UNIVERSIDADE DO SUL DE SANTA CATARINA
ÂNIMA EDUCAÇÃO
CLEUMAR NERICHS DIAS

CRIMES CIBERNÉTICOS:
OS REFLEXOS NA SOCIEDADE CONTEMPORÂNEA

Braço do Norte

2023

CLEUMAR NERICHS DIAS

CRIMES CIBERNÉTICOS:
OS REFLEXOS NA SOCIEDADE CONTEMPORÂNEA

Monografia apresentada ao Curso de Direito da Universidade do Sul de Santa Catarina como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Professora Viviane Coelho de Sellos Knoerr, Dra.

Braço do Norte

2023

CLEUMAR NERICHS DIAS

CRIMES CIBERNÉTICOS SUBTÍTULO
OS REFLEXOS NA SOCIEDADE CONTEMPORÂNEA

Esta Monografia foi julgada adequada à obtenção do título de Bacharel em Direito e aprovada em sua forma final pelo Curso de Direito da Universidade do Sul de Santa Catarina.

Braço do Norte, 20 de novembro de 2023

Professora Viviane Coelho de Sellos Knoerr, Dra.
Universidade do Sul de Santa Catarina

_____

Professor Vilson Leonel, Dr./MSc./Bel./Esp.
Universidade do Sul de Santa Catarina

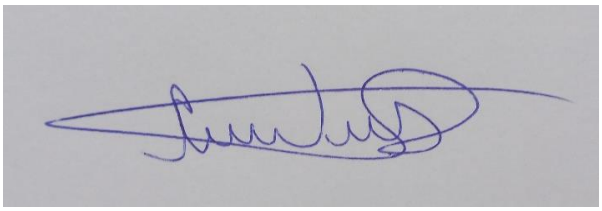
TERMO DE ISENÇÃO DE RESPONSABILIDADE

CRIMES CIBERNÉTICOS:
OS REFLEXOS NA SOCIEDADE CONTEMPORÂNEA

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico e referencial conferido ao presente trabalho, isentando a Universidade do Sul de Santa Catarina, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de todo e qualquer reflexo acerca deste Trabalho de Conclusão de Curso.

Estou ciente de que poderei responder administrativa, civil e criminalmente em caso de plágio comprovado do trabalho monográfico.

Braço do Norte, 20 de novembro de 2023.



CLEUMAR NERICHS DIAS

Dedico este trabalho a DEUS, que me deu forças para não desistir na caminhada, sem a presença Dele nada disso seria possível.

AGRADECIMENTOS

Agradeço primeiramente à Deus, que me deu graça e força para me manter firme no propósito dessa caminhada que era um sonho de infância agradeço a todos que foram apoio e suporte nessa árdua empreitada, por apoiarem minhas escolhas e me compreenderem nos momentos que precisei. Minha mãe que sempre foi uma guerreira, meu pai (*In memoriam*), que foi um homem de grandes princípios, os quais tenho como norte.

Agradeço a todos os meus professores que me guiaram por esta jornada, em especial minha professora orientadora Viviane Coelho de Sellos Knoerr, que acompanhou e auxiliou no desenvolvimento deste trabalho, capítulo por capítulo.

Agradeço também aos colegas de jornada com quem muitas vezes compartilhamos de momentos alegres e de grande proveito.

“Você nunca mudará sua vida até que você mude alguma coisa que você faz diariamente. As recompensas que você recebe na vida são determinadas pelo tipo de problema que você está disposto a resolver para os outros”. Mike Murdock

RESUMO

A chegada da rede mundial de internet trouxe consigo uma crescente digitalização de todas as áreas do comportamento humano, chegando à um nível de estar tão intrínseco à vida humana se tornando indissociável do cotidiano das pessoas na atualidade. Como o Direito é um reflexo das ações humanas, o Direito Brasileiro também sofreu, e continua sofrendo, o reflexo da digitalização da internet, o que acaba culminando em um novo ramo do Direito, o então denominado Direito Digital. Esta pesquisa tem como objetivo central gerar aclaramento, dos reflexos dos crimes cibernéticos na sociedade, mostrar e explicar as carências do ordenamento jurídico, e as mudanças no ordenamento jurídico em busca de uma maior eficiência da legislação em resposta ao avanço desses crimes gerados pela crescente utilização dos meios de comunicações digitais. A pesquisa será científica descritiva, bibliográfica, abordando os problemas gerados pela tecnologia na vida em sociedade.

Conclui-se ao final que o Direito Digital é um ramo complexo, exigindo muito daqueles que o encaram, fato pelo qual muitos profissionais se afastam desta área, especificamente aqueles que não buscam se familiarizarem com os termos técnicos da internet.

Palavras-chave: Direito. Direito Digital. Internet.

ABSTRACT

The arrival of the global internet network brought with it an increasing digitalization of all areas of human behavior, reaching a level that is so intrinsic to human life that it becomes inseparable from people's daily lives today. As Law is a reflection of human actions, Brazilian Law also suffered, and continues to suffer, the reflection of the digitalization of the internet, which ended up culminating in a new branch of Law, the so-called Digital Law. This research has as its central objective to generate clarification, the consequences of cybercrimes in society, show and explain the shortcomings of the legal system, and the changes in the legal system in search of greater efficiency of legislation in response to the advancement of these crimes generated by the increasing use of digital communications media. The research will be scientific, descriptive, bibliographic, addressing the problems generated by technology in life in society.

In the end, it is concluded that Digital Law is a complex field, demanding a lot from those who face it, a fact that is why many professionals stay away from this area, specifically those who do not seek to familiarize themselves with the technical terms of the internet.

Keywords: law, digital law, internet

Sumário

1 INTRODUÇÃO **10**
2 PRINCIPAIS ASPECTOS CONSTITUCIONAIS **13**
2.1 O DIREITO DE INFORMAÇÃO 13
2.2 OS PRINCÍPIOS CONSTITUCIONAIS 15
2.3 PRINCÍPIO DA RESERVA LEGAL 15
2.4 PRINCÍPIO DA ANTERIORIDADE 16
2.5 PRINCÍPIO DA TAXATIVIDADE 17
2.6 PRINCÍPIO DA TERRITORIALIDADE 17
3 O DIREITO A PRIVACIDADE DO CIDADÃO **19**
3.1 VIDA PRIVADA 19
3.2 – HONRA 21
3.3 – A IMAGEM DAS PESSOAS 22
4 A PROBLEMÁTICA DO ANONIMATO NOS CRIMES CIBERNÉTICOS **24**
4.1 – É POSSÍVEL IDENTIFICAR O AUTOR? 24
4.2 CRACKER E HACKER 27
5 OS REFLEXOS DAS REDES SOCIAIS NO PODER LEGISLATIVO **33**
5.1 DISSEMINAÇÃO DAS CHAMADAS FAKE NEWS 33
6 COMO A VITIMA PODE SE DEFENDER NA INTERNET **40**
6.1 ATITUDES PRÁTICAS QUE PODEM GERAR UMA MAIOR SEGURANÇA 41
7 CONCLUSÃO **44**
REFERÊNCIAS **48**

1 INTRODUÇÃO

Os tempos modernos trouxeram uma grande mudança em nossa sociedade, houve a criação de uma nova e moderna ferramenta que surgiu para trazer facilidades ao dia a dia das pessoas. A **World Wide Web** (WWW), a “Rede Mundial de Computadores”. A rede mundial de computadores, (internet) gerou consigo uma grande inovação, que transformou o cotidiano de toda a população mundial, e nossa nação não ficou de fora dessa grande inovação. As tecnologias estão em constante mutação que gera dia após dia avanços fenomenais. Os anos 2000 foram o marco para esse acontecimento que transformou o modo de ver a humanidade.

Grandes são os benefícios dessas mudanças tecnológicas. A tecnologia alargou horizontes, nos mostrando possibilidades inimagináveis num passado não muito remoto, se tornou uma peça essencial para meios de produção da sociedade. As notícias e informações chegam em todo o mundo de forma instantânea para a população.

Como todos os problemas que enfrentamos em sociedade são resultado de desvio de conduta do próprio ser humano, na utilização da tecnologia não é diferente. Pessoas em nosso meio de convívio começam a se utilizar da tecnologia para a prática de delitos, contra indivíduos em particular ou até mesmo contra a sociedade. Delitos esses cometidos de forma virtual, na tentativa ou imaginação de se manter no anonimato.

