Guilherme Pereira da Silva
Hemilly Maciel Diniz

HACKER e CRACKER:Um estudo sobre suas diferenças e os crimes virtuais

Paracatu -MG
Junho - 2017

Guilherme Pereira da Silva
Hemilly Maciel Diniz

HACKER e CRACKER:Um estudo sobre suas diferenças e os crimes virtuais

Trabalho de Conclusão de Curso apresentado ao Instituto Federal de Educação,Ciência e Tecnologia do Triângulo Mineiro, Campus Paracatu, com requisito parcial para conclusão do Curso Técnico em Informática.

Orientador: Ernani Vinicius Damasceno

Paracatu -MG
Junho - 2017

Sumário

1 Introdução

No decorrer da Segunda Guerra Mundial os governantes de parte dos países aliados, se reuniram em Yalta. Nesta reunião ficou determinado as novas divisões da Alemanha. Após o fim da guerra os alemães ficaram com um prejuízo muito alto, assim tendo que pagar indenizações altas e perdendo território. De acordo com pesquisas, a chamada Guerra Fria deu início após reunião entre os governos aliados. Nela chegou num acordo que o país russo possuía mais poder que os demais. Com a separação dos dois lados deu início a essa guerra. Assim, um e outro começaram a espiar para que não sofresse ataque do adversário. Dessa forma estabelecer estabilidade militar, pois o exército russo era o mais poderoso.

Tempos depois – em outubro de 1957 – , os russos lançaram um satélite (*Sputnik*, foi o primeiro da história) para o espaço que fazia a órbita da terra em 90 minutos. Em contrapartida os EUA criaram o sistema militar ARPA (Agência de Projetos e Pesquisas Avançadas –*Advanced Research Projects Agency*), para prevenir ataques tecnológicos surpresos. Segundo Marcelo

> A partir do final da década de 1950, no auge da Guerra Fria, o mundo passou a assistir a uma acirrada corrida espacial, que começou com a liderança isolada dos soviéticos, ao lançarem, em outubro de 1957,o satélite Sputnik I. O departamento de Defesa dos Estados Unidos reagiu criando, em seguida, a Advanced Research Projects Agency (ARPA), uma agência militar de pesquisas, apoiada no discurso do restabelecimento da vanguarda norte-americana em ciência e tecnologia, com a missão de prevenir surpresas tenológicas (como Sputnik) e servir como mecanismo para pesquisa e desenvolvimento de alto risco, nos casos em que a tecnologia estivesse em estágio inicial ou que a oportunidade tenológica fossem além da missão dos departamentos militares."(CARVALHO, 2006)

Porém, com a criação a NASA (Administração Nacional Aeronáutica e Espacial – *National Aeronautics and Space Administration*), o sistema ARPA quase deixou de existir . O seu software foi entregue a nova agência civil. E os outros foguetes foram entregues a outras forças militares. Para evitar que fosse extinguida foi criado o Departamento de Defesa, e o mesmo ficaria com as responsabilidades da ARPA e das demais forças militares. Assim, a mesma começou a atuar em áreas de programação e foi feita a troca de diretor de Roy Johnson para Jack Ruina.

Mais adiante, um grupo de pessoas surgiu, e o mesmo estudava sobre as redes de computadores. Esse grupo possuía o nome de NWG (*Network Working Group* – Grupo de Trabalho da Rede), e com a evolução dos estudos realizados por eles mudaram o nome para NCP (*Network Control Protocol* – Protocolo de Controle da Rede). Esta mesma equipe criaram uma linguagem de programação a qual funcionava em qualquer *hardware*

que a aguentasse. A propósito tal protocolo gerenciava as mensagens que eram enviadas, recebidas, por exemplo.

