

LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
DIREITO

BRUNO WERTER DO REGO HONORATO

**OMISSÃO LEGISLATIVA E CONSCIENTIZAÇÃO SOCIAL MEDIANTE À
TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS E DEEP WEB**

NATAL/RN

2018

BRUNO WERTER DO REGO HONORATO

**OMISSÃO LEGISLATIVA E CONSCIENTIZAÇÃO SOCIAL MEDIANTE À
TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS E DEEP WEB**

Trabalho de Conclusão de Curso em Direito,
apresentado ao Centro Universitário do Rio
Grande do Norte (UNI-RN) como requisito
final para obtenção do título de bacharelado
em Direito.

Orientador(a): Sandresson de Menezes
Lopes

NATAL/RN

2018

BRUNO WERTER DO REGO HONORATO

**OMISSÃO LEGISLATIVA E CONSCIENTIZAÇÃO SOCIAL MEDIANTE À
TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS E DEEP WEB**

Trabalho de Conclusão de Curso em Direito,
apresentado ao Centro Universitário do Rio
Grande do Norte (UNI-RN) como requisito
final para obtenção do título de bacharelado
em Direito.

Orientador(a): Sandresson de Menezes
Lopes.

Aprovado em: ____ / ____ / ____

BANCA EXAMINADORA

Prof. Nome Completo
Orientador

Prof. Nome Completo
Membro

Prof. Nome Completo
Membro

AGRADECIMENTOS

A Deus, por ser o dono de todas as vitórias em minha vida.

A minha mãe, Maria Judite, por ter segurado minha mão em todos os momentos difíceis que passei.

Ao meu avô, João Batista, por ter me educado e me presenteado com a fé em Deus.

A meu tio, tia e seus filhos, Demétria, Adebardo e filhos, por terem me acolhido durante toda a minha vida, me dando a possibilidade de conquistar meus sonhos.

A minhas tias, Maria Antônia e Maria Margarida, por todo o apoio e oração, contribuindo em todo momento de necessidade.

Aos meus amigos, que me ajudaram com palavras de ânimo em momentos de turbulência.

A minha segunda mãe, Ana Cristina, que me acolheu em um período difícil e me ajudou a seguir em frente.

A UNI-RN, me dando todo o apoio para conseguir me tornar um profissional de excelência.

A minha amiga, Isadora Yashara, por ter sido de fundamental importância para o meu amadurecimento pessoal.

Ao meu orientador, Sandresson, por ter tido fé na minha vitória e por me incentivar sempre com suas palavras.

A cada professor e pessoa que passaram pela minha vida, deixando sua devida contribuição para eu me tornar quem sou hoje.

Novamente a Deus, por ser o início e fim dos meus planos.

RESUMO

A internet veio marcar com soberania seu espaço na história, notadamente com transações milionárias, redes sociais que valem bilhões, informações rápidas e de fácil acesso. Esses são alguns dos muitos exemplos que nos possibilitam imaginar o quão presente em nossas vidas essa rede de tecnologia está. Todavia, seria um devaneio imaginar que estaríamos lidando com algo sem defeitos. No Brasil, o aumento de casos nos quais criminosos imaginam possuir imunidade a qualquer tipo de penalidade cresce diariamente, resultando em diversas jurisprudências que possuem como tema questões cibernéticas. Um dos maiores problemas existentes em nosso país, correlacionando os cibercrimes e suas possíveis penalidades, seria o abismo entre sua prática e uma legislação específica para seu controle, ocorrendo um déficit na tipificação desses crimes. Neste contexto, surge a Deep Web (conhecida como internet profunda), a qual tem como suas principais características a compilação de diversos sites com conteúdos ilegais e por ser uma parte da internet não indexada pelo mecanismo de busca padrão, “World Wide Web”, conhecido por “www”. Em virtude do advento desse instrumento de burla virtual, o qual é capaz de extinguir a materialidade das delimitações temporais e geográficas existentes até então, não é difícil perceber que a atuação de criminosos neste ponto da internet é muito mais forte do que na Surface Web, (internet superficial), composta pelos campos indexados que normalmente utilizamos em nosso dia a dia. Independentemente da localidade e do contexto onde é realizado o acesso ao meio virtual, verifica-se a necessidade de uma legislação com participação mais forte neste tema, correlacionando-se a criação de métodos que previnam e conscientizem a população.

Palavras chaves: Cibercrimes; legislação; tipificação; deep web; internet.

ABSTRACT

Internet has marked its space in History with domination, notably with millionaire transactions, social networks that are worth even billions, fast information through such an easy access. These are just some of the several examples that allow us to imagine how present this network of technology is in our lives. However, it would be a dream to imagine that we would be dealing with something without any defects. In Brazil, the increase in cases which criminals imagine to have immunity to any kind of penalty grows daily, resulting in several jurisprudences that have cybernetic issues as their main theme. One of the greatest problems in our country, correlating cybercrime and its possible penalties, would be the gulf between its practice and specific legislation for its control, occurring a deficit in the typification of these crimes. Within this context, the *Deep Weeb* appears, whose main characteristics are the compilation of several sites with illegal content and for being a part of the internet not indexed by the standard search engine – the “world wide web”, well-known as “www”. Due to the advent of this instrument of virtual mockery, which is capable of extinguishing the materiality of the temporal and geographical delimitations that existed until then, it is not difficult to notice that that the activity of criminals in this side of the Internet is much stronger than in the so-called “Surface Web”, composed of indexed fields that we normally use in our daily routine. Regardless of the locality and the context in which access to the virtual environment is made, there is a need for legislation with a stronger participation in this theme, correlating the creation of methods that prevent and raise awareness among the population.

Key-words: Cybercrimes, Legislation, typification, *Deep Web*, Internet.

1. INTRODUÇÃO

A humanidade é marcada por diversas revoluções históricas que definiram novos horizontes, anseios e desbravamentos. A inglesa, por exemplo, com suas treze colônias que rebelaram-se contra o poder britânico, ou a Revolução Francesa, marcada pela agitação social proveniente da fome e raiva popular. Estas datas foram eternizadas em livros por favorecerem o desenvolvimento social, e hoje, estamos inseridos em mais um grande evento, a revolução digital. Somos reféns desse imenso emaranhado de informações, que relacionam-se com nosso dinheiro, saúde e lazer.

Em pesquisa realizada pela CONECTAí Express, revela que “79% dos internautas brasileiros utilizam pelo menos um aplicativo de banco”¹, sendo os mais acessados: o da Caixa e do Banco do Brasil. O estudo é da CONECT, uma plataforma web do IBOPE Inteligência, que consultou 2000 internautas de todo o Brasil, em junho de 2017. Estes dados só reafirmam a ideia que práticas governamentais devem ser inseridas em planos de segurança e que não seria uma barbárie pensar na construção de um “Código Criminal Virtual”, legislado especificamente para este “novo mundo”.

Questões que envolvem segurança online são cada vez mais difundidas em nossa sociedade, entretanto, poucos dão a devida atenção a esta situação, o que acaba resultando em um crescente número de invasões a sistemas.

