografa os arquivos de documentos (.doc, .txt, .xls, .pdf etc.) usando uma chave de 1024 bits. Além disso, o invasor deixa um arquivo pedindo um resgate em dinheiro. A vítima deve pagar, a fim de obter a chave de decodificação dos arquivos.

No ano passado, uma versão anterior desse mesmo vírus cometeu peripécia semelhante. Só que especialistas em segurança descobriram um erro de implementação no algoritmo de criptografia. Assim, foi fácil desarmar a chantagem dos responsáveis pelo Gpcode.

Agora, o Gpcode.ak aparentemente veio sem bugs. A Kaspersky, fabricante de antivírus, lançou uma convocação para que especialistas em criptografia, instituições científicas e outras empresas de antivírus unissem esforços para decodificar o malware ou pelo menos descobrir uma falha em sua implementação. A idéia era montar uma grande rede de grid computing para enfrentar a tarefa.

No entanto, muitos acreditam que essa tarefa é inútil, pois pode demandar meia eternidade para chegar a um resultado positivo. Pouco depois, uma pessoa – possivelmente o autor do Gpcode, contactado por meio de um dos e-mails deixados na mensagem que cobra o resgate – afirmou que as empresas de segurança não vão conseguir quebrar o código. Além disso, a tal pessoa, que diz chamar-se Daniel Robertson, promete ampliar para 4096 o tamanho da chave criptográfica das próximas versões do cavalo-de-tróia.

O cracker faz ainda outras ameaças: diz que vai incluir no Gpcode escudos contra antivírus como criptografia polimórfica, recursos anti-heurísticos e capacidade de autopropagação, transformando o cavalo-de-tróia em vírus. Possivelmente, há nessas ameaças muito de guerra psicológica. Mas não resta dúvida de que Robertson, quem quer que seja, entende do riscado.

Com autores de vírus assim, não é difícil concluir que os problemas de segurança digital tendem a se tornar cada vez mais complicados. Ainda mais quando o objetivo de Daniel Robertson não é outro senão ganhar dinheiro. Ele mesmo diz que o Gpcode "se

Junho

D	S	T	Q	Q	S	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

últimos posts

- 15/12/2008 [Cibercriminosos atacam a Amazônia](#)
- 19/11/2008 [MS desiste do mercado de antivírus](#)
- 14/11/2008 [Vírus móveis atacam smartphones](#)
- 12/11/2008 [Empresas de antivírus criam associação](#)
- 10/11/2008 [Crackers exploram brecha no Adobe Reader](#)
- 04/11/2008 [Microsoft aponta recuo do malware](#)
- 17/10/2008 [Falsos antivírus infectam 30 milhões de PCs](#)

PUBLICIDADE

Aproveite a  
**Cidade Maravilhosa**  
com até **70%** de desconto

## **Obtenção, transferência ou fornecimento não autorizado de dado ou informação**

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 legalmente e com 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.*

### **Ação Penal**

Art. 285-C. Nos crimes definidos neste Capítulo 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 subsidiárias.”

# Quase 80% dos brasileiros temem que informações pessoais sejam acessadas ilegalmente

TI Inside - Windows Internet Explorer fornecido por Opice Blum Advogados

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço <http://www.tiinside.com.br/Filtro.asp?C=265&ID=83274> Ir Links

**Tecnologia**  
Estratégia  
Infra-estrutura  
Gestão

**ESPECIAIS**  
Outsourcing

**HOME**  
QUEM SOMOS  
FALE CONOSCO  
EVENTOS  
CADASTRE-SE  
ASSINE  
ANUNCIE

Pesquisa  OK

**OUTUBRO 2007**  
  
**DUPLA EFICIÊNCIA**  
Nº 29

**News**

**Quase 80% dos brasileiros temem que informações pessoais sejam acessadas ilegalmente**  
Segunda-feira, 03 de Dezembro de 2007, 20h58

Nada menos que cerca de 80% dos brasileiros estão muito ou extremamente preocupados com o acesso ilegal e o uso inadequado de informações pessoais, conforme indica um levantamento feito pela Independent Communications Research, encomendado pela Unisys, fornecedora global de serviços e soluções de TI. Destes, 41% afirmaram estar 'extremamente preocupados', com o roubo de identidade, 38% 'muito preocupados' e 6% não estão 'nada preocupados' com essa ameaça.

Para a pesquisa foram ouvidos aproximadamente 1,5 mil brasileiros de 18 a 60 anos, das classes A, B e C. O grau de preocupação dos entrevistados com o problema foi avaliado por uma escala indicativa de zero a 300, na qual zero representa nenhuma preocupação e 300, preocupação extrema.

"A fraude digital que tem crescido no Brasil, pois a cada dia aumenta o número de pessoas com acesso a internet, consequentemente as movimentações bancárias on-line e as compras virtuais, muitas vezes realizadas por internautas despreocupados com indicadores básicos de segurança", afirma o especialista em segurança digital e diretor da OS&T Informática, Sérgio Leandro. De acordo com um levantamento do instituto e-bit, a participação desses internautas com renda inferior a R\$ 1 mil subiu de 6%, em 2001, para 8% em 2006 e deverá crescer 40% nos próximos cinco anos.

