ESCOLA TÉCNICA ESTADUAL PROF. ARMANDO JOSÉ FARINAZZO
CENTRO PAULA SOUZA

Amyron Nogueira da Cunha
Carlos Carvalho dos Santos
Felipe Kauan Alves Clemente
Guilherme Santa Rosa

CRIMES CIBERNÉTICOS: ANÁLISE DOS PRINCIPAIS CRIMES

Fernandópolis
2019

Amyron Nogueira da Cunha
Carlos Carvalho dos Santos
Felipe Kauan Alves Clemente
Guilherme Santa Rosa

CRIMES CIBERNÉTICOS: ANÁLISE DOS PRINCIPAIS CRIMES

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção da Habilitação Profissional Técnica de Nível Médio de Técnico em Serviços Jurídicos integrado ao ensino médio, no Eixo Tecnológico de Gestão e Negócios, à Escola Técnica Estadual Professor Armando José Farinazzo, sob orientação do Professor Alex Lopes Appoloni.

Fernandópolis
2019

Amyron Nogueira da Cunha
Carlos Carvalho dos Santos
Felipe Kauan Alves Clemente
Guilherme Santa Rosa

CRIMES CIBERNÉTICOS: ANÁLISE DOS PRINCIPAIS CRIMES

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção da Habilitação Profissional Técnica de Nível Médio de Técnico em Serviços Jurídicos integrado ao ensino médio, no Eixo Tecnológico de Gestão e Negócios, à Escola Técnica Estadual Professor Armando José Farinazzo, sob orientação do Professor Alex Lopes Appoloni.

Examinadores:

_____
Nome completo do examinador 1

_____
Nome completo do examinador 2

_____
Nome completo do examinador 3

Fernandópolis
2019

DEDICATÓRIA

A nossa família querida que vem nos apoiando até agora e também a essas vítimas que sofrem desses crimes.

AGRADECIMENTO

Agradecemos à Deus por mais um dia, e, também, por estar aqui aptos para estar realizando essa apresentação transmitindo nosso conhecimento adquirido durante todo o período de ensinamento. Agradecemos aos nossos professores que sempre colaboraram conosco e a nossos pais que colaborarão em nossa formação.

EPÍGRAFE

“Conheça todas as teorias, domine todas as técnicas, mas ao tocar uma alma humana, seja apenas outra alma humana.”

Carl Jung

CRIMES CIBERNETICOS: ANALISE DO PRINCIPAIS CRIMES

Amyron Nogueira da Cunha
Carlos Carvalho dos Santos
Felipe Kauan Alves Clemente
Guilherme Santa Rosa

RESUMO: Os crimes em espécies geralmente são o que abalam nosso cotidiano, sendo razões para que nós percamos grande parte do nosso dia a dia para enfrentar problemas como a falta de moralidade, deixando as inseguras de exercer seu direito de liberdade, por tanto as pessoas se sente mais a vontades e seguras dentro de seus lares sabendo que a chance de ser vitima desses crimes são mais difíceis. Mas o que fazer se mesmo na nossa privacidade ainda podemos ser violados virtualmente? Mas hoje em dia vem acontecendo investigações cibernéticas para que esses autores sejam descobertos e punidos de forma adequada, a partir dai surgem as leis contra os crimes cibernéticos. Juntamente com essas infrações existentes tem os principais crimes sendo assim pornografia infantil, fraudes virtuais, invasão de privacidade, cyberbully, as investigação vem sendo evoluídas mas ainda a uma trava em achar esses autores pois é um amplo mundo virtual e muitas das vítimas nem vão a polícia fazer sua denúncia.

Palavra-chave: Pornografia infantil. Invasão de privacidade. Cyberbully. Fraudes virtuais.

ABSTRACT: Crimes in species are usually what shake our daily lives, and are reasons why we lose much of our day to day to face problems such as lack of morality, leaving the insecure to exercise their right to freedom, so people feel more to the wills and safe within their homes knowing that the chance to be victim of these crimes are more difficult. But what if even in our privacy we can still be virtually violated? But nowadays cybernetic investigations have been taking place to ensure that these authors are properly discovered and punished, and hence the laws against cyber crimes arise. Along with these existing infractions have the main crimes being child pornography, virtual frauds, invasion of privacy, cyberbully, research has been evolved but still a hurdle in finding these authors because it is a wide virtual world and many of the victims do not even go to police make your complaint.

Keyword: Child pornography. Invasion of privacy. Cyberbully. Virtual frauds.

1.INTRODUÇÃO

O tema escolhido trata-se de crimes cibernéticos que é um problema quem vem agravando nossa sociedade nos dias de hoje, um dos principais crimes são o cyberbully, pornografia infantil, invasão de privacidade, fraudes virtuais.

Ainda hoje é muito difícil controlar as redes sociais, pois é um mundo muito amplo e de diversas barreiras, mas investigações vêm evoluindo a cada dia, em diversos casos pais tem que estar intervindo quando a criança é menor de idade. Evite certos acasos de ser ofendido nessas ocasiões e assim evitando certas redes sociais, e para proteger suas contas tenha diversas senhas para dificultar o acesso de pessoas indesejadas.