Em uma pesquisa feita pela Norton, empresa de soluções de segurança cibernética, em 2016, mais de 42 milhões² de brasileiros foram vítimas de crimes virtuais, número superior ao ano de 2015, que contou com 37,8 milhões de vítimas. Segundo levantamento, o prejuízo resultante desta prática para o país foi de US\$ 10,3 bilhões, aproximadamente R\$ 32,1 bilhões de reais.

A complexidade na obtenção de informações sobre local e dados referentes a esses criminosos é elevada, resultando em uma grande possibilidade de impunidade. A utilização desta ferramenta para práticas ilegais, causando

¹ Ver “79% dos internautas brasileiros usam aplicativos de bancos”. Disponível em: < <http://www.ibopeinteligencia.com/noticias-e-pesquisas/79-dos-internautas-brasileiros-usam-aplicativos-de-bancos/>> Acesso em 14 ago. 2018.

² Ver “42 milhões”. Disponível em: < <https://computerworld.com.br/2017/07/28/brasil-esta-entre-os-cinco-paises-que-mais-sofrem-ataques-ciberneticos-no-mundo/>>. Acesso em 14 ago. 2018.

insegurança as pessoas jurídicas e físicas de nossa sociedade só aumenta. Segundo informações disponibilizadas pelo EBC - Empresa Brasil de Comunicação, hoje o Brasil está entre os cinco países com mais crimes cibernéticos, conforme aponta relatórios da ONU – Organização das Nações Unidas.

O Instituto Brasileiro de Geografia e Estatística (IBGE), em 29 de abril de 2015, revela que 49,4% da população brasileira possuía acesso à internet em seus respectivos domicílios, número que equivale a 85,6 milhões de brasileiros, as estatísticas são referentes a Pesquisa Nacional de Amostra de Domicílios (PNAD) de 2013³. É deixado claro uma contínua apresentação de dados, por parte dos usuários, a este mundo digital, o que só certificam a vulnerabilidade de todos os sistemas que integram este meio. O Código Penal que rege e tipifica todas as condutas crimes em nosso país, não tem a força necessária para assegurar um “combate” aos desenfreados casos de cibercrimes e adentrar com segurança nesse “novo espaço”. A caracterização da internet como sendo um novo “mundo”, não foge tanto dos padrões físicos criados para definir uma realidade, já que ela possui sua própria língua, tempo e espaço.

2. REFERENCIAL TEÓRICO

2.1 CIBERESPAÇO

A acomodação é inevitável quando nos encontramos em ambientes fechados, julgamo-nos seguros mediante a iniciativa criminosa física, porém, nos esquecemos que a evolução nos levou a outro espaço/tempo diferente do apresentado por Newton⁴ ou pela Teoria da Relatividade criada por Albert Einstein⁵. O ciberespaço, este foi o termo utilizado por William Gibson, em 1984, no livro *Neuromancer*, referindo-se a um espaço virtual composto por cada computador e usuário conectados em uma rede mundial.

Do mesmo modo que Émile Durkheim (1985) defendeu no livro “As Regras do Método Sociológico”, onde a sociologia precisa descobrir leis explicativas para o

³ Ver “as estatísticas são referentes a Pesquisa Nacional de Amostra de Domicílios (PNAD) de 2013”. Disponível em: < <http://www.ebc.com.br/tecnologia/2015/04/acesso-internet-chega-494-da-populacao-brasileira> >. Acesso em 04 de jul. 2018.

⁴ Ver “Newton”. Disponível em: < <https://super.abril.com.br/ciencia/questao-de-tempo/> >. Acesso 15 ago. 2018.

⁵ Ver “Albert Einstein”. Disponível em: < <https://super.abril.com.br/mundo-estranho/o-que-e-a-teoria-da-relatividade/> >. Acesso em 15 de agosto de 2018.

funcionamento da sociedade, nossos legisladores devem abranger os novos tipos de vidas paralelas a “real”, já que por meio de todas as possibilidades apresentadas por este novo universo, modernos meios de transgredir direitos naturais intrínsecos ao homem foram descobertos, passando a caracterizar-se como verdadeiras armas apontadas aos usuários. Toda sociedade deve ser regida por leis que controlem condutas para um bom convívio, conceituando direitos e garantias a todos. Desse modo, deve surgir, de maneira inicial, programas sociais que invistam na conscientização dos usuários de internet e da criação de um código específico para esta nova realidade, buscando tipificar mais condutas crimes do “New World”, como Willian Gibson descreve.

Mesmo sendo bem quista pela maioria, a revolução-tecnológica afeta os mais variados aspectos humanos. A formação de círculos eletrônicos de amizade, por meio de comunidades, “navegação”⁶ pelos mais diversos conteúdos do mundo e formação de empresas online, são alguns dos meios de se “viver” na internet, entretanto, cada “passo” dado na “Second Life”⁷, como é chamada a “segunda vida” dos usuários virtuais pelo, (Ambulatório Integrado dos Transtornos do Impulso do Hospital das Clínicas de São Paulo), significa mais uma informação disponibilizada a “rede”⁸ sobre a vida real.

2.2 CONTEXTUALIZAÇÃO E CASOS

Fica claro a carência informativa existente em nossos órgãos de controle, quando nos referimos a intervenção legislativa perante estas condutas criminosas, ou na simples proposição de campanhas e incentivos para combater esta lastimosa realidade.

2.2.1 Companhia Docas do Rio Grande do Norte - CODERN

⁶ Categoria “Navegação” – diz respeito ao ato acesso e pesquisa na internet.

⁷ Ver “Second life”. Disponível em: <http://www.psicologiadoesporte.esp.br/Pdf/REVISTA_II_PsicoEsp_orte_2010.pdf>. Acesso em 20 ago. 2018.

⁸ Categoria “Rede” – diz respeito a “web”, ou seja, é a conexão feita por qualquer objeto capaz de acessar a internet.

No dia 08 de julho de 2018, a empresa Companhia Docas do Rio Grande do Norte (CODERN), sofreu invasão a seus servidores⁹, (onde estão, virtualmente, todas as documentações da empresa). O criminoso utilizou de um vírus recém-criado, chamado de CRAB, palavra em inglês que significa caranguejo. Seu mecanismo de infiltração e o de trabalho são os mesmos que o tradicional ransomware, (malware¹⁰ que “sequestra” o computador da vítima e cobra um valor em dinheiro pelo seu resgate). Inicialmente foi pedido R\$ 200.000.000,00 (duzentos milhões de reais), para a liberação do código que viria a desbloquear os arquivos, entretanto a empresa se negou a pagar o valor, preferindo compra de outros servidores para continuar seus trabalhos. A negativa da empresa foi possível mediante o backup (cópia de segurança), de dados corriqueiramente pelos funcionários. Analistas de segurança, da CODERN, identificam o CRAB como um subconjunto de malware, (pode ser um corriqueiramente pelos funcionários. Analistas de segurança, da CODERN, identificam o CRAB como um subconjunto de malware, (pode ser um código malicioso, programa malicioso ou software¹¹ nocivo), em que os dados da vítima são bloqueados usando um algoritmo de criptografia de arquivos forte, logo em seguida é exigido um pagamento a vítima antes que os dados bloqueados sejam descriptografados. A única intenção por trás da criação de um “ransomware” é sempre monetária e, para isso, realizam uma série de tarefas maliciosas dentro do computador sem a conscientização do usuário. Código malicioso, programa malicioso ou software¹² nocivo), em que os dados da vítima são bloqueados usando um algoritmo de criptografia de arquivos forte, logo em seguida é exigido um pagamento a vítima antes que os dados bloqueados sejam descriptografados. A única intenção por trás da criação de um “ransomware” é sempre monetária e, para isso, realizam uma série de tarefas maliciosas dentro do computador sem a conscientização do usuário.

