Necessidade de lei criminal específica para a Internet

17/11/09 – OEA – RJ/RJ

Gilberto Martins de Almeida
mda@all.net.br

História longa, regulação crescente, e irreversível

2003: Lei 10.764 - Alterou o ECA, ref. **pedofilia** na Internet

2003: Lei 10.695 - Alterou o Código Penal – Violação de **direito de autor**

2001: **Convenção de Budapeste**

2000: Lei n. 9.983 – Altera o crime de **peculato**, no Código Penal

2000: PLS 76 Sen. Renan Calheiros – **crimes cibernéticos**

1999: Operação **Catedral** – Rio de Janeiro

1998: Operação **Catedr**al – Interpol

1998: STF julga **pedofilia** on-line

1996: Lei 9.296, art. 10 – Crime **interceptação** sem autorização judicial ou objetivo definido em lei

1996: PLS Sen. Julio Campos – crime contra **inviolabilidade de comunicação** de dados

1995: PLC 1713 Dep. Cássio Cunha Lima (depois, PLC 84/99, Dep. Luiz Piauhylino) – **crimes cibernéticos**

1995: Lei 9.100, art. 67 – **Fraude eleitoral eletrônica**

1986: **Primeiro caso judicial** brasileiro ref. crime informático, no Rio de Janeiro (fraude na IBM)

1984: **Primeira lei** de crimes de informática (em 1986, Computer Fraud and Abuse Act – EUA)

1977: **Primeira proposta** de legislação de crimes informáticos (Sen. Ribikoff – EUA)

I – Hacker deve ser absolvido

“Veja-se que posicionamentos contrários – como a recente decisão argentina que desconsiderou a invasão do website do Judiciário local por um hacker, entendendo que só há crime quando afetados pessoas, animais ou coisas e que um website na internet não se encaixa em nenhuma dessas categorias – parecem ignorar que a prova pericial pode demonstrar a materialidade eletrônica (registros eletromagnéticos, presentes no computador-servidor e no computador-cliente, e rastreáveis) de um website na internet, satisfazendo o conceito de coisa.)”

II – Hacker deve ser condenado

NEGADO PEDIDO DE LIMINAR EM HABEAS-CORPUS A "HACKER"

O vice-presidente Sálvio de Figueiredo, presidente em exercício do Superior Tribunal de Justiça (STJ), indeferiu pedido de liminar em habeas-corpus em favor de César Cristóvão Munhoz, acusado de liderar quadrilha de fraudes bancárias pela internet. O acusado foi preso há 109 dias pela polícia de Goiás, em Nova Xavantina, Mato Grosso. Munhoz comprava cópias de páginas de banco de um programador por R$ 300 e enviava as páginas clonadas a milhares de usuários por meio de um e-mail falso. Ao abrirem o e-mail, as vítimas tinham suas senhas e os números das contas copiados pelos hackers. A quadrilha sacava o dinheiro das contas que possuíam os maiores saldos e transferiam para contas de correntistas "laranjas". O habeas-corpus impetrado pela defesa de Munhoz argumenta que o prazo de prisão preventiva excedeu e requer a imediata soltura do acusado. Munhoz já teve um pedido de liminar em habeas-corpus negado pelo Tribunal de Justiça de Goiás. O ministro Sálvio de Figueiredo alegou ser inadmissível o habeas-corpus contra indeferimento de liminar, a não ser que a ilegalidade esteja evidente. O caso não configura constrangimento ilegal, já que o excesso de prazo na formação da culpa exclui o constrangimento por força do princípio da razoabilidade. Baseado nisso, o ministro indeferiu a liminar, requisitou informações e determinou vista ao Ministério Público Federal. O processo será apreciado pelo ministro relator, Nilson Naves, tão logo retorne do MPF. Fonte: **STJ**

I – Empresas não podem monitorar e-mail

TRT-SP Nº. 20000 34734 0

RECURSO ORDINÁRIO DA 37ª VT DE SÃO PAULO

EMENTA: Justa causa. “Email” não caracteriza-se como correspondência pessoal. O fato de ter sido enviado por computador da empresa não lhe retira essa qualidade. Mesmo que o objetivo da empresa seja a fiscalização dos serviços, **o poder diretivo cede ao direito do obreiro à intimidade** (CF, art.5º, inc.VIII). Um único “Email”, enviado para fins particulares, em horário de café, não tipifica justa causa. Recurso provido.

II – Empresas podem monitorar e-mail

NÚMERO ÚNICO PROC: RR - 613/2000-013-10-00 **PUBLICAÇÃO:** DJ - 10/06/2005
PROC. Nº TST-RR-613/2000-013-10-00.7 A C Ó R D Ã O 1ªTurma JOD/rla/jc

PROVA ILÍCITA. "E-MAIL" CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO.

1. Os **sacrossantos direitos do cidadão à privacidade e ao sigilo de correspondência**, constitucionalmente assegurados, concernem à comunicação estritamente pessoal, ainda que virtual ("e-mail" particular). Assim, apenas o e-mail pessoal ou particular do
empregado, socorrendo-se de provedor próprio, desfruta da proteção constitucional e legal de inviolabilidade.

2. Solução diversa impõe-se em se tratando do chamado "e-mail" corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é
disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma
ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço.