Ainda de acordo com Leandro, para realização das fraudes os invasores estão usando táticas como o envio de e-mails que estimulam a curiosidade dos internautas, por exemplo, anúncios de fotos inéditas de desastres

**Ou aqui?**  
UCan



  
**ti ONLINE**  
O COMPLEMENTO

Internet

Iniciar  TI Inside - Windows I... FS@ ScreenCAP 08:11

# PROJETO DE LEI Nº 84, DE 1999

**Art. 3º** O Título I da Parte Especial do Código Penal fica acrescido do seguinte artigo, assim redigido:

## **“Divulgação ou utilização indevida de informações e dados pessoais”**

**154-A.** Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais ou de pessoas jurídicas 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.

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

**§ 1º.** “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.”

**§ 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 subsidiárias.

**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:

# PROJETO DE LEI Nº 84, DE 1999

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

## **“Inserção ou difusão de código malicioso”**

**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.

## **“Inserção ou difusão de código malicioso seguido de dano”**

**§ 1º** Produzir intencionalmente ou vender código malicioso destinado ao uso em dispositivo de comunicação, rede de computadores ou sistema informatizado.

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

**§ 2º** Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade 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.

**§ 3º** 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.

▷ **Subject:** voce estar sendo...

**From:** [veja as fotos.](#)

***sou um amigo seu esse é um aviso***

Você esta sendo traído, não tive coragem de te falar mas como imagens falam mais que palavras faça o download das fotos e veja com os seus próprios olhos

**[VEJA AS FOTOS](#)**

***Foi a única maneira que encontrei para te avisar***

# DOS CRIMES CONTRA O PATRIMÔNIO

Faça sua parte denuncie você e anônimo.

Arquivo Editar Exibir Ferramentas Mensagens Ajuda

Responder Responde... Encaminhar Imprimir Excluir Anterior Avançar Endereços

De: POLÍCIA CIVIL DO ESTADO DE SÃO PAULO  
Data: segunda-feira, 5 de junho de 2006 09:09  
Para: bvtres@ig.com.br  
Assunto: Faça sua parte denuncie você e anônimo.

 **POLÍCIA CIVIL** 

**Procurados da Justiça**  
Rua Brigadeiro Tobias, 517 - Bairro Luz  
CEP 03032-902 - São Paulo/SP - Brasil  
Fone: (11) 3167  
e-mail: procurados@policiacivil.sp.gov.br

Combatendo os indivíduos mais perigosos para a sociedade a Polícia Civil se arma de todas as maneiras para cumprir sua missão mais nobre: Defender o cidadão, e manter a lei e a ordem.

Para isso contamos com a sua participação faça sua denúncia seja um cidadão.

A polícia civil conta com sua colaboração isto é fundamental denuncie pela INTERNET ou pelo fone 197

Aqui estão os bandidos mais procurados da justiça cuidado ele pode ser o seu vizinho. veja aqui as fotos dos acusado pelos atentados da grande são paulo e demais capitais que aconteceu em varias parte do Brasil [VEJA AQUI AS FOTOS DOS PROCURADOS](#)

ID:SP&M:499.4484975507164701109911

Iniciar

Microsoft Office

Caixa de entrada

Faça sua parte denunci...

Processos Eletrônicos

09:38

# GOLPE NO CELULULAR

Eles costumam usar nomes de empresas famosas



Golpe do Torpedo Premiado

Inventam uma promoção



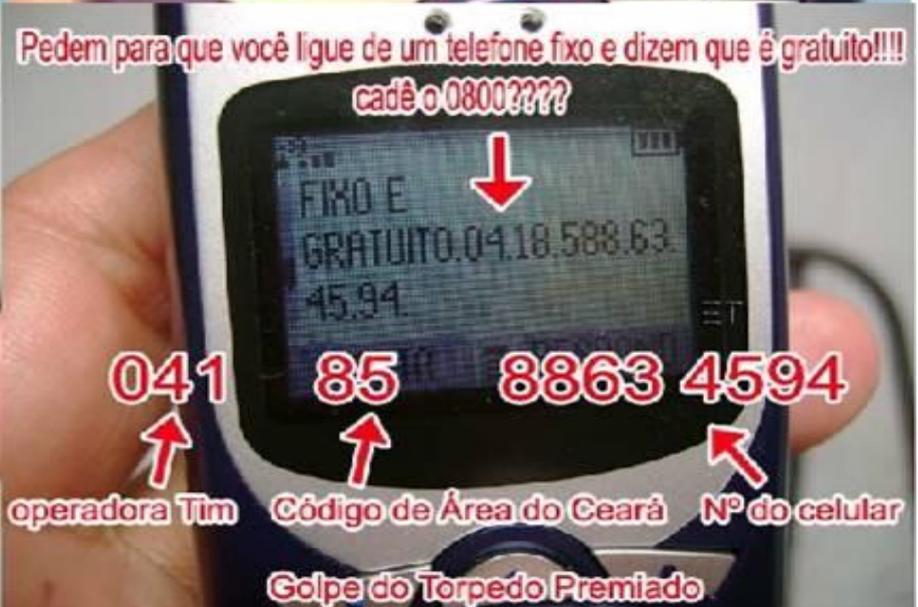
Golpe do Torpedo Premiado

E te oferecem um grande prêmio!!!!



