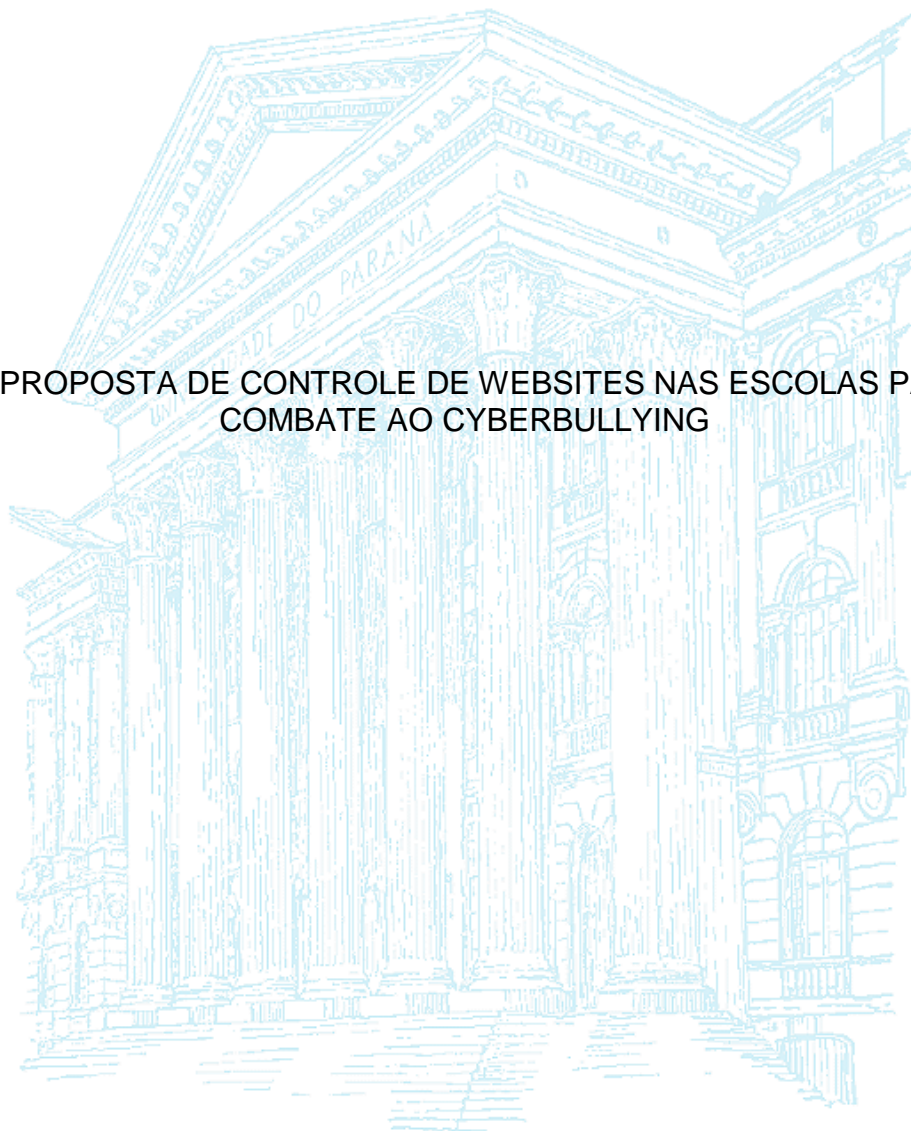


UNIVERSIDADE FEDERAL DO PARANÁ

FRETZ SIEVERS JUNIOR

UMA PROPOSTA DE CONTROLE DE WEBSITES NAS ESCOLAS PARA O  
COMBATE AO CYBERBULLYING



CURITIBA

2016

FRETZ SIEVERS JUNIOR

UMA PROPOSTA DE CONTROLE DE WEBSITES NAS ESCOLAS PARA O  
COMBATE AO CYBERBULLYING

Trabalho de Conclusão do Curso de Pós-Graduação em nível de Especialização em Gênero e Diversidade na Escola, do Setor Litoral da Universidade Federal do Paraná, apresentado como requisito parcial à obtenção do título de Especialista em Gênero e Diversidade na Escola.

Orientador: Prof. Me. Clovis Wanzinack.

Co-orientador Prof. Esp. Christopher  
Smith Bignardi Neves

CURITIBA

2016

## Uma proposta de controle de websites nas escolas para o combate ao *Cyberbullying*

Fretz Sievers Junior<sup>1</sup>; Christopher Smith Bignardi Neves<sup>2</sup>; Clovis Wanzinack<sup>3</sup>

<sup>1</sup>Docente da Faculdade de Tecnologia Mauá/SP; Faculdade de Tecnologia Mogi das Cruzes/SP; UMC – Universidade de Mogi das Cruzes/SP; E-mail: [fretz@uol.com.br](mailto:fretz@uol.com.br)

<sup>2</sup>Graduado em Pedagogia, especialista em Gestão Escolar, Coordenação Pedagógica e em Questão Social. É coordenador pedagógico na Prefeitura Municipal de Paranaguá e professor tutor na UFPR. E-mail: [smithbig@hotmail.com](mailto:smithbig@hotmail.com)

<sup>3</sup> Doutorando em Desenvolvimento Regional (FURB). Docente da Universidade Federal do Paraná E-mail: [cloviswa@gmail.com](mailto:cloviswa@gmail.com)

**Resumo:** Este trabalho tem como objetivo apresentar uma proposta de instalação e configuração de servidores proxy cache nos estabelecimentos escolares para agilizar o acesso à internet e armazenar os dados acessados pelos/as alunos/as na rede mundial de computadores, sendo que esses dados possam ser utilizados para elucidar práticas de *Cyberbullying* entre os estudantes evitando possíveis constrangimentos entre os alunos. Estes servidores podem ajudar no Programa de Combate à Intimidação Sistemática (*Bullying*) em todo o território nacional conforme versa o artigo 1º da lei 13.185, de 6 de novembro de 2015. Foi realizado uma pesquisa quantitativa e qualitativa realizada na rede social *Facebook* e testes realizados com o servidor *Squid* em uma Universidade na cidade de Mogi das Cruzes e como resultados da pesquisa se pode evidenciar que o servidor proposto pode ajudar no combate ao *Cyberbullying* sendo proposta uma infraestrutura de redes com servidores proxy squid através da utilização de software livre.