3. A estreita e cada vez mais intensa vinculação que passou a existir, de uns tempos a esta parte, entre Internet e/ou correspondência eletrônica e justa causa e/ou crime exige muita **parcimônia** dos órgãos jurisdicionais na qualificação da ilicitude da prova referente ao desvio de finalidade na utilização dessa tecnologia, tomando-se em conta, inclusive, o **princípio da proporcionalidade** e, pois, os diversos valores jurídicos tutelados pela lei e pela Constituição Federal. A experiência subministrada ao magistrado pela observação do que ordinariamente acontece revela que, notadamente o "e-mail" corporativo, não raro sofre acentuado desvio de finalidade, mediante a utilização abusiva ou ilegal, de que é exemplo o envio de fotos pornográficas. Constitui, assim, em última análise, expediente pelo qual o empregado pode provocar expressivo prejuízo ao empregador.

I – Não há direito de privacidade ao de/para

"Investigação Criminal – Requisição para que seja apresentado o número de chamadas entre aparelhos telefônicos – Violação do art. 5.º, XII, da Constituição Federal – Inocorrência: 96(b) – Inocorre violação ao princípio constitucional da inviolabilidade do sigilo das comunicações telefônicas, caso para fins de investigação criminal, se pretenda somente a obtenção dos números de chamadas entre aparelhos telefônicos, não sendo pretendida a escuta ou a conversação telefônica entre pessoas, vez que, nessa hipótese, inocorre invasão da privacidade."

II – Há direito de privacidade para cadastros

ProcessoRHC **8493** / SP RECURSO ORDINARIO EM HABEAS CORPUS 1999/0024439-7

Relator(a) Ministro LUIZ VICENTE CERNICCHIARO (1084) **Órgão Julgador**T6 - SEXTA TURMA**Data do Julgamento**20/05/1999**Data da Publicação/Fonte**DJ 02.08.1999 p. 224 JSTJ vol. 9 p. 402 REVFOR vol. 350 p. 375

RHC - CONSTITUCIONAL - PROCESSUAL PENAL - **INFORMAÇÕES CADASTRAIS -SIGILO** - Quando uma pessoa celebra contrato especificamente com uma empresa e fornece dados cadastrais, a idade, o salário, endereço. É evidente que o faz a fim de atender às exigências do contratante.Contrata-se voluntariamente. Ninguém é compelido, é obrigado a ter aparelho telefônico tradicional ou celular. Entretanto, aquelas informações são reservadas, e aquilo que parece ou aparentemente é algo meramente formal pode ter conseqüências seríssimas; **digamos,uma pessoa, um homem, resolva presentear uma moça com linha telefônica que esteja no seu nome. Não deseja, principalmente se for casado, que isto venha a público.** Daí, é o próprio sistema da telefonia tradicional, quando a pessoa celebra contrato, estabelece,como regra, que o seu nome, seu endereço e o número constarão no catálogo; entretanto, se disser que não o deseja, a companhia não pode, de modo algum, fornecer tais dados. Da mesma maneira, temos cadastro nos bancos, entretanto, de uso confidencial para aquela instituição, e não para ser levado a conhecimento de terceiros.

Lição da experiência: necessidade de lei para evitar oscilação dos julgados e para atualizar regras

Pedofilia

- 1998 – STF: Internet está implícita no ECA (“produzir” e publicar”)
- 2000 – TJ-RJ concede habeas corpus
- 2003 – Reforma ECA (“vender” e “divulgar”)
- 2008 – Nova reforma ECA (“reproduzir” e “agenciar”)

O tipo de criminalidade está mudando e a Internet é um dos maiores focos de perigos

Tipos penais

- 1942 – 1957: criados 100 tipos de dano, <u>14 de perigo</u>, e 8 híbridos
- 1985-2000: criados 200 tipos de dano, <u>144 de perigo</u>, e 28 híbridos

(Juliana Cabral, “Os tipos de perigo & a pós-modernidade”, Revan, RJ, 2005, p. 143)

References in the Federal Constitution:
- Security: 15; ii) Privacy: 1

References in search at Rio’s Higher Court web site:
- Security: 300; Privacy: 37

Necessidade de normas legais cíveis e/ou de normas técnicas preenchendo tipos penais

ISO	LEIS
9000 (1987)	Cód.Consumidor (1990)
14000 (1996)	Cód. Civil (2002) / Sarbanes-Oxley (2002)
20000 (2005) / 27000 (2005)	Crimes Eletr. (ECA -2003/08)

ITIL: 1a. versão (80´s); 2a. versão (2001); 3a. Versão (2008)

Os problemas não permitem esperar mais pela introdução de lei penal específica

Fatos:

- Divergências (invasão sem danos; “dado”; analogia; análise de tráfego; competência)
- Cooperação incerta e “informal” ISPs/Telcos (aparelhos; informações; “acordos”)
- Cooperação internacional também “informal”
- Tipos específicos têm sido bem julgados (peculato; direitos de autor; eleições)
- Desafios (criptografia; cloud computing)

Necessidade:

- Lei específica (crimes; terminologia; cooperação)

Obrigado!

Classe / Origem
HABEAS CORPUS **Relator**
Ministro SEPULVEDA PERTENCE **Publicação**
DJ DATA-06-11-98 PP-00003 EMENT VOL-01930-01 PP-00070 **Julgamento**
22/09/1998 - Primeira Turma **Ementa**

EMENTA:

"Crime de Computador": publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores, atribuída a menores: tipicidade: prova pericial necessária à demonstração da autoria: HC deferido em parte.

1. O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" — ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador.

2. **Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia**: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.

3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial.

Observação

Votação: Unânime.

