UNIVERSIDADE DE TAUBATÉ

MARIANA FERREIRA DA SILVA

O DIREITO À LUZ DO MUNDO MODERNO E DO AMBIENTE VIRTUAL

Taubaté – SP

2020

MARIANA FERREIRA DA SILVA

O DIREITO À LUZ DO MUNDO MODERNO E DO AMBIENTE VIRTUAL

Trabalho de Conclusão do Curso apresentado como exigência parcial para obtenção do grau de bacharel em Ciências Jurídicas da Universidade de Taubaté, sob a orientação do Professor Me. Marcos Edwagner Salgado dos Santos

Taubaté - SP

2020

MARIANA FERREIRA DA SILVA

O DIREITO À LUZ DO MUNDO MODERNO E DO AMBIENTE VIRTUAL

Trabalho de Graduação apresentado como exigência parcial para obtenção do grau de Bacharel em Ciências Jurídicas pela Universidade de Taubaté.
Orientador: Professor Me. Marcos Edwagner Salgado dos Santos

Trabalho de Graduação defendido e aprovado em _____/_____/_____ pela comissão julgadora:

_____
Professor Me. Marcos Edwagner Salgado dos Santos, Universidade de Taubaté.

_____

Prof. , Universidade de Taubaté.

Dedico este trabalho a todos que já se sentiram impotentes ao sofrer ou ver injustiças acontecendo na internet. Vocês não estão sozinhos.

AGRADECIMENTOS

Agradeço meus pais por me proporcionarem todos os meus estudos e acreditarem no meu potencial como indivíduo e profissional. Em especial à minha mãe que esteve diretamente envolvida e me ajudando a cada passo deste trabalho.

Também gostaria de agradecer a Universidade de Taubaté pela educação e ensinamentos, fundamentais para a elaboração deste trabalho e para a minha formação profissional.

Ao Professor Marcos Edwagner Salgado dos Santos, meu Orientador, pelo exemplo profissional e pelos ensinamentos; pela paciência com a qual compartilhou seus conhecimentos, e pelo privilégio a mim concedido de me orientar nesse projeto.

À Luiza Dantas, Secretária da Graduação, e a Maria do Carmo, Secretária da Assistência Jurídica pela atenção, paciência e imensa ajuda com a parte burocrática do processo.

Ao meu avô, que não mais se encontra entre nós, mas que sempre me incentivou e torceu pela minha vitória.

“Aquele que luta com monstros deve acautelar-se para não tornar-se também um monstro. Quando se olha muito tempo para um abismo, o abismo olha para você.”

Friedrich Nietzsche

RESUMO

O presente estudo de cunho monográfico e bibliográfico apresenta uma revisão da literatura sobre a problemática da modernização da sociedade e sua integração com tecnologias criando um novo ambiente, o “espaço virtual”. Neste espaço, indivíduos mal intencionados desenvolvem a cada dia novas formas de praticar atos ilícitos e fazer novas vítimas. Este estudo objetivou analisar a Lei Carolina Dieckmann, o Marco Civil da Internet, o serviço especializado para orientar vítimas de crimes na internet da SaferNet e as delegacias de crimes digitais verificando sua eficácia e suficiência em cumprir o propósito de punir os criminosos cibernéticos e trazer sensação de segurança à população no que se diz respeito às novas tecnologias emergentes e ao mundo virtual. Além da revisão da literatura, este estudo realizou uma pesquisa qualitativa, visando compreender a relação entre a população, os crimes cibernéticos e a justiça, realizando uma comparação com dados existentes já existentes.

Palavras-chave: internet, digital, lei.

ABSTRACT

The present monographic and bibliographic study presents a review of the literature on the issue of the modernization of society and its integration with technologies creating a new environment, the “virtual space”. In this space, ill-intentioned individuals develop new ways of practicing illegal acts and making new victims every day. This study aimed to analyze the Carolina Dieckmann Law, the Marco Civil of the Internet, the specialized service to guide victims of crimes on the internet of SaferNet and the digital crime police stations, verifying their effectiveness and sufficiency in fulfilling the purpose of punishing “cybercriminals” and bringing the feeling of security for the population regarding the new emerging technologies and the virtual world. In addition to the literature review, the study proposes a qualitative research to understand the relationship between the population and cybercrimes. In addition to the literature review, this study carried out a qualitative research aimed at understanding the relationship between the population, the cybercrimes and the justice, comparing it with existing data.

Keywords: internet, digital, law

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A internet chegou ao Brasil em 1981 por meio da Bitnet. A Bitnet era uma rede acadêmica que conectava universidades e foi fundada em 1981, ligando a Universidade da Cidade de Nova York (CUNY), à Universidade Yale, em Connecticut e a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) ao Fermilab, laboratório de física especializado no estudo de partículas atômicas, que ficava em Illinois, nos Estados Unidos. Ela realizava a conexão e troca de dados por meio de um fio de cobre dentro de um cabo submarino. (OLIVEIRA, 2011).

A partir de 1994, a internet deixou a exclusividade do meio acadêmico e passou a ser comercializada para a população geral; mas, somente em 1996, as primeiras grandes empresas do mercado de provedores iniciaram suas operações. (KLEINA, 2018).

O Brasil é o quarto país com maior número absoluto de usuários de Internet, ficando atrás apenas dos Estados Unidos, Índia e China, segundo relatório publicado pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) em 2017. (NAÇÕES, 2017). Em 2018, de acordo com a pesquisa TIC Domicílios do Instituto Brasileiro de Geografia e Estatística (IBGE), cerca de 70% dos brasileiros já haviam acessado a internet ao menos uma vez. (AGÊNCIA, 2018).

O Brasil não é considerado um país seguro. De acordo com relatório de 2019 da Organização das Nações Unidas (ONU), o Brasil é o segundo país mais violento da América do Sul e, possivelmente, isso se reflita na sensação de insegurança e medo dos brasileiros, inclusive em relação a questões tecnológicas. (NAÇÕES, 2019). Em pesquisa realizada em 2018 pela Companhia de Segurança da Informação ESET, sediada na Eslováquia, sobre o relacionamento dos brasileiros com a Internet das Coisas (em inglês: Internet of Things, IoT - casas inteligentes, tecnologias interligadas por wi-fi, entre outros) 70% dos usuários consideraram que os dispositivos IoT não eram seguros e 96% dos entrevistados acreditavam que suas informações poderiam ser acessadas por cibercriminosos. As maiores preocupações, segundo esta pesquisa, foram: que os criminosos pudessem se passar pelos usuários, que expusessem suas informações pessoais e que pudessem extorqui-los. (ESET, 2018).

Em levantamento mais recente (2018) feito pela associação SaferNet Brasil, em parceria com o Ministério Público Federal (MPF) foram registradas 133.732 queixas de delitos virtuais, dentre eles: pornografia infantil, conteúdos de apologia e incitação à violência e crimes contra a vida e outros. Em comparação ao ano anterior (2017), a quantidade de ocorrências subiu em quase 110%. (ASSESPRO, 2019).

Hoje para as vítimas existe uma cartilha do passo a passo do que fazer, que inclui: preservar todas as provas, procurar uma delegacia de polícia para registrar ocorrência e solicitar a remoção do conteúdo. Para obter resultados favoráveis nas ações a vítima conta com a Lei Carolina Dieckmann, o Marco Civil da Internet, o serviço especializado para orientar vítimas de crimes na Internet da SaferNet e com as delegacias de crimes digitais, localizadas nas principais capitais do país.

No entanto, mesmo com tantas ferramentas e informações disponíveis, ainda se faz extremamente difícil comprovar a materialidade do crime, criar uma prova concreta acerca da identidade do infrator, além de outras burocracias e dificuldades que são criticadas por outros autores e levam a descrença da população.

Este estudo objetivou trazer à luz as críticas à legislação vigente e compreendê-las revisando a literatura disponível sobre o tema e realizando uma pesquisa qualitativa com a população para melhor compreender suas dificuldades com o direito no meio virtual e tentar propor soluções.

2 DESENVOLVIMENTO

2.1 Os Crimes Virtuais

2.1.1 A origem da internet

A internet surgiu na década de 70, com alcunha de ARPANET; seu intuito inicial era ser uma rede de transmissão de informações militares - interligando centros de comando e de pesquisa bélica. Na década de 80, se tornou uma rede acadêmica, conhecida como BitNET. A BitNET conectava universidades e foi fundada em 1981 ligando, primeiramente, a Universidade da Cidade de Nova York (CUNY) à Universidade Yale, em Connecticut. Entre os anos de 1980 e 1990 foi desenvolvido e lançado o World Wide Web (WWW), que viabilizou a transmissão de imagens, som e vídeo pela rede, popularizando a Internet.

A internet chegou ao Brasil em 1988 por meio da Bitnet, conectando a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) ao Fermilab, laboratório de física especializado no estudo de partículas atômicas, que ficava em Illinois, nos Estados Unidos. Ela realizava a conexão e troca de dados por meio de um fio de cobre dentro de um cabo submarino. Em 1990 foi criada a Rede Nacional de Pesquisa (RNP), pelo Ministério da Ciência e Tecnologia, com o objetivo de implantar uma infraestrutura com abrangência nacional para os serviços de internet. (PRACIANO, 2019).

A partir de 1994, a internet deixou a exclusividade do meio acadêmico e foi iniciada sua comercialização a partir de um projeto piloto da Empresa Brasileira de Telecomunicações (Embratel), com acesso à internet através de linhas discadas. Porém, sua grande popularização se deu, devidamente em 1996, quando as primeiras grandes empresas do mercado de provedores iniciaram suas operações. (CIRIACO, 2009).

Nos primórdios, existiam alguns requisitos para acessar a internet, dentre eles: ter uma linha telefônica, um microcomputador com modem (aparelho de recepção e transmissão de dados por telefone) e um programa de acesso à rede (na época os

principais eram o Navigator, da Netscape, e o Internet Explorer, da Microsoft). Também era necessário se cadastrar em um provedor de acesso à rede. Preenchendo todos esses requisitos o usuário recebia um “username”, uma senha e um endereço na internet.

