Política de Controle da Internet

Bruna Gonçalves Rezende – 5967853
Daniel Yoshinobu Takada Chino – 3456842
Lucas de Barros Rodrigues - 5890073
Paulo de Tarso Correa - 5890389
Instituto de Ciências Matemáticas e de Computação – ICMC-USP

1. Introdução

O primeiro vestígio da internet surgiu em 1969 com a ARPANET. Em 1974 a Arpanet adota um protocolo que permite que qualquer computador se conecte à rede, chamado de TCP/IP (*Transmission Control Protocol/Internet Protocol*) e foi quando começou a ser usado o termo "Internet" . Em 1º de Janeiro de 1983 a primeira rede de grande extensão baseada em TCP/IP entra em operação. Em 1989 Tim Berners Lee (CERN) propõe o projeto de hipertexto que ficou conhecido mundialmente mais tarde por World Wide Web. Em 1990 o número de usuários na internet chega a 25 milhões e o surgimento de WWW começa a atrair grandes empresas e a imprensa. Em 1991 surge a Web.Em 1994 cresce o interesse pela Web que até então era considerada muito técnica e acadêmica. Em 1996 o governo da Alemanha desliga o grupo de discussão Compuserve por uso indevido deste (distribuição de pornografia). Em 1996 Bill Clinton aprova uma nova lei de telecomunicações onde prevê pena para quem distribuir conteúdo indevido na internet.

Crescimento da WEB

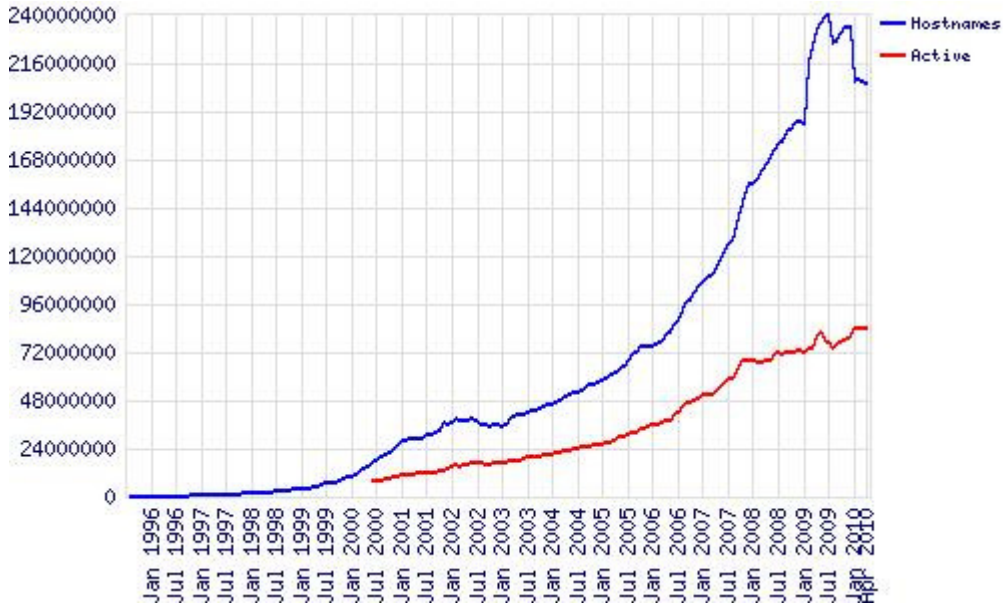

Figura 1: pode-se observar que, desde sua criação, a Internet vem crescendo exponencialmente e em movimento constante.

Como se pode observar pela Figura 1, a Internet tem crescido de forma rápida, esse crescimento proporcionou diversos aspectos positivos a sociedade, estando entre eles o auxilio no ensino e/ou aprendizado, agilizando pesquisas e evitando a dependência de serviços como bibliotecas ou pedidos de artigos científicos. Outro aspecto positivo é a facilidade de comunicação existente devido à vasta cobertura que a rede apresenta, permitindo uma maior liberdade para a troca de conhecimento de forma mais rápida e prática. Porém, essa liberdade permite que exista uma mau uso da rede, como por exemplo roubo de informações sigilosas através da propagação de vírus digitais e/ou estelionatos eletrônicos, divulgação de materiais relacionados a pornografia infantil, difamação e até mesmo os chamados *bullying* existentes nas escolas. Esses aspectos negativos serão explicados a seguir.