O tema foi escolhido no propósito de reconhecer e poder compartilhar o que as redes sociais vêm causando na nossa sociedade e os litígios que ela está proporcionando.

2.1 CONCEITO

Crimes cibernéticos são aqueles crimes que ocorrem em redes virtuais, e vem se agravando cada vez mais, esses crimes são classificados em: puro, mistos e comuns. Os crimes puros são aqueles que tenta atingir computador, sistemas e dados e toda e qualquer informação nele; já os mistos segundo Pinheiro (apud SCHMIDT, 2002) ”os crimes virtuais mistos são aqueles em que o uso da internet é condição sine qua non para a efetivação da conduta, embora o bem jurídico visado seja diverso ao informático. E os comuns é aqueles que utilizam da internet apenas como instrumentos para cometer delitos que já são tipificados em leis.

2.1.1 Cyberbullying

O cyberbullying é todo a violência praticada para intimidar uma pessoa em meio virtual, difamando e hostilizando uma pessoa.

2.1.2 Fraudes Virtuais

Qualquer ato de má-fé, com o intuito de lesar ou enganar outrem, ou de não cumprir determinado dever. As fraudes virtuais são fraudes efetuadas através da internet, como, por exemplo, o crime de estelionato, previsto no art. 171 do Código Penal.

Como crime econômico, que é descrito como o ato de "obter, para si ou para outro, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento."

2.1.3 Invasão de privacidade virtual

Invasão de privacidade é algum individuo invadir um dispositivo alheio conectado ou não a rede de computadores, usando um mecanismo ilegal para ter acesso a dados e destruí-los, adultera-los ou espalha-los.

2.1.4 Pornografia infantil

A pornografia infantil pode ser definida pela utilização ou compartilhamento, ou até pelo acesso a pornografia envolvendo crianças ou adolescentes em desenvolvimento.

2.2 NATUREZA JURÍDICA

A natureza jurídica de crimes cibernéticos é própria e improprias, os crimes próprios são aqueles que necessitam de um computador e danificam seus dados e bens jurídicos.

Os crimes impróprios também são cometidos por uso de computadores, mas não precisa necessariamente dos usos de computadores basta ter um dispositivo que esteja conectado à internet.

2.3 EVOLUÇÃO HISTORICA

Desde o surgimento da internet os crimes cibernéticos começaram a aparecer mais e mais, facilitando com que algumas espécies de crimes fossem mais abrangentes.

2.3.1 Cyberbullying

O bullying ele existe já faz um bom tempo desde a época escolar antiga, o bullying era uma forma de humilhar uma pessoa e rebaixa-la perante a outras, logo depois do surgimento da internet, o bullying começou a se expandir, também causando danos psicológicos a outras pessoas, e assim dando surgimento ao cyberbullying.

2.3.2 Pornografia infantil

A pedofilia não tem um conceito histórico muito definido, mas por conhecimento geral pode-se definir que não surgiu juntamente com a criação da

internet. Desde os tempos passados em que era considerado comum o pai, chefe da família, abusar dos próprios filhos após chegar em casa depois de um dia inteiro.

2.3.3 Fraudes virtuais

As fraudes elas já existiam bem antes do surgimento da internet, essas algumas dessas fraudes eram falsificação de documentos, estelionato entre outros. Após o surgimento da internet essas práticas ficaram mais acessíveis e facilitando esse crime de se expandir

2.3.4 Invasão de privacidade

A internet teve seu auge em 1998, assim sendo conhecido como uma grande rede que conecta maiores números de pessoas a partir de um computador ou celular. E a partir desse tempo começaram a surgir hackers para danificar arquivos de pessoas.

2.4 TIPIFICAÇÃO LEGAL

2.4.1 Cyberbullying

O cyberbullying por sua vez não tem um crime especifico, mas ele é julgado pelos crimes contra a honra que são injuria, calunia e difamação previsto no art.138 do Código Penal – Decreto Lei 2.848/40.

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa. (BRASIL, 2013).

2.4.2 Fraudes virtuais

Os crimes de fraudes virtuais estão previstos no Código penal - Decreto lei 2848/40.

2.4.3 Pornografia infantil

Sobre a Pornografia Infantil, o crime é previsto no artigo 240 ECA (Estatuto da criança e do Adolescente) Lei nº 11.829, de 2008, dessa forma:

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa**.** (Brasil, 2013).

2.4.4 Invasão de privacidade

Situado na lei 12.737/12, conhecida também como lei Carolina Dieckmann. O crime de invasão de privacidade na internet, e o crime para intervir as pessoas que praticam invasões a dispositivos alheios, como computadores, celulares, conectados ou não a redes de wi-fi, para alterar ou destruir dados ou informações sem autorização expressa ou tácita da pessoa dona do aparelho eletrônico ou instalar vulnerabilidades no dispositivo- Decreto da lei 12.737/12.