Os principais serviços da época eram o correio eletrônico, que permitia a troca de mensagens entre usuários de qualquer lugar do mundo e a WWW onde encontravam-se os sites, endereço conjunto de páginas criadas por pessoas, empresas, instituições ou órgãos governamentais.

A partir de 1994, a internet tornou-se também um meio de comercialização de produtos e serviços – possibilitando consultar contas bancárias e fazer compras. O impacto foi tão grande, que em 1996, US$ 2,2 bilhões foram movimentados em transações online. (MONOGRAFIAS, 20--).

2.1.2 O que são crimes virtuais?

Crimes virtuais, crimes cibernéticos, e-crimes, cibercrimes (em inglês, cybercrime), crimes eletrônicos ou crimes digitais de uma forma simples, constituem toda a atividade criminal que envolva o uso da infra-estrutura tecnológica da informática, seja computador, notebook, tablet ou smartphones. Stair (1998) disse que os crimes praticados com o computador possuem natureza dupla: o computador tanto pode ser a ferramenta usada para cometer o crime como também pode ser o objeto do crime.

Os crimes informáticos onde o computador é o “objeto do crime” são aqueles que visam causar algum tipo de dano à máquina da vítima. Ocorrem através de programas maliciosos que se instalam no computador de diversas modos. Muitos são amplamente conhecidos, como os ataques através dos vírus, dos “worms” e “trojans”.

Os crimes informáticos com o computador como "ferramenta do crime" são aqueles com intuito de obter dados/ informações sobre a vítima (usuário da máquina). Normalmente são feitos através de programas espiões (spywares), que acessam desde informações mais simples como sites em que o usuário navega até senhas arquivadas no computador.

Vianna (2003) classifica os crimes informáticos em quatro categorias:

1) crimes informáticos impróprios: aqueles nos quais o computador é usado como instrumento para a execução do crime, porém não há ofensa ao bem jurídico e a inviolabilidade dos dados ou informações. Exemplos de crimes informáticos impróprios podem ser calúnia (art. 138 do CP Brasileiro), difamação (art. 139 do CP Brasileiro), injúria (art. 140 do CP Brasileiro), todos podendo ser cometidos, por exemplo, com o envio de um e-mail.

2) crimes informáticos próprios: aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade dos dados ou informações é atingido. Como exemplo desse crime temos a interceptação telemática ilegal, prevista no art. 10 da Lei 9296/96 (Lei Federal Brasileira).

3) delitos informáticos mistos: são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa.

4) crimes informáticos mediatos ou indiretos: é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.

2.1.3 Como os crimes virtuais se comportam no Brasil

O crime informático é algo recorrente no Brasil. Diversas pesquisas, em anos diferentes, mostram o Brasil como líder nesta modalidade ilegal. A empresa britânica de segurança da informação mi2g, realizou em 2002, um levantamento de crimes cibernéticos e coroou o Brasil como "o maior laboratório do cibercrime em todo o mundo". No mesmo ano, na lista dos dez grupos de hackers mais ativos no mundo o Brasil ocupava todas as posições. A empresa credita a proliferação da modalidade às poucas leis para a prevenção dos crimes digitais e o crescente índice de grupos organizados para explorar oportunidades para o cibercrime. (STAROBINAS, 2002).

Um relatório da Norton by Symantec de 2017, apontou que 62 milhões de brasileiros foram vítimas de cibercrime naquele ano - representando 61% da população adulta conectada do país. (COMPUTERWORLD, 2018). Dados do Ministério Público Federal (MPF) apontavam que entre os anos de 2007 e 2008 o

número de procedimentos abertos na Procuradoria para investigar crimes cibernéticos subiu 318%. Em 2007, foram abertas 620 investigações, menos de um terço dos 1.975 procedimentos abertos no ano seguinte. Outro índice indica que existam, atuando no País, mais de 150 quadrilhas especializadas em fraudes eletrônicas. (JORNAL, 2010).

No dia 05 de Fevereiro de 2019, no “Dia da Internet Segura” a SaferNet Brasil divulgou que em 2018 recebeu e processou 133.732 denúncias anônimas de cibercrimes. O número é cerca de 110% maior do que o registrado em 2017. Os três crimes cibernéticos mais recebidos pela instituição no ano de 2018 foram: pornografia infantil - com 60.002 denúncias, conteúdos de apologia e incitação à violência e aos crimes contra a vida - com 27.716 registros - e, por fim, a violência e a discriminação contra mulheres - com 16.717 queixas. (SOARES, 2019).

2.2 Os crimes virtuais e a legislação vigente

2.2.1 A primeira lei contra os cibercrimes

No dia 24 de Fevereiro de 1999, foi apresentado na Câmara dos Deputados o Projeto de Lei (PL) 84/1999, de autoria do então deputado federal Luiz Piauhylino. Seu intuito principal era alterar o Decreto-Lei n. 2.848, de 07 de dezembro de 1940 (Código Penal), onde pela primeira vez, disporia sobre crimes cometidos no meio digital e suas penalidades. O projeto almejava se tornar a primeira lei brasileira que tratava de forma ampla e sistematizada dos cibercrimes.(CÂMARA, 1999).

No seu projeto inicial, eram criminalizados: a) acessar um sistema informatizado sem autorização; b) obter, transferir ou fornecer dados ou informações sem autorização; c) divulgar ou utilizar de maneira indevida informações e dados pessoais contidos em sistema informatizado; d) destruir, inutilizar ou deteriorar coisas alheias ou dados eletrônicos de terceiros; e) inserir ou difundir código malicioso em sistema informatizado; f) inserir ou difundir código malicioso seguido de dano; g) estelionato eletrônico; h) atentar contra a segurança de serviço de utilidade pública; i) interromper ou perturbar serviço telegráfico, telefônico, informático, telemático ou sistema informatizado; j) falsificar dados eletrônicos ou documentos públicos; k)

falsificar dados eletrônicos ou documentos particulares; l) discriminar raça ou cor por meio de rede de computadores.(LANDIM, 2012).

Em Novembro de 2003, a Comissão de Educação no Senado Federal aprovou o parecer com substitutivo do então senador Eduardo Azeredo ao Projeto de Lei do Senado (PLS) nº 76 de 2000, de autoria do então senador Renan Calheiros, apensado ao Projeto de Lei da Câmara (PLC) nº 89 de 2003, de autoria do então deputado Luiz Piauhylino e ao PLS nº 137 de 2000, do então senador Leomar Quintanilha, tipificando os seguintes tipos penais: a) o acesso indevido a meio eletrônico; b) a manipulação indevida de informação eletrônica; c) o dano eletrônico; d) a pornografia infantil; e) o atentado contra a segurança de serviço de utilidade pública; f) a interrupção ou perturbação de serviço telegráfico e telefônico; g) a falsificação de cartão de crédito; h) a falsificação de telefone celular; i) a divulgação de informações pessoais ou de empresas. Desde então o projeto ficou conhecido como Lei Azeredo. (CONSULTOR, 2006).

Antes do projeto de lei PL 84/1999 ser aprovado e se tornar, efetivamente, a Lei Azeredo (em 2003), haviam apenas duas leis que definiam de forma isolada tipos específicos de crimes digitais. A primeira delas sendo a Lei 9.983, de 14/07/2000, tipificando o crime de divulgação de segredo (art. 153, §1ºA), a qual prevê pena de detenção de um a quatro anos e multa para aquele que divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública - também versou sobre o peculato eletrônico. E a segunda sendo a Lei nº 10.764 de 12/11/2003, alterou a redação do artigo 241 do Estatuto da Criança e do Adolescente, ampliando a descrição do crime de pornografia infantil, para proibir a divulgação e publicação na rede de fotografias e imagens contendo cenas de sexo explícito envolvendo criança ou adolescente, com pena de reclusão de dois a seis anos, além de multa.

2.2.2 A origem da Lei 12.737/2012

Em 29 de novembro de 2011, o então deputado Paulo Teixeira redigiu e propôs o Projeto de Lei 2793/2011 dispondo sobre a tipificação criminal de delitos informáticos; propondo alterações ao Decreto-Lei nº 2.848, de 7 de

dezembro de 1940 - Código Penal. (CÂMARA, 2011). Em 2012, com o advento do caso da atriz Carolina Dieckmann houve mais mudanças no conteúdo e fez com que o projeto tramitasse em regime de urgência sendo aprovado em tempo recorde. Foi sancionado pela ex-presidente Dilma Rousseff no dia 30 de novembro de 2012 e entrou efetivamente em vigor no dia 02 de abril de 2013. (MPSP, 2013) Tornou-se então oficialmente a Lei Brasileira 12.737/2012 e ficou popularmente conhecido como Lei Carolina Dieckmann.

Sendo assim, a Lei Azeredo, supracitada, dos seus 23 artigos originais, sobraram apenas quatro: a) falsificação de dado eletrônico ou documento particular; b) favor a inimigos (traição); c) racismo; d) revisão da criação de estrutura policial para o combate a esses crimes. Uma vez que a Lei nº. 12.737/12 foi aprovada, a Lei Azeredo tornou-se obsoleta. Apesar de alguns argumentarem que a Lei Azeredo e a Lei Carolina Dieckmann apenas se complementam. (GHEDIN, 2012).

2.2.3 O caso Carolina Dieckmann

O caso Carolina Dieckmann acima citado decorreu no dia 04 de maio de 2012. Hackers divulgaram na internet 36 imagens que mostravam uma mulher muito parecida fisicamente com a atriz Carolina Dieckmann. As fotos, que mostravam seios e nus frontais, foram hospedadas em um site de compartilhamento fora do Brasil. Estas imagens rapidamente se disseminaram na internet, e o nome "Carolina Dieckmann" chegou aos assuntos mais comentados da rede social Twitter. No dia 07 de maio as autoridades foram procuradas para dar início às investigações. Carolina Dieckmann informou haver recebido ameaças de extorsão por e-mail e telefonemas desde o fim de março (2012) no valor de R$10.000,00 à época, para a não publicação do conteúdo, e justificou a não prestação de queixa previamente para evitar exposição.