2. A Internet

Com o grande crescimento da internet, aumenta também o mau-uso bem como os crimes relacionados a ela, veremos agora o alguns desse crimes e o que está se tentando fazer com relação a eles.

2.1. Anonimato

Um dos grandes fatores que alimentam o mau uso da internet é o anonimato que ela proporciona aos usuários, já que não é simples ter conhecimento da real identidade das pessoas com quem se possa estar interagindo. Esse anonimato, dá a sensação à usuários mal intencionados de que não há limites legais na rede mundial de computadores. Existe uma comunidade de internautas que se escondem atrás do anonimato para realizar atividades que podem vir a prejudicar o uso comum da internet, esses usuários se denominam como *Anonymous*. Podem ser citadas como atividades realizadas por eles:

- *YouTube Porn Day*: ocorreu em 20 de maio de 2009, os *Anonymous* combinaram através de um fórum de discussões um dia para que fossem publicados diversos vídeos pornográficos no site YouTube. Esses vídeos eram publicados como se fossem de temas infantis, como dos programas *High School Musical*, *Jonas Brothers* e outros, e após 20 a 30 segundos de exibição eram trocados por um conteúdo pornográfico;

- *Operation Titstorm*: ataques contra sites do governo Australiano ocorrido em 10 de fevereiro de 2010, como forma de protesto à censura de pornografias existentes na Austrália.

2.2. Pedofilia

Na internet as redes P2P proporcionam um fácil meio de distribuição de qualquer material, principalmente pornográficos. Um exemplo de como essas atividades são freqüentes e sem controle foi o caso de Cheryl Roberts, de 61 anos,que entrou no site fingindo ser uma menina de 14 anos e pouco depois foi convidada por seu marido, David Roberts, de 68, para se encontrarem e terem relações sexuais.

2.3. Propagação de vírus

O mal mais freqüente da Internet, que causa prejuízos enormes a usuários comuns, empresas e empresas de segurança. Um exemplo de vírus devastador foi o *Doomsday*, descoberto em 1995. Até hoje não se sabe a origem do vírus.

Figura 2: Falso plugin requerido pelo Banco Santander Banespa.

No Brasil, a forma mais comum de propagação desses vírus é através dos chamados Cavalos de Tróia, onde são enviadas informações falsas que fazem com que o próprio usuário infecte seu computador com o vírus. A Figura 2 exibe um caso onde é enviado um e-mail falso do Banco Santander Banespa informando ao usuário que é necessário que seja instalado um novo *plugin* de segurança, sendo que na realidade é um

vírus. Para dar maior credibilidade ao conteúdo do e-mail, são inseridas diversas informações como telefones de atendimento ao cliente.

2.4. *Phishing*

Figura 3: Página falsa, imitando a do Banco do Brasil.

Ataques onde a pessoa copia a imagem do Banco do Brasil para "roubar" a senha do internauta, como podemos ver na Figura 3. O Brasil é o terceiro lugar do ranking mundial de *phishing* (http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=13110&sid=18)

2.5. Cyberbullying

A mesma atividade ocorrente nas escolas estendida para componentes eletrônicos, fazendo com que a criança não tenha mais o refúgio de casa. Isto ocorre em sites de redes sociais como Orkut, *Facebook* e mensagens SMS. Um exemplo foi o caso de *cyberbullying* através de SMS, *Facebook* e pessoalmente levando a adolescente Phoebe Prince ao suicídio.

2.6. Difamação

É a criação de perfis falsos. Um exemplo de vitima foi Roberta Honorato que teve sua foto publicada como garota de programa. Seu perfil falso continha fotos de sexo explicito e insinuações sobre o comportamento sexual.

3. Projeto de Lei Substitutivo

Tendo em vista esses fatores negativos, o senador Eduardo Azeredo (PSDB-MG) propôs um projeto de lei substitutivo que tipifica e criminaliza diferentes tipos de ação criminosa em redes privadas ou públicas de computadores.

SUBSTITUTIVO (ao PLS 76/2000, PLS 137/2000 e PLC 89/2003)
Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências."