Golpe do Torpedo Premiado

Pedem para que você ligue de um telefone fixo e dizem que é gratuito!!!!



Golpe do Torpedo Premiado

**Art. 6º** O art. 171 do Código Penal passa a vigorar acrescido dos seguintes dispositivos:

## **“Art. 171**

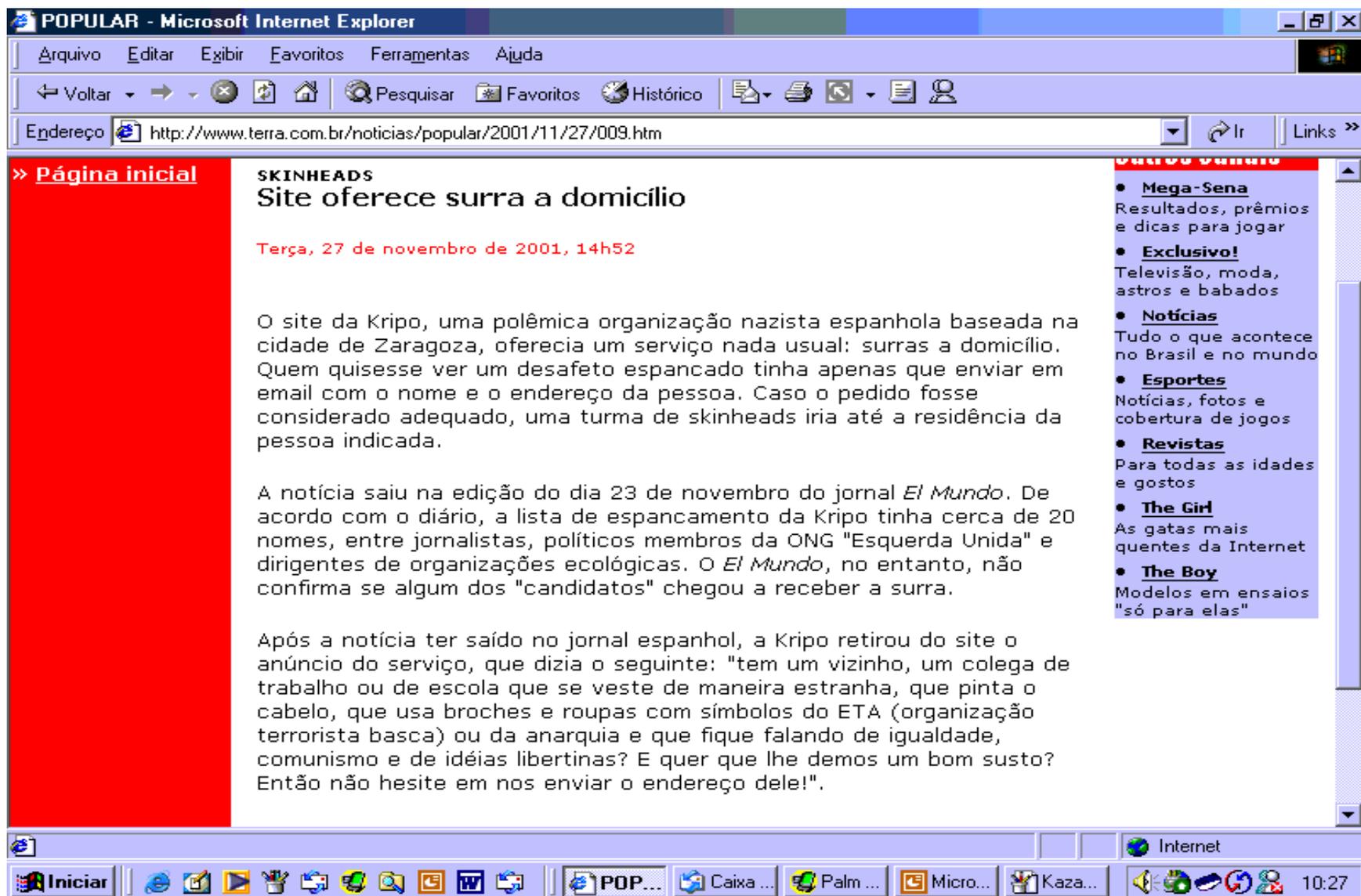
**§ 2º** Nas mesmas penas incorre quem:

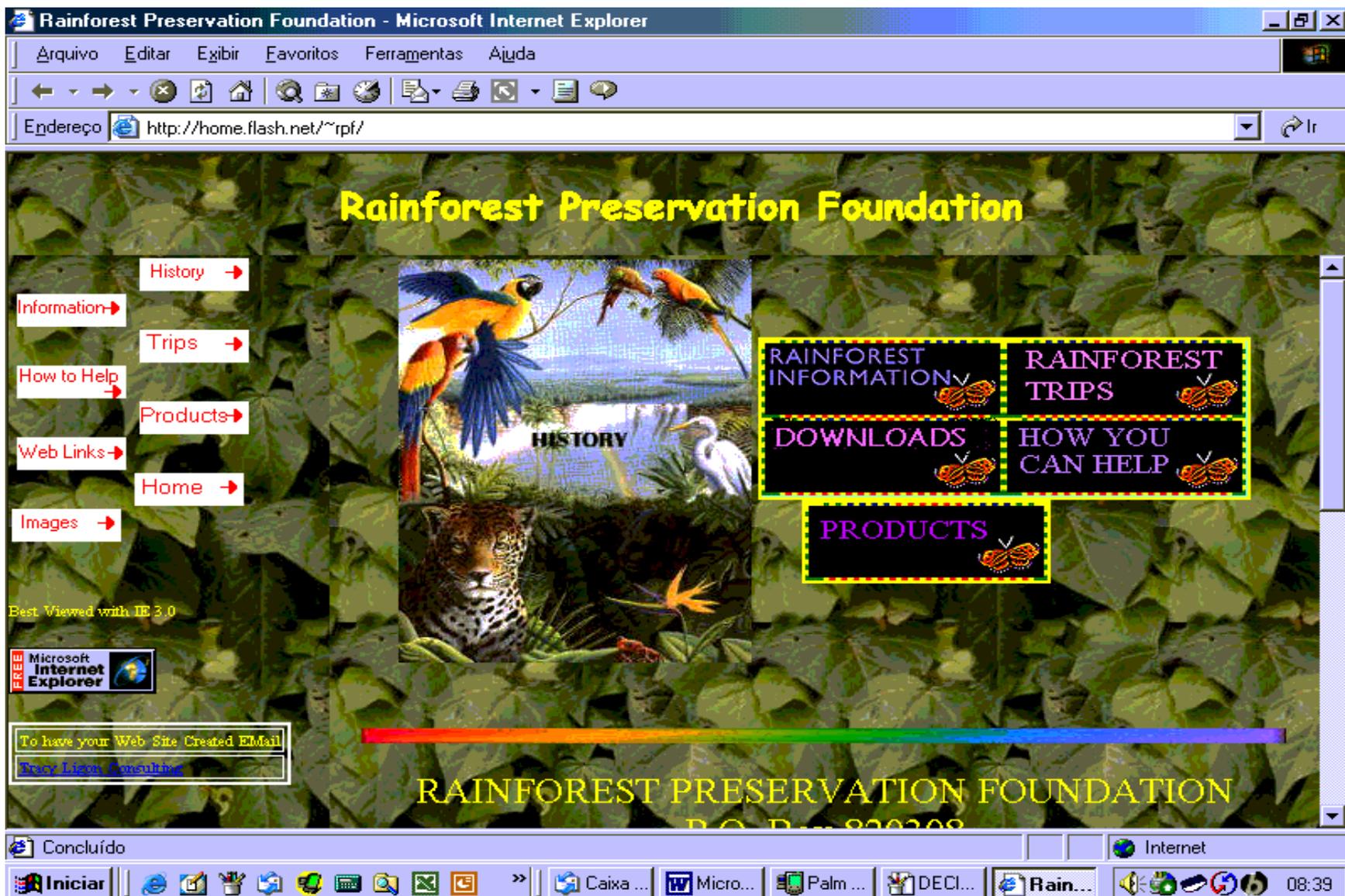
.....

### **Estelionato Eletrônico**

**VII** – difunde, por qualquer meio, código malicioso com intuito de devastar, copiar, alterar, destruir, facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado, visando o favorecimento econômico de si ou de terceiro em detrimento de outrem:

**§ 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.”





# PROJETO DE LEI Nº 84, DE 1999

Art. 7º Os arts. 265 e 266 do Código Penal passam a vigorar com as seguintes redações:

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

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

## **“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema Informatizado.”**

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento: - Pela Supressão deste artigo.  
 ..... “(NR)

# PROJETO DE LEI Nº 84, DE 1999

Art. 8º O caput do art. 297 do Código Penal passa a vigorar com a seguinte redação:

## **“Falsificação ou Alteração de dado informático ou documento público”**

Art. 297. Falsificar ou alterar, no todo ou em parte, dado informático ou documento público verdadeiro: .....”(NR)

Art. 9º O caput do art. 298 do Código Penal passa a vigorar com a seguinte redação:

## **“Falsificação ou alteração de dado informático ou documento particular”**

Art. 298. Falsificar ou alterar, no todo ou em parte, dado informático ou documento particular verdadeiro: .....”(NR)

# PROJETO DE LEI Nº 84, DE 1999

**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;

**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;

# PROJETO DE LEI Nº 84, DE 1999

**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, à 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. – Supressão do Artigo.

