ESCOLA TÉCNICA ESTADUAL PROF. ARMANDO JOSÉ FARINAZZO
CENTRO PAULA SOUZA

Gabriel Souza Pavani
Lucas Henrique Teixeira
Ludimila Gomes
Rafael Neto Pereira de Oliveira

CRIMES CIBERNÉTICOS

Fernandópolis
2019

Gabriel Souza Pavani
Lucas Henrique Teixeira
Ludimila Gomes
Rafael Neto Pereira de Oliveira

CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção da Habilitação Profissional Técnica de Nível Médio de Técnico em Serviços Jurídicos, no Eixo Tecnológico de Gestão e Negócios, à Escola Técnica Estadual Prof. Armando José Farinazzo, sob orientação da Professora Marília Almeida Chinet.

Fernandópolis
2019

Gabriel Souza Pavani
Lucas Henrique Teixeira
Ludimila Gomes
Rafael Neto Pereira de Oliveira

CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado como exigência parcial para obtenção da Habilitação Profissional Técnica de Nível Médio de Técnico em Serviços Jurídicos, no Eixo Tecnológico de Gestão e Negócios, à Escola Técnica Estadual Prof. Armando José Farinazzo, sob orientação da Professora Marília Almeida Chinet.

Examinadores:

_____
Marília Almeida Chinet

_____
Eder Junio da Silva

_____
Maurício Flávio Canada

Fernandópolis
2019

DEDICATÓRIA

Dedicamos este trabalho a todos aqueles que buscam o conhecimento sobre o tema em questão.

AGRADECIMENTOS

Agradecemos à Professora Marília, amigos e professores, que contribuíram para a realização de nossos estudos e objetivos.

EPÍGRAFE

“A imaginação é mais importante que o conhecimento” (Albert Einstein).

CRIMES CIBERNÉTICOS

Gabriel Souza Pavani
Lucas Henrique Teixeira
Ludimila Gomes
Rafael Neto Pereira de Oliveira

RESUMO: O presente trabalho tem como objetivo determinado buscar informações para conscientizar a sociedade sobre os perigos presentes no ambiente virtual, fornecendo conhecimento e apresentando argumentos que caracterizam os crimes cibernéticos, com o propósito de direcionar esta pesquisa a pessoas leigas no tema Crimes Cibernéticos. Também, destacar pontos importantes que influenciam nos dias atuais, referindo-se a informações positivas e negativas sobre o comportamento social inserido pela evolução tecnológica. Com enfoque na área Penal, faz-se exposto neste trabalho os tipos de condutas caracterizadas como criminosas na *internet*, as principais causas dos crimes cibernéticos, bem como a falta de conscientização da população e a falta de fiscalização do Estado. Exibir argumentos e pesquisas, pretendendo-se atrair a atenção para este fim, que é pouco questionado, porém é praticado constantemente no âmbito virtual sem o conhecimento da sociedade sobre o crime.

Palavras-chave: Informações. Crimes Cibernéticos. Conhecimento. Pesquisa.

ABSTRACT: The purpose of this study is to seek information to raising awareness about the dangers present in the virtual environment, providing knowledge and presenting arguments that characterize cyber-crimes, with the purpose of directing this research to lay people in the topic of Cyber Crimes. Also, highlight important points that influence in the present day, referring to positive and negative information about the social behavior inserted by the technological evolution. With a focus on the Criminal area, this work examines the types of conduct described as criminal on the Internet, the main causes of cybercrime, as well as the lack of awareness of the population and lack of State oversight. Show arguments and research, aiming to attract attention to this end, which is little questioned, but is constantly practiced in the virtual environment without the knowledge of society about crime.

Keywords: Information. Cyber Crimes. Knowledge. Search.

1. INTRODUÇÃO

Evolução social tecnológica é o que vivemos hoje. Este trabalho será desenvolvido para apontar lacunas na legislação sobre Crimes Cibernéticos e abranger o conhecimento da sociedade sobre crimes praticados no âmbito virtual, através de pesquisas em doutrina, textos e em jurisprudências criadas pelo STF.

Com a conscientização tomada pelo tema, compreende-se que a falta de informação em relação aos cidadãos é fundamental para que ocorram esses crimes virtuais.

Em relação a leis de crimes virtuais, temos apenas a Lei n. 12.737/2012, a lei conhecida como Carolina Dieckmann, que tipifica os chamados delitos ou crimes informáticos. Com isso, percebe-se um atraso em relação à investigação e punição dos crimes cibernéticos.

2. PRESSUPOSTOS TEÓRICOS

2.1. CONCEITO

Crimes cibernéticos são a tipificação dos crimes padrões em um âmbito virtual, englobando uma categoria de condutas ilegais praticadas nos meios digitais de comunicação, geralmente, por meio de fraudes, estelionato e vazamento de informações contra a imagem social na *internet*.

O uso contínuo e diversificado da *internet* na sociedade vem abrindo novos caminhos para a prática de fraudes ou para novas formas de cometimento de velhos crimes, em casos nem sempre fáceis de enquadrar no ordenamento jurídico.

2.2. NATUREZA JURÍDICA

A natureza jurídica dos Crimes Cibernéticos está presente no Direito Civil, pois há, com frequência, a aplicação de multas e indenizações, com a finalidade de prevenção da imagem da vítima no âmbito virtual.