Além disso, dois dos integrantes deste grupo, o Vinton Cerf e o Bob Khan, mais tarde ficaram conhecido como os pais da internet. Eles tiveram tal reconhecimento pela demonstração do TCP/IP(Protocolo de Controle de Transmissão e o Protocolo da Internet – *Transmission Control Protocol and the Internet Protocol*) que para tanto utilizou as redes ARPANET, RPNET e STATNET foram utilizadas. que era estudante e depois com o avanço de seus estudos ficou conhecido como pai da internet. Hoje esse é o principal protocolo utilizado até os dias atuais. Segundo Manuel Castells:

> " Em 1973, dois cientistas da computação, Robert Khan, da ARPA, e Vint Cerf, então na Universidade de Stanford, escreveram um artigo delineando a arquitetura básica na Internet. Basearam-se nos esforços do Network Working Group, um grupo técnico cooperativo formado na década de 1960 por representantes dos vários centros de computação ligados pela Arpanet, cm o propósito Cerf, Steve Crocker e Jon Postel, entre outros. Para que pudessem falar umas com as outras, as redes de computadores precisavam de protocolos de comunicação padronizados. Isso foi conseguido em parte em 1973, num seminário em Stanford, por um grupo liderado por Cerf, Gerard Lelann (do grupo francês Cyclades), e Robert Mercalfe (então no Xerox PARC), com o projeto do protocolo de controle de transmissão (TCP). Em 1978 Cerf, Postel e Crocker, trabalhando na Universidade da Califórnia do Sul, dividiram o TCP em duas partes, acrescentando um protocolo intra-rede (IP), o que gerou o protocolo TCP/IP, o padrão segundo o qual a Internet continua operando até hoje, A Arpanet, no entanto, continuou por algum tempo a operar com um protocolo diferente, o NCP. Em 1975, a Arpanet foi transferida para a Defense Communication Agency (DCA). Para tornar a comunicação por computador disponível para os diferentes ramos das forças armadas, a DCA decidiu criar uma conexão entre várias redes sob seu controle. Estabeleceu a chamada Defense Data Network, operando com protocolo TCP/IP. Em 1983 o Departamento de Defesa, preocupado com possíveis brechas de segurança, resolveu criar a MLNET, uma rede independente para usos militares específicos. A Arpanet tornou-se a ARPA-INTERNET, e foi dedicada à pesquisa. Em 1984, a National Science Fundation (NSF) montou a própria rede de comunicações entre computadores, a NSFNET, e em 1988 começou a usar a ARPA-INTERNET como seu backbone". (CASTELLS, 2003)

Criada em meio a Guerra Fria, a Internet foi feita para interligar os computadores militares. O intuito era que os computadores fossem criados somente para os militares para quebrar os códigos de comunicação. Os computadores tinham a capacidade de realizar as conexões através de comutação de pacotes. Conforme a Internet foi popularizando, foram surgindo grupos que receberam nomenclaturas que, hoje, conhecidas como os *hackers* e os *crackers*. Segundo Karen Abreu:

> "Os primórdios da Internet remetem à reação do governo norte-americano ao Projeto Sputnik da antiga União das Repúblicas Socialistas Soviéticas (URSS), capitaniadas pela Rússia, durante a guerra fria, em 1957. O nascimento da Internet está diretamente relacionado ao trabalho de peritos militares norte-americanos que desenvolveram a ARPANET, rede

> da Agência de Investigação de Projetos Avançados dos Estados Unidos, durante a disputa do poder mundial com a URSS."(ABREU, 2009)

Atualmente, existe uma grande confusão entre os termos *Hacker* e *Cracker*. Os *Hackers* são indivíduos que usam seus conhecimentos para benefício próprio, para trabalhar, para ajudar outras pessoas. Já os *Crackers* (*cracking*=quebra) são os "Piratas virtuais", eles usam seus conhecimentos para violar sistemas ou redes. Com a criação dos computadores termos como esses foram surgindo para definir cada indivíduo que possuem amplo conhecimento na área de informática.(COURI, 2011)