**Art. 18.** 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.

**Art. 19.** O inciso II do § 3º do art. 20 da Lei nº. 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

**“Art. 20.....**

**§ 3º.....**

**II** – a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.

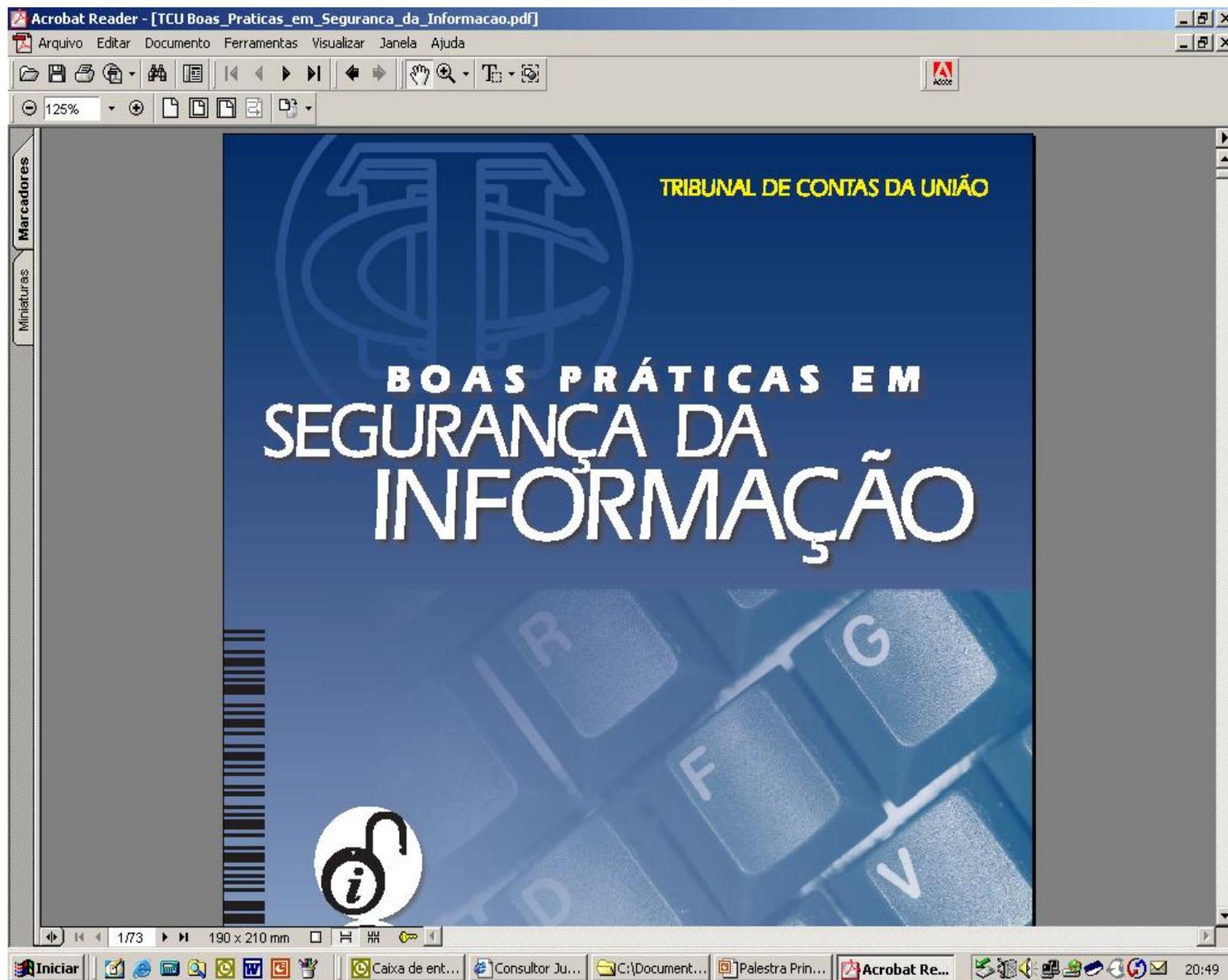
**Art. 20.** O caput do art. 241 da Lei nº 8.069, de 13 de julho de 1990, passa a vigorar com a seguinte redação:

**“Art. 241.** Apresentar, produzir, vender, receber, fornecer, divulgar, publicar ou armazenar, 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)

