



CRIMES

(PL 84/1999)

ELETRÔNICOS

Fernando Neto Botelho



**(Des)
EDUCAÇÃO**

← [PL 84/99 | Lei de crimes na internet: população poderá opinar por chat e Twitter](#)

[Master Boot Record \(MBR\) | Popureb – um rootkit pequeno com uma grande reputação](#) →

Alerta | Primeira turma da escola hacker Anonymous se forma em um mês

12/07/2011 POR [BROADCAST SECURITY LABS](#) [DEIXE UM COMENTÁRIO](#)

Curso foi anunciado há uma semana e tem como objetivo ensinar jovens a invadir sites e roubar informações bancárias.



ANONYMOUS

pelas quais ela ficou famosa.

Pelas informações obtidas pelo CEO, o curso ensinará técnicas básicas, como habilitar botnets Zeus, o principal malware para o roubo de senhas bancárias. "Todo jovem aprendiz será capaz de criar sua botnet", disse. "E por

Daqui a um mês, os primeiros formandos da escola hacker [Anonymous](#) começarão a influir na já tumultuada onda de cibercrimes.

"Poderemos ter mais **250 mil usuários aptos** a causar problemas, que, embora não tenham conhecimento profissional de técnicas hacker, terão responsabilidade sobre o aumento de incidentes a ser sentido nas próximas semanas", afirmou Karim Hijazi, CEO da companhia de segurança Unveillance.

O impacto previsto é baseado no número de seguidores que o grupo hacker LulzSec obteve nos 50 dias em que esteve **ativo**: 285 mil. Quando a equipe anunciou que deixaria de existir, disse também que uma escola seria formada, de modo a dar continuidade às ações

Estadística do Site

1,844 hits

Twitter

LegalTech lança selo de auditoria para leilões de centavos e compras coletivas
<http://t.co/lhYIHCd> 4 hours ago

Master Boot Record (MBR) | Popureb - um rootkit pequeno com uma grande reputação:
<http://t.co/4efA2Nx> 4 hours ago

PL 84/99 | Lei de crimes na internet: população poderá opinar por chat e Twitter:
<http://t.co/8XDRPwX> | [@lincolnwerneck](#)
[@italoadriano](#) 8 hours ago

Ação do LinkedIn supera US\$ 100 na Bolsa de Nova York - Mercados - EXAME.com
<http://t.co/49ChMgP> via [@exame_com](#)
8 hours ago

[Follow](#) [@broadcastlabs](#)

Mais Acessados

[goo.gl/84u1q](#)

■ <http://cyberinvestigation.wordpress.com/2011/07/12/primeira-turma-da-escola-hacker-anonymous-se-forma-em-um-mes/>

Marcos Faria Araujo Assunção

SEGREDOS DO HACKER ÉTICO

3ª Edição atualizada e ampliada

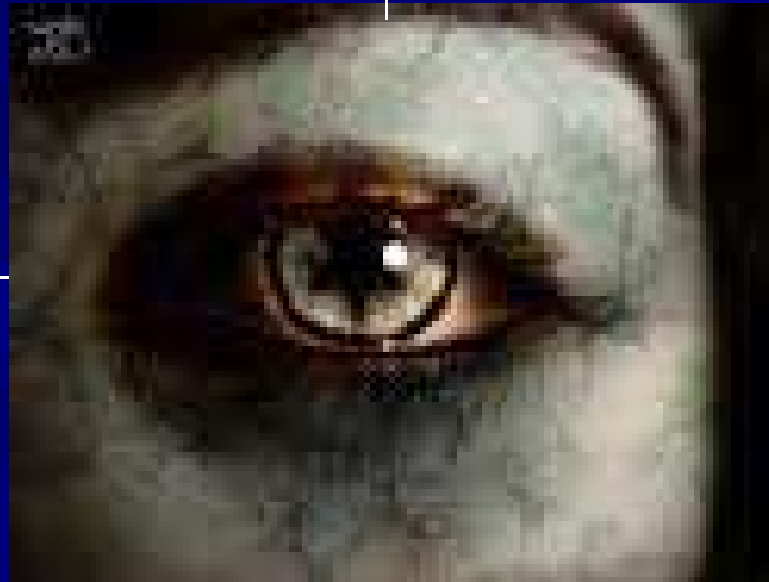
Autor destaque no
New York Times

Footprinting
Wi-Fi AP Spoofing
Engenharia Social
Cross Site Scripting
SQL Injection
ICMP Tunneling
Conexão Reversa
Burlando Firewalls
BackTrack
Backdoors e Trojans
Certified Ethical Hacker
Sniffers
Man in the Middle
Falhas e Exploits
Metasploit
Firewalls
APP Poisoning
Bluetooth Hacking
DNS Spoofing