> "Genericamente HACKER é uma denominação para alguém que possui uma grande habilidade em computação. Cracker, black-hat ou script kiddie neste ambiente denomina aqueles hackers que tem como hobby atacar computadores. Portanto a palavra hacker é gênero e o craker espécie".(TERCEIRO, 2011)

Os *hackers* são indivíduos que atuam no lado bom da informática. Eles fazem *softwares*, programas que ajudam os usuários a usarem a rede. Além disso trabalham em empresa reconhecidas como a Pentágono, FBI para evitar que os indivíduos de má índole invada seu sistema.Hoje, temos vários exemplos de *hackers* pelo mundo, como por exemplo, Bill Gates (criador da *Microsof*), Steve Jobs (criador da *Apple*), que através de seu amplo conhecimento criaram uma das mais importantes empresas da atualidade.

Somando, podemos dizer que todos os *crakers* são *hacker*, porém os *hackers* não são *crackers*. Os *crackers* burlam os sistemas, na maioria das vezes para obter dinheiro, invadir sistemas, decifrar as criptografias, invadir empresas e buscar arquivos confidências. Portanto, os dois grupos são pessoas que possuem um amplo conhecimento sobre a informática e cada um aplica da forma que preferem. Assim, como temos muitos exemplos de *hacker* temos também os *crakers*, como Gary Mckinnon - maior invasor de computadores militares.

Um dos principais motivos da confusão desses termos é a mídia, pois quando divulgam alguma invasão que houve em alguma rede ou sistema eles dizem que são *hackers* e não *crackers*. Devido a isso muitas pessoas não conhecem a palavra *cracker* e se conhecem acham que os dois termos têm o mesmo significado. (TERCEIRO, 2011)

Atualmente, a internet tornou-se uma ampla fonte de tecnologia que permite aos usuários acesso a quaisquer informações que desejar. Porém, não se sabe o que está em oculto na rede de computadores.

Segundo o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e do Núcleo de Informação e Coordenação Ponto BR (NIC.br), que acompanha os dados de ataques cibernéticos, nunca se sabe o que está por trás da rede de computadores. Esse tipo de ataque cresceu 62 por cento em 2011 em relação ao ano de 2010. Os ataques a computadores brasileiros quase triplicaram em 2011 em relação ao ano anterior. No ano de 2012 foram 399.515 registros de problemas com vírus, códigos maliciosos ou tentativas de fraude em 2010 eram 142.844.

Em consequência desse número de invasões, hoje, criptografias fortes são criadas para dificultar o acesso do invasor a informações restritas ao usuário, como por exemplo, fotos, senhas, vídeos e arquivos pessoais. Com isso os crimes cibernéticos diminuem uma certa porcentagem do que ocorre diariamente. Porém os indivíduos, com seu amplo conhecimento, conseguem descobrir as senhas fortes criadas, mas com dificuldade maior.(MOTA,)

1.1 Objetivos

O objetivo geral desse trabalho é esclarecer a diferença os termos "*Hacker* e *Cracker*" e os crimes cibernéticos. Além disso, temos como objetivo desse trabalho atribuir e desenvolver informações de grande importância sobre esse assunto. Pois, ocorre uma série de acontecimentos que envolvem pessoas de todas as classes e idades que talvez ainda não tenha um bom conhecimento e precaução de tomar os devidos cuidados enquanto estão navegando na web. Entretanto, são vitimadas por usuários denominados "*Crackers*" que são pessoas que tem um extremo conhecimento sobre a rede de computadores e usam este conhecimento para o mal.Além disso serão discorridos os seguintes objetivos específicos:

- Esclarecer dúvidas entre os termos *hacker* e *cracke*r;
- Informar sobre crimes que ocorrem na rede;
- Problematizar frequentes na web;
- Informar as leis da justiça quanto aos crimes virtuais e qual e a sua ação em questão;
- Mostrar de alguma maneira como o *cracker* trabalha;