As constantes mudanças e significativos avanços no ramo de tecnologia, trouxeram de carona o surgimento de uma problemática de difícil combate, os crimes cibernéticos. Na atualidade um aparelho celular, um tablet ou um notebook, podem conter todas as informações relacionadas ao seu usuário, desde documentos, cartões de crédito, senhas de banco entre outras informações, que são alvos de criminosos.

Cabe ressaltar que na mesma velocidade que a tecnologia avança, também maior são as possibilidades de meios de fraude para conseguir informações de usuários.

Hoje a internet se popularizou tornando o acesso fácil as pessoas, o que também facilita a possibilidade de pratica de crimes cibernéticos, onde os criminosos se escondem no anonimato, de forma que se torna quase impossível rastreá-los, isso se deve a utilização de programas que conseguem ocultar o endereço de IP (Internet Protocol), o que os torna quase indetectáveis.

Outra problemática é a investigação desses delitos, que, na sua grande maioria, é prejudicada pelo fato de muitos crimes cibernéticos ainda não terem uma norma jurídica especifica os operadores do direito, tem o dever de aplicar princípio da reserva legal, dessa maneira são impedidos de aplicar o princípio da analogia para evitar ou punir esse tipo de crime.

Apesar de já existir normas no ordenamento jurídico brasileiro, que já tipificam alguns desses crimes, sabe-se que ainda não são suficientes para combater ou sanar todos os delitos cometidos de forma virtual. Ainda temos uma demanda de crimes, e, a cada dia, se tem mais notícias de novos e diferentes crimes que vão surgindo junto com a inovação tecnológica.

O ordenamento jurídico brasileiro possui hoje algumas leis que tipificam esses crimes cibernéticos.

A lei 12.735/2012 e a lei 12.737/2012, esta última conhecida como “Lei Carolina Dieckman”, lei esta que foi criada em resposta ao caso envolvendo a atriz, onde ela teve suas fotos pessoais vazadas na internet.

Lei 12.965/2014 sancionada em 2014, conhecida como Marco Civil da Internet, surgiu para regular os direitos e deveres dos usuários da rede.

Essa lei se tornou de extrema necessidade para proteger dados de internautas, para garantir o acesso a informações e conteúdos privados de sites e redes sociais do usuário, somente com autorização judicial. Também trouxe uniformidade de retirada de conteúdo das redes, sejam eles ofensivos, pornográficos ou violentos. A única exceção é a pornografia de vingança, que pode ser retirada por pedido direto da vítima ao site que hospeda conteúdo, para os demais casos é necessário ordem judicial e avaliação para serem retirados da rede.

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), criada para regular as atividades de coleta e tratamento de dados pessoais, alterando os artigos 7º e 16 do Marco Civil da Internet. De forma mais objetiva a LGPD busca proteger a captação, armazenamento e compartilhamento de dados pessoais coletados por sites e empresas online, outra investida para criar um ambiente digital mais seguro.

As leis existentes hoje ainda são insuficientes para regular infrações praticadas, se faz necessário a criação de mecanismos específicos para tornar o combate a esses crimes mais eficiente. É sabido que o ordenamento jurídico não acompanhou na mesma velocidade os avanços dos delitos cibernéticos, por esse motivo existem

brechas que permitem que essas ações passem impunes, sem que se tenha uma base legal em nosso ordenamento jurídico para responsabilizar e punir os criminosos.

Por esse motivo, este trabalho tem o propósito de expor a carência no ordenamento jurídico, mostrar e explicar os reflexos que os crimes cibernéticos causam na sociedade.

É perfeitamente normal e previsível que as leis positivadas não consigam prever todas as possibilidades da vida humana. Tanto as normas materiais quanto processuais estão sujeitas à insuficiência e ineficácia com o passar dos anos.

Essa evolução digital criou uma grande mudança na forma como as pessoas vivem, na forma de interagir, como compram, como procedem operações bancárias, como trabalham, entre outras; a chamada digitalização da vida humana, o que de um lado gerou muitas vantagens para os usuários da rede, de outro, também se abre um leque de possibilidades para novos tipos de ilícitos.

A digitalização da sociedade cria a demanda de uma nova forma de atuar frente aos ilícitos cometidos online.

2 PRINCIPAIS ASPECTOS CONSTITUCIONAIS

Vamos fazer uma análise nos principais aspectos constitucionais, que envolvem o direito de cada cidadão ter preservado sua intimidade e honra, como também o dever de não extrapolar os limites do direito de manifestação sem se esconder no anonimato. O cidadão deve conhecer seus direitos, porém não deve esquecer que tem obrigações.

2.1 O DIREITO DE INFORMAÇÃO

Como direito fundamental, o direito à informação, é frequentemente reconhecido em várias sociedades democráticas como um direito humano. É ele que estabelece que os indivíduos tenham o direito à informações e dados de fontes governamentais, instituições públicas ou privadas, de forma apropriada e justa. Deve haver um equilíbrio entre o direito à informação e o direito à privacidade. Existem leis de proteção de dados que regulamentam como informações de cunho pessoal devem ser tratadas e protegidas. O direito à informação tem um papel crucial na efetivação da democracia, na participação cívica e no acesso a recursos que enriquecem a vida humana. O seu exercício porém deve ser com equilíbrio perante outros direitos e considerações legais.

> A liberdade de expressão, por possibilitar a manifestação de pensamentos, opiniões, ideias e ideologias, exprime, com base na comunicação, uma verdade do próprio indivíduo. Nesse sentido, o exercício da liberdade de expressão leva, por um lado, a que outros indivíduos sejam influenciados por aquilo que está sendo comunicado, pois acaba por consolidar, constituir ou modificar sua percepção e, por outro lado, acaba por configurar a própria imagem social daquele que está emitindo a mensagem com base na opinião dos demais sobre aquilo que está sendo expressado ou comunicado, seja artística, científica, literariamente. Assim é que a liberdade de expressão permite o pleno desenvolvimento da personalidade humana por meio de uma irradiação, com base na comunicação, da expressão da identidade, da autonomia e da dignidade individual, mas encontra limites na razoabilidade da mensagem emitida – é pressuposto que o emissor tenha aqui discernimento para aferir o alcance positivo ou negativo do seu discurso – , no confronto de ideias em âmbito social e na defesa e proteção dos valores da ordem social livre e democrática. (Ana Paula Barbosa-Fohrmann, ,Allan Roch..., Direito digital: direito privado e internet, ano 2019, p.65)

O principal mecanismo que regula e serve como guia de toda ordem jurídica e política do Brasil é a Constituição Federal (CF) de 1998, exercendo ela tamanha importância, não poderia se eximir de tutelar a responsabilidade jurídica dessa nova

realidade social que surgiu com os avanços da rede mundial de internet, com o objetivo de proteger os novos bens jurídicos que nascem junto com a inovação dos meios de comunicação. Esse grande avanço nos mostra, nos dias atuais a importância da informação, que se tornou um bem jurídico de grande importância. Caracterizando um direito fundamental do homem, descrito e assegurado no artigo 5º da Constituição Federal.

> Art. 5 – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: VI – é livre a manifestação de pensamento, sendo vedado o anonimato; V – é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem; IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício ao exercício profissional; XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade de do Estado; LXXII – conceder-se-á habeas data: para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de caráter público; para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;" (Constituição Federal de 1988)

O conjunto de garantias listadas acima no Artigo 5º da Constituição Federal (1988), estão intimamente ligadas a liberdade digital ou informática. Que tem como função principal interligar as pessoas, levar as pessoas a terem acesso a informação e a transmissão dessas informações a outras pessoas. Ocorre que essa transmissão de informações não deve ser feita de forma desordenada. Neste contexto nasce a necessidade de intervenção do Estado, com o devido cuidado para não ferir o princípio da intervenção mínima. O papel do Estado está definido como uma atuação fiscalizatória, buscando prevenir e coibir práticas nocivas para a população, preservar a eficiência e veracidade de informações divulgadas.

Induzido pela necessidade de intervenção do estado o direito penal também tem o dever de gerar mecanismos que visam prevenir e punir de forma objetiva atos lesivos contra bens e valores jurídicos. Porém o crescimento rápido dessa tecnologia acaba gerando uma lacuna ainda não preenchida no ordenamento jurídico, o que nos deixa longe de ter a regulamentação adequada. Essa lacuna acaba por chancelar o mundo virtual como um espaço de propagação de informações falsas e disseminação de práticas lesivas a população.