ECA – pedofilia eletrônica

(se a prova depende) "de informações técnicas de telemática, que pairam acima do conhecimento do homem comum, impõe-se a realização de prova pericial", "A invenção da pólvora não reclamou redefinição do homicídio(..) basta-lhe a idoneidade técnica do meio utilizado." (HC 76.689/PB, STF, 1a. Turma, 22/09/98, Min. Sepúlveda Pertence)

Decisão da Justiça surpreende e pára caso de pedofilia na Web

Por André Felipe Lima
Repórter Canal Web

O combate à pedofilia na Internet no Rio de Janeiro sofreu um tropeção inesperado. Por decisão do Tribunal de Justiça do estado, um dos 15 réus que respondem por tráfego de fotos na Rede de abuso sexual contra crianças, teve um pedido de habeas corpus aceito. Com esta postura da Justiça, o caso fica suspenso.

Os inquéritos foram iniciados a partir de investigações da operação Catedral-Rio, realizada em outubro do ano passado, pelo Ministério Público do Estado do Rio. A grande maioria das residências investigadas na operação fica na zona sul do Rio, e todos os que respondem os inquéritos são de classe média para cima.

19/9/2000 - [Segurança]

- **Pedofilia** - Artigo 241 do Estatuto da Criança e do Adolescente: “Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:

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

“§ 1º Incorre na mesma pena quem:

I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;

II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;

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.”

PLC 89

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, 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:

....." (NR)

Edit View Favorites Tools Help
Back Search Favorites
http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf Go
Conv OK Favoritos 153 bloqueado Verificar Enviar para Convenção de Budapeste
162%

Título 3 – Infracções relacionadas com o conteúdo

Artigo 9º - Infracções relacionadas com pornografia infantil

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:

   a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;

   b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;

   c) Difundir ou transmitir pornografia infantil através de um sistema informático;

   d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;

   e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.

6 of 28 8.26 x 11.69 in
Internet

PLC 89

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

PLC 89

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;

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.

Edit View Favorites Tools Help
Back Search Favorites
http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf Go
Favoritos 153 bloqueado Verificar Enviar para Lei 10.446
162%

Capítulo I –Terminologia

Artigo 1º - Definições

Para os fins da presente Convenção:

a) "Sistema informático" significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;

b) "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;

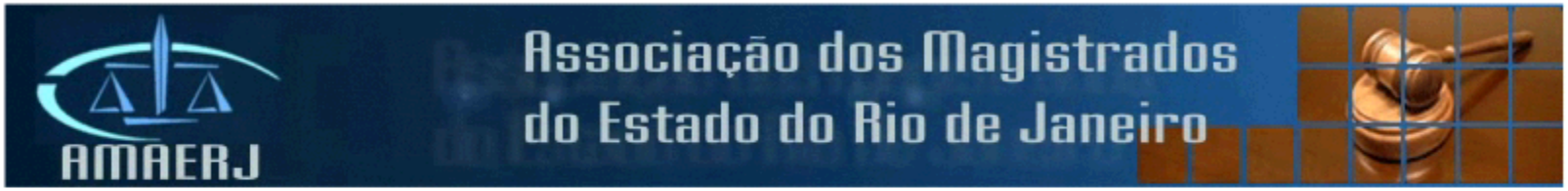
c) "Fornecedor de serviço" significa:

(i) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático e

(ii) Qualquer outra entidade que processe ou armazene dados informáticos em nome do referido serviço de comunicação ou dos utilizadores desse serviço.

3 of 28 8.26 x 11.69 in
Internet

Edit View Favorites Tools Help
Back Search Favorites
http://www.amaerj.org.br/index.php?option=content&task=view&id=306
Go
Favoritos 153 bloqueado Verificar Enviar para Hacker Judiciario Argentina ley



Banner - IV Jogos

INTERNET: CRIMES, IMPRENSA, JUSTIÇA

Gilberto Martins

< anterior | próximo >

A internet, ferramenta de caráter multifacetado, ainda representa um desafio ao Judiciário. Mecanismos de controle aos centros produtores de informação independentes estão por ser desenvolvidos. Gilberto Martins de Almeida é favorável à adoção de um tratado internacional sobre a questão, assim como defende outras iniciativas, expostas neste artigo.

Na década de 1970 Michel Foucault já dizia que o poder se instaura "de maneira móvel e circular", como uma rede, e que "a visibilidade é uma armadilha". Por essa mesma época nascia a internet, com fins acadêmicos e militares. Hoje, na visão de Pierre Lévy, a chamada grande rede marca a passagem da multimídia à hipermídia, a formação de imenso mercado e banco de

Internet

Edit View Favorites Tools Help
Back Search Favorites
http://www.ndc.uff.br/portaldereferencia/noticias.asp?cod=1042 Go
a ley OK Favoritos 153 bloqueado Verificar Enviar para Hacker Judiciario Argentina ley Configuraç

A programação completa da SEMARQ está disponível em nosso site: www.aaerj.org.br

A AAERJ deseja que a atividade seja dotada de grande sucesso. Parabenizamos aos estudantes da UFF pela iniciativa de realizar um grandioso evento.

SITE DA AAERJ

Durante boa parte do mês de outubro, o site da AAERJ esteve fora do ar devido a um ataque hacker. Nosso site vem sofrendo ataques seguidos, que lamentavelmente, prejudicam o trabalho da associação e o direito público dos associados e dos usuários de buscarem informação. O objetivo primordial do sítio da AAERJ é informar a classe com notícias de interesse arquivístico e de oportunidades de trabalho, estágio e concurso público.

Felizmente, o problema foi superado e o site está de volta com força total. Fiquem sempre atentos a tudo que ocorre de mais importante na área. Acesse: www.aaerj.org.br

---

ERRATA

Na edição nº 25 deste Informativo, divulgamos que seria realizada uma Conferência sobre a Arquivologia na Paraíba, UEPB, no dia 28 de outubro. Na verdade, a referida Conferência foi promovida no mês de setembro.

