Cibercrimes

Daiane Oliveira Spurio[1], Josiane Pietrobon França[2], Cineiva Campoli Paulino Tono[3]

[1]UNIBRASIL - Faculdades Integradas do Brasil
Rua Konrad Adenauer, 442. Tarumã.
CEP 82821-020 Curitiba, PR

daianespurio@gmail.com

[2]UNIBRASIL - Faculdades Integradas do Brasil
Rua Konrad Adenauer, 442. Tarumã.
CEP 82821-020 Curitiba, PR

josiane_pietrobon@hotmail.com

[3]UNIBRASIL - Faculdades Integradas do Brasil
Rua Konrad Adenauer, 442. Tarumã.
CEP 82821-020 Curitiba, PR

cineivatono@gmail.com

Resumo. *Esse trabalho propõe alertar os usuários da internet, de modo criterioso, apoiada na gestão da informação sobre cibercrimes em termos preventivos, pois com o passar dos anos a tecnologia de informação e comunicação está cada vez mais presente na atividade humana da sociedade contemporânea. O número de computadores vendidos mundialmente cresce a cada dia e os crimes cometidos por esse meio tecnológico aumentam constantemente. Também abordar-se-á o quanto é relevante informar as crianças, adolescentes e adultos sobre os cibercrimes, pois a maioria dos usuários da internet não tem conhecimento sobre o assunto e nem tem ideia de que providências tomar, caso ocorra algum tipo de intermediação criminosa mediada pela internet. Acrescenta-se, ainda, a importância de se trabalhar tal assunto com os pais de crianças e jovens. A ação criminosa vem tomando conta do ciberespaço e praticamente nada vem sendo discutido nas escolas e nas academias sobre este fato, por negligência ou por desconhecimento. Para tanto, esta pesquisa tem a prerrogativa de alertar a população do mal que a internet pode causar se utilizada de forma ingênua e acrítica.*

1. Introdução

Com o passar dos anos a tecnologia de informação e comunicação está cada vez mais presente na atividade humana da sociedade contemporânea. O número de

computadores vendidos mundialmente cresce a cada dia e os crimes cometidos por esse meio tecnológico (cibercrime) aumentam consequentemente, mas as informações sobre como utilizar de maneira correta essa tecnologia não são devidamente e suficientemente divulgadas em condições de efetivo enfrentamento e prevenção. Paul Virilio [1] (2000, p.11) cita:

> "...sem a liberdade de criticar a técnica, ... não há qualquer progresso técnico, mas somente um condicionamento... e quando este condicionamento se torna cibernético, como é hoje o caso com as novas tecnologias, a ameaça é considerável."

Parte da população que não tem conhecimento sobre cibercrime se torna alvo fácil para que os "vilões" se aproveitem, pois, sem informação, os usuários de internet se tornam "presas fáceis", devido à ingenuidade e até inconsciência em relação aos perigos implícitos na rede.

Em entrevista ao programa "Nós da Educação" da TV Paulo Freire em 10 de dezembro de 2007, o Delegado do Núcleo de Combate aos Cibercrimes (NuCiber) de Curitiba, Demétrius Gonzaga de Oliveira afirma:

> "...esse é um ponto que causa um certo grau de dúvida na população, tendo em vista que eles nem sempre conseguem identificar o que é ou não crime. Calúnia, injúria e difamação por exemplo. São tipos diferentes dentro do código penal, praticado contra a honra."

Neste trabalho busca-se desenvolver mecanismos informacionais e interacionistas para socializar conteúdos relacionados a cibercrimes para produção do conhecimento significativo, na perspectiva de atribuir aos usuários da internet condições plausíveis para desenvolver estratégias que reduza os danos consequentes dos cibercrimes. Apontam-se elementos essenciais que podem contribuir para essa socialização, como por exemplo: a criação de metodologias nas escolas de como utilizar de maneira segura a internet, nas faculdades, com criação de uma disciplina ou trabalhos extracurriculares que integram os cursos de informática e direito. Tal integração nortearia o planejamento e o desenvolvimento de ações para que esse tipo de crime possa ser desvendado com agilidade a partir do contexto jurídico, técnico e metodológico. E também demonstrar como é importante a prevenção sobre crimes cometidos na internet e o quanto é emergente o seu monitoramento, para que as políticas públicas possam ser implementadas nessa área com efetividade.