Em pesquisa realizada em capo, na própria sede da CODERN, em Natal, o coordenador de tecnologia da informação, Eduardo da Silva Marques, relata que em sua grande maioria, esses ataques não são planejados contra uma empresa ou

⁹ Categoria “Servidores” – diz respeito a componentes físicos e virtuais que estruturam e hospedam um ou mais sites.

¹⁰ Categoria “Malware” – diz respeito a programas maliciosos, comumente conhecido por “vírus”.

¹¹ Categoria “Software” – diz respeito ao sistema de processamento de dados do computador. São todos os programas que em ação conjunta fazem o trabalho lógico da máquina.

¹² Categoria “Software” – diz respeito ao sistema de processamento de dados do computador. São todos os programas que em ação conjunta fazem o trabalho lógico da máquina.

pessoa específica, são mecanismo colocados na “rede”, que quando baixados para o computador, “invadem a máquina e executam o trabalho para que foram criados”. “Geralmente são enviados para o e-mail ou em forma de links para redes sociais, disfarçados de cobranças, fotos, assuntos judiciais e outros...”.

2.2.2 Maior ataque da história

No ano de 2015, a agência global de segurança e rede, Kaspersky Lab, jogou que o maior ataque hacker da história¹³ teria sido a invasão a pelo menos 100 grandes bancos, situados em 25 países da Ásia, Europa, Estados Unidos e Brasil. Segundo informações divulgadas pela agência, o grupo infiltrava-se nos computadores de alguns funcionários e monitoravam suas atividades até poderem estabelecer um padrão. Após o fazer, começava-se a imitar as atividades normais dos funcionários, de maneira remota, fazendo transferências para contas “laranjas” e efetuando o saque logo em seguida. Estima-se que conseguirão algo entre US\$ 300 milhões e US\$ 900 milhões (mais de R\$ 2,5 bilhões de reais).

2.2.3 The Homeless Hacker

Outro ocorrido que pode ser usado como base para demonstrar que podemos facilmente nos tornar vítimas de hackers, é o caso de Adrian Lamo, conhecido como “The Homeless Hacker” ou “O Hacker Sem-teto”. Adrian foi responsável por diversas invasões a sistemas de computadores fortemente protegidos, como: The New York Times, Google, Yahoo! e Microsoft. Depois de 15 meses sobre forte investigação da polícia dos EUA, Adrian foi preso em 2003.

Mesmo já existindo leis que tratam sobre alguns temas referentes a cibercrimes, estes fatos só asseguram que deve ocorrer uma intervenção maior sobre esse assunto, mas antes, deve-se ocorrer um entendimento maior sobre o que é crime.

2.2.4 Fake News

¹³ Ver “Maior ataque da história”. Disponível em: < <https://g1.globo.com/tecnologia/noticia/ataque-de-hackers-sem-precedentes-provoca-alerta-no-mundo.ghtml> >. Acesso em 25 jul. 2018.

Pode-se soar estranho a apresentação do tema “Fake News” como um dos casos concretos, entretanto, dentre todos os “ataques” que uma sociedade possa ser vítima, o mais complexo é esse, já que os próprios usuários são coautores desta prática, contribuindo com o compartilhamento da notícia fraudulenta.

A Fake News é um termo originado nos Estados Unidos, em tradução livre para a língua portuguesa, significaria “notícias falsas”. Suas características já eram comuns desde o início da internet, entretanto, com o passar dos anos, este meio adquiriu uma capacidade de divulgação massiva, sobre toda e qualquer notícia disponibilizada na “rede”, tornando-se um perigo para diversos campos sociais.

Aviv Ovadya, chefe de tecnologia do Centro de Responsabilidade para Mídias Sociais e engenheiro formado pelo Instituto de Tecnologia de Massachusetts (MIT), apresenta que o maior problema das informações falsas, é que elas “caminham” em paralelo as verdadeiras notícias, podendo causar problemas a nível mundial, sejam eles políticos, econômicos ou até mesmo sobre a saúde¹⁴. Esta prática não se faz estranha para os brasileiros, pois no presente ano de 2018 (dois mil e dezoito), em período eleitoral, diversas foram as informações falsas disseminadas pelo meio virtual, com intuito de denegrir determinados candidatos ou seus partidos, acarretando inúmeros transtornos aos presidenciais.

As constantes explicações dos candidatos e o sentimento de ódio populacional, chamou atenção do TSE, onde no dia 11 de outubro de 2018, criou um site para esclarecer as informações falsas veiculadas na eleição¹⁵, como poderiam ser identificadas e combatidas. Também ocorreu, no período do segundo turno das votações brasileiras, um encontro entre os advogados, dos até então, candidatos à presidência, Jair Bolsonaro e Fernando Haddad, no dia 17 de outubro de 2018, para tratar sobre alguns temas, tendo como destaque sobre os outros, a Fake News.

Em investigação feita na última semana antes do primeiro turno pelo jornal “O Globo”, “No Facebook, 35 postagens tiveram cerca de 400 mil compartilhamentos e alcançaram milhões de eleitores. Só quatro vídeos publicados na rede social registraram 2,7 milhões de visualizações”. Deste modo, torna-se evidente este

¹⁴ Ver “Políticos, econômicos ou até mesmo sobre a saúde”. Disponível em: < <https://www.uol.com.br/especiais/ele-previu-o-apocalipse-das-noticias-falsas.htm#frases-2> >. Acesso em 29 ago. 2018.

¹⁵ Ver “Criou um site para esclarecer as informações falsas veiculadas na eleição”. Disponível em: < <http://www.tse.jus.br/hotsites/esclarecimentos-informacoes-falsas-eleicoes-2018/> >. Acesso em 23 out. 2018.

epidêmico fato, onde acontecimentos manipulados e inverídicos passam a possuir poder de controle sobre uma sociedade.

Neste mesmo período eleitoral, as revistas de jornal eletrônico: IstoÉ¹⁶, Exame¹⁷ e Terra¹⁸, apresentaram matéria onde um senador chileno propunha a “Lei Bolsonaro”, que estabeleceria uma reforma constitucional para punir candidatos que utilizassem notícias falsas nas eleições.