No direito penal também é englobado o tema Crimes Virtuais, que são tanto praticados na *internet* quanto no mundo físico, como furto de informações sigilosas dos usuários, uso de identidades e perfis falsos com finalidade maliciosa (Falsidade Ideológica), dentre outros.

2.3. EVOLUÇÃO HISTÓRICA

A rede mundial surgiu na época da “Guerra Fria” e seu objetivo era servir e facilitar a comunicação entre militares norte-americanos para sua defesa em supostos ataques inimigos, com o objetivo de proteger os meios convencionais de telecomunicações.

Nas décadas de 1970 e 1980, a *internet* passou a ser utilizada como comunicação acadêmica entre professores e estudantes norte-americanos.

Todavia, antes mesmo de 1990, a *internet* já se mostrou um sistema de comunicação não tão seguro assim, já que havia pessoas que conseguiam burlar o sistema, sendo denominadas “hackers”. Porém não é apenas esse grupo que comete crimes cibernéticos.

A *internet* surgiu no Brasil nos anos 90, porém não era acessível a toda a população, devido à condição financeira das pessoas. Com o tempo, ”*Geeks*” e “*Nerds*” se aprofundaram mais no território cibernético, trazendo, assim, os crimes junto a si.

Não obstante, apesar de existirem normas jurídicas que tipificam os crimes cibernéticos, não são suficientes para abranger os delitos que são cometidos de forma virtual.

Assim, dificulta para os investigadores e para os operadores do Direito punir os infratores, já que no Direito Penal tem que ser respeitado o princípio da reserva legal, legalidade penal e não pode ser aplicado o princípio da analogia.

Existem, hoje, basicamente, no ordenamento jurídico brasileiro, duas leis que regulamentam os crimes virtuais. São elas a Lei Ordinária n. 12.735/2012 e

a Lei 12.737/2012, que ficou conhecida nacionalmente como “Lei Carolina Dieckman”, criada após o vazamento de fotos da atriz do seu computador pessoal.

Apesar de existirem essas duas leis específicas, devemos reconhecer que elas não são suficientes para regulamentar as infrações cometidas, além de haver a necessidade de serem criados mecanismos específicos e suficientes para punir os infratores.

Percebe-se que a norma jurídica brasileira não acompanhou a evolução dos crimes cibernéticos para coibir os crimes virtuais. O mundo virtual ainda é muito carente de leis específicas para punir tal delito, ou seja, existe um vazio normativo, que não permite ao Estado punir os infratores.

2.4. TIPIFICAÇÃO LEGAL

Duas leis que tipificam os crimes na *internet* foram postas em prática em 2012, aplicando penas para delitos como invasão de computadores, disseminação de vírus ou códigos para roubo de senhas, uso de dados de cartões de crédito e de débito sem autorização do titular.

A primeira delas é a Lei dos Crimes Cibernéticos (12.737/2012), conhecida como Lei Carolina Dieckmann, que tipifica atos como invadir computadores, violar dados de usuários ou "derrubar" *sites*. Apesar de ganhar espaço na mídia com o caso da atriz, o texto já era reivindicado pelo sistema financeiro diante do grande volume de golpes e roubos de senhas pela *internet*.

Os crimes menos graves, como uma invasão de dispositivo informático, podem ser punidos com prisão de três meses a um ano e multa. Condutas que causam mais dano, como obter, pela invasão, conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas, podem ter pena de seis meses a dois anos de prisão, e multa.

2.5. DIREITO COMPARADO

Não é novidade para ninguém que os crimes virtuais são cometidos a todo o momento no mundo inteiro. Isso é resultado de uma globalização constante que a todo o momento está deixando o mundo conectado. Assim como a evolução dos crimes, os países vêm se atualizando diariamente para não sofrerem com esse tipo de situação, que todo ano gera prejuízos de bilhões de dólares.

Na Alemanha, os parlamentares adotaram uma lei contra a publicação, nas mídias sociais, de conteúdo com discursos de ódio, pornografia infantil, itens relacionados com o terrorismo e informações falsas. Segundo a lei, as plataformas de mídias sociais devem ser punidas com multas de até 50 milhões de Euros caso eles falhem em remover conteúdo ilegal.

Dois projetos de lei tramitam na Câmara dos Deputados na França. Esses projetos estão relacionados à ‘’manipulação de conteúdo nas mídias socais no período de eleição’’. A legislação daria o poder para um candidato ou partido político pedir a suspensão imediata da publicação de uma informação que possa ser considerada falsa, três meses antes de uma eleição nacional.

Na Malásia, o Parlamento aprovou uma lei em 2018 cujo objetivo é retirar e punir informações parcial ou totalmente falsas da internet, com penas de até 6 anos de prisão e multa de US$ 130.000.

No Quênia, o chefe do Poder Executivo sancionou, em maio de 2018, uma lei contra crimes cibernéticos, criminalizando o *ciberbullying* e também a disseminação de "*fake news*". Uma cláusula combate a publicação de "dados falsos, enganosos ou fictícios" e prevê punição com multa de US$ 50.000, com reclusão de até dois anos.