**Palavras-chave:** *Bullying*; Controle de *Websites*; *Cyberbullying*; Servidor Proxy

**Abstract:** This work aims to present a proposal for installation and configuration of proxy cache servers in schools to speed access to the Internet and store data accessed by / the students / as the World Wide Web, and these data can be used to *Cyberbullying* elucidate practices among students avoiding possible constraints among students. These servers can help in fighting program to Intimidation Systematics (*Bullying*) throughout the national territory as versa Article 1 of Law 13,185 of 6 November 2015 was carried out a quantitative and qualitative research in the social network *Facebook* and tests with *Squid* server at a university in the city of Mogi das Cruzes and how search results can demonstrate that the proposed server can help fight *Cyberbullying* being proposed a network infrastructure with proxy servers squid through the use of free software.

**Keywords:** *Bullying*; Websites Control; *Cyberbullying*; Proxy Server

## INTRODUÇÃO

No Brasil o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.BR)<sup>1</sup>, controla incidentes de segurança que são voluntárias e refletem os incidentes ocorridos que são espontaneamente notificados, onde os incidentes de segurança tiveram um salto significativo do ano de 2013 de 352.925 para 1.047.031 no ano de 2014. Incidentes são considerados como os seguintes tipos de ataques em uma rede de computadores de uma empresa, sendo que escolas, também podem receber esse tipo de ataque. O CERT.BR (2015) considera os seguintes tipos de ataque: *Worm*: notificação de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede; *DoS (Denial of Service)*: notificação de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede; *Invasão*: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede; *Web*: um caso particular de ataque visando especificamente o comportamento de servidores *Web* ou desfigurações de páginas na Internet; *Scan*: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais os serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis possibilidades vulnerabilidades aos serviços habilitados em um computador; *Fraude*: segundo *Houaiss*, é “qualquer ato ardiloso, enganoso, de má-fé, com o intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever logro”. Esta categoria engloba as notificações de tentativas de fraude, ou seja, uma tentativa de obter vantagem; *Outras*: notificações de incidentes que não se enquadram nas categorias anteriores. O Gráfico 1 apresenta os tipos de ataques ocorrido de Janeiro a Dezembro de 2014.

---

<sup>1</sup> CERT.BR, <http://www.cert.br/stats/incidentes/>, acessado em 12/01/2015

### Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2014



Gráfico 1 – Incidentes reportados por tipos. Fonte: Cert.br, 2015

No Gráfico 1 pode-se observar que o maior índice de incidentes reportados é por fraude, que corresponde a 44.66% e isso pode-se inferir que quando uma criança que está utilizando a internet, ela pode ter contato com essa modalidade de incidente na tentativa de enganar os jovens para conseguir algum tipo de vantagem e essa prática pode ser enquadrada em casos de *bullying virtual ou cyberbullying* em crianças e adolescentes.

*Bullying* é todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas. A Lei 13.185 de 6 de novembro de 2015 institui que é dever do estabelecimento de ensino, dos clubes e das agremiações recreativas assegurar medidas de conscientização, prevenção, diagnose e combate a violência e a intimidação sistemática (BRASIL, 2015)

As formas de *bullying* podem ser verbal (insultar, xingar e apelidar pejorativamente), moral (difamar, caluniar, disseminar rumores), sexual (assediar, induzir e/ou abusar), social (ignorar, isolar e excluir), psicológica (perseguir, amedrontar, aterrorizar, intimidar, dominar, manipular, chantagear e infernizar), físico (socar, chutar e bater), material (furtar, roubar, destruir pertences de outrem), virtual (depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social) (BRASIL, 2015).

No formato virtual o *bullying* é intitulado de *cyberbullying*, que utiliza de recursos tecnológicos e a rede mundial de computadores (internet) com mensagens difamatórias, boatos, fofocas, fotos, vídeos entre outros. Os atos são praticados de

formas hostis, configurando-se como uma ferramenta virtual de assédio e agressão, com a intencionalidade de causar dano e sofrimento à vítima (WANZINACK, 2014).

O *cyberbullying* pulam os muros de colégios, tornando até lugares tradicionalmente considerados mais seguros, como os lares, em locais vulneráveis, pois os ataques de *cyberbullying* podem acontecer em momentos inesperados como nas madrugadas, quando a vítima está dormindo em seu quarto, com a sensação de um lugar seguro (WANZINACK, 2014).

Segundo dados do Colégio Notarial do Brasil (CNB), Seção São Paulo, o acesso à informação e a mecanismos de defesa das vítimas também está ampliando o número de registros desses casos junto aos órgãos responsáveis. Pelos dados do CMB-SP, cresceu 70% o número das chamadas atas notariais, registros em cartório que permitem documentar um abuso ou crime para posterior ação legal (IDGNOW, 2014). Em 2012 foram feitas 5.432 atas notariais no Estado de São Paulo; em 2013, foram 9.221 atas e, somente no primeiro semestre de 2014, o total de atos chegou a 6.185. Isso significa um aumento de 69,75% de 2012 para 2013. O total de atos em todo o Brasil chegou a 18.820 em 2012 e a 32.011 em 2013, totalizando um aumento de 70% em nível nacional (IDGNOW, 2014). As atas notariais são utilizadas para documentar os fatos ocorridos, para futuras ações indenizatórias.

A eCGlobal (2012) realizou um estudo com 324 crianças e adolescentes brasileiros com idade entre 8 e 17 anos. Foi perguntado aos entrevistados os seus conhecimentos sobre o *cyberbullying*, sendo de 72,20% das crianças e jovens brasileiros disseram saber o significado desta palavra e os meios pelos quais ela é praticada. Dos 42,52% dos adolescentes brasileiros disseram que sofreram atos humilhantes na internet por outros usuários e 24,88 % admitiram já ter feito algum tipo de brincadeira maldosa através da web para um colega. Para os 74% dos entrevistados, a situação mais vergonhosa que eles poderiam passar na Internet é alguém postar alguma foto íntima deles nas redes sociais (eCGlobal, 2012).