Os pontos mais polêmicos, que impedem que esta lei seja aprovada, são rejeitados por serem abertos a interpretações. A forma como estão escritos não é exata e pode-se derivar interpretações que punam práticas comuns na Internet hoje em dia. O Senador Azeredo afirmou que sua intenção não é criminalizar essas práticas, apenas as que são danosas. Mas não se pode levar a palavra dele como garantia. Vejamos abaixo quais são esses pontos polêmicos:

Acesso não autorizado:

Na teoria: Acesso não autorizado de redes de computadores, **dispositivos de comunicação** ou sistemas informatizados, protegidos por **expressa restrição de acesso**.

Na prática: pune quem acessa, por exemplo, uma rede sem fio do vizinho, vê as mensagens de um celular alheio, lê e-mails ou documentos de outras pessoas, porém é preciso dar a devida atenção à expressão "protegidas por expressa restrição de acesso", ou seja, você tem que por uma senha ou um aviso ostensivo de proibição para poder posteriormente processar quem leu sua mensagem no celular ou entrou na sua rede sem fio. Outro ponto dessa lei é que quem destravar o celular (que se encaixa na definição

do projeto de “dispositivo de comunicação”) para utilizá-lo por outra operadora estará sujeito a pena de um a três anos de prisão. A mesma penalidade sofrerá quem, fazendo uso do direito de acesso a conteúdos em domínio público, destravar um CD ou DVD.

Pena: de um a três anos de reclusão e multa.

Transferência não autorizada:

Na teoria: Obter ou transferir dados sem a autorização do titular da rede, dispositivo ou sistema, protegidos por expressa restrição de acesso.

Na prática: Os dados podem ser acessados, mas não transferidos ou distribuídos. Por exemplo os dados de sua empresa podem ser usados dentro desta, mas não podem ser transferidos para sua casa. Comparando a grosso modo, seria como apropriação indébita, onde o bem já está em seu poder, mas não é seu.

Pena: de um a três anos de reclusão e multa.

Divulgação ou uso indevido dos dados pessoais:

Na teoria: Muito parecida com a anterior, só que mais abrangente, pois a expressão “uso indevido” é bem subjetiva.

Na prática: Por exemplo, uma assistência técnica, onde os arquivos do computador que foi ao conserto são de uso pessoal e estão em seu poder, mas você não pode fazer uso deles, ou divulgá-los por qualquer meio.

Pena: de um a dois anos de reclusão e multa.

Inserção ou difusão de código malicioso:

Na teoria: essa já se restringe às pessoas com conhecimento técnico, que por exemplo pode ao usar um determinado computador, deixar um script que capture dados de quem venha a utilizá-lo.

Na prática: a pessoa usa um script para recolher dados como login e senha de usuários do computador em uma *lan house*, por exemplo. No caso de difusão, pode-se também punir apostilas que divulguem códigos de vírus para exemplificar algum ponto.

Pena: reclusão de um a três anos e multa.

Inserção ou difusão de código malicioso seguido de dano:

Na teoria: agrava a pena do item anterior se do crime resultar destruição, inutilização, deteriorização, alteração, dificultação do funcionamento, ou funcionamento

desautorizado pelo legitimo titular do dispositivo de comunicação, rede de computadores ou sistema informatizado.

Na prática: se o vírus inserido no sistema acarretar a formatação deste, sem a chance de backup.

Pena: reclusão de dois a quatro anos e multa.

Estelionato Eletrônico

Na teoria: pune quem difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à redes de computadores, dispositivos de comunicação e sistemas informatizados.

Na prática: Invasão de sistemas. Em nossa faculdade, temos disciplina em que temos aulas de invasão de redes, que as vezes são necessárias (no caso de uma investigação, por exemplo). Esse ponto da lei torna essas aulas ilegais.

Pena: a mesma que já existe para estelionato.

Pedofilia

Na teoria: Passa a punir também quem guarda e recepta material com pornografia infantil.

Na prática: É punido aquele que distribui,guarda e recebe o material de pedofilia.

Pena: reclusão de um a três anos e multa.

Armazenamento de dados por provedores

Na teoria: Os provedores passam a ter a obrigação de guardar por 3 anos os dados de origem (IP), data, hora e local associados a todos os acessos dos usuários que utilizam sua rede.