3. DESENVOLVIMENTO

3.1 FALTA DE CONHECIMENTO DA POPULAÇÃO

Com o avanço da tecnologia, o acesso à *internet* ficou algo muito fácil para todos. Infelizmente, nem todos que a acessam tem total conhecimento sobre a rede, facilitando, assim, a vida dos criminosos que estão a todo o momento

procurando novas vítimas, leigas no assunto de segurança no âmbito virtual, promovendo um aumento alarmante de crimes na *internet.*

Ao discutirmos soluções para esses problemas, precisamos levar em conta que a nossa rede tem uma segurança fraca, que a todo o momento pode ser invadida por não termos uma criptografia avançada, deixando cada vez mais fácil a invasão dos *crackers* (indivíduo que pratica a quebra de um sistema de segurança de forma ilegal ou sem ética). Outro modo de melhorar a segurança para pessoas sem o conhecimento prévio da *internet* seria ensiná-los a diferenciar suas senhas, pois um dos maiores fatores que levam as pessoas a serem *hackeadas* são a falta de criatividade para criar uma senha.

Uma pesquisa divulgada em janeiro pela empresa americana Symantec, que incluiu o envio de perguntas a 21,55 mil pessoas em 20 países, entre eles o Brasil, buscou entender como as pessoas encaram crimes cibernéticos e que medidas elas têm tomado para se proteger. Nessa pesquisa, 19% das pessoas entrevistadas afirmaram que usam a mesma senha para todos os tipos de contas *on-line* e outros 37% afirmaram que compartilham suas senhas com outras pessoas.

3.2. ACÚMULO DE PROCESSOS NO PODER JUDICIÁRIO

O Poder Judiciário vive lotado de processos de crimes no ambiente físico. Quando acrescentamos novos crimes virtuais sobre ele, não se consegue ter uma eficiência e eficácia na resolução desses atos, pois exigiria a alteração do Código Penal e Processual Penal, para englobar todos os crimes virtuais de uma maneira que não ocorram erros e que as penas sejam devidamente aplicadas.

Cresce, a cada dia que passa, o número de pessoas conectadas através da *internet*. Assim, torna-se necessária a intervenção do Estado de forma a coibir práticas que ultrapassem o limite da esfera de liberdade alheia. Entretanto, para que o Estado exerça tal função, é preciso que estas condutas já estejam tipificadas, o que atualmente não acontece.

Mesmo com a criação das leis 12.735/12 e 12.737/12, que foram marcos importantes, acabou sendo insuficiente, pois ainda há condutas não tipificadas pelo ordenamento jurídico.

3.3. FALTA DE FISCALIZAÇÃO

Como já foi dito anteriormente, a *internet* cresceu muito e, com isso, a fiscalização do Estado tornou-se insuficiente para pegar criminosos que atuam nesse âmbito há muito tempo. Mesmo tendo uma grande melhoria no sistema de fiscalização, ainda temos lacunas gigantes para serem preenchidas. Podemos citar como uma delas o sucateamento da aparelhagem das delegacias especializadas, que mesmo tendo uma tecnologia consideravelmente boa para a localização de *crackers,* ainda não é suficiente para identificar e prender os criminosos cibernéticos.

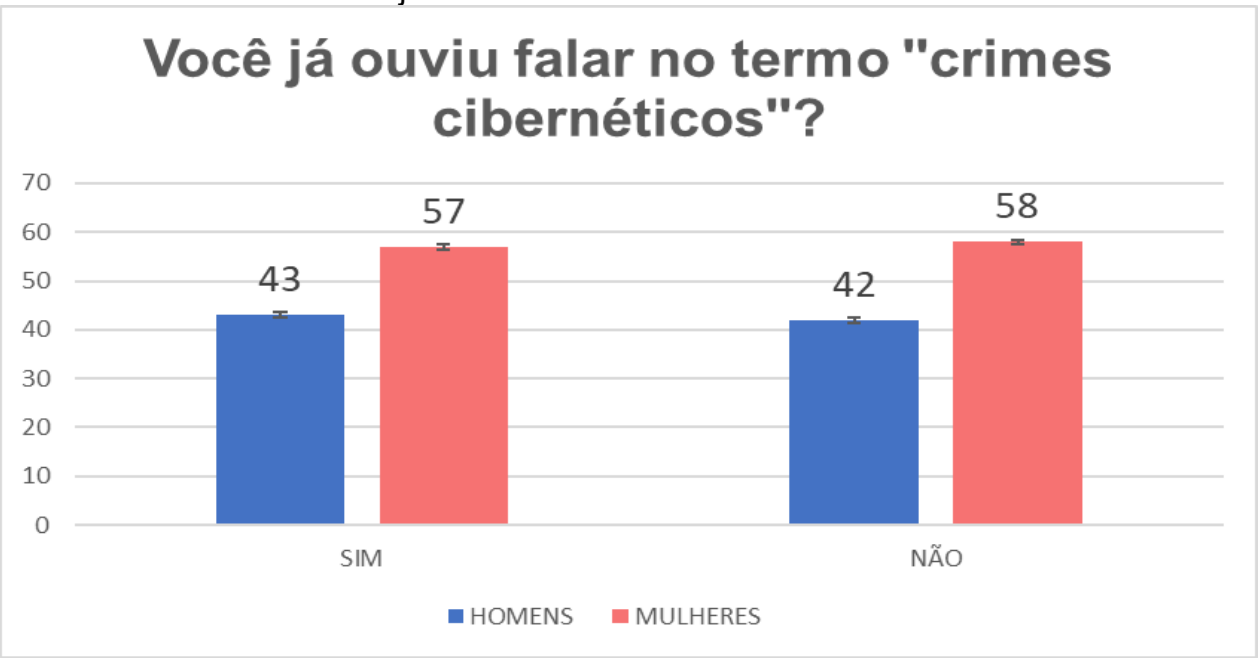
Existem delegacias especializadas para casos de crimes virtuais, porém atuam somente em 15 Estados mais o Distrito Federal. Com tão pouca fiscalização no país fica fácil a atuação de criminosos nesse meio.