2.2 OS PRINCÍPIOS CONSTITUCIONAIS

A base da Constituição Federal (1988), é o princípio de dignidade da pessoa humana, que, por sua vez, é o guia do Estado Democrático de Direito, os moldes da CF se aplicam aos outros ramos do direito, os princípios constitucionais do Código Penal destacam-se os princípios da legalidade (reserva legal), da anterioridade, taxatividade e da territorialidade. Na área cibernética os crimes não são efetivamente combatidos por falta de norma regulamentadora.

2.3 PRINCÍPIO DA RESERVA LEGAL

O princípio da reserva legal, no contexto do ordenamento jurídico brasileiro, é um princípio fundamental que estabelece limitações quanto a proibição ou punição, só podendo ocorrer por meios de leis criadas e pré-estabelecidas anteriormente ao fato ocorrido. Significa que a criação de sanções devem ser estabelecidas por leis especifica, antes que alguém possa ser legalmente responsabilizado por uma ação ou omissão. Esse princípio é uma garantia de que a autoridade estatal e seus agentes não podem agir de forma arbitrária, ou impor restrições ou penalidades ao cidadão.

O princípio da Reserva Legal é a pedra angular do Estado Democrático de Direito, em sociedades democráticas, é um contrapeso que traz equilíbrio à balança da arbitrariedade do governo. Uma restrição de direitos ou imposição de penalidades somente deve ser feita se estiver em pleno acordo com a legislação pré-estabelecida e precisa respeitar os procedimentos legais apropriados. A não observância do princípio da reserva legal pode resultar em sérias violações dos direitos civis e constitucionais.

O princípio da legalidade ou (reserva legal) em relação aos crimes cibernéticos, nos traz luz sobre a necessidade de uma norma penal específica para punir ou prevenir efetivamente tais condutas. O direito brasileiro proíbe fazer analogia para prejudicar o réu, por esse motivo, antes da lei 12.737/2012, não havia meios de combate legal as práticas lesivas cibernéticas.

> O artigo 5º, inciso II, da Constituição Federal dispõe que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". Reforçando essa garantia, o artigo 5º, XXXIX da carta magna (com idêntica redação do artigo 1º do CP) anuncia que "não há crime sem lei anterior que o defina nem pena sem prévia cominação legal".
> Trata-se de real limitação ao poder estatal de interferir na esfera de liberdades individuais, daí sua inclusão na Constituição entre os direitos e garantias fundamentais. (Manual de direito Penal, p.94)

A existência dessa lei possibilita punir os criminosos que tentam lesar a sociedade escondidos atrás de um suposto anonimato nas redes sociais.

2.4 PRINCÍPIO DA ANTERIORIDADE

O Princípio da Anterioridade, dentro do ordenamento jurídico brasileiro é uma importante garantia constitucional também conhecido como "princípio da irretroatividade" da lei penal mais gravosa. Esse princípio estabelece que não pode haver punição por condutas que não eram consideradas crimes no momento de sua ocorrência. A única maneira possível da lei retroagir é se a lei nova for mais benéfica para o réu. Simplificando, a lei penal mais gravosa não pode ser aplicada retroativamente.

O artigo 5º, inciso XXXIX da Constituição Federal e o Artigo 1º do Código Penal, elencam o chamado princípio da anterioridade, que nada mais é do que a previsão legal de não haver punição de crime sem lei anterior as suas práticas, esse é o motivo de ainda hoje termos muitos crimes cometidos no ambiente virtual, que não são punidos.

> Paulo Queiroz, citando Hobbes, esclarece que, se apenas supõe um fato considerado como transgressão à lei, o dano praticado antes de existir a lei que não o proibia não é uma pena, mas um ato de hostilidade, pois antes da lei não existe transgressão à lei. Por isso que a CF (e o CP) dispõe que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", de sorte que a formulação completa do princípio da legalidade compreende, necessariamente, a anterioridade da lei e sua irretroatividade. (Manual de direito Penal, p.94)

O Princípio da Anterioridade é a previsão da criação de tipos penais e a cominação de sanções, que exigem lei anterior que as preveja, sendo vedada a retroatividade maléfica da lei. Sendo possível atacar de forma eficiente e concreta os crimes somente após a criação de uma norma de previsão legal.

2.5 PRINCÍPIO DA TAXATIVIDADE

Esse princípio determina que a criação de uma norma regulamentadora penal deve ser exata, trazendo a tipificação da infração e o detalhamento das condutas praticadas. De acordo com o princípio da taxatividade a lei penal deve ser precisa e completa, não deixando margem para dúvida em relação à uma conduta incriminadora, as delimitações da norma devem trazer clareza, sendo vedado que os legisladores criem tipos penais que com conceitos vagos e imprecisos.

> "O princípio da taxatividade ou da determinação é dirigido mais diretamente à pessoa do legislador, exigindo dos tipos penais clareza, não devendo deixar margens a dúvidas, de modo a permitir à população em geral o pleno entendimento do tipo criado. " (Manual de direito Penal, p.94)

Uma norma clara sem imprecisão, não permitirá brechas que acabem gerando impunidade. O que no caso de crimes cibernéticos, o tipo penal deverá abranger não somente o ato em si, mas poderá abranger os meios utilizados para a prática desses crimes.

2.6 PRINCÍPIO DA TERRITORIALIDADE

Este princípio é talvez o maior desafio para a área penal, pelo simples fato de que os crimes cibernéticos não estão confinados a um território limitado como outros tipos penais. O desafio nos casos de crimes cibernéticos é que eles possuem um alcance a nível global. A internet é uma ferramenta que gera a conexão de pessoas espalhadas pelo mundo todo. O Artigo 5º do Código Penal brasileiro dispõe que aos crimes praticados em território brasileiro, é aplicada a lei brasileira. Mas também temos o princípio da extraterritorialidade. O artigo 7º do Código Penal Brasileiro traz a previsão de que crimes fora do Brasil, somente serão submetidas a legislação brasileira, caso houver, um acordo ou tratado de recíprocidade sobre esse tema.

> O art. 5° caput, do Código Penal determina que a aplicação da lei brasileira, sem prejuízo das convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. (Brasil, 1941)

Acentua se ainda o fato de que o direito penal não consegue acompanhar a evolução constante das novas tecnologias, o que acaba por facilitar as ocorrências de crimes virtuais. Já podemos comtemplar algumas mudanças expressas na constituição visando a prevenção e proteção dos direitos fundamentais. A sociedade tem a urgente necessidade de normas regulamentadoras que combatam com maior eficiência os crimes dessa nova realidade social.

3 O DIREITO A PRIVACIDADE DO CIDADÃO

O artigo 5º, inciso X, da Constituição Federal do Brasil, de 1988, traz explícito o direito a inviolabilidade da vida privada, da honra e da imagem do cidadão. Assegura também o direito à indenização por danos morais ou materiais resultantes dessa violação. É um direito constitucional garantido, e está diretamente ligado ao direito de personalidade da pessoa humana. Qualquer violação nesse sentido resulta em uma interferência nas relações pessoais e de intimidade. Podemos destacar nesse sentido o liame entre crime cibernético e esse direito expresso na Constituição Federal, já que o crime cibernético tem por objetivo central a violação desse direito.

Com o acesso fácil na atualidade, o mundo virtual se torna um campo fértil para o acontecimento desses crimes, somado a rapidez como se propaga essas informações. O Artigo 5º, inciso X, regulamenta o direito à privacidade do indivíduo.

> Art. 5 – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (Brasil, 1988)

Nossa Constituição Federal, tem o objetivo de resguardar e proteger os direitos do cidadão brasileiro ou estrangeiro que resida em solo brasileiro, e garantir um mínimo necessário de segurança jurídica em casos de violações desses direitos.

3.1 VIDA PRIVADA

A vida privada da pessoa humana se refere a uma área da vida de um indivíduo que não está sujeita à interferência indevida ou invasão por parte de entidades, governamentais, empresas, organizações ou outras pessoas, a menos que haja um motivo legalmente justificado. É um direito fundamental reconhecido em muitos sistemas legais e em documentos internacionais de direitos humanos. Não se pode confundir vida privada com a intimidade da pessoa. A vida privada diz respeito aos hábitos, enquanto que vida privada está ligada ao o que a pessoa possui e aos seus relacionamentos. A violação desses dois seguimentos é um desrespeito direto a norma constitucional.

Colocado como base o princípio constitucional, vamos aprofundar um pouco mais dentro desse assunto. Desde já frisando que os crimes cibernéticos causam

reflexos muitas vezes altamente danosos na vida das pessoas que tem o seu direito à privacidade violado.