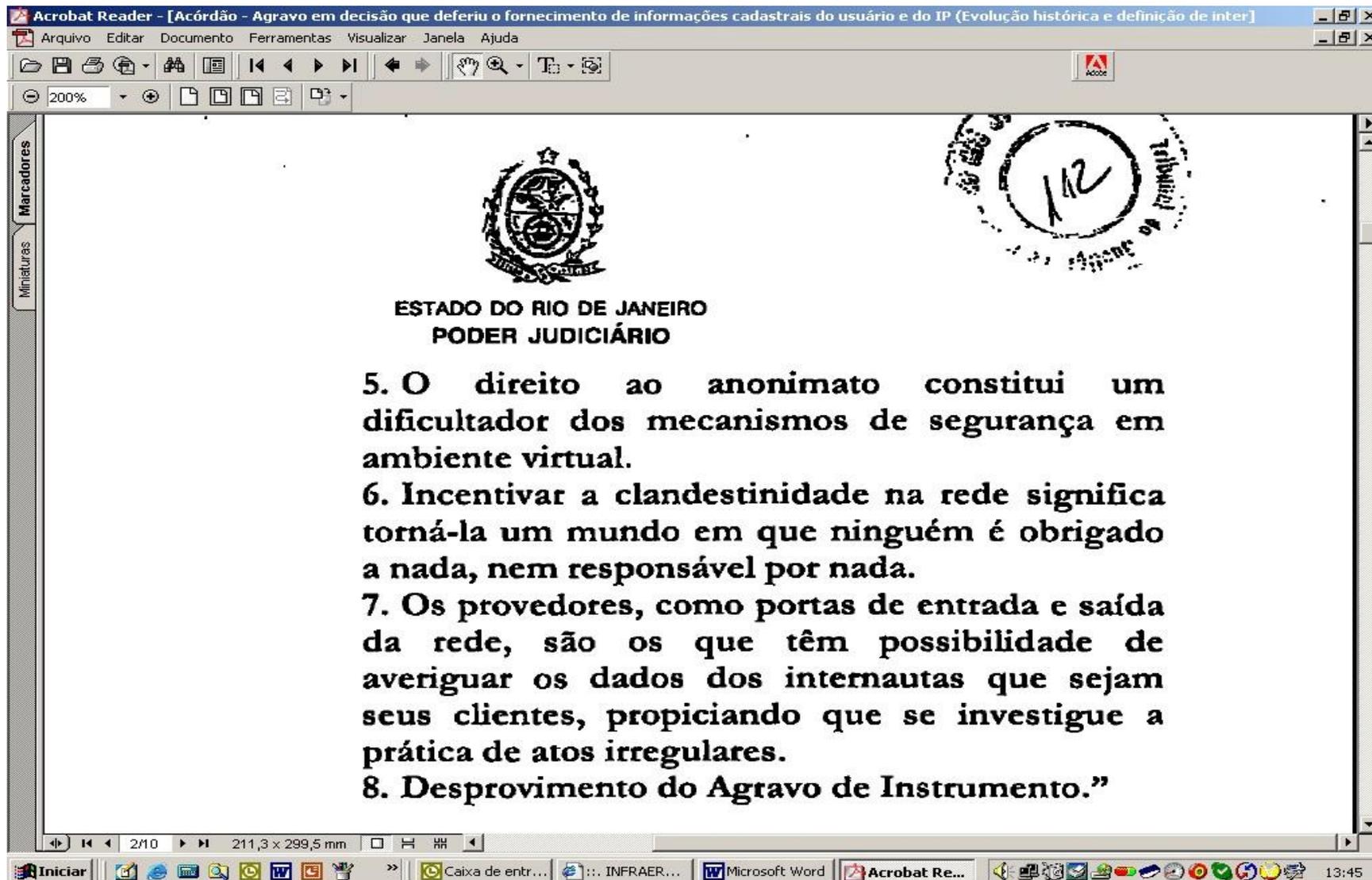


Fonte: Cartoon by Peter Steiner, The New Yorker, July 5, 1993 issue (Vol.69 no. 20) page 61

# Segurança



# TJRJ resp identificação IP



Acrobat Reader - [Acórdão - Agravo em decisão que deferiu o fornecimento de informações cadastrais do usuário e do IP (Evolução histórica e definição de inter)]

Arquivo Editar Documento Ferramentas Visualizar Janela Ajuda

200%

ESTADO DO RIO DE JANEIRO  
PODER JUDICIÁRIO

5. O direito ao anonimato constitui um dificultador dos mecanismos de segurança em ambiente virtual.

6. Incentivar a clandestinidade na rede significa torná-la um mundo em que ninguém é obrigado a nada, nem responsável por nada.

7. Os provedores, como portas de entrada e saída da rede, são os que têm possibilidade de averiguar os dados dos internautas que sejam seus clientes, propiciando que se investigue a prática de atos irregulares.

8. Desprovemento do Agravo de Instrumento.”

210 211,3 x 299,5 mm

Iniciar Caixa de entr... INFRAER... Microsoft Word Acrobat Re... 13:45

# SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO ESPECIAL Nº 1.193.764 - SP (2010/0084512-0)

RECORRENTE : I P DA S B

RECORRIDO : GOOGLE BRASIL INTERNET LTDA

## EMENTA

DIREITO CIVIL E DO CONSUMIDOR. *INTERNET*. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE CONTEÚDO. FISCALIZAÇÃO PRÉVIA DO TEOR DAS INFORMAÇÕES POSTADAS NO *SITE*, PELOS USUÁRIOS. DESNECESSIDADE. MENSAGEM DE CONTEÚDO OFENSIVO. DANO MORAL. RISCO INERENTE AO NEGÓCIO. INEXISTÊNCIA. **CIÊNCIA DA EXISTÊNCIA DE CONTEÚDO ILÍCITO. RETIRADA IMEDIATA DO AR. DEVER. DISPONIBILIZAÇÃO DE MEIOS PARA IDENTIFICAÇÃO DE CADA USUÁRIO. DEVER. REGISTRO DO NÚMERO DE IP. SUFICIÊNCIA.**

5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada.