Para enviar matérias, artigos, sugestões, críticas
Mande um email para a comissão responsável:

Carlos Frederico Machado
Patrícia Kelly dos Santos
Victor Costa
Wagner Ramos Ridolphi
informativo@aaerj.org.br

Data de publicação: 11/17/2006

Internet

PLC 89

“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.

Sem responsabilidade por guardar dados

- Os provedores de acesso a Internet, recebem milhares de acessos diários em suas páginas virtuais e **não há nada que os obriguem a manter o número do IP** (endereço que fica registrado quando uma mensagem é enviada, sendo possível buscar-se o seu autor) de todos os usuários da rede que acessem tais páginas." (Ap. Cív. n. 107.704-3, j. 05/09/01, Rel. Des. José Wanderlei Resende, Apte. Elaine Cristina Denkewski, Apda. Terra Networks Brasil S/A

PLC 89

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 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;

Veja 03/03/99 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://veja.abril.com.br/030399/p_070.html Go Links
Google prove OK Favoritos 153 bloqueado Verificar Enviar para provedor Clinton ameaça Configurações

Terror de brincadeira

Bruno: ameaça a Clinton deflagra investigação

Foto: Marcos Hermes

— *Mr. President, I will kill you.*

— Senhor presidente, vou matá-lo — a mensagem deixou em sobressalto o serviço de correspondências eletrônicas da Casa Branca, sede do governo americano. Todos os dias, dos quatro cantos do mundo, são feitas 300 ameaças virtuais contra Bill Clinton. Aquela, enviada em janeiro passado, era incomum. Curta e enfática, vinha do Brasil. Soou o alerta. Todas as ameaças, veladas ou não feitas ao presidente dos Estados Unidos, são investigadas. O agente do Serviço Secreto Alex Echo, cubano naturalizado americano, foi destacado para investigar o caso. Com base nas informações contidas no cabeçalho da mensagem, Echo rastreou a origem do e-mail. Descobriu o provedor, uma pequena empresa com sede em São Paulo. Faltava, porém, chegar ao autor do texto. Na internet, ele utilizava o nome "Bruno". Só poderia ser uma identificação falsa ou um apelido. Quem se esconderia por trás

Done Internet
start 11:13 AM

PLC 89

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.

Edit View Favorites Tools Help
Back Search Favorites
http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf Go
Favoritos 153 bloqueado Verificar Enviar para Lei 10.446
162%

Artigo 15º - Condições e salvaguardas

1. Cada Parte assegurará que o estabelecimento, a entrada em vigor e a aplicação dos poderes e procedimentos previstos na presente Secção são sujeitos às condições e salvaguardas estabelecidas pela legislação nacional, que deve assegurar uma protecção adequada dos direitos do Homem e das liberdades, designadamente estabelecidas em conformidade com as obrigações decorrentes da aplicação da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e das Liberdades Fundamentais dos Cidadãos (1950), do Pacto Internacional das Nações Unidas sobre os Direitos Civis e Políticos, (1966), bem como de outros instrumentos internacionais aplicáveis relativos aos Direitos do Homem e que deve integrar o princípio da proporcionalidade.

2. Quando for apropriado, tendo em conta a natureza do poder ou do procedimento em questão, as referidas condições e salvaguardas incluirão, designadamente, um controlo judicial ou outras formas de controlo independente, os fundamentos que justificam a sua aplicação, bem como a limitação do âmbito de aplicação e a duração do poder ou procedimento em causa.

3. Na medida em que seja do interesse público, em particular da boa administração da justiça, cada Parte examinará o efeito dos poderes e dos procedimentos da

9 of 28 8.26 x 11.69 in
Internet

Edit View Favorites Tools Help
Back Search Favorites
http://blogdaunr.blogspot.com/2008/08/hacker-brasileiro-preso-na-holanda.html Go
a ley OK Favoritos 153 bloqueado Verificar Enviar para Hacker Judiciario Argentina ley Configuraç

Brasileiro é preso na Holanda por administrar rede gigante de computadores infectados

Um brasileiro que administrava e pretendia vender o acesso a uma rede de **100 mil computadores infectados** foi preso na Holanda, graças a uma **investigação iniciada pelo FBI** e pelo departamento de crimes cibernéticos da **Polícia Federal brasileira.**

Leni de Abreu Neto, de 35 anos, é acusado de manter e permitir o acesso à rede de computadores infectados, que ele **tentou vender para outros hackers,** de acordo com a denúncia de um júri federal de Nova Orleans. Se condenado, Leni pode pegar até cinco anos de prisão e multas que passariam de US$ 250 mil.

Segundo a denúncia, o holandês Nordin Nasiri, de 19 anos, foi o responsável pela infecção dos computadores espalhados por todo o mundo. **Leni fazia uso da rede e pagava os servidores.** Os dois teriam feito um acordo para vender a rede infectada por cerca de US$ 37 mil. Os PCs "zumbis" poderiam ser usados para distribuir spams ou lançar ataques para tirar websites do ar.