Em 13 de maio os quatro hackers suspeitos já haviam sido descobertos e detidos. Em conversas que tinham entre si, através de bate papos pela internet, a quadrilha brincava dizendo: “O trem ficou sério, hein? Em uns dias ‘tá’ a PF (Polícia Federal) interrogando a gente. Hehehe” e demonstravam certeza na impunidade dizendo: “Vai dar nada, não.”

A suspeita inicial da atriz era de que as fotos haviam sido copiadas do seu computador portátil dois meses antes do ocorrido, quando ela o levou para um conserto. No entanto, o delegado do caso, Rodrigo de Souza Valle, esclareceu que foi enviado um e-mail falso como isca (spam), e após a vítima abri-lo liberou uma porta para a instalação do programa malicioso que permitiu aos hackers entrarem no computador da atriz e realizar o roubo dos arquivos - isso é conhecido como phishing (envio de mensagens de spam contendo links para sites falsos). O programa era simples, e a ação dos hackers consistiu meramente no salvamento de arquivos que apareciam na pasta de enviados do e-mail da atriz. O cônjuge da atriz confirmou que as fotos haviam sido enviadas para ele. Apesar de 36 imagens terem sido divulgadas ao público, após varredura no e-mail da atriz foi detectado que os invasores haviam furtado, ao todo, 60 arquivos. (G1, 2012).

2.2.4 A Lei Carolina Dieckmann (Lei 12.737/2012)

Após entrar em vigor, esta lei alterou o Código Penal, nos artigos 154-A a 154B. Os artigos se encontram dentro dos crimes contra a liberdade individual, seção referente aos crimes contra a inviolabilidade dos segredos profissionais.

A Lei Carolina Dieckmann vem tutelar o bem jurídico da liberdade individual, do direito ao sigilo pessoal e profissional, uma vez que o sigilo e privacidade são essenciais ao ser humano e à sociedade em si.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 1940).

No artigo acima vemos a tipificação principal, que é a invasão em si do dispositivo eletrônico e a acessória que é instalar qualquer tipo de vulnerabilidade (programa malicioso). Há de se observar atentamente a escrita da lei, especialmente onde diz “detenção”. Detenção é o tipo de penalidade que admite seu cumprimento no regime semiaberto (em caso de reincidência) ou diretamente no regime aberto (em caso de primeira condenação).

Levando em conta o art. 44, § 2º do Código Penal diz:

"A pena privativa de liberdade quando superior a um ano pode ser substituída por uma pena restritiva de direitos e multa ou por duas restritivas de direitos." Isto significa que se a pena privativa de liberdade for igual ou inferior a 1 (um) ano, o juiz pode substituir pela pena pecuniária. Existe ainda a possibilidade da pena privativa de liberdade ser substituída por pena alternativa, como a restritiva de direitos, no entanto, para que isso ocorra o agente deve ser enquadrado nos quesitos do art. 44, I, II, III, do Código Penal, cumulativamente.

No que diz respeito a ação penal para os casos temos o descrito no Art. 154-B, que diz:

> Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (BRASIL, 1940).

Ou seja, os crimes definidos no artigo 154-A deverão ser lidados mediante ação penal de iniciativa pública condicionada à representação do ofendido ou de seus sucessores (artigo 100, parágrafo quarto, do Código Penal). Quer dizer, mesmo ocorrendo o ilícito em questão, o legislador outorgou para a vítima o direito de procedibilidade, observando-se a legitimidade para tanto e a fluência do prazo decadencial que pode vir a causar a extinção da punibilidade.

No crime em questão, não existindo motivo para aumento de pena, a pena máxima não é superior a dois anos, constituindo assim infração de menor potencial ofensivo, e sendo assim, existe a possibilidade de conciliação e a transação penal (Lei 9.099/95, arts. 61, 72 e 76).

Já em casos com possíveis aumento de pena, e levando em conta a pena mínima cominada não restar superior a um ano, o crime pertence ao rol das infrações penais de médio potencial ofensivo, sendo possível a suspensão condicional do processo, se presentes os demais requisitos legais (Lei 9.099/95, art. 89).

Existe ainda a possibilidade do agravamento da pena, em decorrência da maior reprovabilidade do ato delitivo, estando elas dispostas da seguinte maneira no artigo Art. 154 do Código Penal:

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
>
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940).

2.2.5 As críticas e problemas com a Lei 12.737/2012

No entanto, a lei 12.737/2012 não agrada a todos. A professora de Direito Digital do curso de pós-graduação em Marketing Digital da Impacta, Flávia Penido, escreveu um artigo para o Canal Tech explicitando pontos que criaram preocupação e/ou divergência entre os especialistas.

A palavra "invasão" causa o primeiro problema. Seria considerada a violação e invasão quando o dispositivo não contiver senha, estiver desbloqueado ou não possuir antivírus? Outro ponto relevante com referência ao artigo 154-A, seria a sua segunda parte: “com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”. Quando é colocado o verbo "obter" abre uma discussão no sentido de que haveria a infração apenas caso o invasor olhasse arquivos e dados, mas não os copiasse/obtivesse? (PENIDO, 20--).

2.3 Marco Civil da Internet

2.3.1 A concepção do Marco Civil

No dia 22 de Maio de 2007, o professor Ronaldo Lemos, que na época era coordenador do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (FGV) do Rio de Janeiro e representante da licença Creative Commons no Brasil, escreveu um artigo especial para a coluna do provedor de internet Universo on Line (UOL).

No artigo, ele criticava duramente o projeto de lei de crimes virtuais do senador Eduardo Azeredo (Lei Azeredo). A crítica caía no fato de que o primeiro marco regulatório da internet brasileira seria criminal. Para Ronaldo Lemos, seria necessário que primeiramente existisse/ fosse criado um marco regulatório civil, definindo claramente as regras e responsabilidades com relação a usuários, empresas e demais instituições acessando a rede, para a partir daí, se definirem as regras criminais.

O professor defendia que as regras penais deveriam ser criadas a partir da experiência com as regras civis. Além de acreditar que o projeto utilizava conceitos vagos e muito amplos causando incertezas/ dúvidas ao projeto. (LEMOS, 2010).

Após sua crítica ser publicada, ela inspirou e concebeu o projeto de Lei n° 12.965/2014, conhecido como o Marco Civil da Internet, o qual previa princípios, garantias, direitos e deveres para o uso da internet.

Houve uma primeira e depois uma segunda etapa de debates públicos, tendo por objetivo discutir o uso da internet no Brasil, bem como os direitos e deveres daqueles que, de alguma forma, com ela se relacionavam, seja no papel de provedor, seja no de consumidor ou no de fiscalizador - estes debates se encerraram em 30 de maio de 2010. O desenvolvimento do Marco Civil contou com a participação do povo, que podia comentar os artigos nele incluídos e opinar por meio das audiências públicas ou portais na internet relacionados ao projeto (como o e-Democracia e o e-Cidadania), o Marco Civil foi descrito como "A Constituição da Internet".

Quando chegou em 2012 na Câmara dos Deputados, a votação do projeto não ocorreu por diversos motivos, tendo sido adiado por 29 vezes. Devido a esses atrasos, apenas no dia 25 de março de 2014 o projeto de lei foi aprovado na Câmara dos

Deputados e enviado no dia seguinte ao Senado Federal. No dia 26 de março de 2014, o projeto passou a tramitar pelo Senado. (MINISTÉRIO, 20--).

2.3.2 A necessidade da NET Mundial

No dia 5 de junho de 2013, o jornalista Glenn Greenwald publicou no “The Guardian” documentos vazados pelo analista de segurança de redes Edward Snowden, através da vigilância eletrônica global realizada pela Agência Americana de Segurança Nacional (NSA). (G1, 2014).

Em 8 de Setembro de 2013, o programa Fantástico da Rede Globo de Televisão teve acesso aos documentos vazados por Snowden a Greenwald, os quais revelavam que a vigilância abrangera a Petróleo Brasileiro S.A. (Petrobras) com intuito de beneficiar os americanos nas transações com o Brasil. Os documentos vazados mostravam ainda que a ex-presidente do Brasil, Dilma Rousseff, também havia sido espionada pela NSA. (G1, 2013).

Em 2013, durante a abertura da Assembleia Geral da ONU, a então presidente Dilma Rousseff, propôs sediar um evento sobre a governança da internet após às denúncias de espionagem em massa realizada pelos Estados Unidos.

O evento contou com vários comitês de especialistas, objetivando elaborar princípios de governança para a internet mundial. Estes princípios ficaram conhecidos como a NET Mundial.

Os principais comitês eram dois: o Comitê Multissetorial de Alto Nível, composto por representantes de 12 países (África do Sul, Alemanha, Argentina, Brasil, Coreia do Sul, Estados Unidos, França, Gana, Índia, Indonésia, Tunísia e Turquia), mais 12 membros da comunidade multissetorial internacional e também porta-vozes da União Internacional de Telecomunicações, do Departamento para Assuntos Econômicos e Sociais das Nações Unidas e representações da Comissão Europeia; e o segundo comitê, o Comitê Multissetorial Executivo que foi composto por 9 membros internacionais, membros das comunidades técnicas, civil e acadêmica, setor privado e do Departamento de Assuntos Econômicos e Sociais das Nações Unidas.

Havia também o Comitê de Logística e Organização e o Conselho de Assessores Governamentais. (NETMUNDIAL, 2014).

2.3.3 A aprovação e urgência da lei

Em 22 de abril de 2014, um dia antes do Brasil, mais precisamente da cidade de São Paulo, sediar o encontro multissetorial global sobre o futuro da governança da Internet (o já citado NET mundial), o projeto de lei foi aprovado no plenário do Senado.

E foi durante o evento supracitado, que a então presidente Dilma Rousseff, sancionou a lei aprovada no legislativo em 23 de abril de 2014. (LOURENÇO, 2014).