A tecnologia vem favorecendo os usuários mal intencionados, pois o que se fazia antes no mundo real, hoje é facilitado no mundo virtual, devido ao anonimato prescrito na internet. Os criminosos acreditam que não deixam rastros, o que pode ser um equívoco, porque é possível rastrear o usuário pelo IP da máquina. Eis a importância que deve ser dada para leis de monitoramento de lugares públicos e até privados, com acesso à internet, para que os usuários possam ser identificados, como é o caso da Lei Estadual 16.241 [2], vigente desde outubro de 2009 no estado do Paraná.

Portanto, a preocupação que se deve ter com a disseminação de informação sobre cibercrimes deve ser grande. É preciso pesquisar no Brasil e no mundo sobre leis e

teorias dessa temática, os mecanismos de informação sobre cibercrimes e quais seus impactos na sociedade. Nesta pesquisa será realizado um estudo de caso por meio de entrevistas com profissionais da área jurídica e tecnológica, para que a pesquisa seja fundamentada na real necessidade dos processos de formação para redução de danos causados pelos cibercrimes e também embasadas em teorias científicas.

1.1. Problema E Hipótese

Porque o cibercrime virou um problema na sociedade?

Pela ineficiência de mecanismos de informação sobre cibercrimes. Pelo despreparo de usuários e principalmente professores, quanto ao uso correto para ensinar em sala de aula. Também pela inocência das crianças frente a situações de risco, subordinado ao uso desordenado do computador sem a vigia dos pais, que se omitem perante os filhos e não impõem o uso seguro, moderado e crítico do computador.

1.2. Objetivo Geral

Desenvolver uma pesquisa sobre cibercrimes com informações destinadas a profissionais que atuam direta ou indiretamente com crianças e adolescentes, como: educadores (pais e professores), conselheiros tutelares, entre outros, para que possam assumir a função de orientadores das metodologias de uso responsável da internet para prevenir seus males.

1.3. Objetivos Específicos

Investigar teorias, leis e notícias no Brasil e no mundo sobre cibercrimes; pesquisar sobre os atuais mecanismos de informações sobre cibercrimes e o seu impacto na sociedade; entrevistar profissionais especializados em cibercrimes e professores do ensino básico; propor informações relevantes e coerentes, envolvendo as áreas de Direito e Informática às vistas de cibercrimes.

1.4. Justificativa

O cibercrime vem tomando conta do ciberespaço e pouco tem se discutido sobre o assunto na sociedade. A cada dia criam-se novas ferramentas tecnológicas de informação e comunicação subsidiando usuários mal intencionados na ordem da criminalidade via web, pois o que eles praticam, na concretude, é potencializado na virtualidade, devido às facilidades existentes para o uso dessas ferramentas.

A concepção errônea do criminoso de que não deixará pistas e rastros dos crimes na internet favorecem essas atitudes, o que pode ser um equívoco, pois o usuário pode ser rastreado pelo número de IP da sua máquina. Eis a importância de existirem leis que regulem, monitorem e que desenvolvam métodos eficientes para identificação do usuário de computadores em Lan Houses e em espaços públicos, como Faróis do Saber, Telecentros, Escolas, entre outros.

No Brasil, existem onze delegacias especializadas em crimes na internet, estão situadas no Distrito Federal, Espírito Santo, Goiás, Mato Grosso do Sul, Minas Gerais, Pará, Paraná, Pernambuco, Rio de Janeiro, Rio Grande do Sul e São Paulo.

Em 2005, no Estado do Paraná, foi criado o Núcleo de Combate aos Cibercrimes – NuCiber [3]. Suas competências são de prevenir e reprimir infrações na internet, vistoriar e conceder alvará de funcionamento para locais que tenham jogos em rede ou Internet (Lan House, Ciber Café, entre outros) e auxiliar a Polícia Civil em investigações que necessitem a realização de pesquisas na rede.

2. Revisão De Literatura

Composta de categorias que esclarecem sobre conceitos e histórico do crime na especificidade do cibercrime, leis existentes relacionadas ao cibercrime no mundo, no Brasil e no Paraná.

2.1. Crime

De acordo com Juarez Cirino dos Santos [4] (2007, p.71-79), define crime como uma conduta humana, típica, antijurídica e culpável.

- Conduta Humana: conduta positiva, comissiva (ação) ou conduta negativa, omissiva (omissão).
- Típica: descrita em lei como delito, que é previsto em lei.
- Antijurídica: contrária ao direito, ilícito.
- Culpável: culpa no sentido amplo, doloso ou culposo.

De acordo com o artigo 1º da Lei de Introdução ao Código Penal [5] (2010, p.515): "Art. 1º. Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; [...]".