A divulgação e exposição de informações, da intimidade do indivíduo, para a sociedade, geram, além de transtornos físicos, transtornos mentais para a vítima, que fica exposta ao ridículo e ao julgamento de outras pessoas. O objetivo central dos criminosos que atuam no ambiente dos crimes virtuais, além de visar denegrir a vida pessoal das vítimas, visam também a obtenção de recompensa financeira chantageando as vítimas ameaçando expor as informações da própria vítima. De acordo com Ferraz Junior, e Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*, p. 54:

> Cabe lembrar que no direito brasileiro, discute-se sobre os conceitos de vida privada e intimidade, especialmente na sua configuração como direitos da personalidade. Ambos os termos estão contidos no art. 5o, inciso X, da Constituição Federal: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Além disso, o direito à vida privada é reconhecido também no art. 21 do Código Civil: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". bDesse modo, alguns autores defendem a diferenciação entre os termos, não havendo, contudo, nenhuma uniformização doutrinaria ou legislativa. Assim, a intimidade poderia ser considerada no âmbito do exclusivo, referente ao que alguém reserva para si, sem qualquer tipo de repercussão social, nem sequer ao alcance de sua vida privada. Já a vida privada, por mais isolada que possa ser, sempre se caracteriza pelo viver entre outros (por exemplo, em família, no trabalho, no lazer em comum). *(FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, p. 54.)*
>
> "Para proteger a privacidade (gênero), permitindo ao indivíduo conduzir a própria vida de maneira que julgar mais conveniente, sem intromissão da curiosidade alheia, a Constituição assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem (espécies). A intensidade da proteção deve variar conforme a área da personalidade afetada. Quanto mais próxima das experiências definidoras da identidade do indivíduo, maior deve ser o peso conferido ao direito à privacidade. " (Curso de Direito Constitucional, p.347)

As tecnologias na atualidade proporcionam a condição de armazenamento de grande quantidade de informações. Ocorre que existem muitas brechas que permitem o acontecimento desses crimes. Nem todos os meios de armazenamento de informações são seguros, o que acaba acarretando um crescimento diário do número de crimes cibernéticos direcionados a vida privada e a intimidade do indivíduo.

3.2 – HONRA

Dentro do direito constitucional, a honra faz parte dos direitos fundamentais que protegem a dignidade e a reputação de um indivíduo. A honra é constantemente mencionada como parte do direito à imagem, privacidade e intimidade, e é garantida pela Constituição Federal do Brasil, no seu Artigo 5º, inciso X, que declara invioláveis os princípios fundamentais do direito à intimidade, vida privada, honra e imagem.

Essa proteção da honra no direito constitucional dá origem ao direito de as pessoas não serem difamadas, caluniadas ou expostas de maneira falsa ou prejudicial que afete sua reputação. Essa proteção é aplicável na esfera pública e privada.

Em síntese, o direito constitucional relacionado a honra, está ligado a preservação da dignidade, boa reputação e imagem das pessoas. Este direito fundamental tem como objetivo a garantia de que os indivíduos tenham tratamento respeitoso e não sejam alvos de acusações falsas e prejudiciais que agridam a integridade pessoal e social. Qualquer violação nesse sentido pode ensejar ações legais, como processos por difamação ou calúnia.

A honra da pessoa humana é um valor pessoal, assim como também, a dignidade. A honra possui dois aspectos, o social (objetivo) e o econômico que parte da doutrina de uma honra especial (profissional), que se baseia na confiança que a sociedade tem pelo seu exercício profissional. O aspecto social é a reputação que se tem perante a coletividade.

Nos casos de desconsideração da honra, seja ela atingida em qualquer dos dois aspectos já citados acima, parte-se do princípio que sua posição perante a comunidade foi prejudicada, desrespeitando os princípios constitucionais fundamentais e a norma penal. De acordo com o Curso de Direito Constitucional, p.347:

> A honra consiste na reputação do indivíduo perante ao meio social em que vive (honra objetiva) ou na estimação que possui desse próprio (honra subjetiva). A indenização por danos morais decorrentes de violação à honra deve ser assegurada para pessoas físicas e jurídicas (honra objetiva). (Curso de Direito Constitucional, p.347)

O ordenamento jurídico penal brasileiro traz a previsão de três espécies de crimes contra a honra, calúnia, difamação e injúria. O objetivo não é se aprofundar em

cada um deles especificamente, mas focar o olhar no contexto do cometimento de tais tipos penais no mundo virtual. A internet é um vasto campo onde os muitos crimes contra a honra são cometidos, nos dias atuais, alguns deles casos de total impunidade. Essa impunidade é derivada do anonimato, a maioria dos crimes são cometidos por criminosos que se utilizam de identidade falsa, perfil fake.

3.3 – A IMAGEM DAS PESSOAS

Imagem, é uma palavra derivada do *latim imago,* na definição de Antônio Chaves, é a representação de um objeto pelo desenho, pintura, escultura etc". Para Carlos Alberto Bittar, o direito à imagem se define como:

> O direito que a pessoa tem sobre a sua forma plástica e seus respectivos componentes distintos (rosto, olhos, perfil, busto) que a individualizam no seio da coletividade. Incide, pois, sobre a conformação física da pessoa, compreendendo esse direito um conjunto de caracteres que a identifica no seio social. Por outras palavras, é o vínculo que une a pessoa a sua expressão externa, tomada no conjunto, ou em partes significativas (como a boca, os olhos, as pernas, como individualizadoras da pessoa), (Carlos Alberto Bittar, 2015, 8ª Edição, p. 87)

O direito à imagem, é um dos aspectos da personalidade de um indivíduo, aspecto esse protegido legalmente. O direito à imagem está relacionado à capacidade de uma pessoa controlar a utilização de sua própria imagem, nome, voz e semelhança, para evitar a utilização não autorizada e prejudicial por terceiros.

Vale salientar que o direito à imagem está associado a proteção da privacidade e da dignidade da pessoa. A legislação regulamentadora do direito à imagem pode variar de um país para outro, mas normalmente há uma busca para equilibrar o direito à liberdade de expressão e o direito à privacidade, garantindo que a utilização da imagem de uma pessoa seja consentida ou limitada em certas circunstâncias para proteger seus interesses. A violação do direito à imagem de uma pessoa pode resultar em ações legais, como ações de indenização por danos morais.

O direito a imagem é autônomo, sua base é a personalidade física. Para uma melhor compreensão dessa definição em termos jurídicos, é necessário dividir essa "imagem" em duas: "imagem-retrato", que é a proteção da imagem do corpo físico da pessoa, e a "imagem-atributo" que podemos definir de forma mais simples como a

imagem que a pessoa tem de si próprio perante as pessoas de seu convívio social através de suas atitudes e atos. As duas são independentes e autônomas entres si. O direito de imagem pode ser disponível, podendo ser licenciada pela pessoa ou seus herdeiros.

A imagem da pessoa humana não pode, de forma alguma, ser cedida, vendida ou renunciada, sendo ela, intransmissível, irrenunciável e inalienável. A violação a imagem ocorre por qualquer meio que possa afetar o seu prestigio social, através da divulgação abusiva de sua imagem com o objetivo de obter lucro sem a devida autorização.

4 A PROBLEMÁTICA DO ANONIMATO NOS CRIMES CIBERNÉTICOS

A problemática do anonimato nos crimes cibernéticos é sem dúvida um grande e desafiador problema para a aplicação da lei e a proteção da sociedade no ambiente digital. O anonimato proporciona uma cobertura para criminosos online, tornando mais difícil identificar, localizar e processar aqueles que cometem delitos virtuais. O anonimato é um fator facilitador para a prática de crimes na internet, é senso comum, que a facilidade gerada pelo anonimato acaba por gerar insegurança na utilização dos meios digitais. É incomum deparar na doutrina alguém que defenda o anonimato. A nossa Carta Magna veta expressamente essa prática, traçando um paralelo entre o direito de liberdade e direito de expressão, o qual deve ter uma identificação de forma transparente de qualquer manifestação.

A constituição Federal de 1988 diz no em seu artigo 5º inciso IV, “é livre a manifestação do pensamento, sendo vedado o anonimato”, a vedação do anonimato se dá justamente com a identificação do indivíduo autor do ato.

A internet possui meios que impedem esse anonimato ser descoberto e, cada dia, se cria um ramo novo para o cometimento de crimes cibernéticos. Esse tipo de crime tem um potencial ofensivo ainda maior, pelo fato de que quando são cometidos são invasivos e silenciosos, muitas vezes, a vítima nem tem conhecimento que o crime aconteceu. Em alguns casos a exposição é tão degradante que chega a ser incalculável a dimensão de prejuízos causados a pessoa.