Para a escrita jurídica final desta lei, o Marco Civil da Internet (MCI), dois documentos foram essenciais: a Constituição Federal de 1988 e o conjunto de "Princípios para a governança e uso da internet" elaborado pelo Comitê Gestor da Internet no Brasil – CGI.br, o texto conta com trinta e dois artigos, divididos em cinco capítulos. Dentro destes capítulos, o Marco Civil buscou disciplinar toda a matéria existente sobre o uso da rede no território nacional a partir de princípios como: a neutralidade, a privacidade e a liberdade de expressão.

Os cinco capítulos se subdividem em:

Capítulo I: princípios a serem observados no uso da internet por todos os agentes envolvidos;

Capítulo II: direitos e garantias dos usuários;

Capítulo III: provisão de conexão e de aplicações de internet;

Capítulo IV: atuação do Poder Público;

Capítulo V: disposições finais.

2.3.4 Os principais pontos do Marco Civil da Internet

A Lei nº 12.965/14 ou Marco Civil da Internet diz respeito ao direito dos cidadãos à liberdade de expressão e de comunicação. O usuário da internet tem

garantia de que sua vida privada não será violada, a qualidade da conexão estará em linha com o contratado e que seus dados só serão repassados a terceiros segundo seu consentimento ou em casos judiciais - garantindo o direito à privacidade.

Além da privacidade, o MCI se propõe em cuidar da neutralidade. Não é permitido de acordo com a lei que, visando a um benefício econômico, criem-se barreiras para determinado tipo de conteúdo, sendo assim qualquer dado deve ser feito com a mesma qualidade e velocidade.

Adentrando ainda mais no quesito de privacidade os provedores de internet e de serviços somente serão obrigados a fornecer informações dos usuários se receberem ordem judicial - enquanto isso os registros de conexão, os dados devem ser armazenados por, pelo menos, um ano, enquanto os registros de acesso a aplicações por seis meses.

O projeto exime da responsabilidade as empresas que fornecem conexão deixam de ser responsáveis pelos conteúdos gerados por terceiros e não poderão retirá-los sem determinação judicial, com exceção de casos de nudez ou de atos sexuais de caráter privado.

Por último, a lei também instituiu diretrizes para a atuação do Governo, dentre as quais a criação de “mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica” e o dever de estimular a expansão e o uso da rede, com a finalidade de “reduzir as desigualdades” e “fomentar a produção e circulação de conteúdo nacional”. (MINISTÉRIO, 20--).

2.3.5 As críticas à Lei nº 12.965/14 / Marco Civil da Internet

Uma vez que, como toda lei e projeto que passa por muitas mudanças, o Marco Civil tentou se tornar uma referência justa e confiável para a população no que se trata de crimes virtuais. No entanto, não são todos que acreditam que a solução foi tão eficaz e acreditam que ainda há um grande caminho a se trilhar para que estejamos realmente protegidos dos crimes na internet.

O autor Otavio Luiz Rodrigues (2014) destacou que

> diversos dos artigos da Lei 12.965, de 23 de abril de 2014, [...] reproduzem conteúdos jurídicos constitucionais e não lhes emprestam a necessária — ou a adequada — conformação, o que seria de se esperar quando o legislador exercer suas prerrogativas.

Outra crítica seria a já mencionada isenção de responsabilidade dos provedores de internet pelos danos decorrentes de conteúdos publicados por seus usuários, disposta no artigo 18 da lei, o que gera, certamente, maior ônus às vítimas.

Outro problema da lei, é o requisito estabelecido para a antecipação da tutela pretendida de que seja observado o interesse coletivo sobre o conteúdo. Ou seja, se a informação for socialmente relevante, dever-se-á priorizar a coletividade em detrimento do direito à intimidade. (MINISTÉRIO, 20--).

2.4 Delegacias de crimes digitais

2.4.1 Os primórdios da guerra contra os crimes cibernéticos

Em 2003, para responder e combater as fraudes eletrônicas (como a clonagem de cartões de crédito/débito), a venda de medicamentos na internet, os crimes de "alta tecnologia" e a pornografia infantil foi criado um novo setor dentro da Polícia Federal do Brasil chamada de Serviço de Repressão a Crimes Cibernéticos (SRCC).

Este setor ficava sob o comando da Diretoria de Investigação e Combate ao Crime Organizado (DICOR) e executou operações como: a “COURRIEU” (a qual objetivou desarticular uma quadrilha responsável pelo desvio de cartões bancários), a “IB2K” (que objetivou desarticular uma organização criminosa voltada ao furto de valores de contas de clientes via internet), a “TENTÁCULOS III” (que objetivou desarticular uma organização criminosa especializada em fraude com retenção de cartões bancários nos Estados de São Paulo e Minas Gerais), a “SHEIK” (responsável por prender o maior fraudador Internet Banking da Caixa Econômica Federal - CEF) e a “Darkode” (projeto de cooperação internacional da área cibernética, onde o Departamento de Polícia Federal brasileiro agiu em conjunto com o Federal Bureau of Investigation **(**FBI) e a European Union Agency for Law Enforcement Cooperation

(Europol) contra uma quadrilha de 62 hackers que atuavam em mais de dezoito países). (WIKIPEDIA, 2016).

Em 20 de Dezembro de 2005 foi criada a SaferNet Brasil, uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial - com foco na promoção e defesa dos Direitos Humanos na internet no Brasil. Na época, o país ainda carecia de políticas e ações concretas de enfrentamento do cibercrime e assim a SaferNet Brasil se consolidou como entidade referência nacional no enfrentamento aos crimes e violações aos Direitos Humanos na internet cooperando com diversas instituições governamentais, como por exemplo, o Ministério Público Federal. (SAFERNET, 2005).

Hoje a SaferNet Brasil oferece um espaço para denúncias de crimes contra os Direitos Humanos cuja ação penal é pública e incondicionada à representação (como Pornografia Infantil, Racismo, Homofobia, Xenofobia, Apologia e incitação a crimes contra a vida e Neo Nazismo), também oferece uma linha de ajuda (helpline) para quem procura ajuda ou orientação em casos de crime no ambiente virtual e também produz dados públicos sobre as denúncias recebidas com intuito de conscientizar e divulgar a amplitude e gravidade dos crimes cometidos no âmbito digital.

2.4.2 As delegacias especializadas

Atualmente, as pessoas que se encontrarem vítimas de crimes virtuais podem contar com atendimento de delegacias especializadas. Elas existem em apenas algumas cidades e regiões. Aqueles que moram em locais sem a delegacia especializada podem buscar a delegacia mais próxima de sua residência.

Os Estados/cidades que contam com essa ajuda especializada são:

Bahia/Salvador - Grupo Especializado de Repressão aos Crimes por Meios Eletrônicos (no entanto, eles não registram boletim de ocorrência);

Espírito Santo/Vitória - Delegacia de Repressão a Crimes Eletrônicos;

Maranhão/São Luiz - Departamento de Combate aos Crimes Tecnológicos;

Mato Grosso/Cuiabá - Gerência Especializada de Crime de Alta Tecnologia (GECAT);

Minas Gerais/Belo Horizonte - Delegacia Especializada de Investigações de Crimes Cibernéticos (DEICC);

Pará/Belém - Divisão de Prevenção e Repressão a Crimes Tecnológicos (DRCT);

Paraná/Curitiba - Núcleo de Combate aos Cibercrimes (NUCIBER);

Pernambuco/Recife - Delegacia de Polícia de Repressão aos Crimes Cibernéticos;

Piauí/Teresina - Delegacia Especializada de Repressão aos Crimes de Alta Tecnologia (DERCAT);

Rio Grande do Sul/Porto Alegre - Delegacia de Repressão aos Crimes Informáticos (DRCI) – Departamento Estadual de Investigações Criminais (DEIC);

São Paulo/São Paulo (1) - 4ª Delegacia de Delitos Cometidos por Meios Eletrônicos (no entanto, atende apenas demandas relacionadas a fraudes financeiras por meios eletrônicos);

São Paulo/São Paulo (2) - Departamento de Homicídios e de Proteção à Pessoa (no entanto, atende apenas crimes contra a dignidade sexual de vulneráveis);

Sergipe/Aracaju - Delegacia de Repressão a Crimes Cibernéticos (DRCC);

Rio de Janeiro/Rio de Janeiro - Delegacia de Repressão aos Crimes de Informática (DRCI);

Tocantins/Palmas - Divisão de Repressão a Crimes Cibernéticos (DRCC);

Distrito Federal/Brasília - Delegacia Especial de Repressão ao Crime Cibernético (DRCC). (SAFERNET, 20--).

2.4.3 Crítica à terminologia “delegacias especializadas”

Quando falamos que uma delegacia é especializada o cidadão comum entende que é um local com melhor estrutura tecnológica e profissional, com capacidade para atender qualquer demanda advinda de problemas no ambiente digital.

No entanto, a maior diferença entre uma delegacia especializada e uma "comum" é a preparação dos profissionais. Se espera de um profissional trabalhando em uma delegacia especializada que tenha mais familiaridade com a internet e as situações que podem decorrer da mesma, em uma delegacia digital se espera não ter de explicar o funcionamento, por exemplo, de uma rede social e termos específicos das mesmas.

Outra realidade que vemos é que a grande dificuldade da delegacia digital (ou de qualquer outra) quando se trata de crimes virtuais é o desfalque na infraestrutura para a investigação da atividade ilícita na internet. O que causa uma demora crescente e a sensação de impunidade e burocracia.

Vale também apontar que mesmo existindo delegacias ditas "especializadas", elas se concentram apenas nas capitais dos Estados e em alguns Estados elas ainda restringem o tipo de crimes que elas recebem - tornando assim, cada vez mais difícil receber as denúncias da população.

2.4.4 A competência da polícia em casos digitais

Primeiramente, se faz de suma importância entender os três tipos de ação penais existentes e como elas se aplicam nos crimes digitais mais comuns.