Estes fatos asseguram a importância de um debate jurídico sobre o assunto, adentrando ainda mais sobre a tipificação de todas essas condutas, extraindo suas peculiaridades mediante os episódios, por serem realizados em um “espaço e tempo” diferente do nosso, o “ciberespaço”. Em matéria feita sobre o tema textual do Exame Nacional do Ensino Médio (ENEM), em 2015, pelo Zero Hora, disse que: “a redação é escolhida em consenso por especialistas selecionados pelo Inep, autarquia do Ministério da Educação (MEC) responsável pelo Enem”, este exame trata-se de prova anualmente realizada em todo território nacional, tendo como tema assunto de grande relevância social. No dia 04 de novembro de 2018, na primeira parte da prova então citada, de modo a reafirmar a importância destas palavras, foi feito como tema textual a “manipulação do comportamento do usuário pelo controle de dados na internet”.

Podemos ver que este assunto, em nosso país e no mundo, passou pelo campo político, educacional e judiciário, sua importância e a urgência em debates minuciosos com especialistas, está mais que assegurada!

2.3 CONCEITO DE CRIME

Antes de uma exposição sobre a metodologia, do presente artigo, deve-se ser apresentado algumas questões sobre o entendimento de crimes, se existe alguma lei que venha a pautar questões cibernéticas e quais dificuldades encontradas na aplicação das mesmas.

¹⁶ Ver “IstoÉ”. Disponível em: < <https://istoe.com.br/senador-chileno-propoe-lei-bolsonaro-para-cassar-politicos-que-divulgam-fake-news/> >. Acesso em 30 out. 2018

¹⁷ Ver “Exame”. Disponível em: < <https://exame.abril.com.br/brasil/senador-chileno-propoe-lei-bolsonaro-contra-politicos-que-usam-fake-news/> >. Acesso em 30 out. 2018.

¹⁸ Ver “Terra”. Disponível em: < <https://www.terra.com.br/noticias/brasil/senador-chileno-propoe-lei-bolsonaro-para-conter-fake-news,a46adbe58e2ae876358f7a8df994d7cb71knxwtp.html> > Acesso em 30 out. 2018.

Segundo o art. 1º da Lei de Introdução ao Código Penal (Decreto-lei nº 3.914, de 9 de dezembro de 1941), assim redigido: “Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativamente ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente”.

Tendo em vista nosso posicionamento social perante conceitos jurídicos, não devemos nos prender a uma resposta tão rasa, já que em termos técnicos, o crime pode levar em conta três aspectos: material, legal e formal ou analítico.

2.3.1 Critério material/substancial:

Esse critério define o crime como toda ação ou omissão humana que lesa ou expõe a perigo de lesão, bens jurídicos penalmente tutelados. Definidos por Claus Roxin (2006, p. 18-19)¹⁹, como aqueles bens imprescindíveis para a convivência em sociedade. Exemplos desses bens são a vida, a liberdade, a honra, o patrimônio, etc.

2.3.2 Critério legal

Segundo esse critério, o conceito de crime é o fornecido pelo legislador, sendo utilizado o art. 1º da Lei de Introdução ao Código Penal (Decreto-lei nº 3.914, de 9 de dezembro de 1941), já que não possuímos outro dispositivo que apresente uma definição legal.

2.3.3 Critério analítico

Também conhecido como formal ou dogmático, utiliza como base os elementos que compõem a estrutura do crime. Existem mais de uma corrente que traz consigo sua definição, porém, as duas mais debatidas no Brasil são as correntes **bipartida** e a **tripartida**, em que a primeira corrente é um conceito analítico do crime

¹⁹ ROXIN, Claus. *A proteção de bens jurídicos como função do direito penal*. Org. e Trad. André Luís Callegari e Nereu José Giacomolli. Porto Alegre: Livraria do Advogado, 2006.

como bipartido, diz que o crime é fato típico e ilicitude. Já a segunda corrente, tripartida, denota um crime analítico como fato típico, ilícito e culpável.

2.4 CONCEITO DE CRIME CIBERNÉTICO

Utilizando como ponto de partida toda a fundamentação apresentada pelo conceito detalhado de crime e suas subdivisões, podemos adentrar em uma explicação sobre o que são crimes cibernéticos.

Referem-se a todo e qualquer delito cometido pelo meio virtual, utilizando como acesso computadores, smartphones, internet, seja ela provida por rede pública, privada ou doméstica. Diversos são os objetivos almejados por esses “invasores”²⁰, seja o puro e simples desejo de causar o mal, ou a busca por enriquecimento pessoal.

Os crimes cibernéticos podem ser classificados de diversas maneiras, entretanto, os quatro mais conhecidas e tratadas no Brasil, são os crimes de informática próprios e os impróprios.

2.4.1 Próprios:

Envolvem o bem jurídico protegido pela norma penal que trata sobre a inviolabilidade dos dados ou informações. Exemplo: Art. 313-A, do CP, acrescentado pela Lei nº 9.983/2000, que determina: “Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos ou excluir indevidamente dados corretos nos sistemas informatizados da Administração Pública com o fim de obter vantagem para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos e multa” (VIANNA, 2003) esta citação é da letra da lei. Não precisa citar o nome do autor que citou um artigo do CP.

2.4.2 Impróprios:

São aqueles em que o computador é usado como instrumento para a execução do crime, porém não há ofensa ao bem jurídico que versa sobre a

²⁰ Categoria “Invasores” - diz respeito aos que acessam informações virtuais, de cunho pessoal, sem prévia autorização do proprietário. “Hackers”.

inviolabilidade dos dados ou informações. Exemplo: crimes contra a honra cometidos por meio da Internet.

2.4.3 Mistos:

São crimes complexos em que a norma visa tutelar, além da proteção da inviolabilidade dos dados, bem jurídico de natureza diversa. São delitos derivados do acesso não-autorizado a sistemas computacionais. O autor destaca que, no ordenamento jurídico brasileiro, o delito informático fundamental ainda não foi tipificado, enquanto que um derivado já o foi, a saber: acesso não-autorizado a sistemas computacionais do sistema eleitoral, com a Lei nº 9.100/95, em seu art. 69, VII, que prevê: “Obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos” (apud VIANNA, 2003);

2.4.4 Mediatos/indiretos:

Delito-fim, não-informático, que herdou essa característica do delito-meio informático, realizado para poder ser consumado. Exemplo: o acesso não-autorizado a um sistema computacional bancário para a realização de um furto.

2.5 LEI Nº12.737 DE 30 DE NOVEMBRO DE 2012:

A propositura da lei foi em referência a situação específica vivenciada pela atriz global Carolina Diekmann, que em maio de 2012, teve cópias de fotos e conversas retidas do seu computador pessoal e divulgadas na internet sem sua autorização.

Diversos foram os debates acerca de assuntos cibernéticos até que sancionada a “lei Carolina Diekmann”, deferida pela então Presidente da República Dilma Roulssellff, dias depois do crime.