De acordo com a SaferNet (2015) em 8 anos, foi recebido e processado 3.606.419 denúncias anônimas, envolvendo 585.778 páginas (URLs) distintas escritas em 9 idiomas e hospedadas em 72.739 hosts diferentes, conectados à Internet através de 41.354 números IPs distintos, atribuídos para 96 países em 5 continentes. Ajudou 9.577 pessoas em 24 estados e foram atendidos 914 crianças e adolescentes, 1098 pais e educadores e 7326 outros adultos em seu canal de ajuda e orientação. Além disso, foram realizadas 452 atividades de sensibilização e

formação de multiplicadores em 58 cidades, 20 estados, contemplando 15.162 crianças e adolescentes, 18.234 pais e educadores e 865 autoridades, com foco na conscientização para boas escolhas online e uso responsável da Internet. Entre os tipos de conteúdos denunciados temos Intolerância religiosa, sendo encontrado nos EUA com 481.147 páginas que versam sobre o assunto.

Outros casos relatados de *bullying* extremo sendo a violência de forma reiterada que as vítimas são submetidas, como aponta Wanzinack e Reis (2015), sendo o *cyberbullying* um problema mundial conforme os trágicos casos citados em apertada síntese a seguir:

- 1) Caso da jovem Rehtaeh Parsons, uma canadense de 17 anos, que se enforcou em abril de 2013 após meses de assédio e ofensas pela internet. Sua morte foi atribuída à distribuição de fotos online de um estupro coletivo que ocorreu 17 meses antes do suicídio, causou comoção nacional e motivou a aprovação de uma lei na província canadense de Nova Scotia para punir esse tipo de crime. O Estado também é o único do país a ter criado a primeira unidade de polícia que cuida exclusivamente de queixas de *cyberbullying* (PARSON, 2014)<sup>2</sup>.
- 2) Caso da jovem Amanda Michelle Todd, uma canadense de 15 anos vítima de *bullying* online, comoveu o país e motivou homenagens em várias partes do mundo. Amanda Michelle Todd foi encontrada morta em sua casa depois de postar um vídeo no *You tube* em que contava sua história e pedia ajuda. A adolescente estava em um chat que após receber vários elogios, a pessoa que estava conversando com ela pediu uma foto de seus seios, depois o agressor começou a ameaçar que iria publicar sua foto na internet (TODD, 2012)<sup>3</sup>.
- 3) Caso da brasileira Julia Gabriele de 12 anos, foi vítima de *Cyberbullying* promovidos por algumas páginas de “humor” no Facebook. Foi postado fotos

---

<sup>2</sup> PARSON, Rehtaeh, Um ano depois, pai relata suicídio da filha após cyberbullying, 2014, disponível em [http://www.bbc.com/portuguese/noticias/2014/04/140403\\_bullying\\_suicidio\\_canada\\_fl](http://www.bbc.com/portuguese/noticias/2014/04/140403_bullying_suicidio_canada_fl)

<sup>3</sup> TODD, Suicídio de garota vítima de *cyberbullying* comove Canadá, 2012. Disponível em < <http://veja.abril.com.br/noticia/mundo/suicidio-de-vitima-de-ciberbullying-comove-canada/>>, acessado em 30/12/2015

que fizeram brincadeiras desagradáveis sobre seus pêlos faciais (*TodaTeen*, 2013)<sup>4</sup>.

Outra pesquisa realizada pela CGI.BR (2014) que teve como objetivo medir o uso e hábitos da população brasileira usuária de Internet de 9 a 17 anos em relação às tecnologias de informação e de comunicação (TIC). Esta pesquisa foi realizada com 2.105 usuários. Ponderou os tipos de equipamentos utilizados por crianças/adolescentes para acessar a Internet, sendo o percentual sobre o total de usuários de Internet entre 9 a 17 anos, sendo que a pesquisa constatou que os adolescentes, acessam mais a internet pelos dispositivos móveis (celulares, *tablets*, etc) estão sendo utilizados pelo público jovem sendo que nestes casos o *cyberbullying* pode ser realizado por esses dispositivos. O mesmo foi encontrado na pesquisa realizada por Massad e Wanzinack (2015), sendo direcionada para 350 alunos/as do Ensino Fundamental II e Ensino Médio com idade entre 11 e 18 anos do município de Curitiba – PR sobre o acesso a Internet, constatou que 252 alunos/as (72%) acessam a internet pelo celular; 42 (12%) alunos pelo laptop, 28 (8%) acessam pelo tablete e 28 (8%) acessam de outras formas.

Outro dado interessante é uma pesquisa realizada pela CETIC.br (2015) sobre o perfil próprio em redes sociais mais utilizada por criança/adolescente entre a idade 9 a 17 anos, em uma base ponderada com 2.261 usuários de internet, sendo que a rede social *Facebook* atingiu 77 pontos, o *Orkut* com 1 ponto e outras redes 9 pontos em 2013. Na pesquisa realizada por Massad e Wanzinack (2015), constatou que 273 alunos/as (78%) acessam as redes sociais, dentro dessa faixa, as redes mais acessadas foram o *Facebook* com 68%, *Instagram* com 20% e *You tube* com 12%. Ou seja, com os dados apresentados acima, pode-se concluir que a internet apesar de trazer uma série de serviços aos seus usuários (pesquisa, entretenimento, informação, etc) também oferece um ambiente hostil para crianças e adolescentes que estão em formação e isso pode trazer muitos problemas aos estudantes e que precisam ser monitorados para não afetar a vida das vítimas de *cyberbullying*.

Esta pesquisa será realizada de forma bibliográfica e realizado uma pesquisa de campo de como poderia funcionar os proxy cache nas escolas, visando auxiliar

---

<sup>4</sup> TodaTeen, <http://todateen.uol.com.br/souassimtt/entenda-caso-julia-gabriele-adolescente-brasileira-sofreu-cyberbullying/>, 27/03/2013



no combate de práticas que agredam seus alunos, atrapalhando seu desenvolvimento.