A constituição federal veda essa pratica numa tentativa de frear as práticas de manifestações infundadas que possam prejudicar à honra, à vida privada e à intimidade de uma pessoa ou sociedade, evitando opiniões errôneas motivadas e geradas por exposição fraudulenta. É um pouco difícil aceitar que a mesma rede utilizada para cometer delitos criminosos, também é utilizada para monitorar os usuários da internet, e não tem eficiência para identificar os anônimos.

4.1 – É POSSÍVEL IDENTIFICAR O AUTOR?

Não é um trabalho muito fácil a identificação de crimes cibernéticos, e esse trabalho deve ser realizado por policias especializadas em crimes virtuais, não sendo

uma tarefa apenas para autoridades brasileiras, mas devendo envolver autoridades de todos os países num trabalho de colaboração plurilateral.

Vale destacar que a identificação de criminosos cibernéticos pode ser um processo demorado e complexo, um fato preponderante é que seus autores são pessoas muito bem treinadas, e que fazem uso do que há de mais avançado em técnicas para ocultar sua identidade. Porém com a colaboração de especialistas em segurança cibernética em conjunto com agencias de aplicação da lei, e com a utilização de recursos adequados muitos criminosos podem ser identificados e responsabilizados por seus crimes. Outro fator importante para a diminuição desses crimes é a prevenção e a educação em segurança cibernética. A Deep Web é o principal campo onde prospera o anonimato:

> O anonimato está ligado principalmente a Deep Web. A Deep Web é a parcela da internet utilizada para comunicações e trocas de arquivos de forma anônima, ou seja, não é indexada por mecanismos de busca comuns. Pode ser acessada através de aplicativos da rede TOR (The Orion Rout), que elimina os rastros de acesso, embora tenha toda esta segurança, alguns sites ao serem acessados na rede podem exigir que para acessa-lo o usuário faça um login usando navegador da internet conhecida, comum. Não se pode deixar de citar a Dark Web, que é uma pequena parcela da Deep Web, em que os sites e redes também não são indexados por mecanismos de busca. Porém ela se difere da primeira, pois os domínios nela são voltados para as práticas criminosas, devido a isso se mantém escorada na dificuldade de rastreio nas redes. A principal diferença entre é a supracitada, sendo que a Dark Web é voltada para a prática de crimes, quanto a Deep Web contém domínios necessários para a operação da web. (https://www.jusbrasil.com.br/artigos/crimes-virtuais-e-as-dificuldades-de-combate-los/876548834)

> “Inicialmente, cumpre frisar que o delinquente informático cada vez mais se distancia do “protótipo” jornalisticamente divulgado, qual seja, do estudante de classe média, com alta especialização em Informática, bom, nível de escolaridade, inteligente e etc... Hoje tais delinquentes são, em geral, pessoas que trabalham no ramo da informático, normalmente empregados, não tão jovens e nem tão inteligente. “ (Direito Eletrônico p.209)

Especialistas na área virtual declaram que podemos fazer uma analogia do espaço virtual, com um grande iceberg, o que todos podemos ver seria a ponta do iceberg ou Surface Web, onde podemos acessar, com navegadores comuns, a todos os usuários, como *Google Chrome* e o *Firefox*. A parte submersa do iceberg seria a Deep Web, espaço este onde as ferramentas que a população está acostumada utilizar de um modo geral não conseguem acessar. Este espaço só pode ser acessado

com ferramentas de acesso especificas para ela, um navegador conhecido nesse meio é o TOR. Michael K. Bergman, criador do termo *Deep Web* fala de sua dimensão:

> A Deep Web é cerca de 500 vezes maior do que a Surface Web, com, em média, cerca de três vezes mais alta qualidade com base em nossos métodos de pontuação de documentos em uma base por documento. Em uma base absoluta, a qualidade total da Deep Web excede a da Surface Web por milhares de vezes. O número total de sites na Deep Web provavelmente excede 200.000 hoje e está crescendo rapidamente. O conteúdo na Deep Web tem significado e importância para cada buscador e mercado de informações. Mais de 95% das informações da Deep Web estão acessíveis sem restrição. A Deep Web também parece ser o componente de informação que cresce mais rapidamente na Web (BERGMAN, 2001). (tradução nossa).

Essa proporção gigantesca de possibilidades de uma navegação no anonimato acaba sempre corroborando como possibilitadora de atos ilícitos. O autor Leonardo Andrade, especializado em investigações de cibercrimes, traz em seu artigo as seguintes afirmações sobre a Deep Web:

> Na *Deep Web* encontra-se de tudo. É possível, por exemplo, contratar assassinos de aluguel, comprar cartões de créditos roubados e/ou furtados, é onde se abrigam os maiores exploradores de pornografia infantil, sites de venda de órgãos humanos, armas químicas e de uso exclusivo das forças armadas, com destaque para o comércio de drogas que é altamente estruturado, difundido e rentável, grupos terroristas articulam-se nos fóruns secretos, grupos que discutem técnicas para matar pessoas por meio de práticas satânicas e dos mais variados tipos de parafilias (ANDRADE, 2015).

De acordo com o especialista os crimes cibernéticos atingem o topo da complexibilidade do direito virtual, quando originários da Deep Web, pois neste ambiente não deixam nenhum rastro de suas ações.Desse modo, criminosos virtuais aproveitam da fragilidade das leis, a ausência de fronteiras e da tecnologia, para se manterem nas práticas delitivas, de modo que surge a necessidade de novos operadores da era digital.

A necessidade de novos operadores na área do Direito digital se comprova quando, em entrevista, o perito da Policia Federal Leonardo Bueno de Melo, feita pelo portal Consultor Jurídico, esclarece que:

> O sucesso alcançado pelos criminosos no mundo virtual é resultado da carência de procuradores, juízes e promotores que tenham conhecimento de como agir em tal área. Pois, quando não possuem muito conhecimento desta tecnologia ficam mais inseguros por medo de cometer algum ato abusivo em relação ao direito de privacidade (MELO, 2008).

Atuando de formas diversas e com objetivos diferentes, existe uma denominação para cada tipo de criminoso, ou para cada tipo de crime cometido. Vamos ver algumas dessas denominações a seguir, explicando cada uma delas, alertando que todas estas formas de prática estão ligadas ao anonimato. Condição essa que causa maior dificuldade na prevenção e punição desses crimes.

Há muitos tipos de criminosos que operam na internet, se aproveitam da conectividade global e do relativo anonimato oferecido pelo ambiente online. Esses criminosos exploram uma ampla variedade de táticas e técnicas para cometer crimes cibernéticos.

4.2 CRACKER E HACKER

Hackers são indivíduos com habilidades técnicas que exploram vulnerabilidades em sistemas de computadores e redes para ganho pessoal, seja para acessar informações confidenciais, espalhar malware ou causar interrupções.

Crackers são uma categoria de hackers que se dedicam a violações maliciosas, como quebra de senhas e sistemas de segurança, com o objetivo de causar danos ou obter benefícios ilícitos.

São também chamados de “invasores de sistemas”, são parecidos, porém não iguais.

O cracker é o expert na área que utiliza sua habilidade especifica para causar prejuízo a outros, um exemplo simples de uma ação do cracker é a invasão de um sistema de segurança para causar prejuízo. O hacker também definido como “pirata”, não tem o objetivo de causar prejuízo diretamente, mas o programa que ele cria é quem vai causar o dano. Os dois tem as mesmas características, porém, sistemas de operação diferentes. Os hackers são divididos em dois grupos, os “hackers éticos” e os “hackers não éticos”. Os “éticos” são aqueles que prestam serviços a grandes companhias, testando a segurança e descobrindo pontos fracos por onde os “não éticos” podem invadir os sistemas, causando danos as empresas.

Os “não éticos” são a parcela criminosa, que invadem o armazenamento de informações pessoais com o objetivo de causar prejuízos aos seus donos.