Por ter sido vítima de uma construção rápida e sem grandes estudos sobre o tema, a lei passou a receber diversas críticas providas por juristas, peritos e profissionais de segurança da informação, sobre a confusão e abrangência dos dispositivos tratados, segundo os especialistas, podendo assim condenar criminalmente condutas triviais.

2.6 MARCO CIVIL DA INTERNET, LEI 12.965/2014

Em outubro de 2009, a Secretaria de Assuntos Legislativos do Ministério da Justiça, fez propositura de lei que assegurasse direitos e deveres dos usuários e das empresas provedoras de acesso e serviços online. Com o intuito de garantir uma internet democrática, no Brasil, foi adotada uma ideia chamada de “neutralidade”, proibindo as provedoras de internet de restringirem a conexão ou velocidade dos seus usuários, independente do conteúdo acessado, além de garantir à mesma qualidade de acesso a rede para todos.

A privacidade de sua navegação, juntamente com a contínua verificação de sites, blogs e similares, eliminando qualquer tipo de conteúdo ilícito é um dos temas tratados por essa lei. Vale ser acrescido que esta busca limita-se a “internet superficial”, não se estende a “deep web”.

2.7 PORNOGRAFIA DE VINGANÇA

Trata-se do Projeto de Lei da senadora Vanessa Grazziotin, que passou a vigorar como Lei Ordinária nº 13.718/2018, esta vem modificar o Código Penal, apresentando novas tipificações de condutas crimes e causas para aumento de pena. Segue as mudanças:

- a) Importunação sexual;
- b) Divulgação de cena de estupro;
- c) Tornar pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável;
- d) Estabelecer causas de aumento de pena para esses crimes; e
- e) Definir como causas de aumento de pena o estupro coletivo e o estupro corretivo.

2.8 CRIMES COMUNS POR MEIO DE COMPUTADOR/INTERNET

Diversos crimes cometidos no meio virtual assemelham-se com práticas existentes no mundo real, entretanto nossos códigos não acompanham as

peculiaridades deste meio, que podem ser desde sua elaboração a execução, fazendo que seja necessária uma adequação quanto ao tipo penal.

Segundo pesquisa divulgada pelo jornal Folha de São Paulo, os crimes de informática mais comuns são²¹:

2.9 ROUBO DE IDENTIDADE

Em publicação feita pela Microsoft na sua Central de Segurança, o “roubo de identidade é qualquer tipo de fraude que resulte na perda de dados pessoais, como senhas, nomes de usuário, informações bancárias ou números de cartão de crédito”²². Este ato também pode ser chamado de “Phishing”, no qual os comumente modos usados pelos criminosos para conseguir informações pessoais de suas vítimas, são: Envio de e-mails fraudulentos, sites modificados para roubo de dados e links gerados para esta prática específica.

2.10 PEDOFILIA

Na segunda posição encontramos a pedofilia, que no meio virtual, pode se caracterizar desde a ação pelo indivíduo em possuir ou encaminhar fotos ou vídeos, relacionados ao abuso sexual infantil, estendendo-se a participação ou criação de sites que venham expor estes materiais.

O ECA, Estatuto da Criança e do Adolescente, vem tipificar as condutas crimes que resulta na pedofilia, em seus artigos, 241 – A e 241 – B, da Lei 8069/90. As ações de divulgação, como de armazenamento de “vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente”, tem como pena a reclusão de 3 (três) a 6 (seis) anos, e multa.

Entretanto, mesmo que o artigo 241 – A, venha a citar a divulgação “por meio de sistema de informática”, não se leva em consideração a capacidade de disseminação em massa de qualquer conteúdo, seja ele lícito ou ilícito, nesta

²¹ Ver “os crimes de informática mais comuns são”. Disponível em: < <https://www1.folha.uol.com.br/foha/informatica/ult124u19455.shtml> >. Acesso em 05 jul. 2018.

²² Ver “roubo de identidade é qualquer tipo de fraude que resulte na perda de dados pessoais, como senhas, nomes de usuário, informações bancárias ou números de cartão de crédito”. Disponível em: < <https://www.microsoft.com/pt-br/security/resources/identitytheft-what-is.aspx> >. Acesso em 05 jul. 2018.

ferramenta. Tendo isso em mente, seria certo tratar este fato, como uma agravante da conduta criminosa.

2.11 CALÚNIA E DIFAMAÇÃO

No que refere-se a explicação do Código Penal sobre esses dois pontos, temos que:

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

§ 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.

Art. 139 - **Difamar** alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa. Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Mesmo sendo dois atos já tipificados, as especificidades destas práticas não são agraciadas pelos legisladores, como a permanência do conteúdo calunioso ou difamatório na rede, podendo ser salvo por terceiros, o que o faria perdurar mais tempo na mente dos que o vissem.

2.12 AMEAÇA

Comumente nos deparamos com discursos calorosos em plataformas virtuais. O fato do aconchego e anonimato destes indivíduos, fazem com que tudo se torne mais fácil. Por este fato, diversas ameaças são direcionadas para endereços eletrônicos, redes sociais ou usuários de sites específicos, que podem se sentir verdadeiramente intimidados.

O Código Penal de 1994, no Decreto Lei nº 2.848, artigo 147, apresenta:

Art. 147 - Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:

Pena - detenção, de um a seis meses, ou multa.

Parágrafo único - Somente se procede mediante representação.

2.13 DISCRIMINAÇÃO

Conteúdos que venham a atentar contra raça, cor, etnia, religião ou procedência nacional, tornam-se o quinto crime mais comum na internet. Os locais destas práticas são geralmente as redes sociais ou em comentários de sites.

O artigo 1º da Lei 7.716/89, define quais são os tipos de discriminação que podem sofrer de sanção penal, entretanto, vale ser lembrado que já se acham novos textos legais que abordem, de maneira mais específica, algumas dessas questões: “Art. 1º Serão punidos, na forma desta Lei, os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional”.

2.14 ESPIONAGEM INDUSTRIAL

Seria a transferência de informações sobre uma empresa para outra, geralmente buscando informações sobre avanços tecnológicos.

3. METODOLOGIA

A metodologia trata sobre a apresentação dos meios utilizados para a formação do conhecimento apresentado no artigo, como meio comprovador da validade e utilidade nos diversos campos sociais.

3.1 MÉTODO HIPOTÉTICO-DEDUTIVO

Mediante a formulação do problema e dos fatos, foram geradas hipóteses, sendo elas uma principal e outras auxiliares, tendo como fim, a resolução do fato, com base em uma coleta e análise detalhada dos dados. É apresentado de forma dedutiva, pois toda a pesquisa final, apontam para previsões específicas, tentando ao máximo excluir os pontos que dificultem esta previsão.

Quando os conhecimentos disponíveis sobre determinado assunto são insuficientes para a explicação de um fenômeno, surge o problema. Para tentar explicar as dificuldades expressas no problema, são formuladas conjecturas ou hipóteses. Das hipóteses formuladas, deduzem-se consequências que deverão ser testadas ou falseadas. (GIL, 2008, p. 12).