Na prática: Atualmente quando os peritos estão investigando algum crime, dependem da boa vontade do provedor de colaborar, o que nem sempre acontece. Então quando o provedor não colabora de boa vontade, é preciso conseguir uma ordem judicial, mas isso já causa perda de tempo e facilidades para os criminosos ou os que não querem colaborar com as investigações. Essas informações como IP, data, hora (com minutos e segundos) são essenciais e devem ter precisão máxima, pois posso cometer um crime com um IP em um minuto, desconectar e no segundo seguinte outro computador já se conectar e pegar esse IP que acabou de ser liberado, sem precisão pode-se pegar a pessoa errada. Além do mais, é preciso fazer com que as *lan houses*

também cadastrem quem está usando, pois pesquisando pelo IP, vai se chegar na *lan house*, daí a descobrir quem estava usando determinado computador naquela hora e local, ai já tornou a investigação inviável. Um jeito viável de ligar a pessoa ao IP seria utilizar o CPF para navegar, porém qualquer hacker consegue acesso ao CPF de uma pessoa (que é um dado público), podendo utilizá-lo para cometer seus crimes. Outro ponto é que, com informações pessoais disponíveis na rede, o acesso de hackers a essas informações é facilitado.

Pena: Multa de R$ 2.000,00 a R$ 100.000,00 a cada requisição não atendida.

Como pudemos ver, a lei que propõe o controle da Internet ainda está mal redigida. Com o intuito de considerar a opinião popular, uma *wiki* foi criada para um grupo de discussão a fim de melhorar a lei. Esse grupo pode ser encontrado em http://meta.wikimedia.org/wiki/Wikimedia_Brasil/Legisla%C3%A7%C3%A3o/Lei_sobre_crimes_eletr%C3%B4nicos.

4. Controle da Internet

O controle do mau uso da internet é muito dificil, mas algumas soluções já estão sendo criadas, como no caso da pedofilia. Existem softwares de controle que tentam impedir que este material circule na rede. Exemplos de Software são:

- SurfRecon
- Porn Detection Stick
- PornSeePro

Além disso, no caso de redes P2P, existem grupos na Internet (um exemplo é o P2P Patrol, http://www.p2ppatrol.com/#1) que monitoram e encaminham denúncias de pedofilia nessas redes de difícil monitorização.

Para vermos como o controle da Internet vem sendo debatido desde seus primórdios, temos o exemplo do 1º Encontro Mundial da Sociedade da Informação ocorrido em Genebra em 1993, no qual foi proposta uma legislação unificada mundial para exercer o controle da Internet. O encontro foi um fracasso, com a maioria dos países presentes não assinando o acordo. Não há dúvidas de que para um controle eficiente seja necessário um acordo internacional, mas o principal problema de um acordo desse nível é conciliar o desejo de cada país. No caso do encontro de 1993 tivemos um exemplo claro dessa divergência. Brasil e África do Sul criticaram o acordo, a China pediu a criação de nova organização mundial para o controle, a França

pediu abordagens intergovernamentais democráticas, Cuba e Síria criticaram os EUA como grande ditador da Internet, e até mesmo o ditador do Zimbábue, país que provavelmente não possuía rede naquela época, afirmou que o sistema de controle da Internet é uma forma de neocolonialismo.

5. Conclusão

Como visto existem diversos casos de mau uso na internet que podem ocasionar em crimes envolvendo grandes quantias de dinheiro, nos casos de vírus e *phishing*, distribuição de pornografia infantil e também pode, no pior dos casos, ocasionar em homicídios e/ou tentativas de suicídios, devido a difamação e *bullying*. Logo, levando em consideração todos esses fatores, é notável a importância de leis que regulamentem os crimes eletrônicos, para que as punições possam ser realizadas mais rapidamente, uma vez que é inviável uma auto-regulação da internet, pois por mais que se pregue por liberdade, se há total liberdade para todos os indivíduos isso na realidade pode causar mais males do que bem, uma vez que a liberdade de um indivíduo pode prejudicar a liberdade de outro. Porém, há de ressaltar que a forma como o projeto de lei Substitutivo está escrito, permite interpretações ambíguas, sendo assim necessária uma revisão mais detalhada.

6. Referências Bibliográficas

- http://www.torque.com.br/internet/historia.htm
- http://pt.wikipedia.org/wiki/Internet
- http://news.netcraft.com/archives/web_server_survey.html
- http://jusacademico.blogspot.com/2008/08/entenda-nova-leipara-crimes-de.html
- http://meta.wikimedia.org/wiki/Wikimedia_Brasil/Legisla%C3%A7%C3%A3o/Lei_sobre_crimes_eletr%C3%B4nicos