> “A maior preocupação do chamado “hacker ético” é com a implantação do sistema de segurança e a sua tarefa é a de tentar invadir o sistema das companhias com objetivo de detectar os pontos vulneráveis à ação de outros Hacker. Trabalha para gigantes do ramo dos computadores e para empresas que precisam defender informações confidenciais isso clientes. O hacker não ético (cracker) é o invasor destrutivo que tenta invadir na surdina os portões de entrada dos servidores internet, que são a melhor forma de desse disseminar informações. É forçoso admite que até o momento são os grandes vitoriosos nessa batalha informática. No Brasil, o exemplo mais recente de invasão agressivo correu no dia 6 de junho de 1999, quando as páginas da Presidência na internet foram invadidas por hackers e os textos com ataque ao governo também ocupará o site do Supremo Tribunal Federal. No mesmo

> dia, houve uma tentativa frustrada de entrar no site da Secretaria da Receita Federal. (Direito e Internet, 2000, p.37)

É importante notar que a internet é um ambiente diversificado e a motivação e a conduta dos criminosos cibernéticos podem variar amplamente. O combate a esses criminosos exige uma combinação de esforços de aplicação da lei, segurança cibernética, conscientização do público e regulamentações adequadas. A proteção pessoal online e a adoção de boas práticas de segurança cibernética são essenciais para evitar se tornar uma vítima

Os criminosos cibernéticos financeiros são indivíduos ou grupos que se dedicam a atividades criminosas online com o objetivo principal de obter ganhos financeiros ilícitos. Esses criminosos exploram vulnerabilidades de segurança e técnicas de engenharia social para acessar informações financeiras, roubar dinheiro ou realizar fraudes. Abaixo estão algumas das atividades comuns associadas a criminosos cibernéticos financeiros:

Fraudes de Cartão de Crédito: envolve a obtenção de números de cartão de crédito roubados, podendo utilizar ataques à lojas online, phishing e outras táticas, e a posterior utilização desses números para realizar compras não autorizadas.

Phishing financeiro: criminosos se utilizam de e-mail, mensagens falsas, na maioria das vezes se passam por funcionários de instituições financeiras, o objetivo é induzir a vítima a divulgar informações confidenciais com senhas, códigos de segurança e número de conta bancária.

Fraudes de Transferência Bancária: envolve a manipulação de transferências, alterando detalhes de contas de pagamento com objetivo de desviar fundos para contas controladas pelos criminosos.

Ransomware: se utilizam de malware de ransomware criptografando os dados da vítima para exigir resgate em troca de uma chave para descriptografar os dados. Essa prática é uma espécie de extorsão cibernética.

Esquemas de Investimento Fraudulentos: os criminosos criam sites ou esquemas de investimento falso, prometem retorno mais rentável do que o normal no mercado financeiro real, porém logo em seguida desaparecem com o dinheiro dos investidores.

Ataques a Caixas Eletrônicos: os criminosos cibernéticos realizam o ataque explorando vulnerabilidades do caixa eletrônico para sacar valores ilicitamente.

Fraudes com criptomoeda: a popularidade desse método de investimento também atraiu os criminosos que se aproveitam da falta de regulamentação e segurança para por em prática esquemas fraudulentos.

Fraudes com Cheques Online: os criminosos cibernéticos exploram serviços de pagamento e depósito de cheques online, falsificando cheques e depositando os mesmos.

Pharming: esse tipo de ação criminosa envolve a manipulação de sistemas de DNS (Domain Name System – Sistema de nome de domínio) com o objetivo de direcionar o tráfego da web de vítimas para sites falsos que tentam roubar informações financeiras.

Ataques a Instituições Financeiras: o alvo dos criminosos cibernéticos nesse caso são instituições financeiras, que são atacadas diretamente, o objetivo é acessar informações confidenciais, roubar fundos ou interromper serviços bancários.

Esta lista comtempla apenas alguns exemplos das atividades de criminosos cibernéticos na área financeiros. São crimes que tem potencial de causar prejuízos financeiros significativos para indivíduos, empresas e instituições financeiras.

Spammers são indivíduos ou grupos que enviam spam em grande quantidade por e-mail ou mensagens em massa, geralmente promovendo produtos, serviços ou esquemas fraudulentos.

Crackers de Senhas: Esses criminosos tentam quebrar senhas e acessar contas online ou redes sociais, frequentemente visando informações pessoais e financeiras.

Trolls da internet são indivíduos que assediam, provocam e perturbam comunidades online, frequentemente usando linguagem ofensiva e comportamento abusivo.

Pedófilos online: Esses criminosos usam a internet para a exploração sexual de menores, incluindo o compartilhamento de pornografia infantil e o aliciamento de crianças.

Extorsionistas ameaçam vítimas com divulgação de informações comprometedoras, a menos que um resgate seja pago.

Criminosos Cibernéticos Politicos: Esses indivíduos ou grupos visam instituições políticas e governamentais, realizando atividades como ataques de negação de serviço (DDoS) e vazamentos de informações.

DDoS é a sigla para "Distributed Denial of Service," que, em português, significa "Negação de Serviço Distribuída." Nesse tipo de ataque cibernético, um grande número de dispositivos comprometidos “zumbis”, é utilizado de forma maliciosa para causar uma sobrecarga à um sistema ou serviço online, o que causa impossibilidade de acesso para os usuários verdadeiro.

Por meio de um ataque DDoS, é coordenado por criminosos grande volume de tráfego de dados para um alvo especifico definido por eles, pode ser um site, ou um servidor, ou serviço online. Essa sobrecarga de tráfego excessivo sobrecarrega os recursos do alvo, deixando-o lento ou indisponível para os usuários legítimos.

Haters e Assediadores Online: Os "haters" e os assediadores online são pessoas que se envolvem em comportamentos negativos e prejudiciais na internet, com a intenção de difamar, assediar, provocar ou prejudicar outros indivíduos. Essas ações ocorrem principalmente em plataformas de mídia social, fóruns, blogs, comentários de notícias e outros espaços online. Aqui estão algumas características e distinções entre haters e assediadores online:

Os Haters são conhecidos por propagar mensagens e comentários online que são críticos, negativos e na grande maioria das vezes são ofensivos e grosseiros. Com frequência expressam o seu descontentamento, raiva ou ódio em relação à um produto, uma ideia ou pessoa. A motivação deles pode variar de discordância genuína até pelo simples prazer de perturbar ou provocar, podem ainda simplesmente quererem atrair a atenção para si.

A maioria escolhe de preferência ficar no anonimato, usando pseudônimos ou perfis falsos, o que lhes permitem desfrutarem de uma sensação de impunidade. Com frequência se dispersam deixando comentários negativos em várias postagens, tópicos ou páginas da web. Essas ações normalmente são de duração curta e não são focados em um único alvo.

Os assediadores online têm comportamento hostil e prejudicial, em relação a uma pessoa como alvo específico. Nnormalmente são persistentes e repetitivos em

suas ações. Esse assédio, perturbação e perseguição a uma vítima pode persistir por períodos longos. A motivação desse tipo de assédio pode ser por vingança, ódio, ciúmes, preconceito, ou simplesmente pela sensação prazerosa de causar mal-estar, estresse e sofrimento às vítimas. Perseguem suas vítimas em tantas quantas plataformas conseguirem, invadem a privacidade, ameaçam divulgar informações pessoais. O assédio pode começar com comentários pejorativos, com críticas, porém pode em alguns casos evoluir para ameaças, perseguição e em algumas situações evoluem até para agressão presencial.

Tanto os haters como assediadores online têm potencial de causar sérios danos emocionais e psicológicos às suas vítimas. As plataformas com frequência atualizam políticas de uso aceitável na intenção de combater essas práticas. As vítimas podem tomar medidas para se proteger, denunciando o assédio, bloqueando os indivíduos por essas práticas. É importante também a conscientização da população dá importância do respeito e civilidade nas interações online, para a criação de um ambiente virtual seguro e respeitoso.

Carder, são estelionatários e sua atuação tem foco especifico nas administradoras de cartão de crédito. Se aproveitam de falhas e negligências dos sistemas de segurança do próprio usuário, para efetuarem compra com o cartão de crédito das vítimas. Sua linha de ação também age na obtenção de dados de cartões de conta corrente e contas de sites de transações bancarias. Cometem fraude em benefício próprio, tiram proveito porque nesse tipo de fraude não se descobre de imediato. Em alguns casos conseguem valores altos em dinheiro e geralmente o ganho é usado para compra de produtos, para transações bancárias feitas em nome de laranjas.

Phreaker, são especialistas na telefonia. Utilizam linhas telefônicas de terceiros para usufruírem, realizam escutas telefônicas ilegais, como método de conseguir informações sobre determinada pessoa, com o intuito de cometer atos ilícitos. Na escuta telefônica se utilizam de um computador para fazer a interceptação de ligações da vítima. No caso das escutas telefônicas os criminosos utilizam um computador para interceptar as ligações da vítima. A polícia consegue interceptar esse tipo de prática, mas com o anonimato é impossível identificar o criminoso. Esse tipo de criminoso também se utiliza da clonagem de celulares, utilizados para não serem identificados.