O primeiro tipo de ação penal é a privada que ocorre quando a lei determina exclusivamente à vítima a legitimidade para a propositura da ação penal. O que quer dizer que a existência da ação criminal diz respeito tão somente à pessoa da vítima. Entre os crimes de ação penal privada que demandam o comparecimento a uma delegacia de polícia ou juizado especial criminal estão: os crimes contra a honra como a injúria, a calúnia e a difamação.

O segundo tipo de ação penal é a pública incondicionada que ocorre quando somente o representante do Estado ou o Ministério Público, podem intentar a ação penal sem depender da manifestação de vontade de quem quer que seja. Para prosseguir com a ação basta haver indícios suficientes de autoria e da materialidade

do(s) crime(s). São exemplos dos crimes que incorrem em uma ação penal pública incondicionada: os crimes contra os Direitos Humanos, objetos de denúncias anônimas, como o racismo e homofobia.

O terceiro tipo é a ação penal pública condicionada à representação quando o Ministério Público possui legitimidade para intentar a ação penal somente após a permissão expressa da vítima. Tal previsão legal existe para proteger a imagem e a vítima pois, em determinados casos, poderá existir demasiada exposição, como nos casos de crime com ameaça e corrupção de menores.

Quando falamos da competência da polícia nesses casos, estamos falando da investigação dos casos de crimes virtuais, realizando a instalação da investigação policial da ocorrência buscando verificar a autoria e a materialidade dos fatos contidos no inquérito e simultaneamente isso se espera a manufatura e/ou verificação das provas. Existe uma diferença fundamental entre a criação de provas nos crimes comuns e nos crimes praticados no âmbito da internet. Quando falamos da prática do delito pela internet a apuração inicial busca conservar na íntegra todo o material que possa comprovar o delito, uma vez que todo comportamento criminoso na internet deixa algum resquício. Sendo assim, cabe a polícia a procura dos vestígios deixados para buscar o real autor do crime - a intenção primária é a busca e a identificação, inicialmente e principalmente, através do endereço do Internet Protocol (IP) que é utilizado pelo criminoso durante a ocorrência. Muitas vezes a forma de obtenção deste IP é através dos próprios servidores. Pela Lei 12.965/2014, do Marco Civil da Internet, os provedores de aplicações (Facebook, Twitter, Instagram, WhatsApp, etc.) tem incumbência de preservar os registros de acesso a aplicações por apenas 6 (seis) meses. Já os provedores de acesso à Internet (Vivo, NET, GVT, TIM, Oi, Claro, etc) guardarão os registros de conexão por 1 (um) ano.

Em relação às provas, provas de crimes digitais muitas vezes são prints de telas, fotos, sites e em todos os casos são muito voláteis e faltam com a fé pública, criando a necessidade da ata notarial. A ata notarial é uma ferramenta de extrema importância pois agiliza o processo, pulando uma fase de perícia e análise técnica computacional para comprovar a existência do alegado.

Sendo assim, Teixeira (2012) nos presenteia com um passo a passo, da fase técnica da investigação de um crime virtual:

Análise das informações narradas pela vítima e compreensão do fato ocorrido na internet;

Orientações à vítima com o intuito de preservar o material comprobatório do delito e sua proteção virtual;

Coleta inicial de provas em ambiente virtual;

Formalização do fato criminoso por intermédio de um registro ou boletim de ocorrência, com a consequente instauração do feito;

Investigação inicial referente aos dados disponíveis na rede mundial de computadores sobre prováveis autores, origem de e-mails, registro e hospedagem de domínios;

Formalização de relatório ou certidão das provas coletadas e apuração preliminar;

Representação perante o Poder Judiciário para expedição da autorização judicial para quebra de dados, conexão ou acesso. Também poderão ser solicitados os dados cadastrais para os provedores de conteúdo;

Análise das informações prestadas pelos provedores de conexão e/ou provedores de conteúdo.

2.4.5 O que a vítima pode e deve fazer?

A SaferNet nos dá uma cartilha detalhada das ações que podem e devem ser tomadas pelas vítimas.

O primeiro passo é preservar todas as evidências. A forma mais segura para guardar as provas é a ata notarial supracitada, que "imortaliza" e valida com fé pública trazendo a garantia de que as evidências existiram e não foram alteradas pela vítima. Outra solução viável, mas menos segura e mais lenta, é imprimir e salvar o conteúdo ofensivo em sua totalidade (incluindo os cabeçalhos das mensagens e o máximo de dados possíveis) e preservá-lo em algum tipo de mídia protegida contra alteração, como um CD-R ou DVD-R.

O segundo passo é procurar uma delegacia para o registro da ocorrência levando assim à instauração da investigação e perícia policial em torno do alegado pela vítima e possibilitando uma ação penal.

O terceiro passo é a solicitação da remoção do conteúdo ilegal e/ou ofensivo através do envio de uma Carta Registrada para o prestador do serviço de conteúdo na Internet. (SAFERNET, 20--).

3 PESQUISA

3.1 Métodos

Foi escolhida a pesquisa qualitativa por sua metodologia de caráter exploratório, e seu foco está no caráter subjetivo do objeto analisado, buscando compreender o comportamento dos indivíduos estudados, entendendo as suas particularidades, pensamentos e experiências individuais, entre outros aspectos. E para validar a teoria, é exatamente o tipo de resposta que a autora necessitava para entender a realidade da situação como um todo.

O objetivo desta pesquisa foi obter uma maior compreensão quanto ao cenário geral da população e seu relacionamento com crimes virtuais, buscando compreender as dificuldades do público em geral no âmbito jurídico, comparando com os dados disponibilizados pela SaferNET e assim, fornecer subsídios para mudanças do cenário atual e possibilitar/ motivar futuras pesquisas sobre o tema.

A pesquisa constou de um formulário padrão elaborado em três partes, totalizando dez perguntas entre objetivas e discursivas (Apêndice A). O formulário foi distribuído/ preenchido através da ferramenta do Google Forms pela internet. As respostas foram coletadas/ compiladas no período de 07/05/2020 a 20/05/2020.

A primeira parte do estudo consistiu de dados demográficos dos participantes e algumas informações essenciais para compreender o impacto real dos crimes virtuais (frequência).

A partir daí e abrangendo apenas os participantes que haviam sofrido algum tipo de crime virtual, a segunda parte da pesquisa visou compreender quais eram os crimes virtuais mais comuns e também se as pessoas que vivenciaram tal ilicitude procuraram ou não meios legais para obter justiça para o seu caso.

A terceira parte da pesquisa abrangeu apenas os participantes que não procuraram os meios legais. Consistiu de uma pergunta única visando entender o porquê das pessoas se comportarem dessa forma (não buscar os meios legais).

Os resultados foram ilustrados sob a forma de gráficos.

3.2 Resultados

Durante o período de disponibilidade 510 formulários foram preenchidos.

A idade média dos participantes foi de 25 anos, com idade mínima de 13 e máxima de 74 anos.

Dados mais detalhados quanto à faixa etária e ao gênero dos participantes podem ser observados nas figuras 1 e 2.

Figura 1 – Faixa etária e gênero dos participantes (n=510 indivíduos)

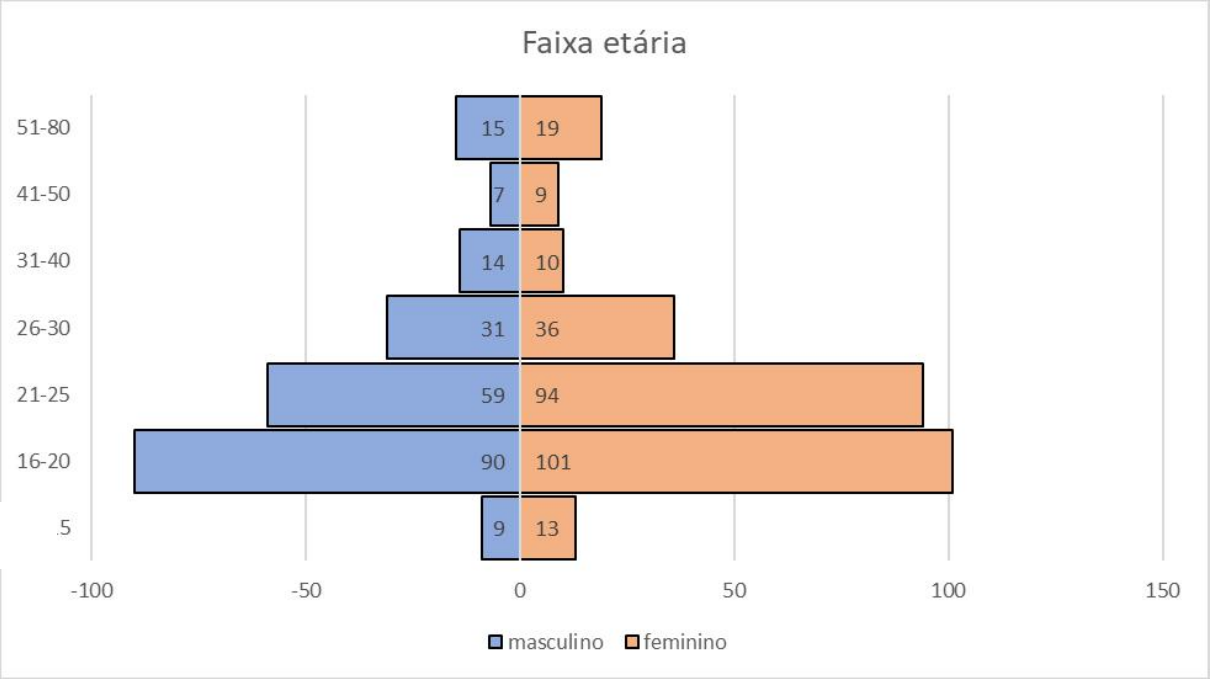
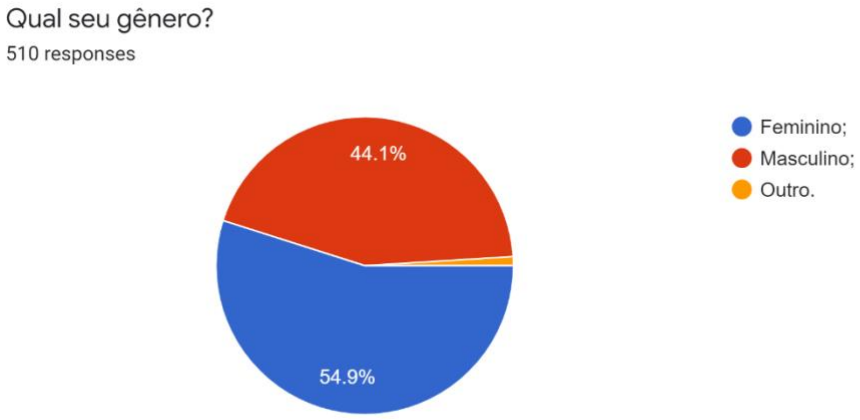