A insuficiência de conhecimento não provém mediante a incapacidade dos pesquisadores, mas, pelo tema tratado ser complexo e muito atual, dificultando a explicação dos seus fenômenos.

3.2 MÉTODO DIALÉTICO

Mesmo sendo tratado de um “novo mundo”, suas características e seus fundamentos são influenciados e influenciam, de maneira direta, todas as questões sociais. Por este fato, a reformulação apresentada por Marx, sobre este pensamento, é uma grande assertiva. Quando relata que todos os elementos apresentam características contraditórias organicamente unidas e indissolúveis.

[...] a dialética fornece as bases para uma interpretação dinâmica e totalizante da realidade, uma vez que estabelece que os fatos sociais não podem ser entendidos quando considerados isoladamente, abstraídos de suas influências políticas, econômicas, culturais etc.(GIL, 2008, p. 14)

A prática desenfreada de crimes no meio virtual, juntamente com seus métodos de ação, são influenciados por todo um conjunto de momentos sociais.

3.3 MÉTODO HISTÓRICO

Mesmo sendo um problema atual, é preciso ser feito um levantamento de estatísticas históricas, buscando conexões, diferenças e modos de ação, no passado para o presente. Utilizando a obtenção de possíveis respostas como um fator explicativo para a conclusão da pesquisa.

3.4 MÉTODO COMPARATIVO

A pesquisa feita em diversas localidades a nível mundial, buscando lugares que apresentaram a ocorrência de casos similares, colhendo informações e comparando com a vivência brasileira, a fim de estudar possíveis adequações de práticas estrangeiras. Sendo que também, este método foi utilizado como ponto demonstrativo de gravidade sobre a problemática apresentada: “Sua ampla utilização nas ciências sociais deve-se ao fato de possibilitar o estudo comparativo de grandes grupamentos sociais, separados pelo espaço e pelo tempo.” (GIL, 2008, p. 16-17).

3.5 PESQUISA DE CAMPO

Como seu próprio título apresenta, trata-se de uma investigação que vai além da documental e bibliográfica, se realiza coleta de dados junto a pessoas que possuem informação sobre o que se procura. Podendo ser utilizado como exemplo, o caso da CODERN.

A pesquisa documental trilha os mesmos caminhos da pesquisa bibliográfica, não sendo fácil por vezes distingui-las. A pesquisa bibliográfica utiliza fontes constituídas por material já elaborado, constituído basicamente por livros e artigos científicos localizados em bibliotecas. A pesquisa documental recorre a fontes mais diversificadas e dispersas, sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, cartas, filmes, fotografias, pinturas, tapeçarias, relatórios de empresas, vídeos de programas de televisão, etc.". (FONSECA, 2002, p. 32).

3.6 PESQUISA DOCUMENTAL

Trata-se de uma pesquisa feita sobre documentos já formados, onde tratam sobre os assuntos pesquisados, geralmente encontrados em livros e artigos científicos. Mesmo sobre bastante dificuldade, pois dificilmente encontramos este assunto em livros e artigos, este tipo de pesquisa foi fundamental para o desenvolvimento do trabalho.

A pesquisa documental trilha os mesmos caminhos da pesquisa bibliográfica, não sendo fácil por vezes distingui-las. A pesquisa bibliográfica utiliza fontes constituídas por material já elaborado, constituído basicamente por livros e artigos científicos localizados em bibliotecas. A pesquisa documental recorre a fontes mais diversificadas e dispersas, sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, cartas, filmes, fotografias, pinturas, tapeçarias, relatórios de empresas, vídeos de programas de televisão, etc.". (FONSECA, 2002, p. 32).

4. DISCUSSÃO DOS RESULTADOS

Números comprovam de maneira nítida que, no compasso da criação de um usuário na internet, disponibilizamos contínuos dados para facilitar nosso dia a dia no mundo "real", nos fragilizando cada vez mais em nossa "second life", ficando a mercê de possíveis ataques. Mesmo possuindo leis de grande importância, como a do Marco Civil da Internet, lei 12.956/14, que ajuda no combate e na investigação de qualquer desvio de conduta feita por seus usuários. Sua ineficácia é gritante, pois

possuímos exemplos na “suface web” como na “deep web”, de aglomerados assuntos que contradizem todas as questões sociais existentes. A natureza do ser humano é completamente exposta nestes pontos da rede, devido a existência de “máscaras” que asseguram a impunidade dos que delinquem.

Torna-se fácil observar que nossos legisladores, mesmo possuindo uma compreensão sobre a existência da problemática tratada, compõem normas deveras imprecisas, deixando a desejar uma atuação mais firme de leis que controlem condutas criminosas, seja pelo próprio desinteresse legislativo, ou mediante a dificuldade de combater o desenvolvimento desenfreado destes casos. Um problema que atenta contra diversos campos sociais e que dispõe de um nível de complexidade nítida, deve ser tema de discussões amplas, com profissionais que conhecem a área, para que as tipificações destas condutas não se tornem muito extremas, podendo ser amenas ou rígidas demais, como a lei nº12.737/12, foco de diversas críticas por especialistas.

Algumas ações que ocorrem no meio virtual, já possuem tipificação presente em nossa sociedade, o que pode deixar o leitor um pouco confuso quanto à necessidade de criação de um novo código que venha a tratar especificamente deste assunto, entretanto, ao pensar deste modo, são totalmente desconsideradas as especificidades destas práticas. Sua capacidade de divulgação, quantidade de vítimas, formação de identidades falsas e outros, são algumas das muitas características que podem ser apresentadas e divergem das costumeiras ações no mundo físico.

Como apresentado no livro Neuromancer, é uma realidade paralela a nossa, possuidora de sua própria língua, tempo e espaço, entretanto, seus controladores ainda são os humanos. Mesmo sendo possuidora de um grande “poder” informacional, a internet não passa de uma ferramenta humana, que segue comandos e possui suas respectivas fragilidades, sendo a maior delas, o conhecimento que um usuário pode adquirir para se precaver destes ataques.

5. CONSIDERAÇÕES FINAIS

“A tecnologia tornou possível a existência de grandes populações. Grandes populações agora tornam a tecnologia indispensável”, Joseph Krutch, escritor. Desconheço frase que caracterize, de maneira mais complementar, o que tratamos

ao decorrer deste artigo. A questão pode ser turva e clara, ao mesmo tempo, o pluralismo de caminhos que podem ser traçados sobre esse tema, fogem do controle, pois tudo é muito novo para conseguir definições de grande abrangência. Por este modo, se faz necessário limitar o pensamento do leitor ao que se tem mais urgência. Uma legislação mais precisa sobre crimes virtuais (a criação de um novo código para tratar destas violações), projetos de conscientização social e incentivos estudantis para o desenvolvimento de campanhas ou métodos de segurança informacional, são os meios de ação mais fortes que podem ser usados para combater esses crescentes desvios de condutas.