3.FRAUDES VIRTUAIS

Apesar da situação crítica do Brasil em meio econômico, a tecnologia se manteve em crescimento nos últimos tempos e este é um possível reflexo da mudança de atitude dos brasileiros. O grande número de transações comerciais e financeiras

pode dar espaço para alguns tipos de fraudes, o que hoje está cada vez mais frequente. “Quando falamos em ambiente digital, efetivamente, a prevenção é o melhor caminho”, alerta Ruy Coppola Junior. Sendo assim, é inevitável contar com boas atitudes em questão da segurança de dados armazenados em sites de lojas e não compartilhar informações pessoais por canais desconhecidos. Alguma dessas fraudes são:

3.1.1 Fraude com cartões de crédito

Ultimamente há várias empresas online que se fazem como loja para vender falsos produtos. Elas pedem um número de cartão de crédito para completar a transação online e seu pedido está a caminho, quando na verdade não. Na maioria dos casos esses são estelionatários.

3.1.2 Notificações de falsos vírus

Há muitas publicidades online que dizem que seu computador está infectado com algum vírus e que deve ser eliminado clicando em uma aba determinada, quando na verdade sua privacidade e dados estão sendo vigiados por um criminoso.

3.1.3 Invasão de contas / Redes sociais

Um dos métodos mais comuns de crime virtual hoje em dia é a invasão das redes sociais. Para os ciber criminosos, redes sociais, como o Facebook e Instagram são muito fáceis para serem invadidas. Os usuários das redes sociais sentem-se seguros para se comunicar abertamente, quando na verdade tem alguém que você não conhece em sua conta.

Outro tipo de fraude comum é aquela empregada na busca de senha de cartão de crédito. Para evitar este tipo de fraude, é sempre necessário consultar o lugar de onde se endereça o vendedor. Se houver algum alerta negativo, não continue a compra. Nunca dê sua informação de cartão de crédito num site como este.

3.1.4 Banner de propaganda

Se você já acessou algum site perigoso, provavelmente viu uma tela de aviso nos navegadores. Elas dizem que a página seguinte é perigosa e, então, seria melhor você voltar a página anterior, mas também dizem que é possível seguir caso você saiba o que está fazendo. Então, permaneça atento.

3.1.5 Falsas notificações do sistema

Um dos métodos mais perigosos, as falsas notificações podem pegar muita gente. Isso porque elas surgem justamente onde as notificações reais de problemas aparecem, contribuindo para pegar os desinformados. De qualquer maneira, vale a pena ficar esperto a alguns pontos.

Se você viu um alerta falso, há algumas maneiras de precaução que podem ser feitas. A primeira de todas é saber de onde ele vem, se veio de uma página da web ou de algum programa instalado em seu computador. Feche as abas da web que possam ser a causa do problema e verifique se o problema se repete.

Em caso de persistência, veja as extensões instaladas em seu computador. Apesar da curadoria das lojas de add-ons, ainda é possível que alguma coisa passe despercebido, então é provável que alguma extensão recém-adicionada ao seu navegador seja a causa do problema. Procure desativá-la e observe o resultados. Se o problema ainda permanecer, é bem provável que ele esteja em algum programa instalado em sua máquina. Tente lembrar se você não instalou algum

aplicativo via instalador de páginas de download ou então se o instalador do próprio programa não pode ter incluído algo em sua máquina.

3.1.6 Invasão de contas / Redes sociais

Senhas longas e com códigos podem ser um bom método para ficar protegido. Assim como, não usar a mesma senha em vários aplicativos, ativar a verificação em duas etapas quando possível também é uma boa opção. Tomar cuidado com redes Wi-Fi gratuitas (muitas podem capturar os dados do seu aparelho).Trocar suas senhas de tempo em tempo, usar antivírus e só instalar softwares ou aplicativos bem avaliados ou conhecidos também ajuda muito na segurança.

Entrevista com Thiago Ribeiro Carneiro é mestre da ciência em computação, professor da Etec e da Fatec de Jales, ele nos informou que na segurança, em termos de computação, nada é 100% seguro. O que pode prevenir a clonagem de cartões é quando você utiliza o seu cartão por contactless, por exemplo, se você pega os novos cartões do Nubank, eles usam uma tecnologia onde não precisa mais inserir o cartão na maquininha. Por uma radiofrequência, as informações são enviadas para a maquininha do cartão e como não precisa colocar o seu cartão dentro da maquininha o ato da clonagem é dificultado, porém abre outras formas de golpe, por exemplo, outras bandeiras de cartão de crédito que trabalham com essa tecnologia, até R$50,00 (cinquenta) não pedem nem a senha, existem relatos de pessoas que chegam com a maquininha, colocam o valor de R$50,00 e aproximam perto do seu cartão, que provavelmente está no seu bolso e acaba debitando em uma conta que você nem sabe da onde veio. Então a maneira seria evitar colocá-lo dentro da maquininha.