A **polícia holandesa prendeu Neto** no dia 29 de julho, graças a informações do FBI e de policiais brasileiros. Ele atualmente está preso na Holanda, aguardando o processo de extradição. O cúmplice está sendo procurado

Você é o Visitante N°

0 0 0 1 9 8 5 9

Bandeira do Brasil

Símbolo Nacional

Hino Nacional Brasileiro

Hino Nacional Brasileiro

Ouviram do Ipiranga as margens plácidas
De um povo heróico o

Internet

INTERNET ***Folha de S. Paulo*** **China também invadiu rede britânica, diz jornal**

"Depois de atingir o Pentágono e a Chancelaria alemã, a guerra cibernética chegou ao governo britânico. Ainda sob o impacto causado pelas invasões de computadores do Departamento da Defesa americano e do governo alemão, o jornal londrino 'The Guardian' noticiou ontem que as redes de vários ministérios britânicos, incluindo o das Relações Exteriores e o da Defesa, sofreram ataques recentemente.

Como nos casos anteriores, o maior suspeito é o Exército chinês, que, segundo especialistas ocidentais, estaria usando a pirataria eletrônica como forma de espionar e desestabilizar seus adversários. O governo chinês nega com veemência as acusações, que chama de 'absurdo', fruto de uma 'mentalidade da Guerra Fria'.

Na última terça-feira, autoridades americanas disseram que militares chineses invadiram em junho uma rede informatizada do Pentágono, no que foi considerado o mais bem-sucedido ataque cibernético já sofrido pelo Departamento da Defesa dos EUA.

O ataque obrigou o Pentágono a fechar parte de um sistema de computadores do gabinete do secretário da Defesa, Robert Gates, e especialistas do governo citados pelo jornal 'Financial Times' afirmaram que uma investigação apontara o Exército de Libertação Popular como a origem da infiltração.

Rede vulnerável

O presidente americano, George W. Bush, admitiu que os EUA são vulneráveis a ataques cibernéticos e disse que poderá levantar a questão no encontro que terá hoje com o presidente da China, Hu Jintao. Eles estão em Sydney, na Austrália, para a cúpula da Apec (Cooperação Econômica da Ásia e do Pacífico).

Para Bush, é essencial que parceiros comerciais respeitem 'os sistemas e bases de conhecimentos' uns dos outros. 'É o que esperamos das pessoas com quem negociamos', disse.

Além da conveniência que a internet proporcionou aos governos de países desenvolvidos em suas relações políticas e comerciais, a rede mundial de computadores também criou uma vulnerabilidade para a qual ainda não há remédios infalíveis. Na semana passada, a revista 'Der Spiegel' afirmou que hackers chineses haviam invadido computadores do governo utilizando um vírus disfarçado do programa Word.

Sobre a reportagem publicada pelo 'Guardian' ontem não houve reação oficial. Mas um especialista em segurança do governo britânico confirmou que são freqüentes as tentativas chinesas de penetrar nos computadores do Estado.

'Eles estão interessados em informação científica e tecnológica, civil e militar', disse ele à agência Reuters, que não identificou sua fonte. 'Estão interessados na aquisição de inteligência política e econômica. E estão interessados em monitorar dissidentes.'

Sandra Bell, analista do Royal United Services Institute, de Londres, comentou que a divulgação das ações de hackers por duas semanas consecutivas parece indicar uma disposição das potências ocidentais em sinalizar ao regime chinês que tais atividades são intoleráveis.

'A comunidade internacional parece estar dizendo: 'Sabemos quem está fazendo e é bom que isso acabe', disse Bell.

Outros observadores lembram que pensadores militares chineses há muito debatem o uso de pirataria cibernética como parte de uma estratégia que definem como 'guerra assimétrica', a qual compensaria a desvantagem em recursos bélicos convencionais de Pequim em relação a seus rivais.

'Na era da informação, a influência de uma bomba atômica é talvez menor que a de um hacker', comenta um relatório do Exército chinês de 1999, intitulado 'Guerra ilimitada'."

PLC 89

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.

BBCBrasil.com | Reporter BBC | Estônia acusa Rússia de 'ataque cibernético' ao país - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.bbc.co.uk/portuguese/reporterbbc/story/2007/05/070517_estoniaataquesinternetrw.shtml Go Links
Google Estôr OK Favoritos 153 bloqueado Verificar Enviar para Estônia ataques Internet Configurações

Primeira Página
Ciência & Saúde
Cultura & Entretenimento
Vídeo & Áudio
Fotos
Especial
Interatividade
Tempo
Aprenda inglês
RÁDIO
Programação
Como Sintonizar
SERVIÇOS
Newsletter
Ajuda
Sobre a BBC
Expediente
Parceiros
Empregos
Fale com a gente
SERVIÇO MUNDIAL
ESPAÑOL
PORTUGUÊS - ÁFRICA
عربي

Atualizado às: 17 de maio, 2007 - 10h43 GMT (07h43 Brasília)

Envie por e-mail Versão para impressão

Estônia acusa Rússia de 'ataque cibernético' ao país

Laura Sheeter
De Tallinn (Estônia)

O governo da Estônia afirma que seu país está sob um "ataque cibernético" russo contra seus sites na internet desde a polêmica retirada de um monumento de guerra soviético do centro da capital do país, Tallin.

Retirada do monumento do centro de Tallinn gerou protestos em abril

Há três semanas, a remoção da estátua, que comemorava os soldados do Exército Vermelho que combateram os nazistas na Segunda Guerra Mundial, provocou confrontos nas ruas de Tallin que deixaram ao menos um morto e vários feridos e detidos.