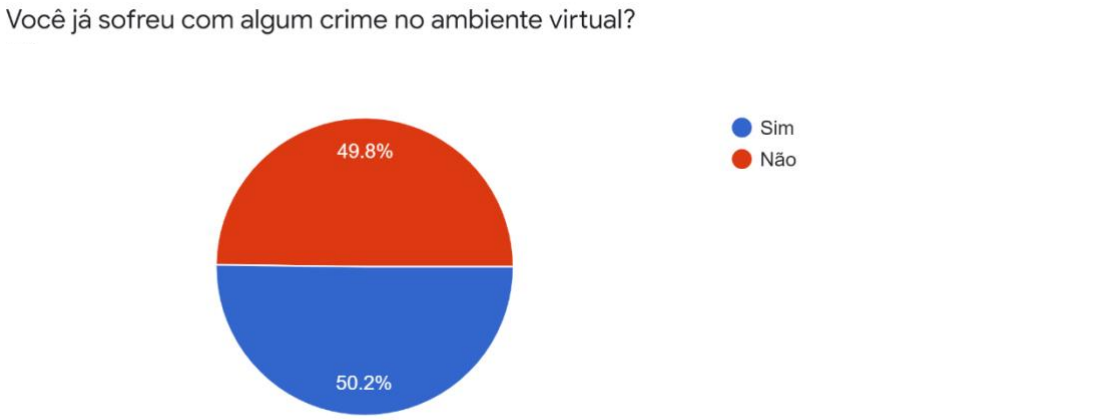
Figura 2 – Gênero dos participantes (n=510 indivíduos)



A figura 3 mostra o acesso dos participantes da pesquisa à internet.

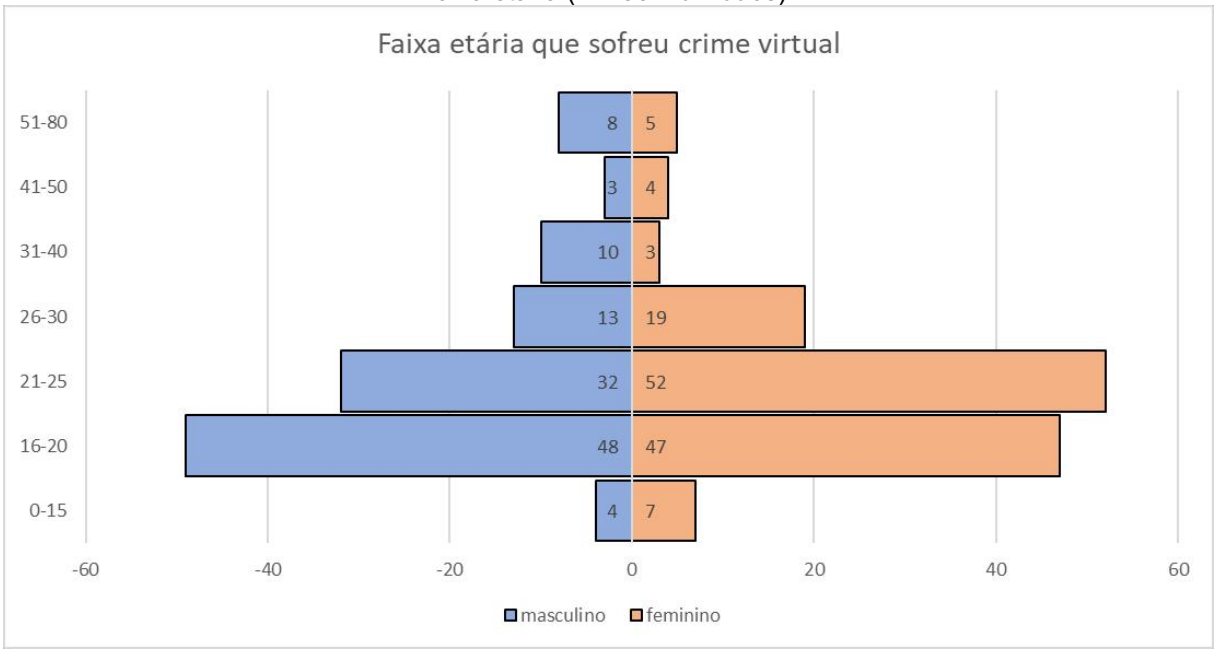
Figura 3 – Participantes da pesquisa quanto ao acesso à internet (n=510 indivíduos)

Figura 4 – Participantes da pesquisa que sofreram algum tipo de crime virtual (n=510 indivíduos)



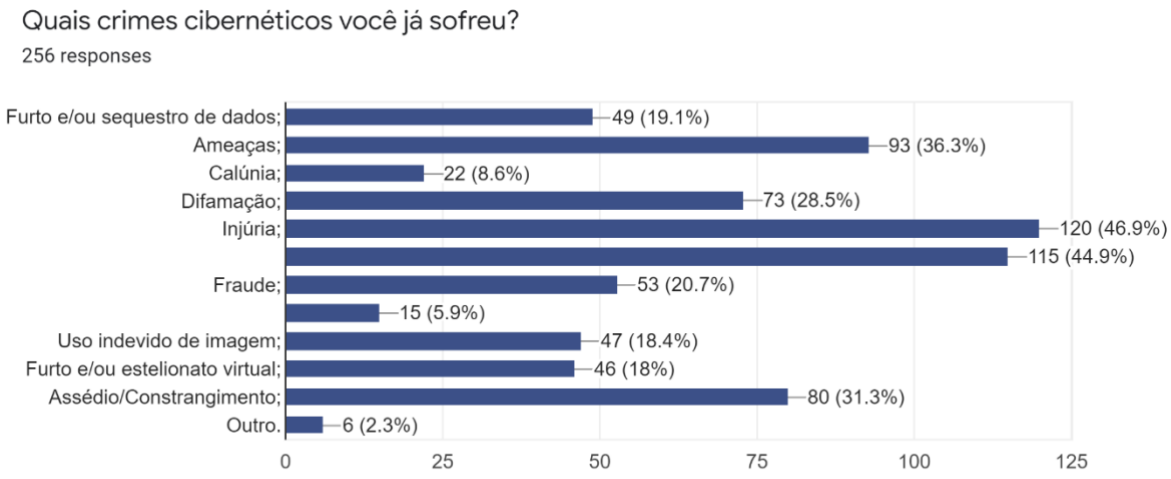
Na figura 4 podemos observar que a metade dos indivíduos que responderam a esta pesquisa sofreram algum tipo de crime virtual (256 indivíduos, 50,2%). A figura 5 detalha esta variável quanto ao gênero e faixa etária.

Figura 5 – Participantes da pesquisa que sofreram algum tipo de crime virtual quanto ao gênero e faixa etária (n=256 indivíduos)



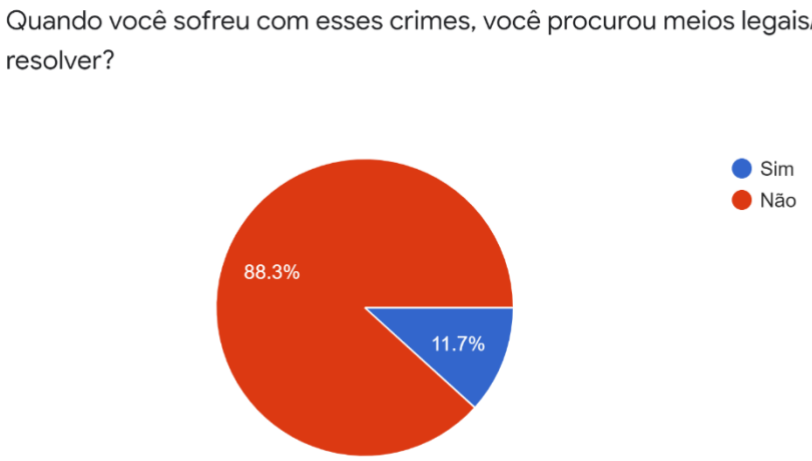
A figura 6 ilustra os crimes virtuais sofridos/ referidos pelos participantes do estudo.

Figura 6 – Crimes virtuais referidos pelos participantes (n=256 indivíduos)



Os crimes virtuais mais comuns foram: a injúria, os crimes de ódio (como o racismo e a homofobia), as ameaças, o assédio e a difamação; a maioria constituindo crimes contra a honra (Figura 6).