4.INVASÃO DE PRIVACIDADE

Invasão de privacidade na internet e algo que vem ocorrendo com muita frequência ultimamente. Sendo assim, o avanço da internet tem sido o principal gerador desse crime. Consequentemente, com o aumento da tecnologia esses crimes irão cada ver mais se expandir, e por conta disso foi criada uma lei em 2012, a lei 12.737/2012, mais conhecida como lei Carolina Dieckmann, que fala sobre a invasão de privacidade na internet, um pouco sobre fraudes virtuais e as penas e sanções desse delito.

> Silveira, Neil et al. Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann. O mundo virtual trouxe benefícios e também desvantagens e malefícios provindos de sua má utilização por pessoas de má-fé que se escondem por trás das telas, e que, muitas vezes, acabamos por nos relacionar sem saber a conduta e a índole de quem trocamos informações. Sabendo de toda a carência e morosidade ao combate a este tipo de delito, os "criminosos informáticos" acabam agindo com certa segurança por tantas vantagens que lhes beneficiam, como a velocidade na hora de cometer tais condutas, o "anonimato" e a carente fiscalização na área."

5. CYBERBULLYING

A sociedade não da muita importância para o assunto do cyberbullying, algumas vezes por falta de empatia, um dos grandes problemas também do cyberbullying é a falta de informação, aonde as pessoas sofrem esses delitos mas não denunciam ou não sabe como denunciar.

Para poder impedir ou evitar essas agressões de ódio, na maioria das vezes feitas anonimamente, para evitar esses delitos bloqueie, denuncie, e conte para alguém seja um responsável, professor ou a um amigo. O cyberbullying ele é um crime aonde o agressor ofende suas vítimas anonimamente, e não deixa marcas de agressão física mas sim psicológicas, aonde não da para identificar quais são as pessoas que sofrem desse crimes contra a honra.

> Injúria é o conceito aviltante, expresso por palavra ou gesto, que ofende a dignidade e o decoro alheios (honra subjetiva). Não é a imputação de um fato, como ocorre na calúnia e na difamação. É uma opinião, um juízo desairoso (exs: “ ladrão”, “burro”, “canalha”), que a lei presume falso de forma absoluta (não admite a exceção da verdade). Não se confunde com mera deselegância (“mulher parida”, “homem careca”). O sujeito passivo é determinado (e com capacidade de compreensão, conforme entendimento majoritário).O sujeito ativo é comum (FUHRERMAXIMILIANO, C; FUHRER MAXIMILIANUS, R,2004,p.60).

Thiago Ribeiro entende que podemos achar que essa seria a maneira correta mas é totalmente inviável, porque a quantidade de conteúdo que é inserido é muito grande. Se você pega um site como o YouTube, são 24 horas de conteúdo por minuto que são publicados no site, como que revisa tudo isso, todas informações, se tem direito autoral sendo respeitado. A inteligência artificial ajuda nisso, existem alguns robôs que ajudam nessa identificação, mas acredito não ser viável e em um curto prazo de tempo nós não conseguiríamos fazer esse tipo de verificação. É um trabalho que várias companhias tentam elaborar, como o Facebook, o Mozilla, o próprio Google tentam fazer a verificação de tudo aquilo que é postado no site, como comentários entre outras coisas, mas a informação dissemina rapidamente e até você conseguir identificar que aquilo foi publicado de maneira errônea ou que tenha algum preconceito, seja uma informação vazada, uma foto indevida de alguém, aquilo já foi propagado e se você só permitir a publicação daquilo depois de feita a verificação, você tira o dinamismo da Internet, a principal característica, que é permitir que informações sejam divulgadas de forma rápida, que tenhamos informação de maneira imediata. E outra questão é que se você passa a fazer isso, você começa a controlar a pessoas e aí a liberdade de expressão começa a ser privada e entra em várias questões éticas e legais e isso é uma discussão para muito tempo.

6. PORNOGRAFIA INFANTIL

Sobre a Pornografia Infantil o problema se agrava devido aos avanços tecnológicos que ocorrem a cada dia fazendo com que os autores do crime façam suas vítimas se sentirem intimidadas, envergonhadas dos atos produzidos pelo Art.240 e seus sucessores. Um ponto claro que é possível ser retratado é a falta de ciência e interesse de responsáveis sobre o tema. Ocorre que ao deixar a criança com algum familiar ou algum contratado para a tarefa é gerada automaticamente uma confiança para com indivíduo, e dentre evidências que acabam ficando na vítima, documentos como fotos e vídeos íntimos podem ser vazados e armazenados na Internet.