4. PESQUISA DE CAMPO

4.1. QUESTIONÁRIO PILOTO

Com o propósito de verificar o quanto as pessoas tem conhecimento sobre os crimes cibernéticos, foi desenvolvida esta pesquisa quantitativa com 200 pessoas que se dispuseram a responder, sendo elas 85 do sexo masculino e 115 do sexo feminino, entre a faixa etária de 14 a 31 anos ou mais, da região de Fernandópolis, no período de 10 a 15 de Maio de 2019, utilizando-se de um questionário piloto com 5 perguntas objetivas relacionadas ao tema. A pesquisa se baseia em noções de conhecimento básico de segurança na *internet.*

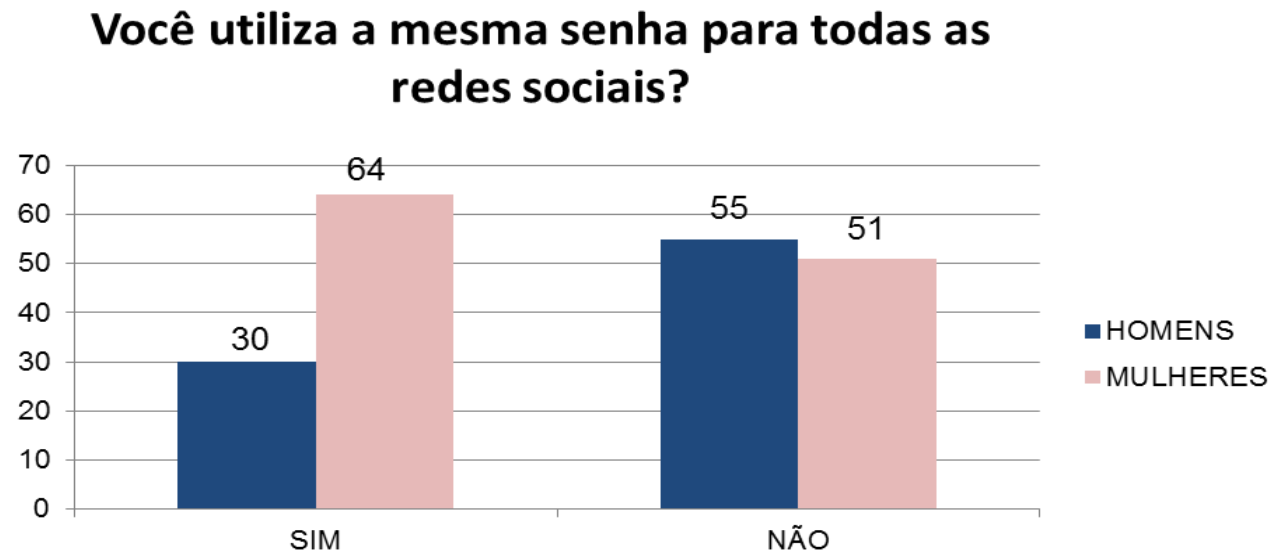
Gráfico 1. Você já ouviu falar no termo “crimes cibernéticos”?



Fonte: (Dos próprios autores, 2019).

A partir dos dados coletados na questão acima, 43 homens e 57 mulheres responderam que já ouviram falar no termo crimes cibernéticos, e 42 homens e 58 mulheres alegaram que nunca ouviram falar no termo. Assim, percebe-se que praticamente apenas metade dos entrevistados tem conhecimento sobre o tema.

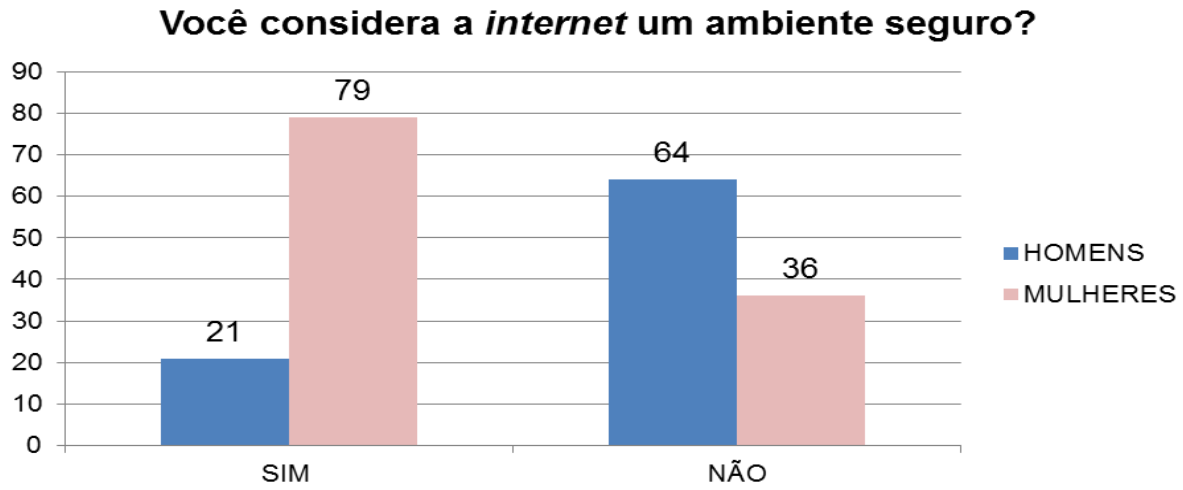
Gráfico 2. Você utiliza a mesma senha para todas as redes sociais?