Mesmo tendo consciência que já foi apresentado, o Código Penal brasileiro foi criado em 1940, sendo fácil idealizar o quão desajustadas as práticas de crimes virtuais se encontram. Agregar tipificações a ele, mediante ocorrências criminosas na internet, não é a solução. Fazendo uma comparação com a ideia apresentada no livro de Michael Foucault, Vigiar e Punir "...esse Estado condicionava a existência de um direito muito vago", "não era justiça e legalidade era só força". A punição é o único fator almejado, não havendo preocupação sobre as atenuantes e agravantes de cada conduta. Os brasileiros estão a mercê de leis sem uma estruturação adequada, que podem prejudicar inocentes e favorecer delinquentes. Deve-se tratar a internet como sendo um espaço paralelo ao nosso, todas as condições comparativas mediante as ideias entre físicos sobre espaço e tempo de um mundo, se adequam a ela, então, torna-se claro que, como em toda sociedade, este mundo virtual deve possuir um código que venha a controlar "seus habitantes", operando sobre questões específicas. Deste modo, o primeiro ponto é tipificar toda e qualquer ação criminosa que possamos nos deparar, pois o Princípio da Legalidade do Direito Penal, que tem manifesto direto no artigo 1º, CP - "não há crime sem lei anterior que o defina, nem há pena sem prévia cominação legal".

Segundo ponto, entretanto, não menos importante, são a organização de campanhas e a criação de métodos para a segurança informacional. Estamos tratando sobre uma ferramenta, sendo assim, como toda e qualquer outra, se faz necessária a intervenção humana para o seu desenvolvimento e sua ação, deste modo, o maior nível de segurança que pode ser realizado não provém da criação de aplicativos ou meios similares, vem do conhecimento dado aos usuários sobre esse mundo. A maior fiscalização que um indivíduo pode fazer, é sobre si mesmo. Este é o ponto abordado por Kevin Mitnick, ex hacker mundialmente famoso, autor do livro

Engenharia Social: O malware mais antigo do mundo. Ele apresenta que, do mesmo modo que ocorre no mundo real, onde abrimos uma porta para um estranho, por simpatizar com sua fala, na internet ocorre do mesmo modo, entrando em links estranhos que possuem temas que gostamos, baixando o que aparentemente seriam fotos com amigos e outros, estaríamos abrindo a porta para um estranho entrar em nossa “casa”. O livro apresenta que cada passo dado no meio digital, deve ser feito com os devidos cuidados, policiando-se para não ser mais uma das muitas vítimas. Propagandas com informações básicas e cartilhas de fácil compreensão, divulgadas em colégios e faculdades, podem livrar milhares de pessoas de serem futuras vítimas, tendo em mente que a informação divulgada em sala de aula seria repassada para o restante do grupo familiar, caso fosse pedido.

A criação de métodos de segurança, caminham em paralelo com a conscientização social, muitas vezes sofremos o furto de informações e não possuímos conhecimento ou a informação de como agir e quem procurar, pensando nisso, em parceria com aluno da UFRN, Kelvem Katson, iniciamos o desenvolvimento de uma ferramenta de aplicação prática para reverter esta situação, o Deepman.

O sistema em questão é uma ferramenta de alerta e prevenção de crimes cibernéticos, que orienta e aconselha internautas a como se prevenir aos golpes praticados pelos chamados “hackers”, além de prestar suporte as vítimas desse tipo de delito, indicando quais medidas devem ser tomadas para solucionar suas lides. A nível de pesquisa, o sistema irá armazenar informações genéricas sobre o seus usuários, montando um banco de dados que relacione possíveis padrões entre as infrações cometidas e suas localidades. Consta em anexo1 e anexo2, tabelas que apresentam; Detalhamento dos Requisitos Funcionais e Requisitos não Funcionais do Deepmann.

Deste modo, apresento-lhes, não só a ideia de como combater esta crescente demanda de crimes, mas também, a sua execução.

O trabalho usou como referencial diversos pensamentos, para construir, com base, uma ideia a ser defendida, entretanto, acima de tudo, esse será o primeiro passo para que meus posicionamentos sejam a base de estudo para outros que tenham cede de conhecimento. Muitos copiam grandes nomes, e utilizam como referência, eu trabalho para me tornar uma.

REFERÊNCIAS

MASSON, Cleber. **Direito penal esquematizado** – Parte geral – vol. 1 / Cleber Masson. 10.^a ed. Ver., atual. E ampl. – Rio de Janeiro: Forense; São Paulo: MÉTODO, 2016.

ROXIN, Claus. **A proteção de bens jurídicos como função do direito penal**. Org. e Trad. André Luís Callegari e Nereu José Giacomolli. Porto Alegre: Livraria do Advogado, 2006.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. – São Paulo: Atlas, 2008.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático**. Rio de Janeiro: Forense, 2003.

IBOPE INTELIGÊNCIA (Ed.). **79% dos internautas brasileiros usam aplicativos de bancos**. 2017. Disponível em: <<http://www.ibopeinteligencia.com/noticias-e-pesquisas/79-dos-internautas-brasileiros-usam-aplicativos-de-bancos/>>. Acesso em: 14 ago. 2018.

COMPUTERWORLD (Ed.). **Brasil está entre os cinco países que mais sofrem ataques cibernéticos no mundo**. 2017. Disponível em: <<https://computerworld.com.br/2017/07/28/brasil-esta-entre-os-cinco-paises-que-mais-sofrem-ataques-ciberneticos-no-mundo/>>. Acesso em: 14 ago. 2018.

EBC (Ed.). **Acesso à internet chega a 49,4% da população brasileira**. 2015. Disponível em: <<http://www.ebc.com.br/tecnologia/2015/04/acesso-internet-chega-494-da-populacao-brasileira>>. Acesso em: 04 jul. 2018.

SUPERINTERESSANTE. **Questão de tempo**. 1988. Disponível em: <<https://super.abril.com.br/ciencia/questao-de-tempo/>>. Acesso em: 15 ago. 2018.

SUPERINTERESSANTE. **O que é a Teoria da Relatividade?** 2013. Disponível em: <<https://super.abril.com.br/mundo-estranho/o-que-e-a-teoria-da-relatividade/>>. Acesso em: 15 ago. 2018.

PRESSE, France. **Ataque de hackers 'sem precedentes' provoca alerta no mundo**. 2017. Disponível em: <<https://g1.globo.com/tecnologia/noticia/ataque-de-hackers-sem-precedentes-provoca-alerta-no-mundo.ghtml>>. Acesso em: 25 jul. 2018.

UOL. **O "infocalipse" vem aí**. 2018. Disponível em: <<https://www.uol/noticias/especiais/ele-previu-o-apocalipse-das-noticias-falsas.htm#o-infocalipse-vem-ai>>. Acesso em: 29 ago. 2018.

TSE. **ESCLARECIMENTOS SOBRE INFORMAÇÕES FALSAS VEICULADAS NAS ELEIÇÕES 2018**. 2018. Disponível em:

<<http://www.tse.jus.br/hotsites/esclarecimentos-informacoes-falsas-eleicoes-2018/>>. Acesso em: 23 set. 2018.