Como é considerado que a criança não tem um certo discernimento para entender as coisas, acabam não levando em conta os registros feitos na ausência do responsável. Como a Pedofilia é considerada uma doença aqui no Brasil, e não tem como descobrir antes dos atos concretizados do indivíduo. O que se pode fazer para que esses efeitos indesejados sejam punidos de forma certa:

-Boletim de Ocorrência (ou BEO – Boletim Eletrônico de Ocorrência)

-Histórico de registros e acessos do usuário sejam todos investigados

-Rastreamento através de links suspeitos

-Aplicativos sociais pessoais sejam investigados

-Operações da Polícia Federal pela internet para vasculhar as conexões e rastrear arquivos

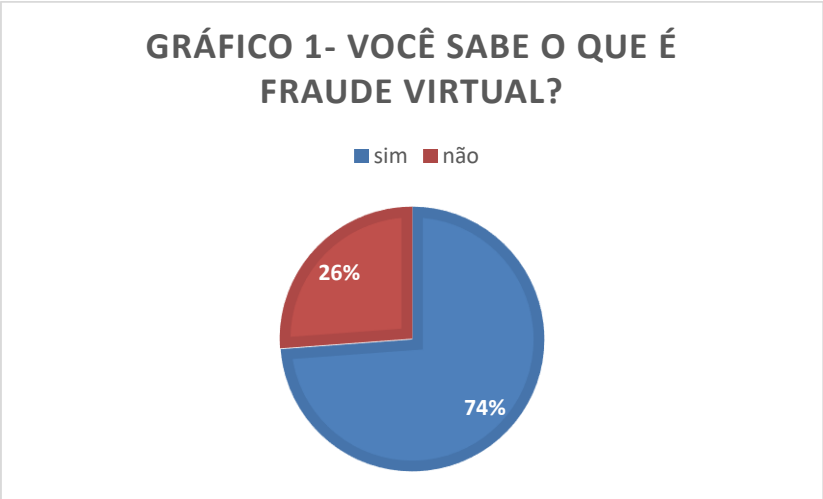
Como ensina Monteiro:

> “No Brasil situações de abuso sexual contra criança envolvendo médicos, padres, educadores, síndicos e empregados de condomínio, entre outros profissionais, também tem sido denunciadas. O uso da Internet para divulgação da pornografia com crianças e adolescentes

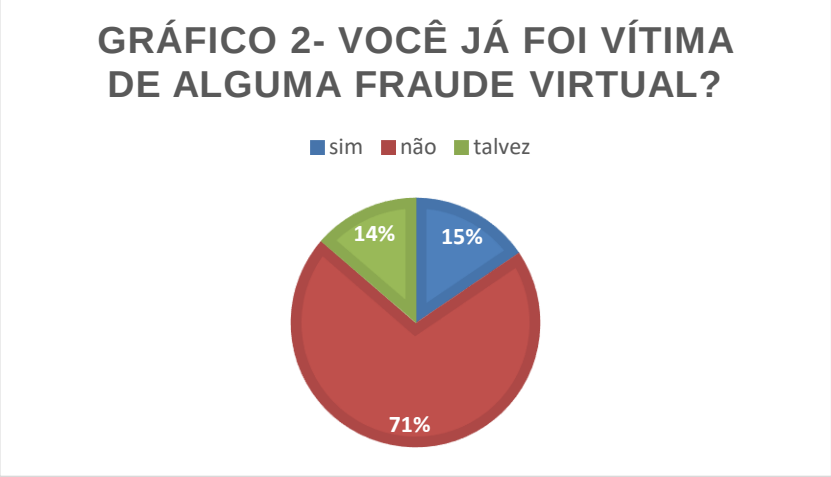
por pessoas da classe média tem sido denunciado em vários estados brasileiros (MONTEIRO,2002, p.20)

7. PESQUISA DE CAMPO.

Segundo a pesquisa de campo que fizemos a respeito de fraudes virtuais, entrevistados alegaram que:



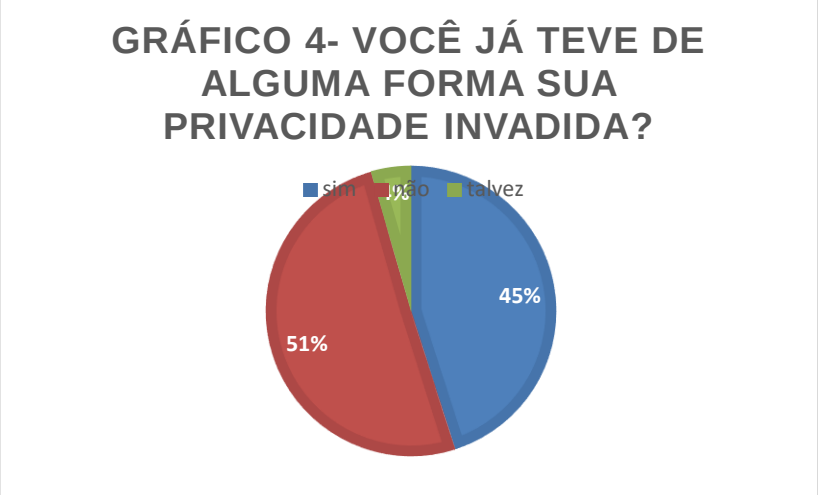
Fonte(Dos próprios autores, 2019)



Fontes(Dos próprios autores, 2019)