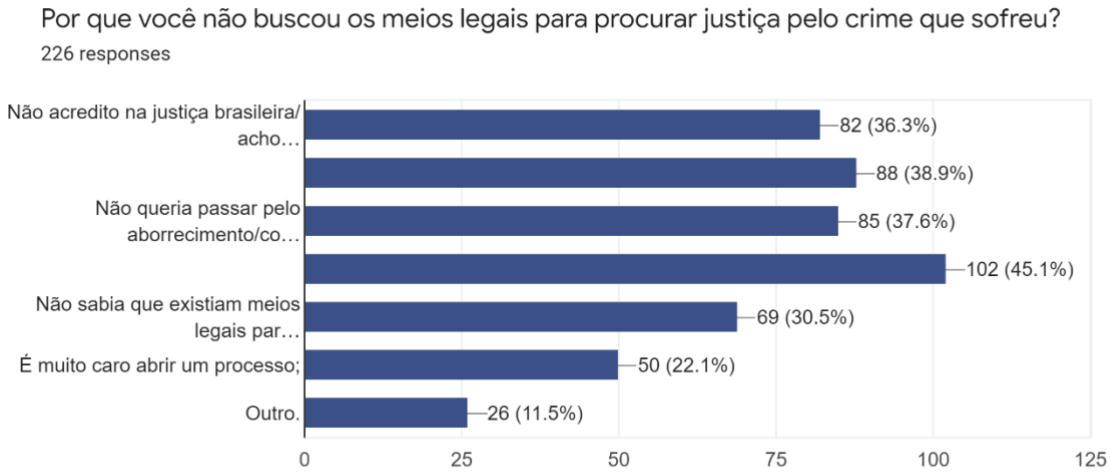
Figura 7 – Participantes que procuraram meios legais/ jurídicos (n=256 indivíduos)



Outro dado importante observado na figura 7 é que 88,3% dos participantes que sofreram crime virtual (226 de 256 indivíduos) não procuraram seus direitos e/ou suporte legal possível para a infração sofrida.

A figura 8 detalha o porquê/ motivos da não procura pelos meios legais.

Figura 8 – Motivo pelos quais os participantes não procuraram os meios legais (n=226 indivíduos)



Os motivos predominantes foram: não saber como agir para iniciar o procedimento jurídico (45,1%), achar um processo algo muito demorado e burocrático (38,9%) e não querer passar pelo aborrecimento (37,6%).

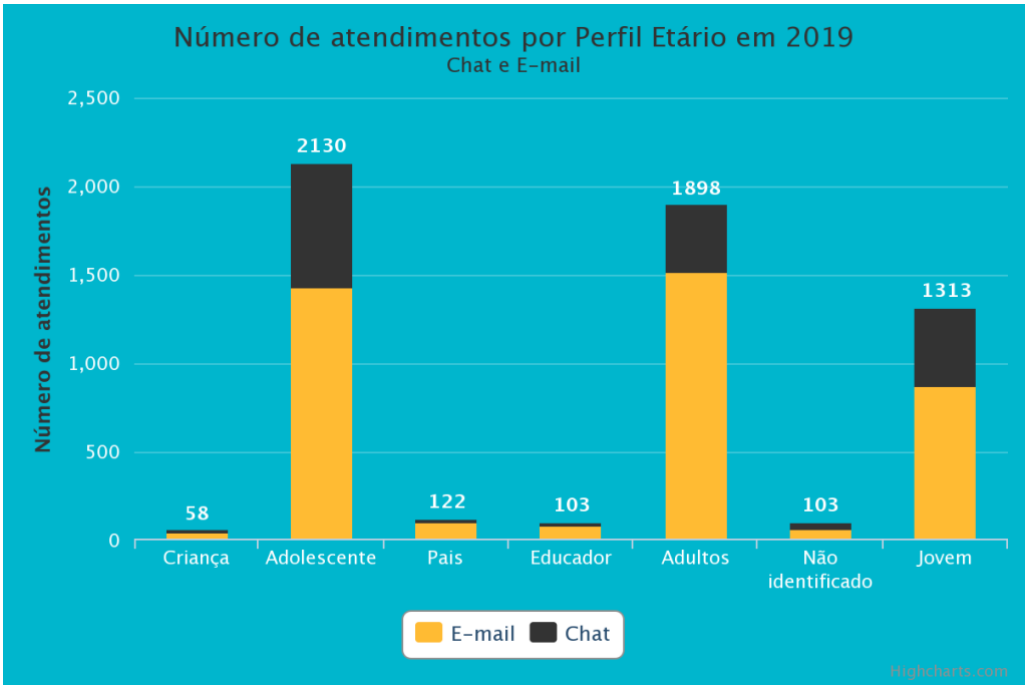
3.3 Discussão

Trata-se de um estudo pioneiro sobre o assunto.

Dados comparativos para uma discussão mais aprofundada sobre o tema são escassos restringindo-se aos indicadores da SaferNET que é o site especializado e confiável que também recebe denúncias.

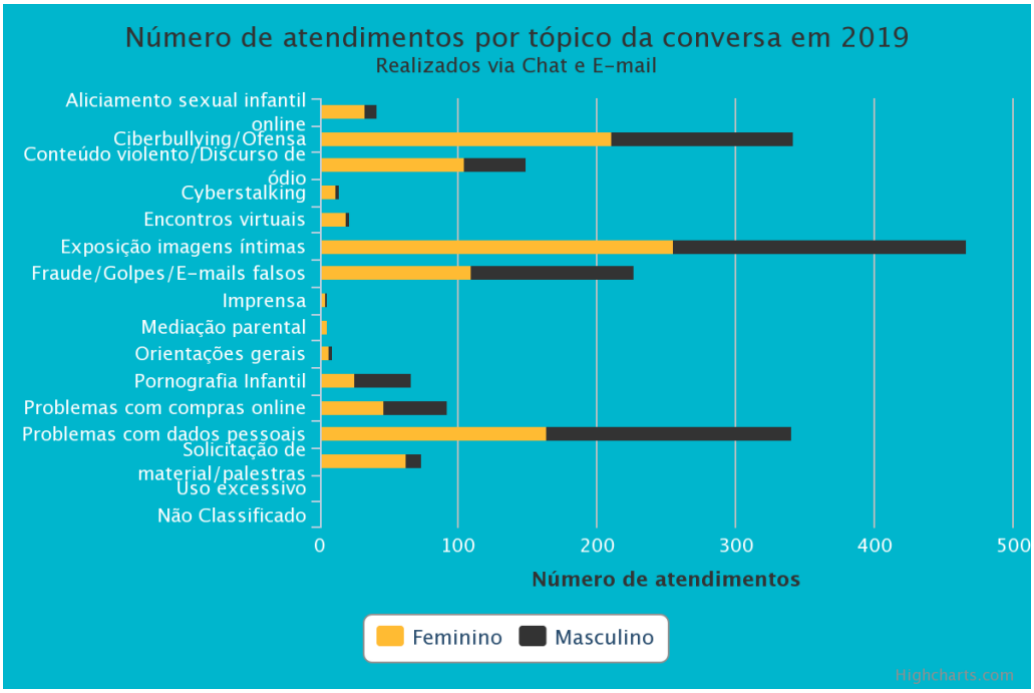
Abaixo representados os dados da Safernet (Figuras 9 e 10).

Figura 9 – Faixa etária e gênero dos indivíduos que fizeram uma denúncia através da SaferNET em 2019



Fonte: (DATASAFER, 2019)

Figura 10 – Crimes virtuais que as pessoas denunciaram na SaferNET em 2019



Fonte: (DATASAFER, 2019)

Comparando os dados obtidos nesta pesquisa com os dados acima obtidos pela SaferNET observam-se que os achados não são tão divergentes. A maioria das reclamações procedem de adolescentes e adultos jovens, com um leve predomínio do gênero feminino. Quanto aos crimes virtuais mais comuns, os resultados também são concordes com destaque para o cyberbullying e as ofensas.

As leves discrepâncias se dão pelas categorias de crimes adicionadas a pesquisa serem divergentes as existentes no SaferNET e também porquê, como dito no próprio site da SaferNET, a SaferNET “só pode encaminhar às autoridades competentes as denúncias de crimes contra os Direitos Humanos cuja ação penal seja pública e incondicionada à representação”. Sendo assim, o site só recebe na sua central de denúncias crimes como pornografia infantil, racismo, homofobia, entre outros.

Uma curiosidade é que durante essa fase da pesquisas muitos dos participantes demonstraram uma grande confusão em relação ao que era considerado ou não um crime virtual – sendo assim, é justo entender que falta informação para as massas sobre seu direito e também que os dados podem não ser tão precisos.

4 CONSIDERAÇÕES FINAIS

Este estudo permitiu trazer à luz as críticas à legislação vigente e compreendê-las.

Através deste estudo pudemos ver a criação histórica da internet, a inclusão digital da população e do mundo e decorrente disto a gênese do ambiente virtual. A partir daí, vimos esta realidade se expandir e tornar-se parte de nossas vidas, e com isso, houve a necessidade da modernização da sociedade, comunicação e também do nosso sistema judiciário.

Criamos um novo mundo e com ele novas tipificações criminais. Houve uma evolução clara das nossas leis para suprir a necessidade da população em se sentir segura e ver a justiça realmente ser feita de forma eficiente. Através da elaboração de leis e projetos como a Lei Azeredo, Marco Civil da Internet e Lei Carolina Dieckmann tivemos grandes avanços.

A pesquisa realizada neste estudo corroborou a vasta extensão quando pensamos na quantidade de crimes virtuais e seus danos e como eles impactam a vida das vítimas. Adolescentes e adultos jovens são a população mais atingida. Observamos que grande parte do problema é a falta de informação em vários âmbitos. Inclua-se: disseminar a informação do que é um crime virtual, de como produzir e preservar evidências, de que existem leis e meios para responsabilizar os culpados e/ou indenizar as vítimas, entre outros.

Concluindo, acreditamos que da mesma forma de se fazem necessárias as campanhas contra a violência mulher, violência doméstica, estupro, entre outras também se faz necessário uma campanha para conscientizar a população contra os crimes virtuais, para que a mesma procure a justiça e seus direitos e consequentemente desmistifique essa impressão de que a internet é um território sem lei em que não há solução para as vítimas e punição para criminosos.

REFERÊNCIAS

AGÊNCIA IBGE. **PNAD Contínua TIC 2017:** Internet chega a três em cada quatro domicílios do país .2018. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>. Acesso em: 11 jun. 2020.