Apresentar uma proposta de instalação de servidores de controle de sítios visando identificar ações de *cyberbullying* no ambiente escolar que se trata de uma ameaça na formação do cidadão, causando dano moral e material para suas vítimas.

## **METODOLOGIA**

As pesquisas citadas acima demonstram uma acentuada violência nas escolas, mesmo que os casos relatados sejam poucos estamos tratando de vidas sendo o bem mais valioso e neste caso toda a vida é importante. Esta pesquisa focou na em uma proposta para o problema do *cyberbullying*. A pesquisa iniciou-se com o curso de Especialização de Gênero e Diversidade na Escola, sendo este tema uma das disciplinas deste curso.

Trata-se de um estudo exploratório transversal de caráter qualitativo e quantitativo. A amostra foi construída por cento e vinte um (n=121) sendo uma pesquisa realizada na rede social *Facebook*, sendo que as pesquisas supracitadas indicam essa rede social sendo a mais utilizada e também a mais utilizada para o *cyberbullying*. Neste artigo será descrito os resultados sobre o *bullying* e *cyberbullying* e realizar uma proposta para ajudar no combate dessa prática. As idades dos participantes variam entre 16 a maiores de 28 anos, que responderam anônima e voluntariamente a um formulário de pesquisa contendo 15 questões objetivas através da ferramenta de criação de formulários do *google docs*, o qual foi postado na rede social *Facebook* que possui cerca de 2160 pessoas cadastradas que receberam o convite. A pesquisa versa a respeito da violência no contexto escolar *bullying* e *cyberbullying* e seus desdobramentos. Os dados quantitativos foram tabulados em uma base de dados online e analisados mediante estatística descritiva enquanto os dados qualitativos foram transcritos e analisados tematicamente a partir de categorias emergentes.

Foi realizado uma pesquisa em campo para demonstrar como os servidores proxy podem ajudar no combate ao *cyberbullying* utilizando um servidor Squid (squid, 2015), instalado em um sistema operacional Linux e simulando casos que

poderiam acontecer e como eles podem ser detectados. No final será realizado uma proposta de uma arquitetura de servidores.

## RESULTADOS E DISCUSSÃO

A partir de uma pesquisa de campo realizada com estudantes no Estado de São Paulo, utilizando o método quantitativo. A primeira pergunta foi “*Qual seu gênero?*”, sendo que o formulário tinha as seguintes opções: masculino, feminino, lésbicas, gays, bissexuais, transexuais, outros. Sendo que 48% dos participantes se declararam do feminino, 45% do gênero masculino e 6% não informaram seu gênero.

A segunda pergunta feita foi: “*Qual sua idade?*”, sendo que foi observado que 54% dos participantes possuem mais de 28 anos, isso se dá pelo fato que são oriundos dos cursos de ensino superior, isso foi constatado através de entrevista por redes sociais nas ferramentas de comunicação. Sendo que 20% dos participantes possuem de 26 a 28 anos, 13% dos participantes possuem entre 23 a 25 anos, 9% dos participantes possuem de 20 a 22 anos e somente 2% dos participantes com idade entre 17 e 19 anos. Todos os participantes da pesquisa já passaram pelo ensino básico e por isso responderam a pesquisa através de suas experiências. Os dados podem ser observados no Gráfico 2.

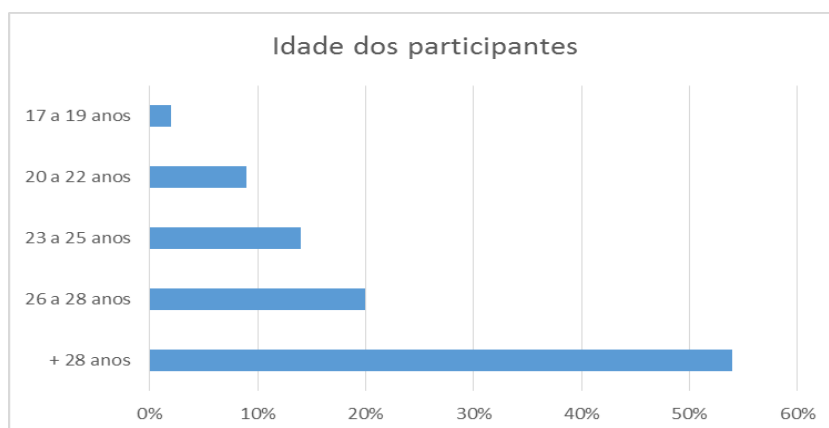


Gráfico 2 – Idade dos participantes. Fonte: dos autores

Na questão 3 foi realizada a seguintes pergunta: “*Já ouviu falar sobre bullying ou cyberbullying?*”, dos entrevistados que participaram da pesquisa, 98% responderam que sim, sendo que 2% deixaram essa questão em branco. Isso mostra que o tema tratado é de conhecimento da maioria dos entrevistados.

Na questão 4 foi perguntado aos entrevistados se já sofreram algum tipo de violência no ambiente escolar. Do total de participantes, 77% dos entrevistados responderam que sim e 21% responderam que não, 2% não responderam. Sendo que as implicações de exposição à violência no ambiente escolar praticada na rede de computadores ou no ambiente escolar, refletem em dificuldade de concentração, queda do desempenho escolar/acadêmico e medo de frequentar o ambiente escolar (WANZINACK e REIS, 2015b *apud* MALDONADO, 2011; RIBEIRO et al.,2009).

Na questão 5 foi realizada a pergunta: “*Que tipo de agressão você sofreu no ensino médio ou fundamental ?*” Esta questão os entrevistados poderiam escolher mais de um tipo de violência, sendo que 87 informaram que sofreram agressão verbal (insultar, xingar e apelidar pejorativamente), como e o caso de serem xingados como “gordos”, magrelos”, etc. O segundo tipo de violência mais votado foi a violência social (ignorar, isolar e excluir) com 47 pontos, ou seja, pessoas foram ignoradas no ambiente escolar através de grupos que não aceitavam alguns tipos de pessoas em seu convívio social. Os dados apresentados se encontram no Gráfico 3 Em seguida temos violência moral (difamar, caluniar, disseminar rumores) com 38 pontos, sendo que essas práticas no ambiente escolar não forem evitadas podem constituir em crime no futuro que são previstos no Código Penal Brasileiro como crimes contra a honra previstos nos artigos 138, 139 e 140.