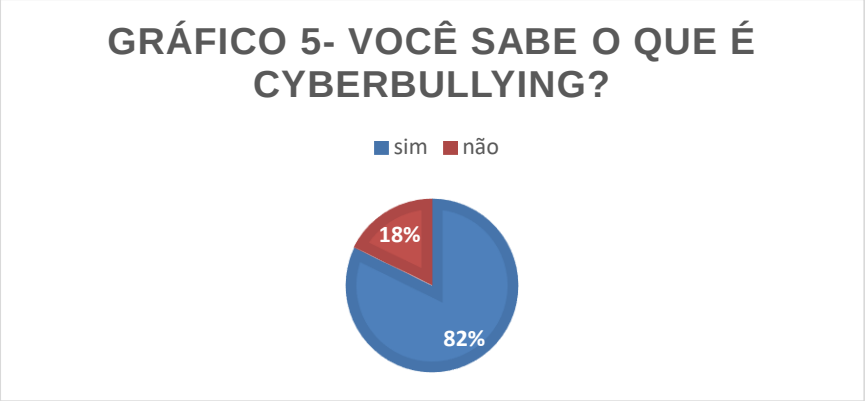
Segundo a pesquisa de campo que fizemos a respeito de invasão de privacidade, entrevistados alegaram que:

Fontes (Dos próprios autores,2019)

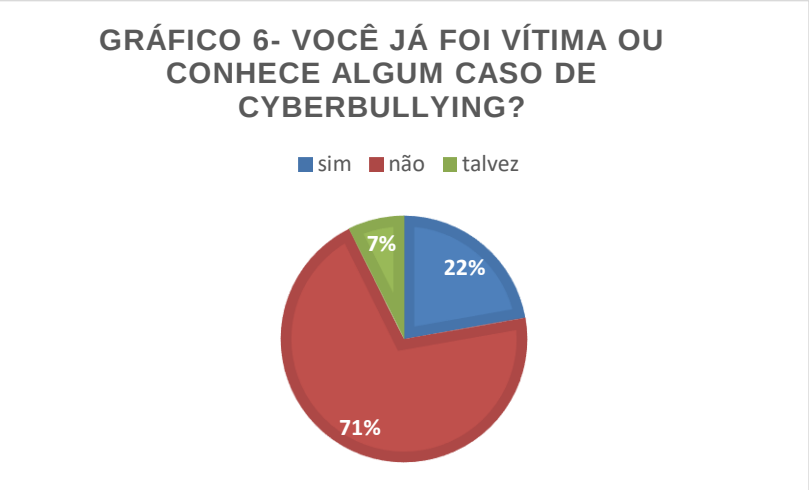


Fontes (Dos próprios autores,2019)

Segundo a pesquisa de campo que fizemos a respeito de cyberbullying, entrevistados alegaram que:

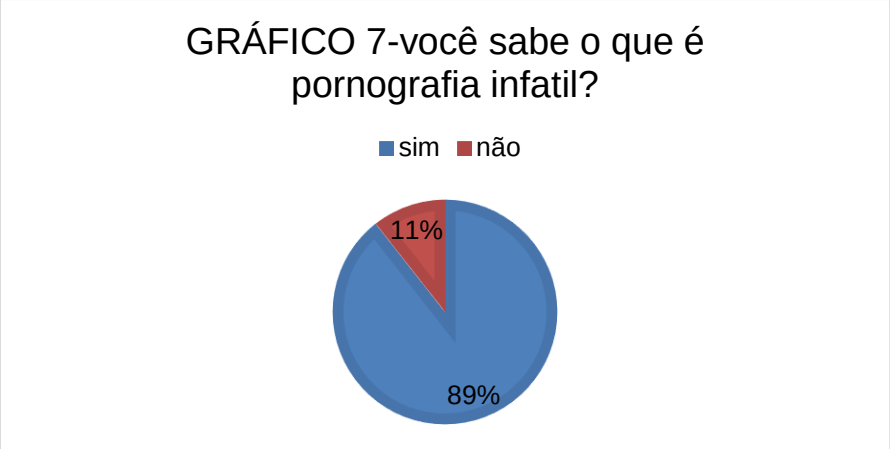


Fontes (Dos próprios autores,2019)

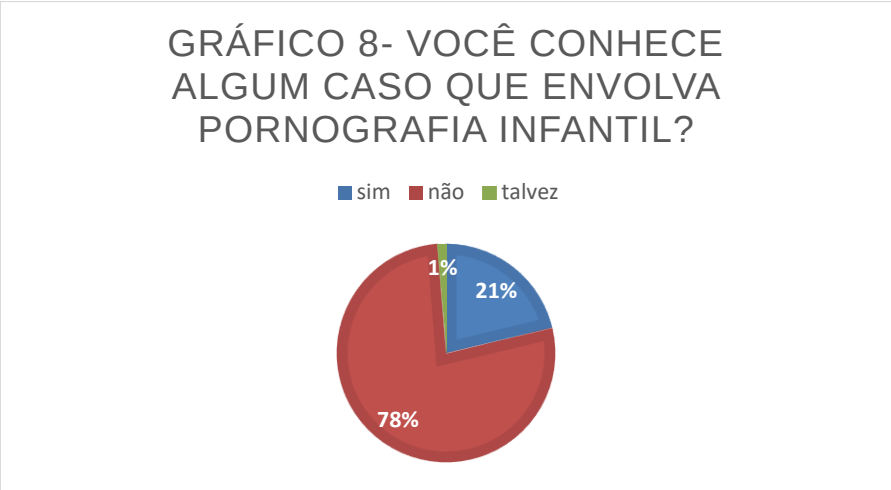


Fontes (Dos próprios autores,2019)