ISTOÉ. **Senador chileno propõe ‘Lei Bolsonaro’ para cassar políticos que divulgam fake news.** 2018. Disponível em: <<https://istoe.com.br/senador-chileno-propoe-lei-bolsonaro-para-cassar-politicos-que-divulgam-fake-news/>>. Acesso em: 30 out. 2018.

EXAME. **Senador chileno propõe “Lei Bolsonaro” contra políticos que usam fake news.** 2018. Disponível em: < <https://exame.abril.com.br/brasil/senador-chileno-propoe-lei-bolsonaro-contrapoliticos-que-usam-fake-news/>>. Acesso em: 30 out. 2018.

TERRA. **Senador chileno propõe "Lei Bolsonaro" para conter fake News.** 2018. Disponível em: < <https://exame.abril.com.br/brasil/senador-chileno-propoe-lei-bolsonaro-contrapoliticos-que-usam-fake-news/>>. Acesso em: 30 out. 2018.

MICROSOFT. **O que é phishing?** 2012. Disponível em: <<https://www.microsoft.com/pt-br/security/resources/phishing-what-is.aspx>>. Acesso em: 05 jul. 2018.

CARPANEZ, Juliana. **Conheça os crimes virtuais mais comuns.** 2006. Disponível em: <<https://www1.folha.uol.com.br/folha/informatica/ult124u19455.shtml>>. Acesso em: 25 jun. 2018.

ANEXOS**Anexo1****Detalhamento dos Requisitos Funcionais**

IDENTIFICAÇÃO	DESCRIÇÃO DO REQUISITO
RF001	É necessário que o administrador tenha acesso às informações que lhe são pertinentes no sistema, como o número de usuários que responderam questionários, suas respostas e as estatísticas geradas a partir delas. É através desse ambiente de gerenciamento que serão administradas as informações presentes na tela inicial e serão visualizadas as mensagens e feedbacks dos usuários.
RF002	Disponibilizar inicialmente, aos usuários, informações sobre os crimes digitais, maneiras de se proteger, quais são os tipos de delitos, como deve ser a reação ao presenciar um crime desse gênero, informações sobre as leis vigentes que punem tais práticas, notícias de casos de maiores repercussões na mídia, opiniões de especialistas sobre crimes cibernéticos e se possível sobre o sistema. Esse primeiro ambiente será acessado pelos usuários, para que esses disponibilizem essas informações logo na primeira visualização do sistema. O conteúdo desta página poderá ofertar oportunidades do sistema ser referenciado em artigos e periódicos em geral. Essa página possibilita ao cliente, que prefere ficar no anonimato, ter acesso a informação sem precisar informar seus dados ao sistema, mesmo que os dados exigidos para resposta do questionário sejam genéricos.
RF003	Os usuários que se sentirem à vontade para interagir com o sistema, serão direcionados para a área de questionário, onde o cliente passará por uma triagem de informações básicas, sem precisar identificasse, e logo após poderá responder, através da múltipla escolha, perguntas que auxiliaram a traçar um perfil daquele usuário, ou da situação pela qual ele passou. Mesmo o questionário disponibilizando um sistema de múltipla escolha para responder as perguntas, em casos onde o utilizador não sente-se amparado pelas opções disponíveis, será possível dar um feedback para o administrador do sistema, marcando uma opção que possibilita responder a

	pergunta desejada, de maneira subjetiva. Essa utilidade vai possibilitar que os usuários indiquem novas opções de respostas para as perguntas.
RF004	O usuário deverá fornecer informações do tipo: nome, idade, gênero, grau de escolaridade, etnia, dados sobre situação financeira e etc. Essas informações servirão como base para a geração de gráficos e estatísticas do sistema, é através delas que será possível indicar se existe um determinado grupo de usuários que está mais vulneráveis a ataques.
RF005	Armazenar a posição geográfica do paciente (Latitude e Longitude), é importante para sabermos a localização dele, seu estado, cidade e bairro. Dessa forma podemos montar mapas que apresentem regiões (estados e/ou municípios) com maiores taxas de crimes virtuais, ou até mesmo ligar aquela localidade a um perfil padrão de crime, como por exemplo: indicar que em regiões periféricas é maior o índice de crimes. Essa informação pode ser acessada assim que o usuário abre o navegador, sem que o mesmo tenha que informar no sistema. A localização será usada também para indicar o usuário onde procurar ajuda.
RF006	Esse artifício pode ser acessado através do próprio navegador, servirá para sabermos se antes de chegar ao nosso sistema o usuário já vinha buscando sobre o assunto e se existia um eixo específico pesquisado, se sim, o conteúdo inicial e as perguntas mostradas ao usuário estará ligadas a essa pesquisa realizada previamente.
RF007	As perguntas do questionário serão divididas em algumas partes e vão desde dizer se você passou ou presenciou um cibercrime, até quem foi o agressor e se o indivíduo já tinha ideia de que aquela ação se configura ou não como um crime. A próxima pergunta, em muitas situações, dependerá diretamente da resposta concedida anteriormente.
RF008	Ao fim do questionário o utilizador do sistema terá um parecer da sua situação, lhe será dito se a ação descrita por ele se configura como um delito, se sim, quais as leis que podem lhe amparar. Neste momento será exibido ao usuário instruções de como agir de acordo com seu caso.
RF009	Sendo constatado que o utilizador da aplicação necessita de ajuda, uma série de instituições (delegacias, advogados, psicólogos e etc) mais próximas lhe serão disponibilizadas, com rotas e informações de contato.
RF010	Sistema simples de avaliação, através de estrelas, mas será possível nesse momento, enviar um e-mail para a administração do sistema, com críticas e sugestões que serão analisadas pelo suporte da aplicação.
RF011	Essa utilidade poderá ser usada pela administração do sistema,

	que poderá gerar gráficos que indiquem por exemplo se a maior taxa de vítimas de delitos virtuais abrangem homens ou mulheres; negros, brancos ou amarelos e etc. Esses dados poderão facilmente serem aplicados a pesquisas futuras.
--	---

Anexo2**Requisitos Não Funcionais**

IDENTIFICAÇÃO	DESCRIÇÃO DO REQUISITO DETALHAMENTO DO REQUISITO
RNF001	O sistema deve ter uma arquitetura cliente-servidor no formato de uma aplicação web.
RNF002	Usabilidade. O sistema deve apresentar uma interface intuitiva e eficiente para os seus usuários, sendo prático para o uso diário das empresas e microempreendedores.
RNF003	Autenticação. O administrador deve se autenticar para poder fazer uso das funcionalidades do gerenciamento.
RNF004	Todos os dados devem ser armazenados em um SGBD relacional, que apresente disponibilidade constante dos dados.
RNF005	Segurança. O Sistema deve garantir total proteção aos dados dos usuários.
RNF006	Portabilidade. O Sistema deve ser desenvolvido tendo a perspectiva que ele será bastante utilizado em telefones móveis.