Visual Books

ILÍCITOS – ELETRÔNICOS

Maldade

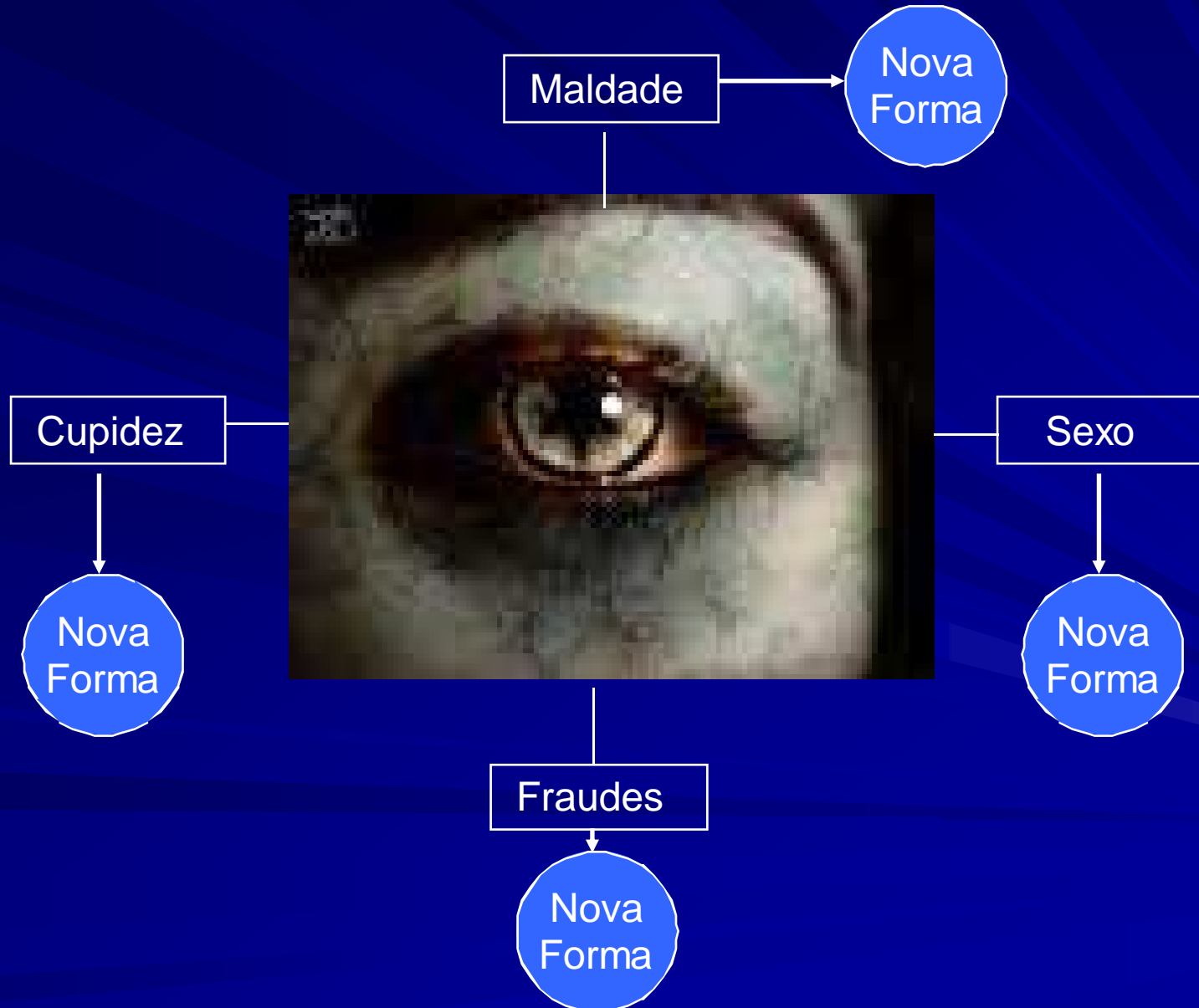


Cupidez

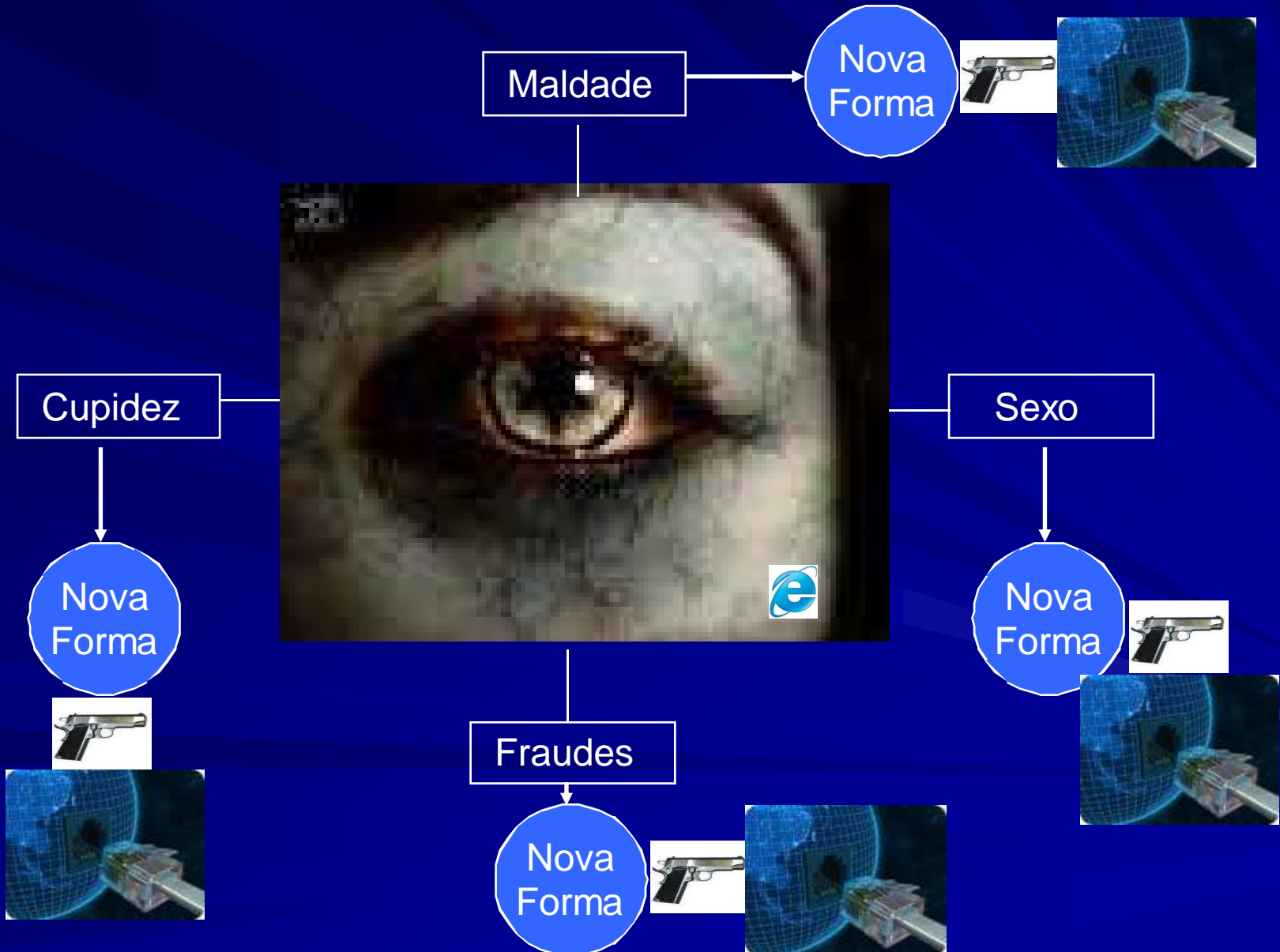
Sexo

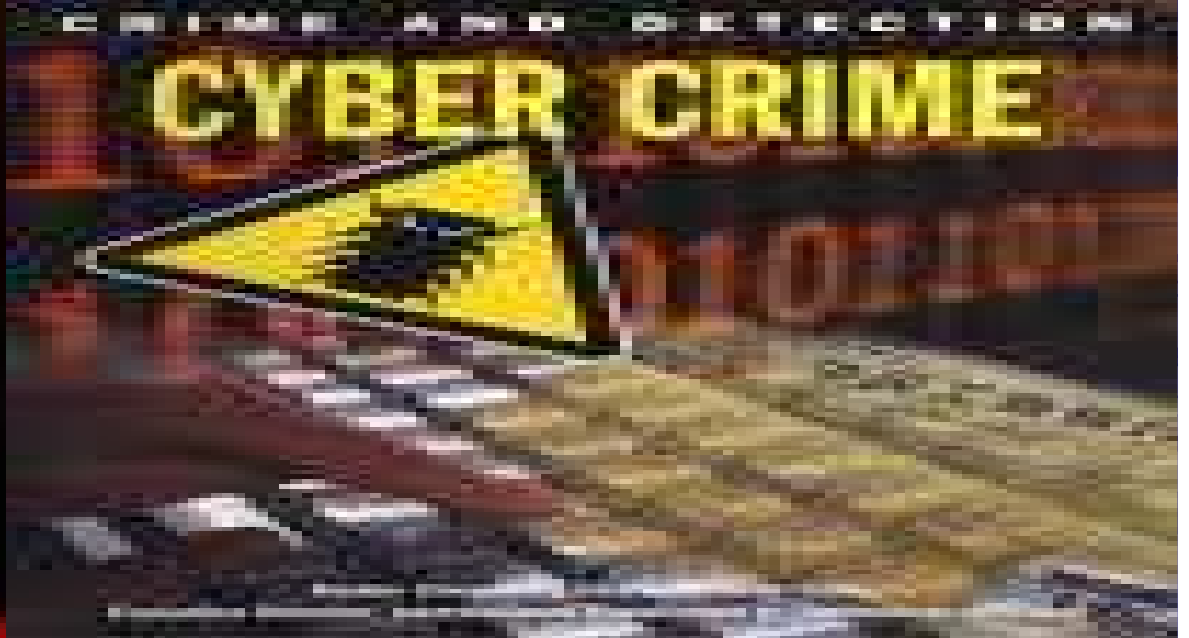
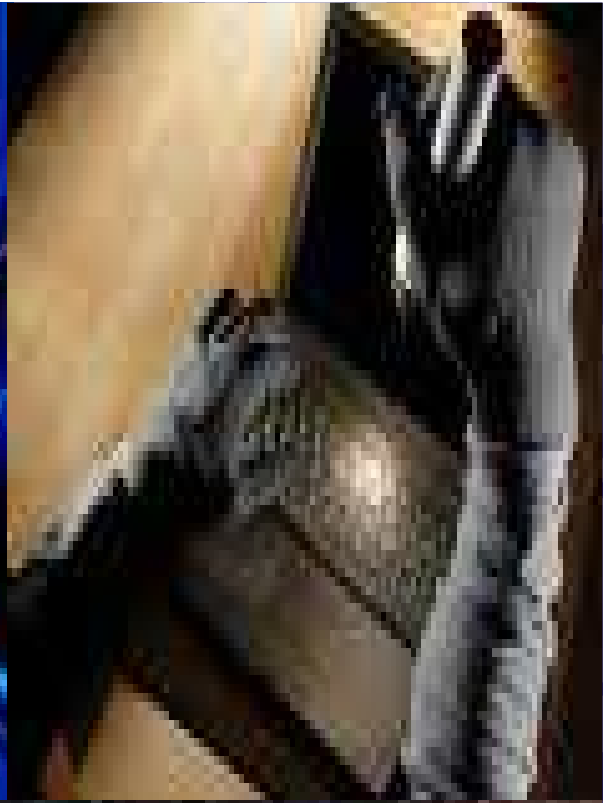
Fraudes

ILÍCITOS – ELETRÔNICOS



ILÍCITOS – ELETRÔNICOS





CONVENÇÃO EUROPÉIA DE CYBERCRIMES

* 2001 (G8)

* 2010

(+ 47 países ocidentais e orientais)

PL 84/1999

MUDANÇAS

Mudanças

- Código Penal (D.L. 2848/40): + 11 Crimes
- Código Penal Militar (D.L. 1001/69): + 9 Crimes
- Lei 7.716/89 (Racismo eletrônico)
- Lei ~~8.069/90 (Pedofilia eletrônica-armazenam.)~~
- Lei 10.446/2002 (Delitos Eletrônicos/Repercussão Interestadual e Internacional/Polícia Federal)
- Definições Penais elementos eletrônicos
- Aspectos Processuais e Procedimentais/Administr.