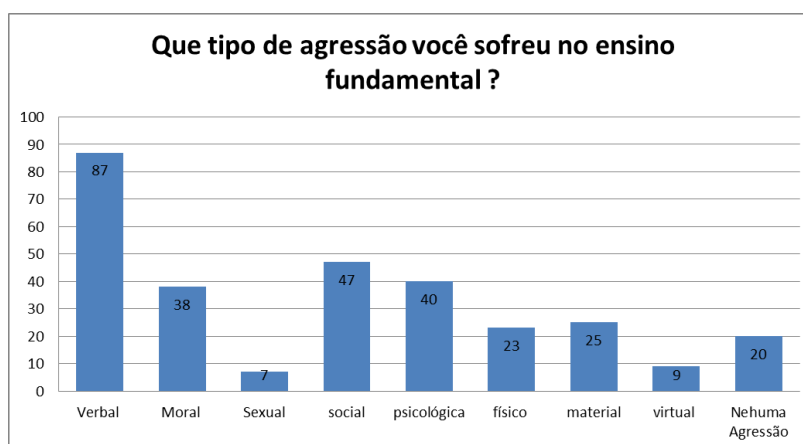


Gráfico 3 – Que tipo de agressão você sofreu no ensino fundamental? Fonte: dos autores

Somente é considerado crime para os maiores de 18 anos de idade, menores não podem responder por crimes do código penal, mas podem ser aplicadas medidas socioeducativas sendo medidas aplicáveis a adolescentes autores de atos infracionais e estão previstas no art. 112 do Estatuto da Criança e do Adolescente (ECA). Apesar de configurarem resposta à prática de um delito, apresentam um

caráter predominantemente educativo e não punitivo. Pessoas na faixa etária entre 12 e 18 anos, podendo, excepcionalmente, estender sua aplicação a jovens com até 21 anos incompletos, conforme previsto no art. 2º do ECA. O Juiz da Infância e da Juventude é o competente para proferir sentenças socioeducativas, após análise da capacidade do adolescente de cumprir a medida, das circunstâncias do fato e da gravidade da infração (TJDFT, 2015). Se esses tipos de violência ocorrem na escola, algo está errado, pois não é cabível a escola formar agressores e fazer vítimas, mas sim é formar cidadãos saudáveis preparados para viver em sociedade.

Com 40 pontos notamos a violência psicológica (perseguir, amedrontar, aterrorizar, intimidar, dominar, manipular, chantagear e infernizar). Segundo (AMADO et al., 2009), as novas tecnologias de informação, e comunicação são cada vez mais utilizadas para fins ilícitos, entre os quais se destacam a perseguição sistemática entre colegas e outros. Trata-se neste caso uma forma indireta de *Bullying* e que se tem designado como *Cyberbullying*. Em seguida com 25 pontos a violência material (furtar, roubar, destruir pertences de outrem), encontra-se o verbo furtar e roubar no Código Penal Brasileiro nos artigos 155 e 157. A violência física (socar, chutar e bater) teve 23 pontos. Essas ações do agente, pode levar a lesão corporal que pode ser classificada como leve, grave ou gravíssima, que conforme previsto no Código Penal Brasileiro que versa no Art. 129: “Ofender a integridade corporal ou a saúde de outrem: Pena - detenção, de três meses a um ano”.

Com 8 pontos, aparece a violência virtual (depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social). O *Cyberbullying* pode ser causado colocando uma foto íntima que a própria vítima divulgou em sua rede social ou para o próprio atacante que muitas vezes utiliza a Engenharia Social. Conforme Parodi (2008), Engenharia Social é aquele conjunto de métodos e técnicas que tem como objetivo obter informações sigilosas e importantes através da exploração da confiança das pessoas, de técnicas investigativas, de técnicas psicológicas de enganação etc. Ou seja, o Engenheiro Social pode se passar por outra pessoa. A rede mundial de computadores permite de várias formas você conseguir passar por outra pessoa, através de perfis falsos, nas redes sociais, chats, fóruns entre outros e os alunos podem estar expostos a esse tipo de ataque.

Após as pesquisas feitas pode-se verificar que os alunos do ensino fundamental e ensino médio estão sujeitos a diversos tipos de violência e a internet

precisa ser monitorada para impedir que nossos alunos sejam vítimas de qualquer tipo de violência, e caso ocorra, que a escola tenha ferramentas para identificar os atos violentos e conseguir intervir, para que nem autores e vítima dessa violência tenha sua formação deturbada, e possam formar pessoas de boa índole.

Uma dos recursos do servidor proxy é o controle de acesso, conforme ensina Ricci e Mendonça (2006) é o servidor WebProxy/Cache que centraliza as conexões http e https, pois possui a capacidade de interpretá-la, armazenando o conteúdo mais acessado e permitindo os benefícios de velocidade de acesso, economia de recursos e controle de acesso. O software *Squid* utilizado nessa pesquisa é um software livre, totalmente gratuito.

No caso em tela, o benefício que nos interessa é o controle de acesso, que permite caso o administrador de rede deseje, fazer uma auditoria de como a internet da escola está sendo utilizado. A Figura 1 apresenta uma arquitetura de redes.