1.2 Metodologia da Pesquisa

Esse trabalho será feito exclusivamente utilizando a internet como ferramenta principal de pesquisa e práticas para mostrarmos como o assunto tratado em nossas pesquisas é realizado. Pesquisas de campo procedendo à observação de fatos e fenômenos exatamente como ocorrem na realidade, à coleta de dados referentes aos mesmos e, finalmente, à análise e interpretação desses dados, com base numa fundamentação teórica consistente, objetivando compreender e explicar o problema pesquisado. Também é indispensável à utilização de livros e artigos contendo informações verdadeiras sobre o assunto que serão retirados de sites e jornais confiáveis. as investigações mais detalhadas serão feitas para que nenhuma informação falsa seja utilizada neste trabalho.

Além disso, realizaremos pesquisas com os alunos do Instituto Federal de Ciência, Tecnologia e Educação, campus Paracatu. Nessa mesma será aplicado um questionário

que contém perguntas sobre o tema abordado. Com os resultados teremos o conhecimento sobre o que os alunos do instituto sabem sobre *hacker* e *cracker*

2 Embasamento Teórico

Desde a criação da informática surgiram dois grupos de indivíduos que utilizam as redes, e dentro desses dois grupos foram criados outros, por exemplo, *cypherpunks*,*phreakers*.

Além disso, os *hackers* são indivíduos que usam a rede para seu benefício próprio. Eles também invadem sistemas, porém é para descobrir invasores que tem por objetivo danificar um sistema. Os *hackers* usam seu conhecimento para trabalho, para criar novos aplicativos, redes sociais, programas, por exemplo. Em adição temos exemplos de *hackers* famosos – Steve Wozniak, Steve Jobs por serem uns dos mais conhecidos. Apesar da informática ser uma invenção recente, já temos muitos exemplos de pessoas que têm um amplo conhecimento sobre a área. Existem pessoas bilionárias que por aperfeiçoar seu conhecimento conseguiram criar novas redes, programas, redes sociais, para que o usuário tenha facilidade de utilizar. A cada dia novos programas são criados, novos *hackers* são descobertos. Podemos dizer que dentro de *hacker* existem outros grupos que visam proteger, ajudar, o usuário. Com por exemplo, os *cypherpunks* que visam à privacidade dos usuários e fazer criptografias para que seus dados não sejam roubados. Muitas pessoas pensam que os *hackers* não invadem sistemas, estão enganados, pois, eles invadem sim sistemas, mas é para benefício, para verificar se existe algum invasor nas redes.

Dessa forma, os *crackers* são pessoas que possuem um amplo conhecimento assim como os *hackers*. "Todo *cracker* é um *hacker*", pois têm o mesmo conhecimento sobre as redes, porém os *crackers* invadem sistemas para malefício da rede, diferentemente dos *hackers*. Nos dias atuais, por meios da internet todos têm a oportunidade de ter um conhecimento amplo sobre as redes, tanto o jovem quanto o idoso. Segundo o site www.oficinadanet.com.br, Raphael Gray é um exemplo, ele é um jovem britânico que conseguiu furtar cerca de 23 milhões de cartões de créditos, ele conseguiu furtar até o cartão de Bill Gates que é um dos maiores *hackers* do mundo. O jovem foi preso e condenado. Soma-se a isto, grupos de *crackers*, como por exemplo, os *phreakers* que são invasores de telefone e navegam na rede gratuitamente.(LEMOS, 1999)

2.1 Criptografia

Foi criada no Egito por Khnumhotep II ,teve início em 1900 a.C, onde as mensagens eram transmitidas em símbolos, para que outras pessoas, que não entendessem o que significava cada símbolo, não tivessem acesso. Essa era uma forma de transmitir mensagens secretas e que ninguém conseguisse decifras. Na maiorias das vezes as mensagens que são enviadas somente o emissor e receptor conseguirá entender o que está escrito nela. Dessa forma somente o receptor da mensagem conseguia decifrar e interpretar as mensagens en-

viadas. Para realizar a quebra dessa criptografia é realizada a criptoanálise para decifras os códigos.