Mudanças – CÓDIGO PENAL

- 1 Crime (eletrônico) contra a liberdade individual
- 3 Crimes (eletrônicos) contra o patrimônio
- 5 Crimes (eletrônicos) contra a incolumidade pública (segurança de sistemas informatizados)
- 2 Crimes (eletrônicos) contra a fé-pública
- NOTA 1 : CRIMES DOLOSOS
- NOTA 2 : PENAS CONVERSÍVEIS

PL 84 – 1999

(As principais
disposições)

CP – Art. 285 - A

- [Título VIII - Incolumidade Pública)
- “**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.

CP – Art. 285 - A

■ O DELINQUENTE



CP – Art. 285 - B

- [Título VIII - Incolumidade Pública)
- “**CAPÍTULO IV**
- **DOS CRIMES CONTRA A SEGURANÇA**
- **DOS SISTEMAS INFORMATIZADOS**
- **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 por expressa restrição de acesso, dado ou informação neles disponível:**
- Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
- Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

CP – Art. 285 - A

■ O DELINQUENTE



CP – Art. 154-A

- [Título I – Crime Contra a Pessoa]
- “**CAPÍTULO I**
- “***Divulgação ou utilização indevida de informações e dados pessoais***
- **Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações PESSOAIS contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:**
- ***Pena – detenção, de 1 (um) a 2 (dois) 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.”***

CP – Art. 154 - A

■ O DELINQUENTE



CP – Art. 163

■ [Título I – Crime Contra o Patrimônio]

■ “**Dano**

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

■
”
.....

CP – Art. 163

■ O DELINQUENTE



CP – Art. 163 - A

- [Título I – Crime Contra o Patrimônio]
- ***“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 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.***
- ***§ 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.”***

CP – Art. 163 - A

■ O DELINQUENTE



CP – Art. 171

■ [Título I – Crime Contra o Patrimônio]