6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do *site*, sob pena de responsabilização subjetiva por culpa *in omittendo* .

7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na *internet* (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de *internet* .

# PROJETO DE LEI Nº 84, DE 1999

**Art. 21.** 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) – Supressão do artigo.

**Art. 22.** O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público, bem como os prestadores de serviço de conteúdo, são obrigados a:

**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, destino, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória e o Ministério Público mediante requisição;

**II** – preservar imediatamente, após requisição, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

# PROJETO DE LEI Nº 84, DE 1999

**III** – informar, de maneira sigilosa, à autoridade policial ou judicial, informação em seu poder ou que tenha conhecimento e que contenha indícios da prática de crime sujeito a acionamento penal, cuja prática haja ocorrido no âmbito da rede de computadores sob sua responsabilidade, ressalvada a responsabilização administrativa, civil e penal da pessoa jurídica, sem exclusão das pessoas físicas, autoras, co-autoras ou partícipes do mesmo fato.

**§ 1º** Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a perícia à qual serão submetidos e a autoridade competente responsável por requisitar a perícia, bem como as condições para que sejam fornecidos e utilizados, serão definidos nos termos de regulamento, preservando-se sempre a agilidade na obtenção destas informações e o sigilo na sua manipulação.

**§ 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, considerando-se a natureza, a gravidade e o prejuízo resultante da infração, assegurada a oportunidade de ampla defesa e contraditório.

**§ 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, assegurada à distribuição igualitária entre os Estados membros, na forma de regulamento.

# Quanto aos tipos penais:

## CP Alemão:

Espionagem;

Estelionato informático;

Utilização abusiva de cartão bancário e cartão de crédito;

Falsificação de dados;

Modificação de dados;

Sabotagem informática.

# Quanto aos tipos penais:

## CP Holandês:

Invasão de domicílio informático;

Sabotagem informática;

Falsificação de documento;

Falsificação de cartão de pagamento ou cartão de valor;

Estelionato;

Dano informático.

# Quanto aos tipos penais:

## CP Austríaco:

Acesso ilícito a um sistema informático;

Interceptação abusiva de dados;

Dano Informático;

Perturbação do funcionamento do sistema informático;

Utilização abusiva de programa de computador ou de dados de acesso;

Utilização abusiva e fraudulenta de processamento de dados;

Falsificação de dados.

# Quanto aos tipos penais:

## CP Belga:

Falsificação informática;

Estelionato informático;

Crimes contra a confidencialidade, a integridade e a disponibilidade dos sistemas informáticos e dos dados que são armazenados, processados ou transmitidos por esses sistemas.

# Quanto aos tipos penais:

## CP Suíço:

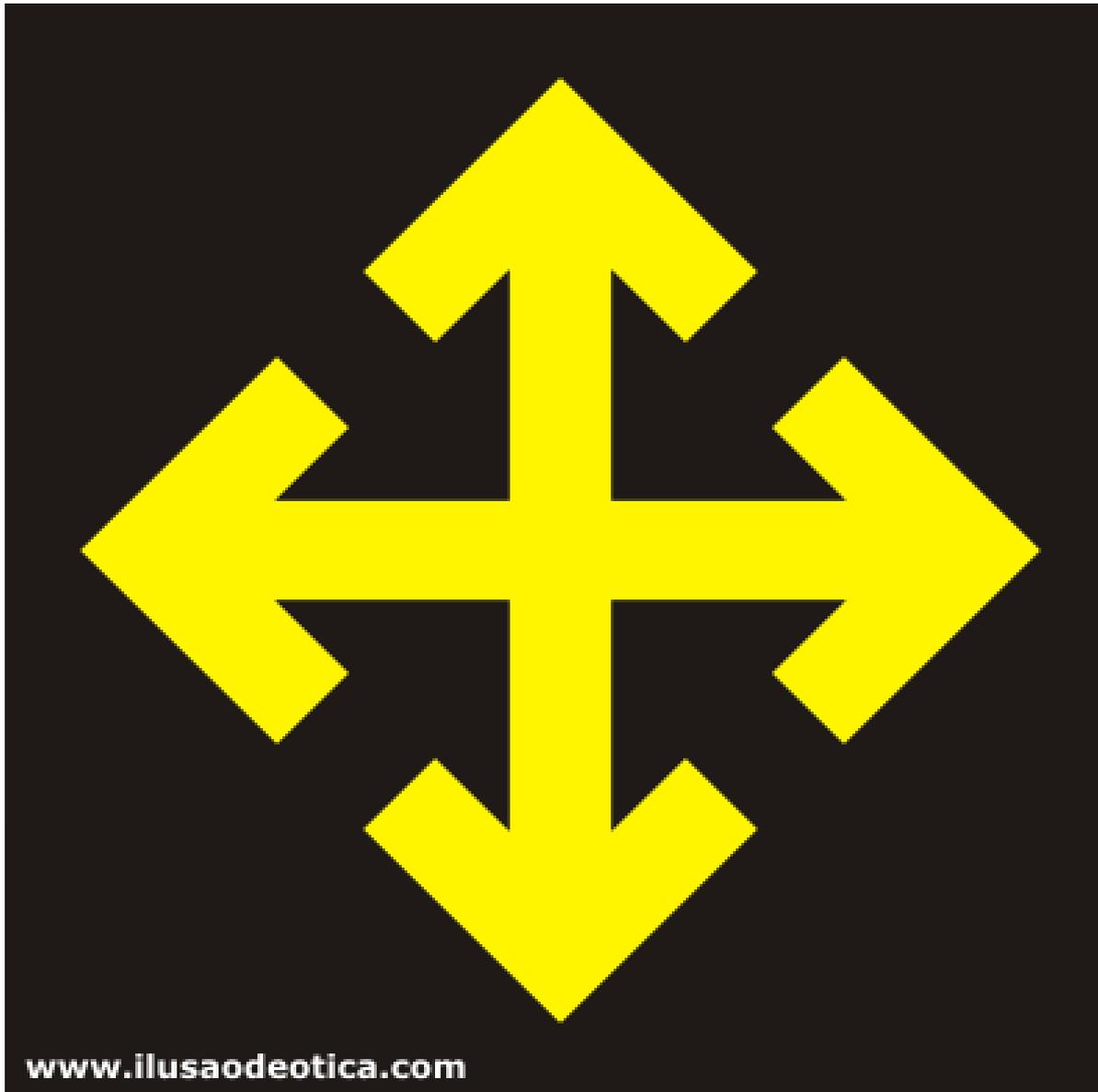
Obtenção não autorizada de dados;