2. Cibercrime

O termo começou a ser usado nos anos 90 com o aumento do uso do computador, não apenas por empresas, mas também por usuários domésticos [6] (2002, p.35). No Brasil, o assunto cibercrime está começando a se difundir, várias notícias já circulam na mídia como forma de tentar alertar os usuários sobre os perigos de um uso incorreto do computador.

O crime na internet, ou cibercrime, nada mais é do que uma conduta ilegal realizada por meio do uso do computador e da internet [6] (2002, p.53-57). Os crimes mais comuns são pirataria, pornografia infantil, contra a honra, espionagem, entre outros.

Pode ser dividido em 3 tipos:

Crime Virtual Puro: "O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou

técnico ao equipamento e seus componentes, inclusive dados e sistemas.” [7] (2003, p.69).

Crime Virtual Misto: “Crime virtual misto seria aquele em que o uso da internet é condição *sine qua non* para a efetivação da conduta [...]”. [7] (2003, p.69).

Crime Virtual Comum: “Crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal.” [7] (2003, p.69).

2.3. Tipologia De Cibercrimes

- Pornografia infantil na internet: Imagens ou vídeos de pornografia envolvendo menores de idade. De acordo com o Estatuto da Criança e do Adolescente [8], o simples armazenamento desses arquivos já é caracterizado como crime.

- Fraude: Pode ocorrer através do phishing, spam, vírus, etc.

Phishing/Spam: E-mails que são enviados com informações falsas, muitas vezes se passando por empresas bancárias, para coletar dados das contas dos clientes.

Vírus: É um tipo de software que pode espalhar-se no computador da vítima, causando danos e até roubos de informações.

- Contra a honra: Estão entres eles a calúnia, a difamação e a injúria.

- Pirataria: Incluem cópias não autorizadas de músicas, filmes, seriados, livros, artigos, entre outros. São protegidos pela Lei dos Direitos Autorais, Lei nº 10.695/03 [9]. Também é considerado pirataria o uso de programas de computador sem suas respectivas licenças originais. Protegidos pela Lei nº 9.609/98 [10].

- Pichação: É a invasão de um site para fazer marcas, textos, desenhos e/ou alterações no layout da página.

- Falsa identidade: Usar nomes falsos ou de terceiros para efetuar cadastros na internet.

2.4. Leis Sobre Crimes Na Internet

2.4.1. No Mundo

Vários países já criaram leis específicas para punir os criminosos. Entre eles: Chile, Itália, França, Estados Unidos, Inglaterra, Espanha, Portugal e outros [6].

Estados Unidos: Desde o final da década de 70 já existe uma legislação para combater os crimes na internet.

França: Em janeiro de 1988 já começa a legislar sobre os crimes na internet.

Inglaterra: Elaborada em 1990 a lei inglesa dos crimes de informática.

Portugal: Em 1991 faz lei que tipifica 6 tipos de crimes na área de informática.

Itália: No período de um ano (1992 a 1993), fez várias modificações em suas leis para incluir os crimes cibernéticos.

Chile: As leis específicas começaram a entrar em vigor em 1993.

Espanha: Em 1995 começam as modificações que abrangem os crimes informáticos.

2.4.2. No Brasil

Desde 1999 está em tramitação no Congresso Nacional o Projeto de Lei sobre Crimes Eletrônicos, a PL 84/1999 [11]. Ela divide opiniões, pois alguns itens sobre sua tipificação não são claros o suficiente, levando as pessoas a acharem que ela interferiria na questão de privacidade quanto ao uso da internet. Com isso, o projeto fica apenas sofrendo alterações ao longo dos anos e não é votado de fato para entrar em vigor. A partir desse projeto de lei surgiu outro, o PL 587/2011 [12], que segue o mesmo intuito, mas com algumas modificações, e assim como o outro, também é polêmico quanto ao seu teor.

Enquanto isso, o Código Penal Brasileiro é usado para punir os casos de crimes que ocorrem no Brasil, adaptando as leis existentes aos casos que ocorrem na rede.

2.4.3. No Paraná

No Paraná, existe a Lei Estadual nº 16.241/2009 [2], que determina a obrigatoriedade do uso de monitoramento por câmeras e identificação dos usuários em todos os estabelecimentos que comercializam o acesso a internet, e também estabelecendo um prazo de dois anos para o armazenamento dos cadastros desses usuários.

3. Metodologia Da Pesquisa

Este capítulo traz os tipos de pesquisas aplicadas para o desenvolvimento do mesmo.