A retirada do monumento também provocou uma crise nas relações entre a Estônia e a Rússia. O governo russo classificou a atitude do governo estoniano de "um insulto" contra os soldados que morreram para livrar a região dos

NOTÍCIAS RELACIONADAS
- Remoção de estátua causa mais violência na Estônia
  28 de abril, 2007 | Notícias
- Remoção de estátua acaba em protesto e morte na Estônia
  27 abril, 2007 | BBC Report

ÚLTIMAS NOTÍCIAS
- Parlamento russo apóia autonomia da Ossétia e Abecásia
- Ex-premiê deixa coalizão de governo no Paquistão
- Democratas buscam união em convenção
- Corte saudita julga pedido de divórcio de garota de 8 anos

Done Internet
start 11:03 AM

PLC 89

“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:

Páginas falsas e seus aliados (Matéria) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://superdownloads.uol.com.br/materias/paginas-falsas-seus-aliados/229,1.html Go Links

Google falsa OK Favoritos 153 bloqueado Verificar Enviar para página falsa Configurações

Páginas falsas e seus aliados

Da redação em 08/Abr/2004

BOOKMARK Aimensa quantidade de páginas falsas disponíveis na Internet, principalmente de instituições bancárias, tem se mostrado um grande problema na vida dos internautas. Elas dificultam a vida de muitos usuários que simplemente levam prejuízos, e causam, além de constrangimentos e problemas financeiros,
falta de confiança no serviço prestado via Internet e também dificuldades para conseguirem o dinheiro de volta.

Na maioria das vezes as páginas falsas usam simplesmente um endereço semelhante, mas com pequenas diferenças em seu nome como, por exemplo: www.bradescoo.com.br (repare, dois "o" no final). Além do método citado acima, existem outros os quais não entraremos em detalhes, mas que são igualmente perigosos.

Recentemente foi descoberta uma "pequena" falha, que pode comprometer ainda mais os usuários. Esta falha, localizada no Internet Explorer, tenta enganar o usuário, fazendo com que o conteúdo de uma página falsa seja apresentado, mas com o endereço verdadeiro.

Veja um exemplo do funcionamento desta falha:

Se seu anti-vírus mostrar uma mensagem quando você clicar no botão abaixo não se preocupe, é sinal que você estará sempre sendo avisado quando spoofs como esse aparecerem. Não é nenhum vírus.

Testar falha

Com este pequeno código, ao ser pressionado o botão, o conteúdo da página http://www.unibanco.com.br será apresentado, mas o endereço será

Done Internet

start 11:09 AM

PLC 89

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

“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:

.....”(NR)

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

“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:

Terra - Vírus e Cia - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://informatica.terra.com.br/interna/0,,OI480348-EI559,00.html

Colunistas
Download
E-business
Games
Imagens
Vírus e Cia.

Macmania
Outer Space
Tucows

Especiais
- Spam
- Cartilha de segurança
- Guia de compras
- Banda larga
- Windows XP
- Mais especiais

Vírus e Cia

Terça, 1 de março de 2005, 13h25

Sexkut é isca para novo golpe na Internet

Um convite para entrar no Sexkut, rede de relacionamento sexual similar ao Orkut, está invadindo as caixas postais de internautas. Mas é uma mensagem falsa: trata-se de mais uma tentativa de golpe para enganar usuários desavisados e fazê-los baixar um arquivo malicioso.

A falsa página do Sexkut aponta para um endereço "myhome.bananaweb" com um link que termina em "Cadastro.exe". Ou seja, um arquivo executável que certamente é perigoso.

A mensagem recebida por Terra Informática veio com a seguinte linha de assunto (Subject:) *Cadastre-se agora mesmo!*. No campo do remetente (From:) consta o e-mail *cadastro@sexkut.com*

Se você receber tal mensagem, basta apagá-la, sem baixar o arquivo sugerido.

Golpes online
As fraudes por e-mail normalmente utilizam o nome de instituições ou atividades conhecidas. Banco do Brasil, Editora Abril, Big Brother Brasil e Show do Milhão, entre outras, já foram utilizados como isca. O internauta recebe uma mensagem que oferece promoções, convida para

Multimídia
Infográfico

» Clique para ver maior

Notícias
» Sexkut: site de paródias 'apronta' mais uma
» Sexkut põe no ar uma rede de relacionamento sexual

Últimas sobre Vírus e Cia
» Acusado de matar por comentário em site é solto
» McAfee alerta para mensagem falsa da VoxCards
» Netsky.P é o vírus mais agressivo do mundo
» Novo vírus usa fofocas de Hollywood como isca

Busca
Saiba mais na Internet sobre:
Download

Torpedo Terra
Fique bem informado com o serviço de Notícias do Terra no seu celular!
» SAIBA MAIS

TerraShopping
MINICAM CÂMERA
3 Funções em 1 só Produto. Aproveite!
Apenas 9x R$14,11
SEU PC TEM ERROS?
Acelere e otimize seu PC em 5 minutos.
Imperdível.
MINI CÂMERA ESPIÃ
Sem Fios e de Fácil Camuflagem.
Frete Grátis Hoje!
SUPER BINÓCULO
Alcance de 1Km e lentes a prova d água
Compre Hoje!
EXTRA.COM.BR

Low Battery
You should change your battery or switch to outlet power immediately to keep from losing your work.

Internet

start 11:16 AM

PLC 89

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 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.

§ 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.”

Edit View Favorites Tools Help

Back Search Favorites

http://www.pichacao.com/ Go

Favoritos 153 bloqueado Verificar Enviar para pichação com

PICHAÇÃO.COM | info@pichacao.com **English version**

APRESENTAÇÃO | PRESENTATION

O site pichacao.com foi concebido tendo como base a pesquisa de mestrado (Os Tipos Gráficos da Pichação). O conteúdo do site a princípio ficaria restrito à pesquisa, mas com o tempo foram incorporados outros assuntos. Sendo assim, qualquer contribuição relativa ao assunto pode ser enviada. Se o assunto for relevante será incorporado ao site.