Todas essas práticas criminosas visam causar prejuízo e obter alguma vantagem. Na atualidade, com o acesso ilimitado às redes de internet, não é difícil cair em alguma fraude. A legislação é falha quando a fraude acontece, porém já existem meios de segurança que podem ser utilizadas que vão diminuir as chances de se tornar vitima desses crimes.

5 OS REFLEXOS DAS REDES SOCIAIS NO PODER LEGISLATIVO

Nos moldes da Constituição Federal do Brasil (Brasil, 1988), os parlamentares são os representantes legítimos do povo. Nas ações e opiniões do parlamento está refletida a vontade de seus eleitores, dessa maneira, quando a sociedade se manifesta se posicionando, exteriorizando a sua vontade, isso acaba desencadeando atos legislativos que veem para regulamentar as ações relacionadas ao anseio da sociedade.

Quero demonstrar a incorporação da internet na vida da sociedade, e possíveis consequências legislativas e sociais causadas.

5.1 DISSEMINAÇÃO DAS CHAMADAS FAKE NEWS

A tradução literal do termo *Fake New* significa notícia falsa, ou noticia fraudulenta, como explicam, Rais e Sales (2020):

> [...] talvez um conceito aproximado do Direito, porém distante da polissemia empregada em seu uso comum, poderia ser identificada como uma mensagem propositadamente mentirosa capaz de gerar dano efetivo ou potencial em busca de alguma vantagem.

Os termos notícia fraudulenta ou notícia falsa, ainda são bastante vagos, em uma tentativa de melhor expressar o que seria *fake news*, a escritora e jornalista britânica Claire Wardle (2017, tradução nossa) elaborou uma lista com sete espécies de notícias falsas que poderiam ser identificadas, são elas:

> Sátira ou paródia: sem intenção de causar mal, mas tem potencial de enganar;
> Falsa conexão: quando manchetes, imagens ou legendas não mantêm relação com o conteúdo;
> Conteúdo enganoso: uso enganoso de uma informação para usá-la contra um assunto ou um indivíduo;
> Falso contexto: quando um conteúdo genuíno é compartilhado com um contexto falso;
> Conteúdo impostor: quando fontes genuínas são falsamente representadas[1]
> Conteúdo Manipulado: quando uma informação genuína ou imagem é usada para enganar;

> Conteúdo fabricado: novo conteúdo 100% falso e construído com o intuito de enganar e causar mal. (Claire Wardle, 2017)

A lista vai servir como alicerce para melhor compreender o que seriam as notícias fraudulentas. Essa lista não deve ser aceita como taxativa, já que podem surgir novas formas de *fake news*, o que devemos considerar é que a evolução tecnológica é constante e o surgimento das chamadas *fake news é recente.*

Já com o conceito de *fake news* em mente, é preciso ainda compreender os motivos que levam a criação dessas notícias. A escritora Claire Wardle (Wardle 2017), apresentou um rol de possíveis motivos geradores de notícias fraudulentas, são eles: jornalismo ruim, parodiar, provocar, por paixão, por partidarismo, por lucro, por influência política, por poder ou propaganda.

Com toda certeza a internet não é a responsável direta pela criação de *fake news*, porém podemos afirmar sem sombra de dúvidas, que ela é a maior facilitadora de propagação dessas notícias. A reunião de um tráfego de pessoas muito grande e de fácil acesso, possibilitou o compartilhamento em fração de segundos, além de proporcionar uma sensação de anonimato aos usuários, isso facilita a criação de notícias fraudulentas.

O Dr. Wilson Gomes(2019), afirma que as *fake news*, contemporâneas são feitas exatamente para circularem no meio digital, apenas causando seus efeitos no mundo físico.

Uma das ferramentas mais utilizadas e talvez a maior contribuição digital para a propagação de *fake News,* são os chamados robôs, **segundo Ruediger (2017**) os robôs são contas controladas por *softwares* se fazendo passar por seres humanos, que já dominam parte da vida nas redes sociais e participam ativamente das discussões em momentos políticos de grande repercussão.

As contas robotizadas agem no mundo virtual se passando por seres humanos, participam de debates, emitem opinião, publicam notícias, e em grande parte notícias fraudulentas, com o objetivo de influenciar a opinião dos usuários. Essas postagens acontecem em uma velocidade inimaginável ao ser humano, dessa maneira boa parte dos debates online acabam sendo dominados pelos robôs. Falando sobre o assunto Ruediger (2017) explica que um estudo feito pela FGV/DAPP aponta que esse tipo de conta chegou a ser responsável por mais de 10% das interações no Twitter nas eleições presidenciais de 2014, e durante os protestos pelo Impeachment, essas

interações provocadas por robôs representaram mais de 20% do debate entre apoiadores de Dilma Rousseff.

Como se não fosse o suficiente, a criação robotizada em massa de notícias falsas, uma pesquisa realizada pelo Instituto de Tecnologia de Massachusetts, comentada por Cymbaluk (2018), revela que a chance de uma notícia falsa ser repassada é 70% maior do que a de notícias verdadeiras.

O tamanho do sucesso alcançado no compartilhamento dessas notícias é devido ao apelo emocional em seu conteúdo, devido à sua falsidade ele é criado para ser um conteúdo viral, não há uma preocupação em manter uma relação com a verdade, e nem com a lógica. É criado com o objetivo de trazer irritação ou assustar, o que acaba gerando um maior engajamento social.

Vamos deixar um pouco de lado as *fake news* criadas somente para causar alvoroço, focando nesses esquemas organizados de disseminação em massa de notícias falsas, podemos afirmar que as *fake news* atingiram seus interesses?

Respondendo essa pergunta, vamos ao caso emblemático dos efeitos causados pelas notícias fraudulentas: a campanha eleitoral brasileira de 2022, onde se utilizando de notícias fraudulentas, soltaram o maior corrupto da história de nossa nação, senão o maior corrupto conhecido pela humanidade, anularam sentenças baseadas em mentiras e o tornaram elegível. Como se não bastassem disseminaram notícias fraudulentas de que ele teria sido inocentado. Tivemos um corrupto praticamente nomeado presidente pelo Supremo Tribunal Federal, já que de um lado podia fazer e falar o que queria, por outro lado o candidato foi proibido de fazer sua campanha. Fraudes na inserção de propagandas principalmente na região norte e nordeste prejudicaram o candidato de direita, e ainda existem pessoas que acreditam em nosso sistema eleitoral. Tudo isso é gerado pela manipulação de fake News que influenciam um povo sem discernimento do que é melhor para uma nação, um povo que se acostumou a viver de migalhas que os políticos dão.

O conteúdo de uma *fake new* é criado para viralizar, no caso daquelas notícias que circulavam à época das eleições de 2022, elas eram carregadas de informações difamadoras, criadas para causar desconforto e até ódio pelo candidato, como a acusação de que o candidato de direita era pedófilo, canibal, que odiava negros, que é machista, e assim vai uma lista interminável de acusações falsas que visavam apenas denegrir a imagem do candidato.

Falando sobre o assunto, com muita propriedade, escrevem Rais e Sales (2020):

> É claro que a desinformação polui o debate e cria uma atmosfera de incertezas e desconfiança, mas talvez o que parece ser ainda mais perigoso é a capacidade que essa poluição tem de alimentar e ampliar a polarização de opiniões na sociedade. Talvez a polarização seja a infecção, enquanto a desinformação seja apenas uma de suas febres.

Os chamados políticos do amor se apresentaram como aqueles que iriam unir o país, como se não fossem eles os responsáveis pela polarização, durante 35 anos da redemocratização do Brasil eles dominaram o poder, passaram por cima de tudo e de todos para perpetuar um esquema cleptocrático de poder, onde o império da propina e da corrupção predominou, quando o povo abriu a visão para mudar a história do pais, eles manipularam tudo o que puderam para voltar ao poder. São agressivos, e violentos, quem disser o contrário vem falar comigo que já fui vítima da violência dos chamados grupos sociais criados por esses políticos. Tentam jogar nos outros aquilo que eles são, mentirosos, farsantes, corruptos, prepotentes, nunca pesam no povo, somente pensam em encher os seus bolsos de dinheiro enquanto o povo é enganado e manipulado. Usam as pessoas, como usaram a morte da vereadora Marielle Franco, tentando acusar os adversários do assassinato, não tem respeito nem pelos mortos.