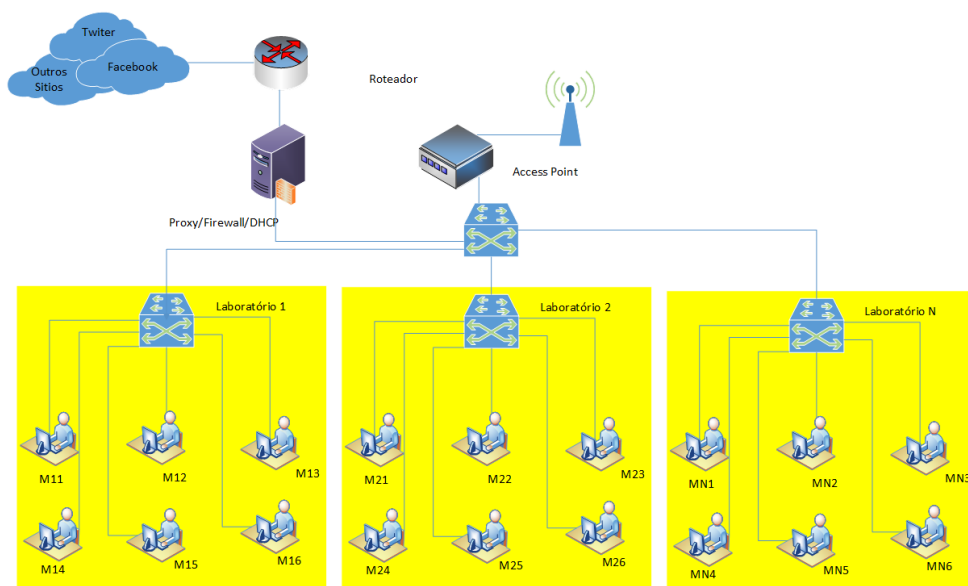


Figura 1 – Proposta de Instalação de um Proxy nas Escolas Fonte: dos autores

Lunardi (2005), nos simplifica o entendimento de como isso funciona, supondo que o/a aluno/a da máquina M14 solicita um site qualquer, como por exemplo ([www.seusite.com.br](http://www.seusite.com.br)) será realizado uma solicitação ao proxy que por sua vez fará o acesso ao [www.seusite.com.br](http://www.seusite.com.br), guarda no cache e entrega a máquina M14. Supondo que o aluno que está usando o computador M24 solicita o mesmo site ao Proxy, o Proxy como ele já possui esse site, ele entrega para a máquina M24 sem ter a necessidade de consumir banda da internet. Essa é a função de cache do *WebProxy*.

Outra função possível do Servidor Proxy é o bloqueio do acesso, exemplo: o professor do Laboratório 2 não deseja que seus alunos acessem a internet em um determinado momento, neste caso, uma das formas de fazer o bloqueio e através do número ip do computador ou de um endereço de placa de rede intitulado *MAC Address*, que pode identificar cada computador de forma única.

Todas as páginas que são acessadas pelos alunos/as na rede de computadores é armazenado em um arquivo intitulado *access.log* que permite saber qual o site foi acessado, o horário e qual a máquina, neste caso é possível descobrir quais tipos de sites e em que horário os alunos estão acessando. Supondo que em uma aula de matemática no qual os alunos irão trabalhar com um software específico e ao analisar o log verifica que o aluno acessou um site não recomendado. Isso pode apresentar que o aluno não está realizando as atividades sugeridas pelos docentes; e caso tenha ocorrência de *cyberbullying* pode-se verificar o que esse aluno estava acessando e em qual horário. Isso pode ser utilizado na casa do aluno para seus pais.

O *proxy* permite a criação de regras de acesso. Supondo que se deseja criar uma regra para restringir o acesso a internet no horário de aula, ou seja das 08:00 as 22:00 hrs de segunda a sexta-feira para a sub-rede 192.168.0. No arquivo de configuração colocaria a seguinte configuração apresentado na Listagem 1.

```
acl rede_escolar src 192.168.0.0/24  
acl hescolar_acl time M T W H F 08:00 -18:00  
http_access allow rede_internet_escolar hescolar_acl
```

Listagem 1-Exemplo de regras para restringir horário Fonte:(dos autores)

É possível também fazer o bloqueio através de palavras chaves encontrado nas páginas, porém vale lembrar que esse bloqueio deve ser feito com cautela, pois caso seja bloqueado a palavra sex, caso encontre uma palavra sextavada, será bloqueado também. Para bloquear sites de acordo com uma lista de palavras-chave ou expressões regulares contidas em um arquivo texto a Listagem 2 apresenta a configuração que deve ser feita:

```
acl palavrasproibidas_acl url_regex "/usr/local/squid/etc/palavrasproibidas.txt"  
http_access deny palavrasproibidas_acl
```

Listagem 2-Exemplo de regras para restringir palavras proibidas Fonte: (dos autores)

No arquivo texto `palavrasproibidas.txt`, localizado no diretório `/usr/local/squid`, inclui palavras proibidas uma por linha. Caso o administrador de rede decida bloquear sites específicos pode-se utilizar a seguinte Listagem 3.

```
acl sitesproibidos_acl dstdomaus "/usr/local/squid/etc/sitesproibidos.txt"  
http_access deny sitesproibidos_acl
```

Listagem 3-Exemplo de regras para restringir sites proibidos Fonte: (dos autores)

Pode-se permitir que usuários específicos tenham acessos diferentes, supondo que os professores precisam ter acesso ao site youtube mas os alunos não, nesse caso pode-se criar a seguinte regra, conforme implementada na Listagem 4.

```
acl prof_youtube sec "/src/local/squid/etc/prof_youtube.txt"  
http_access allow prof_youtube
```

Listagem 4-Exemplo de regras para restringir sites proibidos Fonte: (dos autores)

O software Squid permite adicionar outros tipos de regras de acesso a internet como integração com firewalls, autenticação com outras bases de dados, que podem ser interessantes ao ambiente escolar que podem melhorar o gerenciamento dos recursos da Internet e ao combate ao *cyberbullying*.

## CONSIDERAÇÕES FINAIS

Com as novas tecnologias da informação surgiu a sociedade da informação, que tem acesso a diversas ferramentas de comunicação (e-mail, fórum, chat, redes sociais, serviços de mensageria instantânea, etc). Essas ferramentas ajudam muito a vida moderna, mas também podem ser utilizadas de forma pejorativa como é o caso do *cyberbullying*, sendo uma maneira de cometer alguns tipos de violência (verbal, moral, social, psicológica, material) só que sem a presença física do agressor e da vítima, podendo ser realizado a qualquer hora e em qualquer lugar. O lugar físico foi substituído por redes sociais (*facebook*, *twiter*, etc) ou por ferramentas de mensageria instantânea como Messenger ou WhatsApp que podem ser acessados via computadores desktop ou dispositivos mobile.