Fonte: (Dos próprios autores, 2019).

Constata-se, por meio dos dados coletados, que 30 homens e 64 mulheres utilizam a mesma senha para todas as redes sociais. Nota-se que o ato de utilizar a mesma senha para todas as redes sociais está mais presente no cotidiano das mulheres entrevistadas.

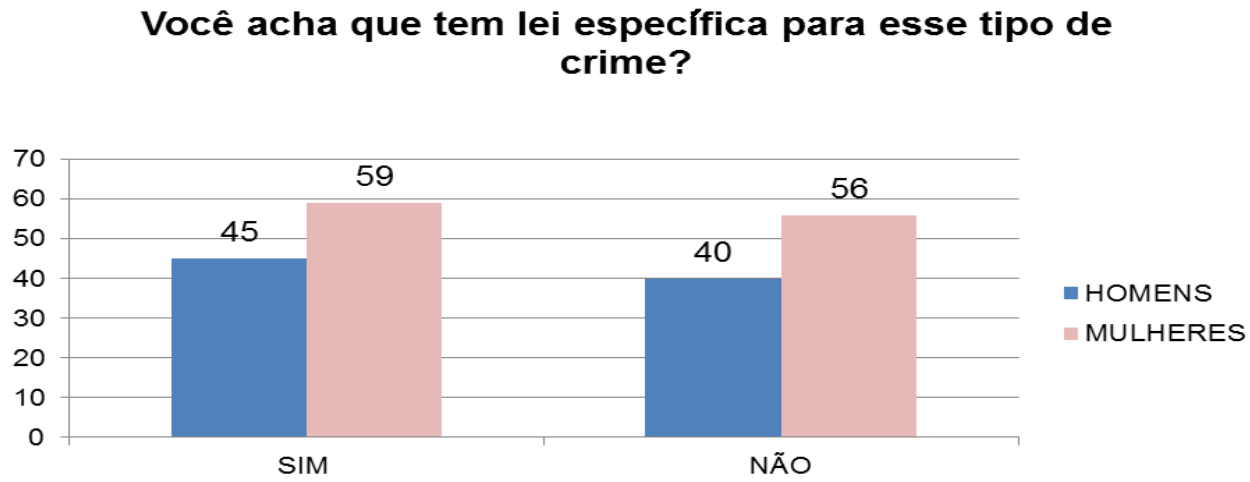
Gráfico 3. Você considera a *internet* um ambiente seguro?



Fonte: (Dos próprios autores, 2019).

Pode-se observar que, somando as respostas, 100 pessoas pensam que o ambiente virtual (*internet*) é seguro e outras 100 pessoas pensam o contrário. Constata-se que apenas metade dos entrevistados se sente segura ao acessar a *internet*.

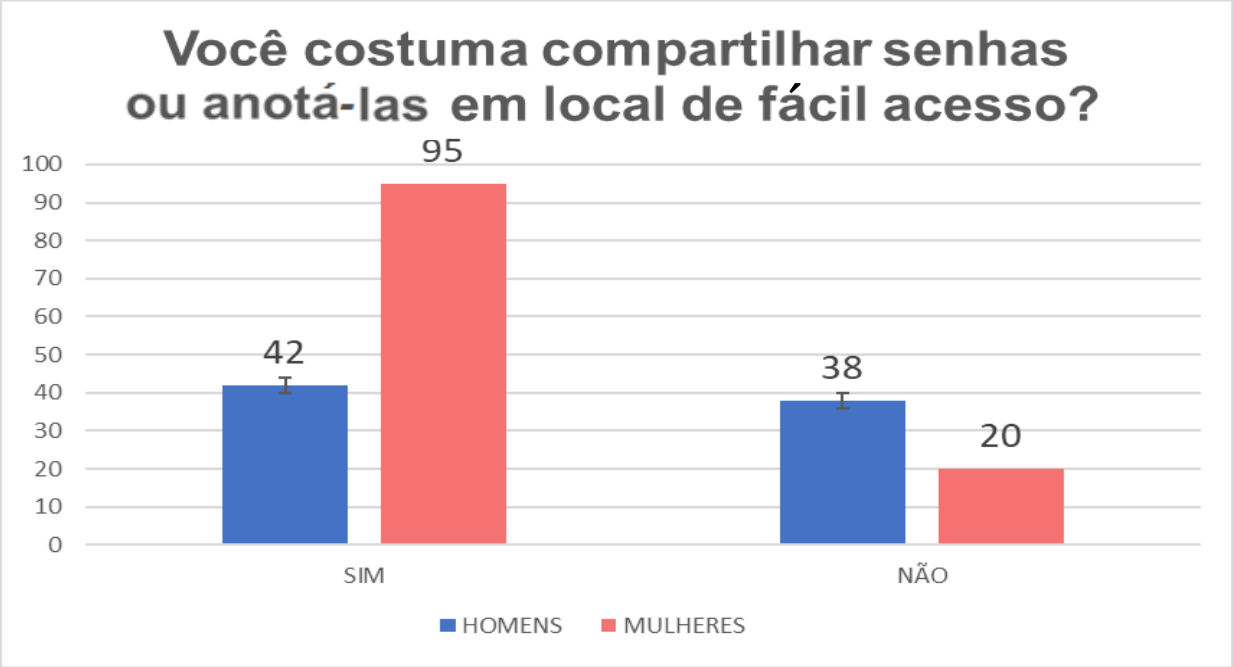
Gráfico 4. Você acha que tem lei específica para esse tipo de crime?



