Disputa entre TVs revela novas estratégias e soldados virtuais

Na terça-feira passada a população brasileira pôde presenciar o início da maior demonstração de desrespeito para com telespectadores, desde os tempos da ditadura militar. A briga entre TVs mais do que desmascarou os tão apregoados “critérios de imparcialidade informativa”, o que agora sabe-se, são inexistentes, mas acima de tudo, evidenciou uma nítida agressão a direitos difusos e coletivos.

Você, seu pai, seu irmão ou seu amigo podem não saber, mas no momento em que as televisões em conflito exibiam “dossiês” em seu horário nobre, preterindo a qualidade da informação, milhões de usuários tinham direitos constitucionais agredidos e arranhados, sem se quer se darem conta. O quanto deixamos de nos informar enquanto lavava-se roupa suja em programas que deveriam ser informativos?

Mas o pior, a batalha não ficou nas ondas hertazianas e tivemos que assistir outras mídias do grupo das emissoras replicarem as ofensas ou contra-ataques, como numa ordem ditatorial *top-down*! Revistas, jornais e como se não bastasse, a internet.

Achávamos que já tínhamos visto tudo, mas tivemos conhecimento da ação de um grupo de *hackers* brasileiros, “Skynet Group”, que acessou indevidamente o site da Record e proferiu ofensas aos seus proprietários. Dúvidas à parte sobre tal ação ter sido patrocinada pela outra empresa, o fato é que esta conduta embasa uma série de reflexões que propomos no artigo da semana.

O fato é que, hoje percebemos que a motivação do atacante virtual não é mais a mesma. Se outrora agia por emulação, visando destaque em seu grupo, em outro momento agindo impulsionado pela ideologia (comum em países do oriente médio), hoje sabemos que o hacker brasileiro age, preponderantemente, pelo dinheiro. Até aí nem uma novidade. Ocorre que agora este dinheiro pode ser da vítima, mas também pode ser do mandante do crime. O Hackerismo agora pode ser encomendado, assim como se encomenda um homicídio.

No caso da Rede Record, a técnica utilizada é conhecida como “Defacement”, do inglês, ato de modificar a superfície de um objeto. O “deface”, no jargão geek é considerado uma técnica de “pichação”, em que o invasor modifica o site da vítima, normalmente com textos ofensivos.

Mas é crime alterar um “*index*” de uma página qualquer? Ora, qual seria sua reação se chegasse para trabalhar em sua empresa e a sede estivesse completamente em chamas? A analogia é pertinente, pois aquele que altera página da internet de terceiros, mais que destruir a página inicial, afeta sua relação com clientes, terceiros e principalmente, gera o chamado impacto de imagem, um dos mais difíceis de serem contingenciados.

Mas é possível punir estes criminosos, que realmente pensam que são úteis, libertários ou ideologistas? Para o mestre penalista Nelson Hungria, dados não poderiam ser objeto de destruição pelo crime de dano, eis que "o objeto material do crime de dano é a coisa imóvel ou móvel, devendo tratar-se obviamente, de coisa corpórea ou no sentido realístico, pois somente pode ser danificada por ação física".

Por outro lado, esta interpretação não mais resiste a análise contemporânea, considerando que aplicando-

se a chamada “interpretação histórico-evolutiva” muitos juizes no Brasil já condenam por dano informático, crime previsto no artigo 163 do Código Penal, aqueles que destoem sistemas informáticos, de grandes ERPs à páginas na internet.

Tanto é verdade que no Projeto de Lei de Crimes de Informática, o PL 84/1999, já aprovado no Senado, teremos a criação clara do crime de “Dano Informático”, que expressamente prevê que dados digitais podem ser passíveis de destruição:

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.”*

Assim, ao difundir código malicioso em sistema informatizado que resultou em mera “alteração” do funcionamento do website, estes hackers já poderiam ser punidos. Poderiam, não fosse a morosidade legislativa em aprovar o Projeto de Lei em análise. E se for constatado realmente que os ataques ao site da Record tiveram um “mandante”?

O Código penal deixa claro em seu artigo 29 que quem, de qualquer modo, concorrer para o crime, incide nas penas a este cominadas, na medida de sua culpabilidade. Assim, pela teoria monística, todo aquele que concorre para o crime, em verdade, causa-o. De modo que, autor é quem tem poder de decisão sobre a realização do fato e não só quem executa a conduta típica.

Outro ponto merece reflexão. Ao pixar o site da Record e colocar um “logo” da Rede Globo, estes imaturos bandidos simplesmente nos enalteceram mais uma característica do Direito Digital: a facilidade de alterar o estado das coisas e atribuir a autoria de crimes a outras pessoas! Assim como no Direito Digital é possível furtar e deixar a coisa furtada, também é possível facilmente utilizar ou subtrair credenciais alheias, e usá-las para um crime virtual. Aqui identificamos casso clássico de calúnia (artigo 138) e denunciação caluniosa (artigo 339 do Código Penal). Agora, até “explicar que focinho de porco não é tomada…”

Onde queremos chegar? Discernimento. Autoridades, peritos digitais e poderes constituídos terão que

aprender rápido com os exemplos como este, cada vez mais gritantes em nossa sociedade, ou injustiças serão cometidas!

Estes são os “novos soldados”, soldados cibernéticos com superpoderes nas mãos, capazes de achincalhar qualquer conceito de prova eletrônica concebido ou chacotear os métodos ortodoxos de investigação policial. Pessoas que são mais nocivas não por praticarem os crimes na internet, mas por poderem se passar por qualquer outra pessoa e principalmente, por nunca revelarem a quem efetivamente servem.

Date Created
11/09/2009