Visando essa nova modalidade de violência surge a proposta de instalação de servidores de controle de sítios visando identificar ações de *cyberbullying* no ambiente escolar que se trata de uma ameaça na formação do cidadão, causando dano moral e material para suas vítimas. O software *Squid* é um proxy livre e

gratuito que neste caso as escolas teriam que realizar um investimento com hardware e uma mão de obra especializada em redes de computadores, para analisar o comportamento dos estudantes na rede mundial de computadores e neste caso da proposta vir ser aceita será necessário um profissional de redes de computadores para a realização da análise dos dados ou realizar um treinamento com um funcionário da escola.

Na pesquisa quantitativa revelou que 93% dos entrevistados já sofreram *bullying* ou *cyberbullying*, sendo que 6% já viram colegas sofrerem *cyberbullying*, apesar do número parecer relativamente pequeno, deve-se lembrar que estamos considerando uma violência a vida e mesmo que fosse 1% seria muito pois não pode-se tolerar tipos de comportamentos que ferem os direitos humanos e a vida como citado, caso levaram à ceifar vida, assim, a escola deve-se preparar para combater o *cyberbullying*, para saber como agir quando casos narrados nessa pesquisa ocorra, identificando indícios o mais rápido possível sendo que a ferramenta *proxy* pode auxiliar nessa tarefa.

Na pesquisa qualitativa foi realizado testes na configuração do servidor *Squid* o qual apresentou uma ferramenta que permite colocar regras no uso da internet e permitindo verificar o tipo de sites acessados, propiciando configurações porá o combate ao *cyberbullying*.

## **AGRADECIMENTOS**

Agradeço aos egrégios docentes da UFPR – Universidade Federal do Paraná – Litoral pelo excelente curso oferecido de Especialização em Gênero e Diversidade na Escola. Aos meus orientadores Prof. Christopher Smith Bignardi Neves e Prof. Clovis Wanzinack que sempre esteve ativamente ajudando nessa pesquisa e a todo o corpo docente que ministrou com esmero e dedicação as aulas presenciais e ofereceu a todos os discentes um material de ótima qualidade.

## **REFERÊNCIAS BIBLIOGRÁFICAS**

AMADO, J. MATOS, A. PESSOA, T. Cyberbullying: um novo campo de investigação e de formação, Actas do X Congresso Internacional Galego-Português de Psicopedagogia. Braga: Universidade do Minho, 2009.

BRASIL. Lei 13.185 de 06 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Disponível em



[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2015/Lei/L13185.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13185.htm) acessado em 21/01/2016.

\_\_\_\_\_. Lei 8069 de 13 de julho de 1990. Estatuto da Criança e do Adolescente. Disponível em [http://www.planalto.gov.br/ccivil\\_03/LEIS/L8069.htm](http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm) Acesso em 21/01/2016

\_\_\_\_\_. Decreto Lei nº 2.848, de 07 de Dezembro de 1940. Código Penal. Disponível em [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm) Acessado em 21/01/2016.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, ano 2014, acessado em 12/01/2015

CETIC.BR, Pesquisa sobre o uso da internet por crianças e adolescentes no Brasil [livro eletrônico]: TIC Kids Online Brasil 2014 coordenação executiva e editorial Alexandre F. Barbosa, São Paulo: Comitê Gestor da Internet no Brasil, 2015.

CGI.BR, [http://data.cetic.br/cetic/explore?idPesquisa=TIC\\_KIDS](http://data.cetic.br/cetic/explore?idPesquisa=TIC_KIDS), ano 2014, acessado em 01/01/2016

eCGlobal, Pesquisa sobre Cyberbullying, <http://pt.slideshare.net/ecglobal/resultados-da-pesquisa-sobre-o-cyberbullyng-15516417>, publicada em 06/12/2012, acessada em 30/12/2015

IDGNOW, Revista de Tecnologia, <http://idgnow.com.br/internet/2014/10/21/cartorios-sinalizam-alta-no-registro-de-assedio-e-crimes-virtuais-no-brasil/>, data de publicação 21/10/2014, acessado em 30/12/2015.

LUNARDI, Marco Agisander, Squid: Prático e didático, Rio de Janeiro, Editora Ciência Moderna, 2005.

MASSAD, C. E; WANZINACK, C. Cyberbullying: Uma proposta de discussão e sensibilização na educação básica. In: Wanzinack, C; Signorelli, M. C. Violência Gênero e Diversidade: Desafios para a educação e o desenvolvimento. Rio de Janeiro: Autografia, 2015. cap.07, p.149-167.

PARODI, Lorenzo, Manual das fraudes, 2º ed, Rio de Janeiro, Brasport, 2008

PARSON, Rehtaeh, Um ano depois, pai relata suicídio da filha após cyberbullying, 2014, disponível em [http://www.bbc.com/portuguese/noticias/2014/04/140403\\_bullying\\_suicidio\\_canada\\_fl](http://www.bbc.com/portuguese/noticias/2014/04/140403_bullying_suicidio_canada_fl) Acessado em 21/01/2016

RICCI, Bruno e MENDONÇA, Nelson, Squid – Solução Definitiva, Rio de Janeiro, Ciência Moderna, 2006

SAFERNET, <http://indicadores.safernet.org.br/indicadores.html>, acessado em 30/12/2015

SQUID, <http://www.squid-cache.org/>, acessado em 30/12/2015

TJDFT, Tribunal de Justiça do Distrito Federal e dos Territórios, <http://www.tjdft.jus.br/cidadaos/infancia-e-juventude/informacoes/medidas-socioeducativas-1>, acessado em 05/01/2015.

TODATEEN, <http://todateen.uol.com.br/souassimtt/entenda-caso-julia-gabriele-adolescente-brasileira-sofreu-cyberbullying> de 27/03/2013 acessado em 21/01/2016.