Fonte: (Dos próprios autores, 2019).

Com base nos dados coletados da questão acima, pode-se analisar que a maioria dos entrevistados acredita na existência de uma lei sobre o tema abordado. Conclui-se, portanto, que a maioria das pessoas entrevistadas tem conhecimento sobre a lei dos crimes cibernéticos.

Gráfico 5. Você costuma compartilhar senhas ou anotá-las em lugares de fácil acesso?



Fonte: (Dos próprios autores, 2019).

Ao analisar os dados acima, compreende-se que, entre os entrevistados, uma grande parcela das mulheres compartilha suas senhas, portanto, estas são mais propícias a sofrerem ataque de *ciber*-criminosos.

4.2. ENTREVISTA

Outro método de pesquisa de campo utilizado foi a entrevista, que foi realizada com um profissional que possui relação com o tema abordado, sendo ele professor na área da informática.

O profissional entrevistado, Professor Gustavo Tadeu Moretti de Souza, afirma que já ficou sabendo de casos de crimes cibernéticos, porém nunca

presenciou nenhum. Por já ter ouvido falar de vários crimes no âmbito virtual, citou alguns, sendo eles roubos de informações de banco, roubo de documentos e arquivos.

Disse, ainda, que as principais causas que favorecem a ocorrência dos crimes cibernéticos é a segurança, a arquitetura dos sistemas, que não tem uma proteção eficaz e gera uma balança desnivelada, onde a cada dia nasce um vírus novo e não se tem a competência para conseguir acompanhar esse desenvolvimento. Não só os sistemas nos proporcionam problemas. As falhas mais comuns são humanas, quando as pessoas compartilham senhas ou deixam-nas a mostra em lugares de fácil acesso, abrindo grandes brechas para os roubos de arquivos.

O entrevistado declara que, do seu ponto de vista, a taxa de crimes cibernéticos vem crescendo largamente, não só no Brasil. Existem três grupos de ciber criminosos ao redor do mundo que tem domínio avançado na área da informática, estando entre os Americanos, Russos e Chineses, sendo eles os melhores no sentido de roubo de informações, aumentando, assim, o nível dos crimes cometidos na *internet*.

Ao ser questionado se a fiscalização por parte do Estado está sendo realizada de maneira eficaz no combate aos crimes cibernéticos, o professor Gustavo afirmou que não temos infraestrutura suficiente para combater os crimes cibernéticos, o que podemos ver na delegacia que trabalha com essa área, que não consegue combater esse tipo de delito. Se os *hackers* norte-americanos fizerem um ataque ao nosso sistema, não conseguiríamos nos defender.

Por fim, o professor ainda alega que, para se prevenir dos crimes cibernéticos, são importantes os cuidados para as pessoas não saírem divulgando suas senhas, não escrevendo em lugares de fácil acesso, não guardando em qualquer lugar. A parte de *e-mails* também pode ser algo a sempre ser analisado, tendo atenção com *e-mails* falsos, não confiando em qualquer *link* ou *site.* Devemos ter um conhecimento prévio sobre segurança. Os cuidados e a desconfiança nunca são demais nesse ambiente.

5. METODOLOGIA

A pesquisa foi desenvolvida por métodos fundamentados com base em materiais disponibilizados por *sites*, artigos científicos, legislação e jurisprudência, com o auxílio de pesquisas que tem como objetivo gerar conhecimentos úteis a toda sociedade.

Assim, é importante ressaltar que as pesquisas realizadas foram de total significância para a finalização deste artigo, sendo que os métodos utilizados para pesquisa foram de total utilidade para adquirir e contextualizar os conhecimentos obtidos.

Um dos métodos de pesquisa para realização do trabalho ocorreu por meio de entrevista com um professor especializado na área de informática e, por fim, foi utilizado questionário piloto, aplicado na cidade de Fernandópolis e região, acerca do tema crimes cibernéticos.