Acesso não autorizado a um sistema informático;

Dano informático;

Utilização fraudulenta de uma instalação de processamento de dados.

# AS SETAS APONTAM PARA...



# CARTILHA – USO SEGURO DA INTERNET



The cover features a central illustration of a family (father, mother, and two children) standing in front of a large smartphone. From the phone, several colorful icons representing internet activities are projected outwards: a green 'WWW' icon, a blue play button, an orange '@' symbol, a blue camera, a yellow airplane, a red shopping cart, an orange RSS feed, a purple cat face, a blue envelope, and a green soccer ball. In the top right corner, there is a logo for 'SÃO PAULO' with a globe and the letters 'AB'.

recomendações e boas práticas para o  
**USO SEGURO DA INTERNET  
PARA TODA A FAMÍLIA**

1ª edição

## Objetivos

Ao final do curso o aluno estará apto a : Compreender o que há de mais moderno no direito digital; interpretar a jurisprudência nacional e internacional relacionada à internet e suas ferramentas, incluindo as redes sociais; Adotar ações específicas de preservação de evidências eletrônicas, com a identificação de criminosos digitais; debater questões atuais sobre privacidade, proteção de dados pessoais e riscos corporativos; identificar os limites éticos e mercadológicos da atuação do profissional especializado.

## Programa

- Direito Digital no Brasil e no Mundo
- Informatização do Judiciário e seus reflexos na atividade profissional
- Uso da internet no ambiente corporativo
- Proteção do conhecimento na era Digital
- Contratos Eletrônicos
- Crimes Digitais
- Prova e Perícia digital
- Consumidor e o Comércio Eletrônico
- Tributação nos Meios Eletrônicos
- Privacidade e Proteção de Dados
- Redes Sociais e Riscos
- Marketing Jurídico na era digital
- Responsabilidade dos Intermediários de Serviços de Internet
- Função Social da Propriedade Intelectual ante ao Avanço Tecnológico



Embaixador Roberto Campos: “os que ficam nesta Casa têm pela frente uma formidável agenda reformista. Desejo-lhes, como na oração do teólogo Reinhold Niebuhr:

“Que Deus lhes dê serenidade para aceitar as coisas que não possam mudar, coragem para mudar as que possam mudar e sabedoria para saber a diferença.”



**Renato Opice Blum**  
renato@opiceblum.com.br



- @ Advogado e economista;
- @ Coordenador do curso de MBA em Direito Eletrônico da EPD e do curso de Direito Digital da GVLaw;
- @ Professor convidado da USP (PECE) e Mackenzie;
- @ Presidente do Conselho de Tecnologia da Informação e Comunicação da FECOMERCIO/SP e do Comitê de Direito da Tecnologia da AMCHAM;
- @ Membro da Comissão de Direito da Sociedade da Informação – OAB/SP;
- @ Coordenador e co-autor do livro “Manual de Direito Eletrônico e Internet” e “Direito Eletrônico: a internet e os tribunais”;
- @ Sócio – CEO de [www.opiceblum.com.br](http://www.opiceblum.com.br);
- @ Currículo Plataforma Lattes: <http://lattes.cnpq.br/0816796365650938>