O autor do site tem atualmente três produções relacionadas ao tema.

A primeira é uma fonte digital chamada Adrenalina. Você pode ter mais detalhes sobre o projeto clicando aqui ou pode compra-la direto pelo site Myfonts.com.

A segunda produção é um website de nome Pich(x)ação selecionado para o FILE 2006. O web site tem a finalidade de criar experimentação digital usando como inspiração: fotos, sons e letras de pichação capturadas em São Paulo - Brasil. Veja o site clicando aqui.

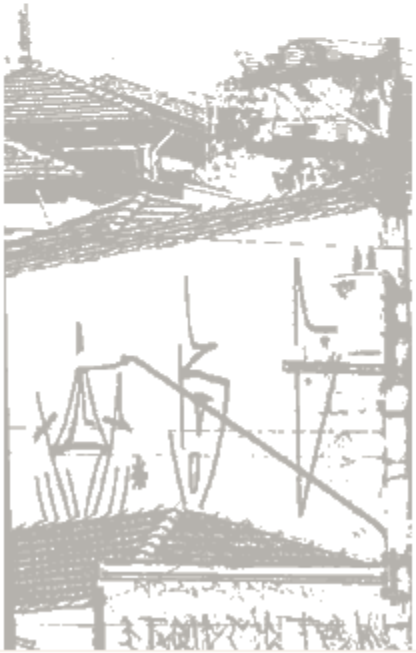
O terceiro produto é uma pequena seleção de fotos de pichação com comentários divertidos intitulada Devaneios Pichográficos. As fotos foram selecionadas dentre mais de 1.000 fotos tiradas no bairro da Mooca em São Paulo entre 2005 e 2006. Veja as fotos clicando aqui.

www.gustavolassala.com

Site Pich(x)ação

Digital font Adrenalina

Devaneios pichográficos (Flickr)



Internet

INFO Online - Plantão Info - Verme Fili envia e-mails e desativa firewall - (06/10/2004) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://info.abril.com.br/aberto/infonews/102004/06102004-13.shl Go Links
Google desat OK Favoritos 153 bloqueado Verificar Enviar para desativa firewall Configurações

[an error occurred while processing this directive]

plantão info / Tecnologia Pessoal

Verme Fili envia e-mails e desativa firewall

Quarta-feira, 06 de outubro de 2004 - 18h32

SÃO PAULO – O verme W32.Fili@mm, também identificado como Bloodhound ou I-Worm.VB.q, se dissemina via Outlook, redes de compartilhamento de arquivos e canais de bate-papo. Além disso, desativa programas de segurança.

O Fili chega como anexo de e-mail, num arquivo executável de extensão .scr, .pif, .bat, .com, .cmd ou .exe. O assunto da mensagem varia, mas dois deles, em inglês, são algo como "Ajude-nos a manter nosso direito à liberdade de expressão".

Ao se instalar na máquina, o Fili tenta localizar os diretórios de programas de compartilhamento, onde deposita cópias de si mesmo que fingem ser programas de interesse. Em seguida, o invasor envia cópias de si mesmo para todos os contatos no livro de endereços do Outlook.

O próximo passo do programa intruso é localizar programas de bate-papo como o objetivo de auto-enviar-se por esse canal. Por fim, ele tenta desativar programas de segurança como antivírus e firewalls. O Fili é classificado com nível de risco médio-baixo.

Carlos Machado, da INFO

iPhone estréia em 10 países da AL (25/08/2008, 10h02)
Anatel pode endurecer regra para banda larga (25/08/2008, 09h18)
T-Mobile já vendeu 120 mil iPhones 3G (25/08/2008, 09h42)
ABC cria blog para o webcast World News (25/08/2008, 09h00)
Dispositivos serão controlados pela língua (25/08/2008, 08h37)
Blog: Brasil é pior que Paraguai para Apple (24/08/2008, 15h37)

Done Internet
start 11:19 AM

PLC 89

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**:

Segurança

- Previna-se
- O que o HSBC faz para você
- O que você deve fazer
- Guia de Segurança
- Quiz de Segurança
- Fraudes
- Artigos
- Sites Externos
- Glossário

Como ocorre o roubo de identidade na Web e como evitá-lo - Parte 2

A segunda forma básica que os golpistas usam para se apoderar de dados alheios na Internet é induzindo os próprios usuários da rede a fornecer estas informações. Isto pode ser feito de várias maneiras:

- Por intermédio de e-mails fraudulentos, que usam o nome de instituições confiáveis ou trazem ofertas tentadoras para que os internautas preencham cadastros com dados pessoais (truque muito comum atualmente, conhecido como phishing scam).
- Copiando fielmente páginas de bancos e outras empresas conhecidas e levando os usuários a acessá-las para preencher formulários.
- Criando páginas com serviços gratuitos, cujo único objetivo é recolher dados privados.
- Abrindo lojas virtuais com o intuito de obter números de cartões de crédito e outras informações dos consumidores.
- Enganando os usuários para que instalem programas espiões disfarçados de utilidades ou promoções.

E tudo o mais que permitir a imaginação de um golpista. Para se proteger destes truques, siga os passos abaixo:

- Jamais responda a e-mails que chegam sem que você os solicite e pedem informações privadas.
- As aparências enganam, e na Internet este ditado é ainda mais verdadeiro. Não forneça seus dados em sites de bancos, de comércio eletrônico e outros sem ter certeza de que se trata de uma página legítima. Aqui, o certificado digital novamente é a melhor forma de garantir a autenticidade de um site.