6. CONSIDERAÇÕES FINAIS

Analisando a existência de falhas na forma com que a sociedade faz o uso do meio tecnológico, que é tão poderoso nos dias atuais, a ponto de ter o poder de prejudicar a vida de outrem, temos, assim, um avanço desenfreado de crimes cibernéticos e um ordenamento jurídico que não acompanha essa evolução.

Atualmente, a legislação brasileira não está atualizada e nem preparada para acompanhar tamanha evolução, obrigando os aplicadores do Direito a se basear em jurisprudência, pois o nosso Código Penal é arcaico no âmbito dos Crimes Cibernéticos.

No Brasil, os crimes cibernéticos, na maioria das vezes, passam despercebidos, pois falta fiscalização por parte do Estado. Porém, como não se trata de crimes comuns, o assunto vem ganhando uma repercussão cada vez maior, por estar diretamente ligado aos meios de comunicação.

As leis no Brasil que abordam este tema são desatualizadas ou, na maioria dos casos, nem existem. O que se encontra atualmente são jurisprudências para tentar preencher lacunas que abrangem esse setor do Direito. Existem, também, delegacias especializadas nos crimes cibernéticos em alguns Estados,

porém não ocorre um investimento necessário na infraestrutura por parte do Governo.

Em relação a leis de crimes virtuais, temos apenas a Lei n. 12.737/2012, a lei apelidada de ‘’Carolina Dieckmann’’, que tipifica os chamados delitos ou crimes informáticos. Com isso, entendemos um atraso em relação à investigação e punição dos crimes cibernéticos.

Por fim, vale ressaltar que a maioria dos crimes cibernéticos ocorridos no país é consequência da falta de conhecimento que a sociedade tem sobre o tema abordado. Destaca-se que o país precisa de mais estrutura para combater tais delitos, pois eles também afetam diretamente o cotidiano da sociedade.

REFERÊNCIAS BIBLIOGRÁFICAS

CNJ. **Crimes digitais:** o que são, como denunciar e quais leis tipificam como crime? Disponível em: http://www.cnj.jus.br/noticias/cnj/87058-crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime. Acesso em: Mar. 2019

CONSULTOR JURÍDICO. **STJ divulga jurisprudência sobre conceitos de crimes pela internet.** Disponível em: https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet. Acesso em: Out. 2018.

DIREITOS BRASIL. **Crimes cibernéticos:** o que são e como reagir? Disponível em: https://direitosbrasil.com/crimes-ciberneticos/. Acesso em: Mar. 2019

DICIONARIO DIREITO. **O que são Crimes Virtuais?** Disponível em: https://dicionariodireito.com.br/crimes-virtuais. Acesso em: Out. 2018

DIREITO BRASIL. **Lei Carolina Dieckmann:** o que ela diz? Disponível em: https://direitosbrasil.com/lei-carolina-dieckmann/. Acesso em: Nov. 2018.

GOCACHE. **Os 10 principais países em quantidades de cybercrimes.** Disponível em: https://www.gocache.com.br/seguranca/dez-paises-com-mais-ataques-de-hackers/. Acesso em: Mar. 2019

JUSBRASIL. **Crimes Cibernéticos.** Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos. Acesso em: Mar. 2019

JUSBRASIL. **Justiça usa Código Penal para combater crime virtual.** Disponível em: https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual. Acesso em: Mar. 2019

JUSTIFICANDO. **Crimes digitais:** quais são, quais leis os definem e como denunciar. Disponível em: http://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/. Acesso em: Mar. 2019

LINK DESIGN. **A evolução da internet até os dias atuais.** Disponível em: https://www.linkdesignbrasil.com/a-evolucao-da-internet-ate-os-dias-atuais/. Acesso em: Mar. 2019

MACHADO, L, A. **Crimes cibernéticos.** Disponível em: https://www.direitonet.com.br/artigos/exibir/8772/Crimes-ciberneticos. Acesso em: Mar. 2019

MIRANDA, T. **Projeto agrava pena para crimes cibernéticos.** Disponível em: https://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/572711-PROJETO-AGRAVA-PENA-PARA-CRIMES-CIBERNETICOS.html. Acesso em: Mar. 2019

NORTON. **Como reconhecer e se proteger contra o crime cibernético.** Disponível em: https://br.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html. Acesso em: Mar. 2019

OFICINA DA NET. **Quais são os crimes virtuais mais comuns?** Disponível em: https://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns. Acesso em: Mar. 2019

PICOLO, J. F. **Criminologia em torno do crime cibernético.** Disponível em: http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=18112&revista_caderno=3. Acesso em: Mar. 2019

ROCHA, C, B. **A evolução criminológica do Direito Penal:** Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Disponível em: https://jus.com.br/artigos/25120/a-evolucao-criminologica-do-direito-penal-aspectos-gerais-sobre-os-crimes-ciberneticos-e-a-lei-12-737-2012. Acesso em: Mar. 2019

SAFERNET. **Delegacias Cibercrimes.** Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: Mar. 2019

SANCHES, A, G. **Insuficiência das leis em relação aos crimes cibernéticos no Brasil.** Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: Mar. 2019

SIMÃO, P. L. **Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade.** Disponível em: http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3. Acesso em: Mar. 2019

SILVEIRA, A. B. **Crimes Cibernéticos.** Disponível em: http://www.conteudojuridico.com.br/artigo,crimes-ciberneticos,590897.html. Acesso em: Mar. 2019