■ “ **Art. 171.**

■

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

■

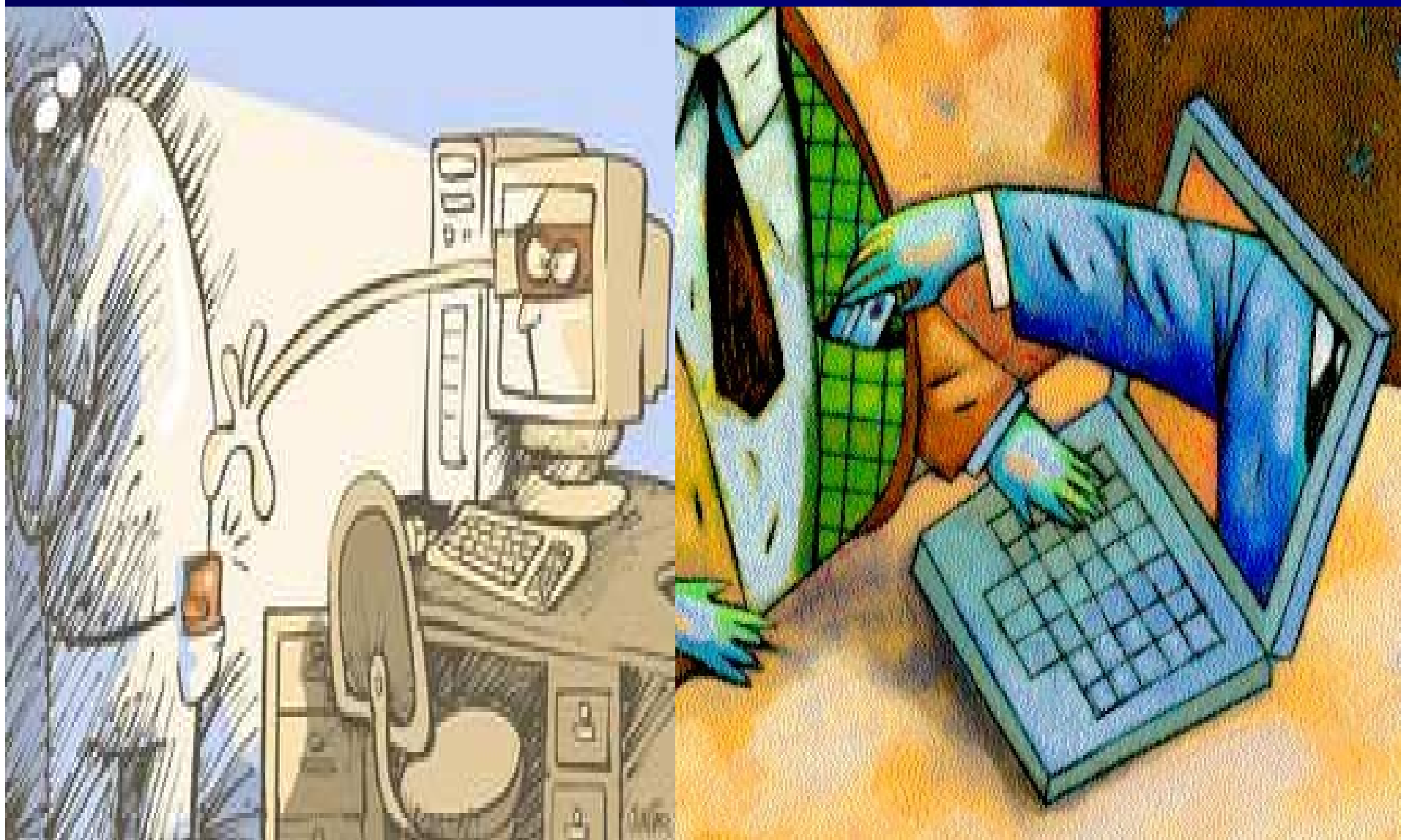
■ **ESTELIONATO ELETRÔNICO**

■ **VII – difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado.**

■ **§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte.”**

CP – Art. 171

■ O DELINQUENTE



CP – Art. 171

■ O DELINQUENTE



PL 84/1999

- ASPECTOS PROCESSUAIS -

POLÍCIA JUDICIÁRIA – PRINCÍPIO DA ESPECIALIZAÇÃO OBRIGATÓRIA:

- 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.



Não-autoaplicável
(Decreto Regulamentar)

PL 84/1999

- ASPECTOS PROCESSUAIS -

POLÍCIA JUDICIÁRIA – PRINCÍPIO DA COMPETÊNCIA CONCORRENTE:

- 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.

Art. 1º - Na forma do inciso I do § 1º do art. 144 da Constituição, quando houver repercussão interestadual ou internacional que exija repressão uniforme, poderá o Departamento de Polícia Federal do Ministério da Justiça, sem prejuízo da responsabilidade dos órgãos de segurança pública arrolados no art. 144 da Constituição Federal, em especial das Polícias Militares e Civas dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais:

PL 84/1999

ASPECTOS PROCEDIMENTAIS-ADMINISTRATIVOS -

Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

- I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial;
- II – preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
- III – informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.
- § 1º Os dados de que cuida o inciso I deste artigo, as condições de segurança de sua guarda, a auditoria à qual serão submetidos e a autoridade competente responsável pela auditoria, serão definidos nos termos de regulamento.
- § 2º O responsável citado no caput deste artigo, independentemente do ressarcimento por perdas e danos ao lesado, estará sujeito ao pagamento de multa variável de R\$ 2.000,00 (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.
- § 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.

PL 84/1999

ASPECTOS PROCEDIMENTAIS-ADMINISTRATIVOS -

Art. 22



JURISPRUDÊNCIA CRIMINAL (PESQUISA)

99% Condenatória dos Maiores Tribunais Estaduais (Crimes Eletrônicos COMUNS):

- * Ofensa à honra (difamação, injúria, calúnia – eletrônicas)
- * Pedofilia

Escassa e Insegura quanto aos crimes cibernéticos próprios (absoluções por atipicidade):

- * Phishing-Scam
- Difusão de Vírus
- Ataque/DNS + Negação Serviços

- TRIBUNAL DE JUSTIÇA DE SP - Apelação Criminal nº 993.07 .031921-6

- Relator DESEMBARGADOR LOPES DA SILVA (j. em 2010)

- **Absolvição de acusação do “phishing scam”** (art. 10 da Lei 9296/96):

- “ Art. 10. Constitui crime **realizar interceptação** de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.”