2.2 Cracker

Com o surgimento da informática algumas pessoas começaram a ter interesse sobre essa área e começaram a estudar e adquirir conhecimento sobre a mesma. Com isso, foram surgindo novos grupos de pessoas e dentre eles se encontram os *crackers*. Os *crackers*, são indivíduos que possuem amplo conhecimento sobre a área de informática. Tais indivíduos usam seu conhecimento para o malefício da rede, dessa maneira eles invadem sistemas quebram criptografias, roubam bancos por exemplo.

Para realizar seu serviço (quebrar as criptografias) eles usam programas, que são feitos por eles mesmos, para realizar essa tarefa. Isso facilita para que eles consigam encontrar as senhas mais rapidamente e com mais eficiência.

Hoje, as pessoas confundem os termos *Hackers* e *Crackers*. A maioria delas nem sabem que existem os crackers ou pensam que os mesmos são i. A mídia é um dos principais fatores que ajudam na confusão de tais termos. Na maioria das vezes, em suas matérias, que relatam algo sobre computadores, eles dizem que são hackers sendo que são *crackers*.

Dessa forma, conclui-se os *hackers* possuem uma grande habilidade com computadores e têm intuito de danificar os mesmos. Soma-se a isso que uma solução possível para amenizar tal problema seria a mídia evitar de tratar os *crackers* como *hackers* e começarem a falar corretamente o que cada um faz, e qual é o seu trabalho e função.

3 Crimes Cibernéticos

Os crimes cibernéticos tiveram seu início na década de 1960, através de um projeto do Governo Americano no combate as guerras com intuito de golpear o mundo físico ou o universo real, ameaçando ou burlando diversas informações do seu inimigo. De acordo com a legislação Brasileira:(ROCHA,)

> "Um exemplo aqui no Brasil digital de crime digital determinou a aprovação da Lei n. 12.737, de 30 de novembro de 2012. apelidada de Lei Carolina Dieckmann, modificada no velho Código Penal e tipifica uma série de condutas no ambiente digital, principalmente em relação à invasão de computadores, até de estabelecer punições específicas. Crimes semelhantes já estavam ocorrendo – com pessoas comuns, causando prejuízos inimagináveis para os envolvidos. No caso de Carolina Dieckmann, ela teria mandado consertar um computador e não protegeu o que havia arquivado nele. Na oficina de manutenção técnica, as fotos íntimas de Carolina Dieckmann foram copiadas. Talvez tivesse ficado por ali mesmo se o autor do "roubo" não tivesse usado essas imagens para tentar obter vantagens por meio de chantagem, esse sim, um crime que consta no Código Penal. Por conta de esse fato ter sido amplamente divulgado na mídia, surgiu pressão sobre o legislador para que surgisse algum tipo penal que tutelasse os dados informáticos e, assim, restou aprovado no PL n.35/2012 na Câmara dos Deputados, inicialmente originado pelo PL n. 2.793/2011"

Infelizmente crimes como esses a cada dia se tornam mais comuns em nossa sociedade. Por esse motivo, deve-se ter cautela quando for concertar um computador ou qualquer outro aparelho eletrônico que cotenha arquivos que possam comprometer sua privacidade. Manter dados pessoais com senha de segurança é de suma importância.

3.1 Ciberbullyng

É um dos crimes mais comuns nas redes sociais, caracterizados por intimidações e o incentivo a violência. Crime como esse tem o quase o mesmo significado do bullying, porém ele é um crime cometido na internet, por meio de redes sociais. O bullying é a prática de criticar, humilhar alguma pessoa que é considerada inferior à outras. O cyberbullying espalha o bullying através da internet de forma rápida, compartilhamentos são feitos a todos os momentos e assim facilita que outras pessoas têm acesso aquele bullying praticado.(WENDT; LISBOA, 2013) (WENDT; CAMPOS; LISBOA, 2010)