Segundo a pesquisa de campo que fizemos a respeito de pornografia infantil, entrevistados alegaram que:



Fontes (Dos próprios autores,2019)



Fontes (Dos próprios autores,2019)

8. CONCLUSÃO

O grupo concluiu que a internet é essencial para o nosso cotidiano, a internet é um meio amplo de comunicação, informações, dados e entretenimento. Assim como todas as cousas por sua vez, a internet também deve ser usada corretamente, e por isso devemos prestar muita atenção no que vemos e com quem falamos, pois, existem pessoas bem-intencionadas e pessoas mau- intencionadas. Sendo assim, a internet nos traz muitas coisas boas, mas, abre várias brechas para crimes cibernéticos como invasão de privacidade, fraudes virtuais, pornografia infantil e cyberbullying, entre outros.

Crimes cibernéticos são aqueles que são praticados conectados ou não a uma rede wi-fi. Esses crimes são classificados em três espécies, são elas puras mistas e comuns. Crimes puros são aqueles crimes que tentam danificar dados, sistemas e computadores de terceiros. Já os mistos são aqueles que utilizam da internet para praticas criminosas e visa sempre algum bem da vitima, como pegar senhas de redes sócias para ter acessos a informações que estão em sigilo. Já os crimes comuns são aqueles que usam da internet para cometer crimes que já estão tipificados em lei.

Cyberbullying que é uma maneira de ofender pessoas por ambiente social de comunicação como Whatsapp, Instagram, Facebook, entre outras.

Também procuramos sobre fraudes virtuais, que é um crime de qualquer ato de má-fé, praticado para clonar cartões, contas de redes sócias, praticar estelionato, e entre outros tipos de crimes. Pesquisamos sobre a invasão de privacidade na internet, que é alguma pessoa má intencionada invadir um dispositivo que esteja ou não conectado a uma rede de internet, não necessitando do uso das redes de computadores para destruir, adulterar ou compartilhar dados de uma pessoa qualquer. Observamos também o delito de pornografia infantil que fala sobre, o acesso e compartilhamento de imagens e vídeos de crianças e adolescentes. Geralmente os “doentes” são pessoas comuns do nosso dia a dia, que usufruem dos meios tecnológicos para acesso a esses conteúdos ilícitos.

Escolhemos o tema à cima para nosso conhecimento pessoal e para trazer informações a pessoas que por maioria não sabem das praticas ilícitas que são executadas através da internet.

REFERENCIAS BIBLIOGRAFICAS

ASSI, Marcos. Fraudes e crimes virtuais, como prevenir. https://politica.estadao.com.br/blogs/fausto-macedo/fraudes-e-crimes-virtuais-como-prevenir/. Acesso em: 18 de setembro de 2019.

AZEVEDO, Camila Kuster. De Invasão de privacidade em redes sociais. https://www.profissionaisti.com.br/2011/11/invasao-de-privacidade-em-redes-sociais/ Acesso em: 21 de agosto de 2019.

BRASIL. Decreto-Lei n. 2848, de 07 de dezembro de 1940, disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 de setembro de 2019.

FILHO, Lauro Monteiro. Abuso sexual. Mitos e realidades. Abuso Sexual. Bvsms, disponívelem:http://bvsms.saude.gov.br/bvs/publicacoes/Abuso_Sexual_mitos_realidade.pdf. Acesso em:25 de setembro de 2019.

FRANZONI, Larissa. Como evitar e o que fazer em caso de invasão de privacidade pela internet. http://franzoni.adv.br/como-evitar-e-o-que-fazer-em-caso-de-invasao-de-privacidade-pela-internet/. Acesso em: 21 de agosto de 2019

SANTOMAURO, Beatriz. Cyberbullying, a violência virtual, disponível em https://novaescola.org.br/conteudo/1530/cyberbullying-a-violencia-virtual. Acesso em: 04 de setembro de 2019.

SILVEIRA, Neil, Crimes cibernéticos e invasão de privacidade à luz da Lei Carolina Dieckmann. https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann. Acesso em: 21 de agosto de 2019.

APÊNDICE

APÊNDICE A- Modelo do Questionário Piloto

APÊNDICE B- Entrevista com o Professor Thiago Ribeiro Carneiro

APÊNDICE C- Entrevista com o Professor Fernando Corsini

APÊNDICE- A

CRIMES CIBERNETICOS E ANALISE DOS PRINCIPAIS CRIMES

1-Você sabe o que são crimes cibernéticos?
( )Sim
( )Não
( )Talvez

2- Você sabe o que é cyberbullying?
( )Sim
( )Não

3-Você sabe o que é fraude virtual?
( )Sim
( )Não

4-Você sabe o que é pornografia infantil?
( )Sim
( )Não

5-Você sabe o que é invasão de privacidade?
( )Sim
( )Não

6-Você já foi vítima ou conhece algum caso de cyberbullying?
( )Sim
( )Não
( )Não sei o que é

7-Você conhece algum caso que envolve pornografia infantil?
( )Sim
( )Não
( )Não sei o que é

8-Você já teve de alguma forma sua privacidade invadida?
( )Sim
( )Não
( )Não sei o que é

9-Você já foi vítima de algum tipo de fraude virtual?
( )Sim
( )Não
( )Não sei o que é

APÊNDICE B-

Entrevista com Thiago Ribeiro Carneiro

Pergunta: Como você acha que as investigações sobre crimes cibernéticos podem melhorar?

