

# CRIMES ELETRÔNICOS: OS PERIGOS DO MUNDO DIGITAL

CC Paschoal Mauro Braga Mello Filho

## O INÍCIO DE TUDO

Com a Guerra Fria no auge e a possibilidade sempre presente de um conflito nuclear em escala global, havia nos Estados Unidos (EUA) a preocupação em montar um sistema logístico auxiliado por computadores que concentrasse toda a informação estratégica, mas que não fosse vulnerável a um único ataque nuclear.

A solução encontrada foi distribuir os recursos de computação por todo o país, mantendo-os interligados na forma de uma grande rede, mas de tal modo que a destruição de alguns não impedisse o funcionamento dos restantes. Uma rede de computadores em que nenhum isoladamente fosse vital para todo o sistema.

O objetivo da rede era permitir às universidades e empresas clientes do governo (geralmente envolvidas em projetos militares) o compartilhamento dos então caríssimos recursos de computação, distribuição de arquivos de dados e programas. Utilizavam também a rede para a transmissão instantânea de mensagens de um computador a outro, dando origem ao hoje essencial correio eletrônico (e-mail).

## TEMPOS ATUAIS: A ERA DIGITAL E AS SUAS CONSEQÜÊNCIAS

Com a disseminação em larga escala da Internet e a evolução tecnológica, hoje as pessoas se comunicam, trocam dados, realizam negócios e se relacionam pela *Web*, o que vem permitindo também a ocorrência de diversos crimes pela rede.

O mundo digital possui características próprias e existem muitas situações nas quais crimes diversos podem acontecer. Já há leis previstas na legislação brasileira que podem ser utilizadas por analogia, mas há necessidade de se criar outras especialmente para contemplar as novas tecnologias que fazem parte da realidade e do dia-a-dia das pessoas.

Atualmente, alguns tipos penais praticados na *Web* são enquadrados por analogia em nosso Código



Penal, dentre eles: Violação de Sigilo Funcional, Violação de Correspondência, Crimes contra a Honra (Calúnia, Injúria e Difamação), Ameaça, Crimes contra o Patrimônio, Falsa Identidade, Falsidade Ideológica, Quebra de Sigilo Bancário, Interceptação de Dados Informáticos, Pornografia Infantil, Tráfico de Entorpecentes, dentre outros.

Alguns dos crimes cometidos na grande rede já estão com proposta de inclusão em nosso Código Penal, a saber: Roubo de Senha, Falsificação de Cartão de Crédito, Falsificação de Telefone Celular, Difusão de Código Malicioso com Dano e Interrupção de Serviço Telefônico.

A grande questão que ainda incentiva o cometimento de tais tipos de crimes é a sensação de que o anonimato impossibilita a punição, justificando a prática de infrações *on-line*. Entretanto, a Justiça brasileira já aceita como prova judicial impressos extraídos da Internet e registrados em cartório. Em alguns casos, como e-mails e *sites* de relacionamento, nem há a necessidade de registro.

## OS PERIGOS QUE ESTÃO POR TRÁS DOS SITES DE RELACIONAMENTO

Um dos *sites* de relacionamento mais difundidos hoje no país é o *Orkut*. Um caso em que esse *site* serviu de prova essencial para que um juiz pudesse qualificar o crime de Difamação foi o cometido por duas jovens, que criaram uma comunidade no aludido *site* para ofender e denegrir a imagem de uma terceira jovem,

pois esta havia iniciado um relacionamento com o ex-namorado de uma das infratoras. Após análise das provas, o juiz declarou culpadas as jovens, que responderam penalmente e também na esfera cível por danos morais, tendo que indenizar a vítima.

Outro caso em que o *Orkut* foi crucial para a decisão judicial sobre concessão de pensão alimentícia em ação de divórcio foi o do ex-marido que alegava não ter condições financeiras de custear a pensão requerida pela sua ex-esposa, mas constavam, em sua página pessoal do site em tela, fotos de uma recente viagem feita à Europa após a separação. O juiz entendeu que tais fotos eram provas contundentes da real situação financeira do indivíduo, obrigando-o a pagar a referida pensão.