TOOD,2012, Suicídio de garota vítima de cyberbullying comove Canadá, 2012. Disponível em < <http://veja.abril.com.br/noticia/mundo/suicidio-de-vitima-de-cyberbullying-comove-canada/>>, acessado em 30/12/2015

WANZINACK, C., REIS, C., Cyberbullying e Globalização da Tecnologia: Um estudo Territorial no Litoral do Paraná. Divers@ Revista Eletrônica Interdisciplinar, Matinhos, v.8, n.1, p. 51-57, jan/jun 2015a.

WANZINACK, C, Cyberbullying e violência na rede: relações entre poder e desenvolvimento no litoral do Paraná. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, Rio de Janeiro, 4 a 07/09/2015b.

\_\_\_\_\_., Violência de gênero no ambiente escolar: Estudo territorial do litoral do paraná. In: SIERRA, J. C.; SIGNORELLI, M. C. Diversidade e Educação intersecções entre corpo, gênero e sexualidade, raça e etnia, Matinhos: UFPR Litoral, 2014, p.67-82

## ANEXO

### Pesquisa sobre *Bullying* e *Cyberbullying*

Convidamos o(a) Sr.(a) para participar de uma pesquisa intitulada PESQUISA SOBRE BULLYING E CYBERBULLYING, que objetiva apresentar uma proposta de instalação de servidores de controle de sítios, visando identificar ações de *cyberbullying* no ambiente escolar que se trata de uma ameaça na formação do cidadão, causando dano moral e material para suas vítimas. Desenvolvida como Trabalho de Conclusão do Curso de Especialização em Gênero e Diversidade na Escola da Universidade Federal do Paraná, sob orientação do Prof. Christopher Smith Bignardi Neves e Prof. Clovis Wanzinack. Consideramos que sua participação será de extrema importância, uma vez que essa pesquisa possibilitará saber qual sua opinião a respeito do *bullying* e *cyberbullying*. Gostaríamos de acrescentar que todos os cuidados éticos serão respeitados, principalmente o que concerne ao seu anonimato, confidencialidade e ao sigilo das informações que a Sr.(a) nos prestar. Os dados serão armazenados em local próprio, com acesso realizado apenas pelos pesquisadores. Os resultados do estudo poderão ser publicados apenas em eventos/periódicos de cunho científico, sempre sem a identificação dos participantes. Realizaremos uma pesquisa quantitativa e qualitativa. A participação nesse estudo é voluntária e, caso o(a) Sr(a) aceite participar, ainda assim, poderá desistir a qualquer momento sem qualquer consequência ou prejuízo. A participação na pesquisa não terá nenhum custo financeiro.

1 – Qual seu gênero?

- masculino  
 feminino  
 outro

2 – Qual sua idade?

- 08 a 10 anos  
 11 a 13 anos  
 14 a 16 anos  
 17 a 19 anos  
 20 a 22 anos  
 23 a 25 anos  
 26 a 28 anos  
 maior que 28 anos

3 – Já ouviu falar sobre *Bullying* ou *Cyberbullying*?

- sim  
 não

4 – Já sofreu algum tipo de violência no ambiente escolar?

- sim  
 não

5 – Que tipo de agressão você sofreu no ensino médio ou fundamental?

- verbal (insultar, xingar e apelidar pejorativamente)  
 moral (difamar, caluniar, disseminar rumores)  
 sexual (assediar, induzir e/ou abusar)  
 social (ignorar, isolar e excluir)  
 psicológica (perseguir, amedrontar, aterrorizar, intimidar, dominar, manipular, chantagear e infernizar)  
 físico (socar, chutar e bater)  
 material (furtar, roubar, destruir pertences de outrem)

- virtual (depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social)  
 não sofreu nenhum tipo de agressão

6 – Você já viu algum colega na escola do ensino fundamental ou médio sofrer algum tipo das agressões abaixo?

- verbal (insultar, xingar e apelidar pejorativamente)  
 moral (difamar, caluniar, disseminar rumores)  
 sexual (assediar, induzir e/ou abusar)  
 social (ignorar, isolar e excluir)  
 psicológica (perseguir, amedrontar, aterrorizar, intimidar, dominar, manipular, chantagear e infernizar)  
 físico (socar, chutar e bater)  
 material (furtar, roubar, destruir pertences de outrem)  
 virtual (depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social)  
 nunca vi nenhum colega sofrer nenhum tipo de agressão

7 – Já aconteceu de alguém querer depreciar sua reputação pela internet por ferramentas de comunicação (email, fórum, *Facebook*, *Twitter*, *Instagram* ou outro)?

- sim  
 não

8 – Já aconteceu de receber mensagens intrusivas da sua intimidade através da Internet?

- sim  
 não

9 – Já ouviu algum caso de pessoas enviarem fotos ou adulterar dados pessoais na Internet no meio escolar com o intuito de criar meios de constrangimento psicológico e social?

- sim  
 não

10 – Supondo que você seja pai ou mãe, gostaria de ter o controle do que seus filhos estão acessando na internet, de forma gratuita, para que a escola tome alguma ação sobre o cyberbullying?

- sim  
 não

11 – Você já foi ameaçado/a ou insultado/a com mensagens em seu telefone ou correio eletrônico?

- sim  
 não

12 – Caso tenha sofrido cyberbullying, qual foi o meio utilizado

- Mensagens por telefone  
 Contas de email falsas  
 Perfil falso em redes sociais  
 Serviços de Mensageiria Instantânea (whatsapp, chat, etc)  
 Outros

13 – Já contou a alguém que foi vítima de bullying/cyberbullying?

- Nunca fui vítima  
 Fui vítima mas não contei a ninguém  
 Fui vítima e contei a alguém

14 – Você já ouviu falar da LEI 13.185/2015 que institui o programa de combate à intimidação sistemática (bullying) ?

- sim  
 não

15 – Como você que já passou por algum tipo de violência se sentiu?

- triste  
 com medo  
 com vontade de morrer  
 deixou de ir para a escola  
 com depressão  
 não senti nenhum desses sentimentos