SILVEIRA, A. B. **Os crimes cibernéticos e a Lei nº 12.737/2012.** Disponível em: http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-127372012,52253.html. Acesso em: Mar. 2019

TECMUNDO. **Crime virtual:** o que é e como se proteger das ameaças. Disponível em: https://www.tecmundo.com.br/crime-virtual/97401-crime-virtual-proteger-ameacas.htm. Acesso em: Mar. 2019

WIKIPÉDIA. **Crime informático.** Disponível em: https://pt.wikipedia.org/wiki/Crime_informático. Acesso em: Mar. 2019

APÊNDICE

APÊNDICE A - Modelo do Questionário Piloto

APÊNDICE B - Informativo

APÊNDICE C - Entrevista com o Professor de Informática Gustavo Tadeu Moretti de Souza

APÊNDICE A

CRIMES CIBÉRNETICOS
QUESTIONÁRIO

Sexo: Feminino ( ) Masculino ( )

Idade: 14 a 20 ( ) 21 a 30 ( ) 31 ou mais ( )

Orientações: Assinale a resposta escolhida com um X

1. Você já ouviu falar no termo ‘’crimes cibernéticos’’?

SIM ( ) NÃO ( )

2. Você utiliza a mesma senha para todas as redes sociais?

SIM ( ) NÃO ( )

3. Você considera a internet um ambiente seguro?

SIM ( ) NÃO ( )

4. Você acha que tem lei especifica para esse tipo de crime?

SIM ( ) NÃO ( )

5. Você costuma compartilhar senhas ou anotá-las em lugares de fácil acesso?

SIM ( ) NÃO ( )

APÊNDICE B

CRIMES CIBERNÉTICOS
INFORMATIVO

Crimes cibernéticos são os crimes padrões que podem ser cometidos no ambiente virtual, no qual a facilidade de cometer esses atos ilícitos se torna comum devido a informações que temos atualmente através da internet.

A Lei Brasileira 12.737/2012 é conhecida como Lei Carolina Dieckmann onde engloba uma pequena quantidade de crimes cometidos na internet, tendo somente utilização no ambiente virtual. Essa lei foi criada depois que a atriz Carolina Dieckmann foi ‘’hackeada’’ e teve suas fotos intimas vazada na internet.

Uma pesquisa realizada recentemente feita por 21,55 mil pessoas em 20 países. Nessa pesquisa 19% das pessoas entrevistadas afirmaram que usam a mesma senha para todos os tipos de contas on-line, e outros 37% afirmaram que compartilham suas senhas para outras pessoas. Tendo em vista isso percebemos que essas pessoas correm maior risco de serem ‘’hackeadas’’ ou sofrer algum tipo de crime cibernético.

APÊNDICE C

CRIMES CIBERNÉTICOS
ENTREVISTA

Pergunta: O senhor já presenciou ou ficou sabendo de casos de crimes cibernéticos?
Resposta: Sim, já fique sabendo. Não cheguei a presenciar, mas já fiquei sabendo de roubos de informações de banco, de documentos, arquivos.

Pergunta: Em sua opinião, quais são as principais causas que favorecem a ocorrência dos crimes cibernéticos?
Resposta: A maior motivação é a segurança. A arquitetura dos sistemas que não tem uma proteção eficaz gera uma balança desnivelada, onde a cada dia nasce um vírus novo e não se tem a competência para conseguir acompanhar esse desenvolvimento. Não só os sistemas nos proporcionam problemas. As falhas mais comuns são humanas, onde as pessoas compartilham senhas ou deixam elas a mostra em um lugar de fácil acesso, abrindo grandes brechas para os roubos de arquivos.

Pergunta: Do seu ponto de vista, a taxa de crimes cibernéticos vem crescendo no Brasil?
Resposta: Largamente, não só no Brasil, mas existem três grupos que são: Os Americanos, Russos e Chineses, sendo eles os melhores no sentido de roubar informações, aumentando, assim, o nível dos crimes cometidos na *internet.*

Pergunta: Atualmente, a fiscalização por parte do Estado está sendo realizada de maneira eficaz no combate aos crimes cibernéticos?
Resposta: Não temos infraestrutura suficiente para combater os crimes cibernéticos, podemos ver tanto na delegacia civil que mexe com essa parte e não consegue combater. Se formos pegar os E.U.A: se fizerem um ataque no nosso sistema não conseguiríamos nos defender.

Pergunta: Para se prevenir dos crimes cibernéticos, quais atitudes devem ser evitadas na *internet*?

Resposta: Cuidados pessoais para as pessoas não saírem divulgando suas senhas, não escrevendo em lugares de fácil acesso, não guardando em qualquer lugar. A parte de *e-mails* também pode ser algo a sempre ser analisado, prestando atenção quando estão criando *e-mails* falsos e te mandando, não confiando em pessoas que são os famosos ‘’hackers de engenharia social’’, tendo, assim, o conhecimento prévio para a segurança. Em vista, cuidados e desconfiança nunca são demais nesse ambiente. Eu já ouvi uma frase que resume tudo, ‘’não precisamos de antivírus se soubermos utilizar a *internet* de maneira inteligente’’.