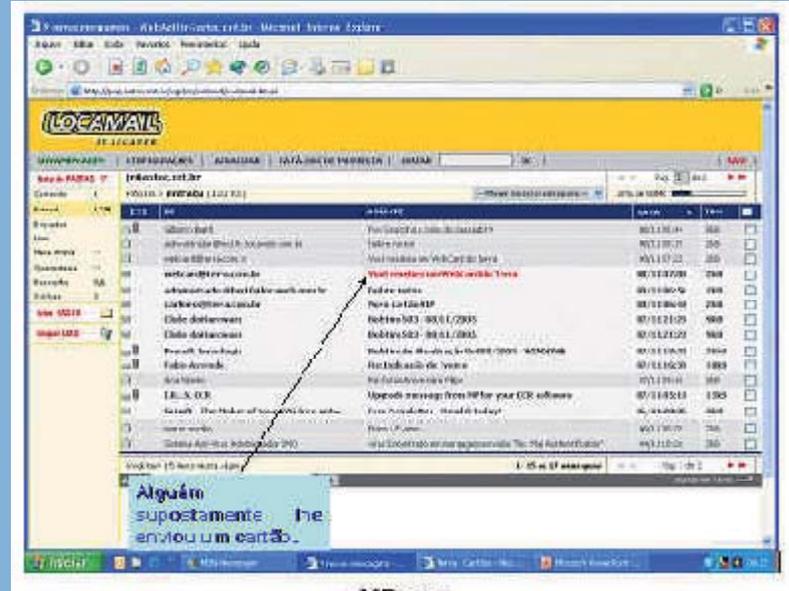
Além disso, ainda há outros tipos penais tão graves quanto os anteriores, que também podem ser praticados por meio do *Orkut*, como o Racismo, a Pedofilia e o Tráfico de Entorpecentes. Nesses casos, não só o dono da comunidade pode ser processado, mas também quem adere a uma comunidade que pratica um crime, mesmo que não tenha deixado mensagem. Isso vale para comunidades que incitam preconceito de raça, religião ou opção sexual (pena de um a três anos de prisão), pedofilia (dois a seis anos) e apologia às drogas (três a seis meses).

Patrícia Peck, especialista em direito digital, explica que as penas são diferentes para quem cria ou participa da comunidade, mas que todos respondem criminalmente.

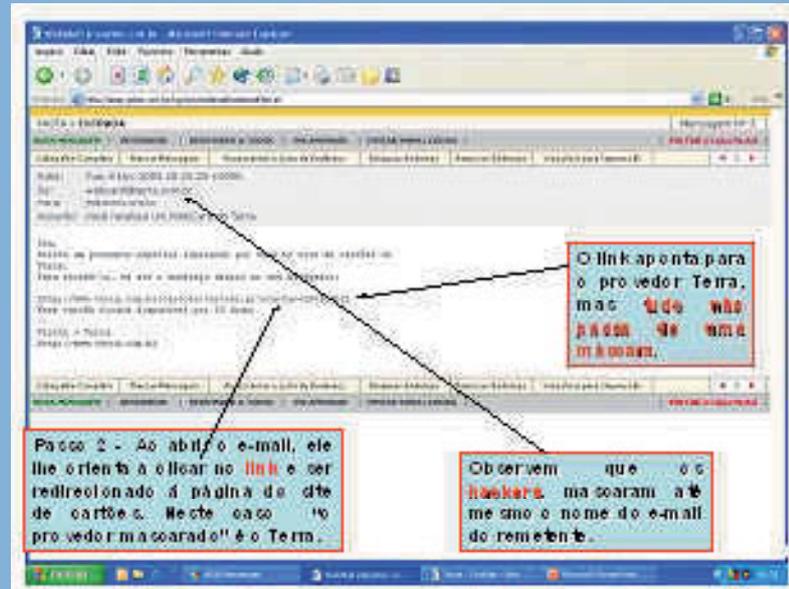
No ano passado, houve a primeira condenação de usuário que cometia pirataria pela Internet, uma decisão contra um funcionário que usava o e-mail da empresa para assuntos pessoais e outra contra um que acessava sites pornográficos do computador do trabalho. O grande problema é que a maioria dos internautas desconhece que, apesar de não haver ainda lei específica, os crimes praticados pela *Web* têm punição.