ANATEL. **Norma 004/95.** Uso de meios da rede pública de telecomunicações para acesso à internet. Disponível em: <https://www.anatel.gov.br/hotsites/Direito_Telecomunicacoes/TextoIntegral/ANE/prt/minicom_19950531_148.pdf>. Acesso em: 11 jun. 2020.

ÂNGELO, Fernanda K. **Brasil lidera ranking mundial de hackers e crimes virtuais.** 2002. Disponível em: <https://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml>. Acesso em: 15 maio 2020.

ASSESPRO RS. **Ocorrências de Crimes Cibernéticos crescem 110% de 2017 para 2018.** 2019. Disponível em: <http://www.assespro-rs.org.br/ocorrencias-de-crimes-ciberneticos-crescem-110-de-2017-para-2018/>. Acesso em: 11 jun. 2020.

BRASIL ESCOLA. **Internet.** Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/internet.htm>. Acesso em: 15 ago. 2020.

BRASIL. Decreto-Lei n° 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União.** Rio de Janeiro, 31 dez. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 20 jul. 2020.

CÂMARA dos Deputados. **PL 84/1999.** Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A68FFA2837134B20490EB82BA93820E6.proposicoesWebExterno1?codteor=589359&filename=Tramitacao-PL+84/1999>. Acesso em: 18 jul. 2020.

CÂMARA dos Deputados. **PL 2793/2011.** Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>. Acesso em: 20 jul. 2020.

CIRIACO, Douglas. **A história da conexão.** 2009. Disponível em: <https://www.tecmundo.com.br/banda-larga/2543-a-historia-da-conexao.htm>. Acesso em: 18 jun. 2020.

COMPUTERWORLD. **6 a cada 10 brasileiros adultos são vítimas de cibercrimes em 2017.** 2018. Disponível em: <https://computerworld.com.br/2018/01/22/6-cada-10-brasileiros-adultos-sao-vitimas-de-cibercrimes-em-2017/>. Acesso em: 22 ago. 2020.

CONSULTOR Jurídico. **Veja parecer sobre a tipificação de crimes na internet.** 2006. Disponível em: <https://www.conjur.com.br/2006-jun-27/veja_parecer_tipificacao_crimes_internet>. Acesso em: 22 jun. 2020.

DATASAFER. **Indicadores Helpline.** Disponível em: <https://helpline.org.br/indicadores/>. Acesso em: 20 jul. 2020.

ESET. Welivesecurity. **70% dos usuários consideram que os dispositivos IoT não são seguros.** 2018. Disponível em: <https://www.welivesecurity.com/br/2018/03/20/70-dos-usuarios-consideram-que-os-dispositivos-iot-nao-sao-seguros/>. Acesso em: 22 jul. 2020.

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito & internet:** aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008, v. 2. p. 210.

G1. **Carolina Dickmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'.** 2012. Disponível em: <http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>. Acesso em: 20 jul. 2020.

G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA.** 2014. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 11 jun. 2020.

G1. **Petrobrás foi espionada pelos EUA, apontam documentos da NSA.** 2013. Disponível em: <http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html>. Acesso em: 15 fev. 2020.

GHEDIN, Rodrigo. **Lei Azeredo - ou o que restou dela - está prestes a ser aprovada.** 2012. Disponível em: <https://gizmodo.uol.com.br/reduzido-e-inofensivo-pl-azeredo-esta-prestes-a-virar-lei/>. Acesso em: 09 jun. 2020.

JORNAL do Comércio. **Estado ganha delegacia de crimes virtuais.** 2010. Disponível em: <https://www.jornaldocomercio.com/site/noticia.php?codn=32939>. Acesso em: 15 jun. 2020.

KLEINA, Nilton. **Como tudo começou: a história da internet no Brasil.** 2018. Disponível em: <https://www.tecmundo.com.br/mercado/129792-tudo-comecou-historia-internet-brasil-video.htm>. Acesso em: 11 jun. 2020.

LANDIM, Wikerson. **Conheça a Lei Azeredo, o SOPA brasileiro.** 2012. Disponível em: <https://www.tecmundo.com.br/ciencia/18357-conheca-a-lei-azeredo-o-sopa-brasileiro.htm>. Acesso em: 19 ago. 2020.

LEMOS, Ronaldo. **Ronaldo Lemos:** Proposta de novo texto da Lei Azeredo piora o original. 2010. Disponível em: <http://www1.folha.uol.com.br/multimidia/podcasts/819694-ronaldo-lemos-proposta-de-novo-texto-da-lei-azeredo-piora-o-original.shtml>. Acesso em: 11 ago. 2020.

LOURENÇO, Luana. **Dilma sanciona lei que reduz meta do superávit para 2014.** 2014. Disponivel em: <https://agenciabrasil.ebc.com.br/politica/noticia/2014-12/dilma-sanciona-lei-que-reduz-meta-do-superavit-para-2014>. Acesso em: 09 jun. 2020.

MINISTÉRIO Público Federal. 2ª Câmara de coordenação e revisão. **Crimes Cibernéticos.** Coletânea de Artigos. Brasília: MPF, 2018, vol. 3.. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos>. Acesso em: 11 jun. 2020.

MINISTÉRIO Público do Estado de São Paulo. **Marco Civil da Internet.** Perspectivas gerais e apontamentos críticos. Disponível em: <https://criminal.mppr.mp.br/arquivos/File/Cartilha_Marco_Civil_da_Internet.pdf>. Acesso em: 20 jul. 2020.

MPSP. Ministério Público do Estado de São Paulo. **Boletim n° 132, abril 2013.** Disponível em: <http://www.mpsp.mp.br/portal/page/portal/comunicacao/news_letter/Newsletter4_2013/Boletim%20n%C2%BA%20132%20abril2013.pdf>. Acesso em: 20 jul. 2020.

MONOGRAFIAS Brasil Escola. **Internet.** [20--]. Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/internet.htm>. Acesso em: 11 jun. 2020.

NAÇÕES Unidas Brasil. **Brasil é o quarto país com mais usuários de Internet do mundo, diz relatório da ONU.** 2017. Disponível em: <https://brasil.un.org/pt-br/77784-brasil-e-o-quarto-pais-com-mais-usuarios-de-internet-do-mundo-diz-relatorio-da-onu>. Acesso em: 20 jul. 2020.

NAÇÕES Unidas Brasil**. Brasil tem segunda maior taxa de homicídios da América do Sul, diz relatório da ONU.** 2019. Disponível em: <https://nacoesunidas.org/brasil-tem-segunda-maior-taxa-de-homicidios-da-america-do-sul-diz-relatorio-da-onu/>. Acesso em: 22 jul. 2020.

NETMUNDIAL. **NETmundial: o início de um processo.** 2014. Disponível em: <https://netmundial.br/pt/about/>. Acesso em: 28 maio 2020.

OLIVEIRA, Marcos de. **Primórdios da rede:** A história dos primeiros momentos da internet no Brasil. 2011. Disponível em: <https://revistapesquisa.fapesp.br/2011/02/18/prim%C3%B3rdios-da-rede_/>. Acesso em: 11 jun. 2020.

PENIDO, Flávia. **Os crimes previstos na Lei Dieckmann.** [20--]. Disponível em: <https://canaltech.com.br/juridico/Os-crimes-previstos-na-Lei-Dieckmann/>. Acesso em: 11 jun. 2020.

PRACIANO, Daniel. **Saiba como foram os primeiros passos do Brasil na internet antes da era comercial.** 2019. Disponível em: <http://blogs.diariodonordeste.com.br/narede/internet/saiba-como-foram-os-primeiros-passos-do-brasil-na-internet-antes-da-era-comercial/10669>. Acesso em: 22 ago. 2020.

RODRIGUES JUNIOR, Otavio Luiz. **Marco Civil e opção do legislador pelas liberdades comunicativas.** 2014. Disponível em: <https://www.conjur.com.br/2014-mai-14/direito-comparado-marco-civil-opcao-pelas-liberdades-comunicativas>. Acesso em: 20 jul. 2020.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal.** São Paulo: Memória Jurídica, 2004.

SAFERNET. **Calúnia/difamação Crimes da WEB.** [20--]. Disponível em <https://new.safernet.org.br/content/cal%C3%BAnia-difama%C3%A7%C3%A3o>. Acesso em: 11 jun. 2020.

SAFERNET. **Delegacias Cibercrimes.** [20--] Disponível em: <https://new.safernet.org.br/content/delegacias-cibercrimes>. Acesso em: 19 jan. 2020.

SAFERNET. **Institucional.** 2005. Disponível em: <https://new.safernet.org.br/content/institucional>. Acesso em: 15 maio 2020.

SOARES, Iarema. **Dia da Internet Segura 2019:** denúncias contra crimes na web aumentam quase 110%. 2019. Disponível em: <https://gauchazh.clicrbs.com.br/tecnologia/noticia/2019/02/dia-da-internet-segura-2019-denuncias-contra-crimes-na-web-aumentam-quase-110-cjrs1hmpm00xc01li6bvmmymp.html>. Acesso em: 15 mar. 2020.

STAIR, Ralph M. **Princípios de sistemas de informação:** uma abordagem gerencial. 2. ed. Rio de Janeiro: LTC, 2008.

STAROBINAS, Marcelo. **Brasil é líder mundial em crimes na internet.** 2002. Disponível em: <https://www1.folha.uol.com.br/fsp/mundo/ft2011200205.htm>. Acesso em: 19 ago. 2020.

SYNNEX Westcon. **Saiba quais são os 4 princípios da segurança da informação.** Disponivel em: <https://blogbrasil.westcon.com/saiba-quais-sao-os-4-principios-da-seguranca-da-informacao>. Acesso em: 23 ago. 2020.

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

WIKIPEDIA. **Serviço de Repressão a Crimes Cibernéticos.** 2016. Disponível em: <https://pt.wikipedia.org/wiki/Servi%C3%A7o_de_Repress%C3%A3o_a_Crimes_Cibern%C3%A9ticos>. Acesso em: 11 jun. 2020.