3.1. Tipo De Pesquisa

Realização de um estudo de caso por meio de entrevistas com profissionais das áreas de direito e informática, e também a aplicação de questionários em alunos e professores, para identificar o nível de conhecimento sobre a temática cibercrimes.

A tipologia da pesquisa segundo os meios é exploratória e aplicada, e também bibliográfico sobre o que é considerado crime, sobre as leis aplicadas a cada caso e a subjetividade na interpretação da lei.

3.2. Levantamento De Requisitos

Requisitos para o desenvolvimento da pesquisa.

3.2.1. Entrevista Com Profissional Da Área

Foi feita uma entrevista com o Analista de Segurança Paulo José Ribas, que é dono de uma empresa que atua, desde 2007, com Segurança de Dados (Corporativo), Segurança para transações via Internet, Leis e Normas para a Tecnologia da Informação e Forense Digital.

De acordo com o entrevistado, faltam profissionais no mercado tecnológico voltados para as áreas de Direito, Leis e Tecnologia.

Prosseguindo a entrevista, fala que a procura do público doméstico para os serviços de perícia vem crescendo. Com o rápido aumento das redes sociais e a facilidade de acesso à internet, esse público virou alvo fácil dos criminosos pela falta de informação quanto a esses atos irregulares.

Perguntado sobre quais as dificuldades para obter provas durante as investigações, Paulo Ribas pronuncia:

> "Em relação as empresas geralmente se alteram a localização das provas dificultando um pouco o nosso trabalho. Para o público doméstico é que geralmente a vítima ou o agressor utilizam diferentes equipamentos como os pessoais, lan houses, faculdade, escolas, bem como shopping e restaurantes (cybercafés)."

Analisando tais abordagens, é importante que haja regulamentação na utilização da internet, principalmente dos lugares públicos, pois isso facilitaria as investigações e diminuiria os índices desses crimes.

3.2.2. Questionário Com Público Variado

Foi aplicado um questionário com os alunos do Projeto Informática Cidadã e também com algumas professoras e pedagogas que fazem parte do Grupo de Pesquisa Informática para o Desenvolvimento Humano da UNIBRASIL.

Foram 44 participantes, com idades que variam de 10 a 82 anos. Sendo 16 do sexo masculino (36,4%) e 28 do sexo feminino (63,6%).

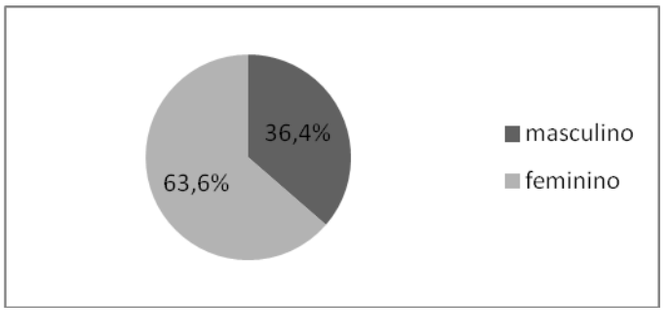

Gráfico 1. Sexo dos participantes.

Perguntado se possuíam internet em casa, apenas 8 pessoas (18,2%) responderam que não tinham, as outras 36 (81,8%) responderam que sim, já contam com o serviço de internet.

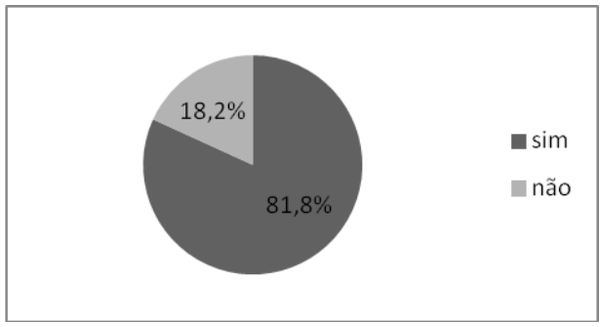

Gráfico 2. Possui conexão a internet em casa?

Dos 44 participantes, 18 souberam responder de forma correta o que é cibercrime. Isso equivale a 40,9% do total, ou seja, menos da metade sabe o que é crime na internet. 12 pessoas (27,3%) não sabem o que é, 11 (25%) sabem parcialmente e 3 (6,8%) não responderam.