Recentemente, foi firmado um acordo entre o Google e o Ministério Público (MP), pelo qual a empresa terá uma equipe para atender rapidamente os pedidos da Justiça. Para facilitar a identificação dos criadores e

## UM EXEMPLO PRÁTICO PARA SER OBSERVADO

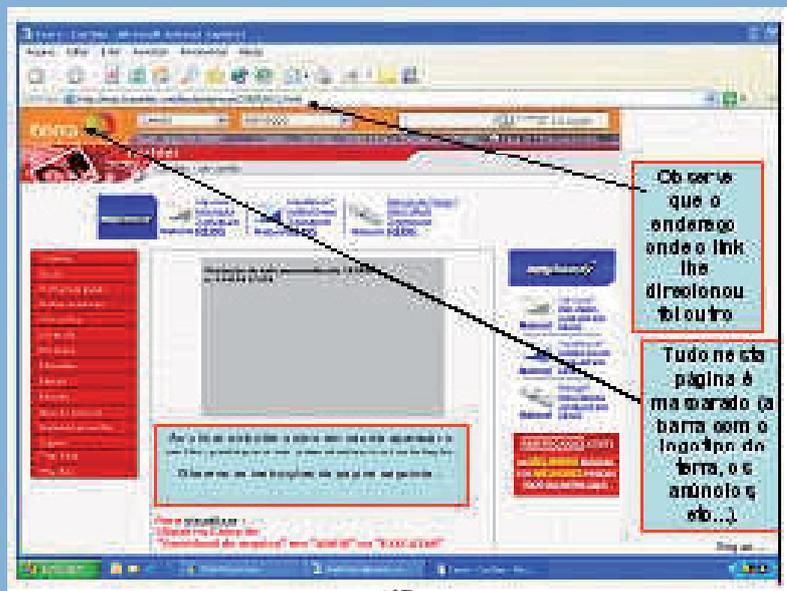


1º Passo



2º Passo

participantes das comunidades ilegais e produzir provas para ações penais, o *Google* poderá guardar por seis meses os endereços IP de usuários do *Orkut*, se assim for pedido pelos promotores do MP. Por enquanto, o acordo não se aplica ao *Youtube*, que também pertence ao *Google*.



3º Passo



4º Passo

### ALGUMAS INFORMAÇÕES ÚTEIS PARA NÃO SER VÍTIMA OU PRATICAR ATO ILÍCITO NA INTERNET

· Escolha senhas que são fáceis de serem lembradas apenas por você. (Fuja de datas

comemorativas, nomes de parentes ou placa de carro);

· Evite deixar seu computador ligado e aberto quando você estiver longe da estação. Pratique o bloqueio do equipamento;

· Cuidado com comunidades *on-line*. Sem saber, você pode se envolver com algum conteúdo que possa gerar problemas legais, tanto no âmbito civil como no criminal;

· Não passe informações de CPF, cartão de crédito e dados de conta bancária por e-mail sem um nível mínimo de segurança da informação. Use, pelo menos, criptografia na mensagem, PGP, assinatura ou certificação digital;

· Evite abrir e-mail de estranhos;

· Cuidado com os vírus em fotos enviadas por e-mail. Sempre utilize um antivírus, um *firewall* e um *anti-spyware*;

· Evite clicar em *links* diretos na mensagem. Sempre verifique se o endereço do site realmente está correto. Na dúvida, se suspeitar que seja um *Scam* ou fraude eletrônica, sempre verifique a informação do e-mail ligando para um "fale conosco", ou entrando diretamente no site da empresa;

· Cuidado com suas senhas, não as empreste para ninguém, nem coloque anotada em papéis ou *post-its*®; e

· Pratique navegação segura.

Fontes:

- *Jornal Gazeta Mercantil*, 15/01/2007;

- *Palestra sobre Crimes Tecnológicos*, ministrada pelo Dr. Rony Vainzof do OPICE BLUM Advogados Associados, na OAB-RJ, em 15/06/2007; e

- *Patricia Peck Pinheiro Advogados* (<http://www.pppadvogados.com.br>).