3.2 Liberdade na Web

Hoje, com o avanço da computação, encontra-se grande compreensão de qualquer indivíduo, que possui um conhecimento médio/avançado sobre informática, entrar e sair,

acessar qualquer dado, servidores, entre outros. Com a Internet, a facilidade de saber o que se deseja na rede aumente a cada dia. Temos leis de privacidade, porém não são bem aplicadas no Brasil. Infelizmente pelo fato de não ter jurisdicionalmente uma lei, a própria web cria uma política de privacidade. A liberdade de cada usuário se torna cada vez mas escassa, pois as facilidades que se tem, hoje em dia, facilita que outros usuários (*crakers*) invadam as contas privadas, por exemplo.

3.3 Cavalo de Tróia

Também conhecido como *Trojan Horse*, é um tipo de vírus que atua por meio da internet. É um dos vírus mais comuns que existem na internet. Esse tipo de autônimo da rede criam páginas na inernet que os usuários terão confiança de entrar. Porém, ao acessar os mesmos, automaticamente o computador estará infectado. Após o vírus inVaDir o computador o cracker terá total acesso aos dados do usuários.Somado a isso, ele consegue capturar as senhas de redes sociais que forem acessadas, contas bancárias,fotos pessoais enfim, tudo que o indivíduo acessar o vírus terá total controle. Além disso, em alguns casos, eles roubam os dados do usuário e pedem dinheiro em troca dos dados de volta. (BUENO; COELHO, 2008) (VIANNA, 2000)

4 BitCoins

A bitcoin é uma moeda, assim como o dólar, euro ou real, mas fisicamente bem diferente. O primeiro aspecto é quem é uma moeda totalmente virtual, não é uma moeda controlada por um Banco Central. O processo de criação da bitcoin é feito por meio de vários computadores, esse processo é chamado de "mineração", onde computadores conectados na rede competição na resolução de problemas matemáticos, quem ganhasse recebia um bloco da moeda. Além da mineração, é possível possuir bitcoins comprando unidades em lojas virtuais específicas ou aceitando a moeda ao vender coisas na internet. As moedas virtuais são guardadas em uma espécie de carteira, criada quando o usuário se cadastra no software .

> Hoje, um novo ataque de ransowares está infectando computadores em todo o mundo na tarde desta terça- feira (27). Enquanto países na Europa e Europa Orientao tiveram máquinas sequestradas, servidores e computadores no Brasil também começaram a ser invadidos pelo suposto ransoware Petva – similar ao WannaCry, que invadiu 300 mil Pcs em mais de 150 países no começo de maio deste ano. O Petva está cobrando 30 doláres em bitcoins para liberar os arquivos tornou-se possível acompanhar as transações do Petva após vítimas postarem online o endereço da carteira virtual dos cibernéticos.(NADA, a)

5 WikiLeaks

A organização WikiLeaks é uma empresa onde trabalham vários hackers que utilizam ferramentas altamente tecnológicas para recolher informações anônimas de três maneiras distintas: envio postal, pessoalmente e, principalmente, por meio do compartilhamento em pastas online protegidas por criptografia que a mantém anônima. Após o recolhimento destas informações, a equipe da empresa verifica a sua veracidade, e faz um resumo do material explicitando a importância de tal assunto para a sociedade.

> Victor Sampedro, catedrático de opnião pública e comunicação políticana Universidade Rey Juan Carlos, de Madrid, apresenta neste livro uma análise detalhada do jornalismo atual. Partndo desse exercício, projeta um cenário de renovadas possibilidades informativas, muito alicerçadas n potencial tecnológico, que recoloca a premência do jornalismo como prática que aspira ao bem comuns. Nos exemplos que vai trazendo ao longo do texto, documentando as aividades dos hackitivistas como Julian Assange, Chelsea Manning ou Edward Snowden – protagonistas e propulsores dos últimos casos de fugas de informação -, Sampedro reflete sobre o controle e o poder da informação num contexto de crise jornalística, mudança social e revolução tecnológica (FARPÓN, 2017)