- Texto do acórdão-fundamentação:

- **“..... Não há propriamente uma interceptação, mas, sim, uma invasão seguida da indevida captação dos dados dos correntistas, isto é, número de contas bancárias, de cartão de créditos e respectivas senhas.**
- **De qualquer forma, a conduta efetivamente imputada neste processo, não obstante rotulada como interceptação de comunicação de informática, como a própria denúncia descreve e restou amplamente confessada pelo apelante Tiago, aliás compatível com a documentação apreendida com os acusados, é a de furto pela internet, que é objeto de outro processo.”**

■ Tribunal de Justiça de São Paulo - Apelação Criminal nº 941.943.3/6 – 1ª. Câmara Criminal do TJSP, 14.12.2007 –

■ Relator Desembargador José Coelho, Relator

■ “ A denúnciaimputa....conduta de, mediante emprego de senhas de terceiros, obtidas clandestinamente, terem furtado tempo de acesso à Internet. Obtendo por meios ainda desconhecidos arquivo de dados contendo nomes e senhas de usuários de determinado provedor de acesso à Internet, os apelados teriam efetuado conexão (por meio de ligações telefônicas) com o provedor e, apresentando nomes e senhas de terceiros, teriam também conseguido acesso ao conteúdo da rede mundial de computadores, isto em várias ocasiões.”

■ nomes e senhas teriam sido assim indevidamente utilizados.A respeitável sentença - a meu ver acertadamente -reconheceu a atipicidade da conduta.O objeto da pretensa subtração não seria propriamente o

■ tempo de acesso à internet, mas sim o conteúdo acessado, vale dizer, as

■ informações, consubstanciadas em imagens, sons (voz) e escrita. Apenas para efeito da exploração econômica do fornecimento a tais informações é que se institui a cobrança conforme a duração, no tempo, do acesso a elas.

■ Informações são algo essencialmente abstrato, incorpóreo.

■

■ Assim, tal como se dá com direitos e ações, todos os bens incorpóreos não são passíveis de furto.

-informações não têm o menor vínculo com
- qualquer forma de energia (artigo 155, § 3º, do Código Penal). São coisas ontologicamente diferentes. Assim, a equiparação entre ambas, como pretendido no recurso, vai além da analogia in mala partem, esta que já seria vedada no âmbito do direito penal.
- Muito menos a informação poderia ser confundida com o
- pulso telefônico, este um mero meio de transmissão dos dados. Os apelados.....efetuaram ligação telefônica para o provedor de acesso à internet. E pelos pulsos telefônicos consta que efetuaram o pagamento correspondente, à concessionária deste serviço público. Sendo assim, por aí já se vê que não se deu qualquer desvio ou subtração de energia eletromagnética (pulso telefônico). O que os apelados teriam obtido, indevidamente, foi algo distinto dos pulsos telefônicos, a saber, a informação (imagem, voz e dados) fornecida pelo provedor e cobrada à parte da ligação telefônica. Tão impossível se mostra a subtração de conteúdo de informação como seria impossível, numa conversa telefônica qualquer, furtar as idéias comunicadas pela fala, entre uma pessoa e outra.
- Pelo que se expôs já se percebe que a subtração de informação não é juridicamente possível e escapa por completo à tipificação dada
- pelo artigo 155 e §§ do Código Penal

A PROPOSTA
ALTERNATIVA AO PL
84/99

2 Crimes: Acesso
Indevido +
Inserção/Difusão de
Vírus

Acesso indevido a sistemas informatizados

- Art. 285-A Invadir rede de computadores, dispositivo de comunicação ou sistema informatizado sem autorização de seu titular com o fim de obter vantagem ilícita.
 - Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.
-
- 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.

FIM

ARTIGO: “O BRASIL DOS CRIMES ELETRÔNICOS”
(<http://www.aliceramos.com/view.asp?materia=1440>)

*Fernando Neto Botelho –
fernandobotelho@terra.com.br*