Meu HSBC Internet

Agência e Conta OK

CPF (Acesso para clientes com e sem conta corrente) OK

Novidades no acesso

Connect Bank

Chave da Empresa

Chave do Operador OK

Cadastre-se aqui

Saiba mais

Conta Corrente

Abra sua Conta

Ferramentas Úteis

Fale Conosco

PLC 89

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 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.

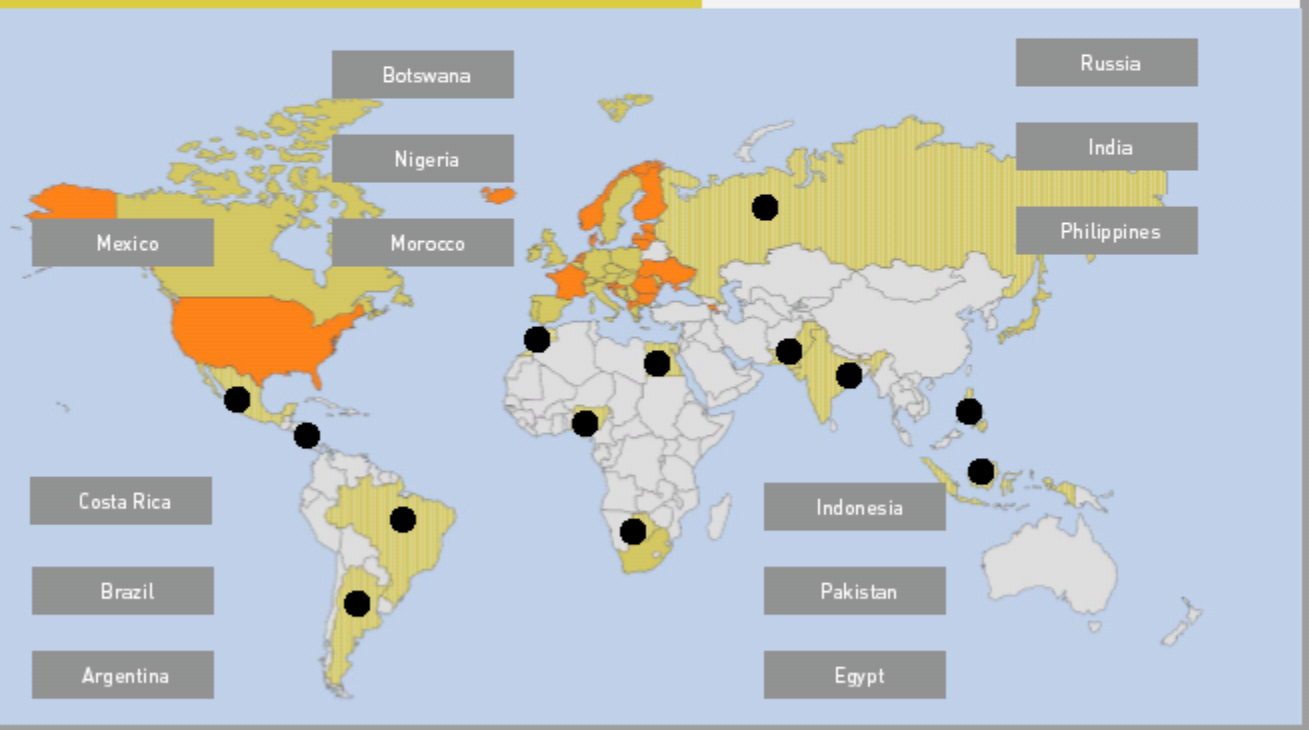
Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada da sexta parte.”

ile Edit Document Tools View Window Help

100%

GERCKE

MODEL LAW



5 of 5 11.69 x 8.26 in

PLC 89

- **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.

PLC 89

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)

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 Civis dos Estados, proceder à investigação, dentre outras, das seguintes infrações penais:

http://ccji.pgr.mpf.gov.br/documentos/docs_documentos/convencao_cibercrime.pdf - Microsoft Internet Explorer

4. A presente Convenção não exclui qualquer competência penal exercida por uma Parte em conformidade com o seu direito interno.

5. Quando mais que uma Parte reivindique a competência em relação uma presumível infracção prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal.

Capítulo III – Cooperação Internacional

Secção 1 – Princípios gerais

Título 1 – Princípios gerais relativos à cooperação internacional

Artigo 23º - Princípios gerais relativos à cooperação internacional

As Partes cooperarão entre si, em conformidade com as disposições do presente capítulo, em aplicação dos instrumentos internacionais pertinentes

Desafios

- **Instituições precisam investir no estado da arte em tecnologia e contratos**
- **Responsabilidades civil e criminal interligadas (normas penais em branco)**
- **Perícia computacional se expande (análise tráfego, esteganografia, etc.)**
- **Conflito privacidade vs segurança aumenta e se agrava**
- **Forte pressão regulatória para se adotar e declarar controles**
- **Integração com GRC**
- **Aproximação maior entre perícia computacional e perícia forense**

Conclusões

- Experiência brasileira com tipos referentes a crimes on-line tem sido adequada
- PLC 89 atualiza e complementa as leis vigentes
- Convenção de Budapeste pode inserir o Brasil no quadro de cooperação internacional formal e eficaz

Gilberto Martins de Almeida

- Introdutor da cadeira “Direito da Informática” em universidades no Brasil
- Filiado a Associação de Peritos
- Árbitro aceito pela Organização Mundial da Propriedade Intelectual
- Especialista em casos de Informática e de Segurança da Informação
- Membro do Conselho Consultivo da Associação Brasileira de Direito da Informática