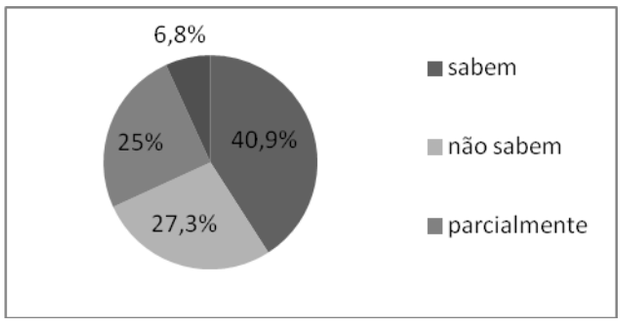

Gráfico 3. Você sabe o que é Cibercrime?

3.2.3. Pesquisa Sobre Lan Houses Na Cidade De Curitiba

Foi realizada uma pesquisa de campo em 6 lan houses de Curitiba, com o objetivo de obter informações sobre o processo utilizado para liberar um computador para o cliente e se esses locais possuíam câmeras de segurança. Foram pesquisadas lan houses nos seguintes bairros: 2 no Boqueirão, 2 no Centro, 1 no Hauer e 1 no Tarumã. Os locais foram escolhidos aleatoriamente.

O objetivo principal era ver como as lan houses estão se comportando depois da aprovação da Lei Estadual nº 16.241/2009 [2]. Foram observados os seguintes itens, processo de solicitar um computador e se haviam câmeras.

Das 6 lan houses pesquisadas, 3 possuíam processo de cadastramento de usuário, 2 tinham circuito fechado de câmeras e em 3 havia comércio de alimentos. Nas lan houses do centro os computadores e as mesas eram melhores e havia mais espaço, já a

maioria das lan houses dos bairros tinham um espaço menor e os computadores não eram muito atualizados.

Lan House	Bairro	Possui cadastramento de usuário	Possui sistema de câmeras de segurança	Possui comercio de alimentos
1	Centro	X	X	X
2	Centro			
3	Boqueirão	X	X	X
4	Boqueirão	X		
5	Hauer			X
6	Tarumã			

Quadro 1. Lan Houses Pesquisadas

4. Conclusão E Trabalhos Futuros

Com o levantamento de dados obtido no decorrer da pesquisa, principalmente na aplicação do questionário, conseguiu-se perceber o quanto a sociedade ainda é mal informada sobre os crimes que podem ser cometidos na ou pela internet.

Ao analisar a pesquisa, é visível que se faz necessário um investimento maior em informação para prevenir de que o crime aconteça e não somente punir e sobrecarregar o sistema judiciário.

Levando em conta o questionário aplicado, a conversa com as crianças que o responderam, crê-se que é de muita valia investir em informação para que educadores possam transmitir o conhecimento a elas.

Um trabalho futuro é desenvolver um site para informar e interagir com esses educadores de forma a alertar os perigos que os crimes na internet geram e suas possíveis prevenções.

Referências

[1] Virilio, P. Cibermundo: A Política do Pior. 1. ed. São Paulo: Teorema, 2000.

[2] Lei Estadual nº 16.241, de 06 de outubro de 2009. Disponível em: http://www.legislacao.pr.gov.br/legislacao/listarAtosAno.do?action=exibir&codAto=52465&indice=1&anoSpan=2009&anoSelecionado=2009&isPaginado=true Acessado em: 17 de junho de 2011.

[3] Instituto Brasileiro De Política E Direito Da Informática - IBDI. Disponível em: http://www.ibdi.org.br/site/legislacao.php?id=9 Acessado em: 18 de abril de 2011.

[4] Santos, J. C. dos. Direito Penal: Parte Geral. 2. ed. Curitiba: ICPC; Lumen Juris, 2007.

[5] Vade Mecum. 9. ed. São Paulo: Saraiva, 2010.

[6] Rosa, F. Crimes de Informática. 1. ed. Campinas: Bookseller, 2002.

[7] Furlaneto Neto, M.; Guimarães, J.. Crimes na Internet: elementos para uma reflexão sobre a ética informacional. Revista CEJ, América do Norte, 720 03 2003.

[8] Lei nº 11.829, de 25 de novembro de 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm Acessado em: 17 de junho de 2011.

[9] Lei nº 10.695, de 1º de julho de 2003. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.695.htm Acessado em: 17 de junho de 2011.

[10] Lei nº 9.609, de 19 de fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm Acessado em: 17 de junho de 2011.

[11] Câmara dos Deputados. Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028 Acessado em: 18 de junho de 2011.

[12] Câmara dos Deputados. Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=493377 Acessado em: 18 de junho de 2011.

[13] Greco, R. Curso de Direito Penal. 11. ed. Rio de Janeiro: Impetus, 2009.