Resposta: A primeira forma é capacitando os peritos forense porque hoje o que acontece é que há uma defasagem muito grande dos peritos, muitos dos peritos não estão preparados para coletar provas ou coisas nesse sentido para que possa fazer um julgamento justo de um crime cibernético. E por outro lado também é necessário que você faça uma capacitação do profissional que trabalha com a área jurídica, porque eles não tem conhecimento técnico para poder julgar por exemplo se uma informação realmente foi hackeada, se aquela informação realmente é falsa, se é oriunda de uma coleta de informações indevida, de algum vazamento de informações ou de algum roubo de informações, então acho que o princípio disso tudo é capacitar o pessoal envolvido na análise desses crimes.

Pergunta: Na sua opinião, existe algum meio de prevenção de clonagem de cartão?

Resposta: Na segurança, em termos de computação, nada é 100% seguro. O que pode prevenir a clonagem de cartões é quando você utiliza o seu cartão por contactless, por exemplo, se você pega os novos cartões do Nubank, eles usam uma tecnologia onde não precisa mais inserir o cartão na maquininha. Por uma radiofrequência, as informações são enviadas para a maquininha do cartão e como não precisa colocar o seu cartão dentro da maquininha o ato da clonagem é dificultado, porém abre outras formas de golpe, por exemplo, outras bandeiras de cartão de crédito que trabalham com essa tecnologia, até R$50,00 (cinquenta) não pedem nem a senha, existem relatos de pessoas que chegam com a maquininha, colocam o valor de R$50,00 e aproximam perto do seu cartão, que provavelmente está no seu bolso e acaba debitando em uma conta que você nem sabe da onde veio. Então a maneira seria evitar colocá-lo dentro da maquininha.

Pergunta: Você diria que todo conteúdo publicado na internet deveria ser revisado pelos responsáveis dos sites?

Resposta: Podemos achar que essa seria a maneira correta mas é totalmente inviável, porque a quantidade de conteúdo que é inserido é muito grande. Se você pega um site como o YouTube, são 24 horas de conteúdo por minuto que são publicados no site, como que revisa tudo isso, todas informações, se tem direito autoral sendo respeitado. A inteligência artificial ajuda nisso, existem alguns robôs que ajudam nessa identificação, mas acredito não ser viável e em um curto prazo de tempo nós não conseguiríamos fazer esse tipo de verificação. É um trabalho que várias companhias tentam elaborar, como o Facebook, o Mozilla, o próprio Google tentam fazer a verificação de tudo aquilo que é postado no site, como comentários entre outras coisas, mas a informação dissemina rapidamente e até você conseguir identificar que aquilo foi publicado de maneira errônea ou que tenha algum preconceito, seja uma informação vazada, uma foto indevida de alguém, aquilo já foi propagado e se você só permitir a publicação daquilo depois de feita a verificação, você tira o dinamismo da Internet, a principal característica, que é permitir que informações sejam divulgadas de forma rápida, que tenhamos informação de maneira imediata. E outra questão é que se você passa a fazer isso, você começa a controlar a pessoas e aí a liberdade de expressão começa a ser privada e entra em várias questões éticas e legais e isso é uma discussão para muito tempo.

Pergunta: Se você tivesse um drone e ele invadisse uma residência e sem querer filmasse alguém que estivesse em seus momentos íntimos, o que você faria?

Resposta: A primeira atitude é apagar a filmagem, porque eu não tenho o direito de divulgar a imagem de outra pessoa, porque ela não me autorizou a fazer aquilo, independente se ela esteja em momento íntimo ou não, eu não tenho em hipóteses alguma direito de disseminar imagem ou vídeo de outra pessoa à qual eu não fui autorizado a fazer isso.

APÊNDICE C-

Entrevista com Fernando Corsini

Pergunta: Se o seu drone invadisse uma residência e sem querer filmasse alguém que estivesse em seus momentos íntimos, o que você faria?
Resposta: O orientador iria orientar o aluno a retirar o drone do local para não invadir a privacidade da pessoa. Essa questão é um pouco complicada porque apesar da tecnologia no Brasil não ser tão nova assim, eles não exigem legislação específica sobre isso, invasão de privacidade em uma área onde tem casas e observaria pessoas, por enquanto no Brasil não há uma legislação que contemple isso. Nós fazemos mapeamento dos voos fora da cidade e sempre que mapeamos alguma casa sempre avisamos o dono da residência para evitar algum ato constrangedor.