6 Conclusão

Através desse trabalho, concluímos que, os grupos que aparecem depois da criação dos computadores, das redes de telecomunicações usam seus conhecimentos de acordo com o que acha melhor fazer. Nele também compreendemos os crimes praticados na web e como nos prevenir. Foi um grande aprendizado. A partir dele, vimos que se têm várias formas, e definições dos termos *hacker* e *cracker*, por exemplo, que são de conhecimento de poucos. Há uma grande confusão entre esses termos e definimos cada um desses. Analisando os dados e percebível que a legislação relacionada a internet é bastante fraca no Brasil , e as leis que existiam ate 2012 era direcionadas de forma geral aos crimes e não especificamente a crimes cibernéticos.

Após bastante estudos e analises chegamos a conclusão que é impossível acabar totalmente com esses crimes com as ferramentas de defesas que nos são proporcionadas, mas é possível evitar que os mesmos aconteçam tomando cuidado ao navegar na web. (CARNEIRO, 2012) (PINHEIRO, 2006).

Referências

PINHEIRO, Emeline Piva.

ABREU, K. C. K. História e usos da internet. *Biblioteca on-line de Ciências da Comunicação. Universidade da Beira Interior. Covilhã*, 2009.

BUENO, J. N.; COELHO, V. Crimes na internet. *JUS-FADIVA. ISSN*, p. 2176–2686, 2008.

CARNEIRO, A. G. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. *Revista Jurídica Eletrônica Âmbito Jurídico. Rio Grande do Sul, XV*, n. 99, 2012.

CARVALHO, M. A trajetória da internet no brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança. *Unpublished Estudos de Ciência e Tecnologia no Brasil, Universidade Federal do Rio de Janeiro, Rio de Janeiro*, 2006.

CASTELLS, M. *A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade*. [S.l.]: Zahar, 2003.

COURI, G. F. Crimes pela internet. *Disponivel em: http://tinyurl. com/6khbmqx. Acesso em: maio de*, 2011.

FARPÓN, C. R. Sampedro, víctor (2015). o quarto poder em rede. por um jornalismo (de código) livre. lalín, pontevedra: Abooks,(254 páginas). isbn: 978-84-15045-51-9. *Comunicação Pública*, Escola de Superior de Comunicação Social, v. 12, n. 22, 2017.

LEMOS, A. L. Ciber-rebeldes. *Universidad Federal de Bahia, http://www. cfh. ufsc. br/˜ cso5421/bibliografias/rebelde. html*, 1999.

MOTA, D. F. Principais ameaças à segurança dos sistemas de informação. *MUNDO TECNOLÓGICO*, p. 24.

PINHEIRO, E. P. Crimes virtuais: Uma análise da criminalidade informática e da resposta estatal. *Graduaçao, Pontificia Universidade Católica do Rio Grande do Sul (PUCRS), Porto alegre, RS*, 2006.

ROCHA, C. B. A evolução criminológica do direito penal: Aspectos gerais sobre os crimes cibernéticos e a lei 12. 737/2012. *Jus Navigandi, Teresina, ano*, v. 18.

TERCEIRO, C. d. F. V. R. *O problema na tipificação penal dos crimes virtuais*. 2011.

VIANNA, T. L. Dos crimes pela internet. *Revista do CAAP*, p. 367–385, 2000.

WENDT, G. W.; CAMPOS, D. M. d.; LISBOA, C. S. d. M. Agressão entre pares e vitimização no contexto escolar: bullying, cyberbullying e os desafios para a educação contemporânea. *Cadernos de Psicopedagogia*, UNIFIEO, v. 8, n. 14, p. 41–52, 2010.

WENDT, G. W.; LISBOA, C. Saraiva de M. Agressão entre pares no espaço virtual: definições, impactos e desafios do cyberbullying. *Psicologia Clínica*, Pontifícia Universidade Católica do Rio de Janeiro, v. 25, n. 1, 2013.