Agora que entendemos um pouco desse fenômeno das notícias falsas, como acontece sua propagação, a pergunta que fica é: como funciona a responsabilização das pessoas por traz dessas notícias?

As notícias consideradas fraudulentas não são abrangidas pelo direito fundamental da liberdade de expressão, como julgado na ADI 4451, o motivo é que as notícias fraudulentas causam modificação na realidade, com o objetivo de manipular e controlar a opinião, talhando a própria liberdade nas manifestações, nas palavras do ministro Luiz Fux:

> Nós temos hoje, basicamente, dois princípios no campo das fake news, essas notícias enganosas. Em primeiro lugar, há necessidade da lisura informacional, porque o voto é livre na medida em que ele é livre de suborno, corrupção e desinformação também. Se nós queremos um voto livre e consciente, não podemos chancelar fake news, que são notícias sabidamente inverídicas, propagáveis, massificadas, que viralizam num tempo recorde, sob o pálio da liberdade de expressão (BRASIL, 2019).

Ainda tratando de responsabilização, iniciando pelas pessoas (naturais ou jurídicas) autoras de notícias fraudulentas, para Camillo (2020), desde que estejam provados os pressupostos da responsabilidade civil, é cabível, na forma do art. 12 do CC (direitos de personalidade), a obtenção de tutela preventiva ou repressiva,

reclamando-se, em qualquer hipótese, perdas e danos, sem prejuízo de outras sanções.

Quando se trata de responsabilidade pela criação e divulgação de *fake news* devemos lembrar dos provedores de internet, a Lei do Marco Civil da Internet (Lei nº 12.965/2014) apresenta dois tipos de provedores, os provedores de conexão com a internet e os provedores de aplicação de internet (BRASIL, 2014).

Há uma diferença na responsabilização para os dois provedores, o provedor de conexão, a Lei nº 12.965/2014 afirma que este não será responsabilizado civilmente por danos causados por terceiros (art. 18), os provedores de aplicação, também não são responsáveis por danos causados por terceiros, a não ser que, após ordem judicial específica, não tome as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário (art. 19) (BRASIL, 2014).

Mas essa postura branda adotada pela LMCI talvez esteja com os dias contados, isso porque tramita no Congresso Nacional um Projeto de Lei (PL 2630/2020) que pretende instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, com o objetivo principal de combate à desinformação e, para atingir tal objetivo, atribui vários deveres aos provedores de aplicação (BRASIL, 2020), o PL não faz menção aos provedores de conexão, o que faz concluir que o texto do art. 18 da LMCI continua inalterado. Esse PL traz em seu texto inicial várias responsabilidades aos provedores de aplicação, como a obrigatoriedade de o provedor desenvolver procedimentos para melhorar as proteções da sociedade contra comportamentos ilícitos (art. 5º, §3º); dever de transparência que determina a publicação pelo provedor de aplicação de várias informações, principalmente relacionadas à contas que promovem conteúdo desinformativo (art. 6º e ss.); adoção de medidas contra desinformação (art. 9º e ss.) e; limitação de número de encaminhamento de mensagens em épocas de eleições, calamidades públicas e situações de emergência (art. 13, §1º), entre outras (BRASIL, 2020).

É um PL 2630/2020 muito polêmico desde a sua criação, o motivo é que apesar dele conter vários artigos que garantam a liberdade de expressão, fazendo menção aos princípios da Lei do Marco Civil da Internet, ele não foi visto com bons olhos, há um

receio traria uma limitação injustificada à liberdade de expressão e, por consequência o ressurgimento da tão temida censura.

Antes de nos prender nessa preocupação, precisamos lembrar que o STF já decidiu que disseminar notícias fraudulentas não é abrangida pela liberdade de expressão.

Segundo a opinião da advogada Raquel Saraiva (2020), a PL chega a censurar na medida em que as pessoas não vão conseguir se expressar, havendo uma ameaça clara aos debates públicos em ambientes como o Twitter, pois a qualquer momento a conta poderá ser denunciada e o usuário terá que se identificar, a advogada ainda acrescenta que esse fenômeno causaria uma autocensura nas mídias sociais.

Já de um outro lado, também falando sobre a supervalorizar da liberdade de expressão em detrimento de outros direitos, Martins e Longhi (2020) citam:

> [...] há quem sempre levante a bandeira da liberdade de expressão independente do conteúdo do que é dito. Qualquer restrição seria censura e ponto. Criticando essa posição, tendo em mente o sistema americano, Mary Anne Franks chama de "fundamentalistas" da Primeira Emenda os que justificam queima de bandeiras, saudações nazistas, pornografia infantil virtual, videogames violentos, doações corporativas a políticos, pornografia de vingança, instruções de fabricação de bombas, vídeos de recrutamento de terroristas, teorias da conspiração, registros médicos hackeados, spam, vírus de computador e até impressoras 3D. Caso de alguma maneira se restrinja o conteúdo ou se responsabilize seu criador: "Censura. Censura em qualquer lugar".

De acordo com o pensamento de Martins e Longhi (2020), contrariando o que alguns autores pensam, a PL 2630/2020 irá promover censura, mas vai atribuir aos provedores de aplicação deveres de combate à desinformação, e assegura em sue texto a liberdade de expressão, citam o art. 5º, §1º da PL, que dispõe: “as vedações do *caput* não implicarão restrição ao livre desenvolvimento da personalidade individual, à manifestação artística, intelectual, de conteúdo satírico, religioso, ficcional, literário ou qualquer outra forma de manifestação cultural [...]” (BRASIL, 2020).

Afirma ainda Nohara (2020) que a PL 2630/2020 tem a intenção exatamente garantir a liberdade de expressão na rede:

> [...] O Estado não pode exercer censura, mas não significa que ele não deva criar, via regulação condições para que haja uma internet livre. Ademais, um dos grandes desafios de manter as condições para que haja reflexões mais equitativas a partir do acesso à informação seria a manutenção da neutralidade da rede.

Com relação ainda a uma possível censura, causada pela PL essa não é a única crítica a ela, de acordo com Saraiva (2020) esse projeto traz ameaças também relacionadas a privacidade do usuário, traz a obrigação das plataformas identificarem as contas de usuários que forem denunciados, argumenta ainda que o artigo é muito vago e pode ser usado como instrumento para que usuários venham a sofrer perseguições online por alguma denúncia gerada por opositores que tenham uma opinião divergente..

Com a intenção de provar a necessidade da criação da PL, Martins e Longhi (2020) lembram do sistema americano de responsabilização dos provedores, que baseia-se no *notice and takedown* (notificação e retirada), o que basicamente significa a retirada ou remoção do conteúdo somente após notificação, muito semelhante ao art. 19 da LMCI, esse sistema "é alvo de críticas pela doutrina local, já que a imunidade dos provedores criou ao longo de décadas uma situação que incrementa riscos de discursos de ódio, desinformação, *cyberbullying* às vítimas".

Concluindo sobre o assunto, Martins e Longhi escrevem (2020):

> [...] o Marco Civil, ao imunizar o provedor antes de ordem judicial nos termos do art. 19, deixa as vítima de ataques *online* em situação de vulnerabilidade agravada, pois põe sob seus ombros o dever de procurar a Justiça, indicar os *links* e aguardar o cumprimento de decisão judicial pelo provedor para retirar um conteúdo que lhe cause dano. Ao mesmo tempo, enaltece o poder privado dos provedores pois são eles que redigem unilateralmente as cláusulas contratuais de suas políticas de conteúdo, e têm ampla liberdade para retirar ou não determinado conteúdo, taxá-lo de violento, falso ou qualquer outro, mas, acima de tudo, lucrar com a publicidade advinda dos dados dele decorrentes sem se responsabilizar.

A ascensão da internet trouxe a possibilidade de qualquer um falar qualquer coisa, isso acabou desaguando em uma inundação de notícias fraudulentas, algumas vezes carregadas de discursos de ódio, o que gera um comportamento radical de muitas pessoas, que ameaçam a honra e a segurança dos envolvidos.

Dentro desse contexto é que nasceu a PL 2630/2020, que Senado Federal aprovou, e com grande possibilidade de ser aprovado na Câmara dos Deputados, o que deixa claro que o movimento social reflete e influencia diretamente na renovação legislativa do país, o direito é moldado de acordo com as necessidades manifestadas pela população.

6 COMO A VITIMA PODE SE DEFENDER NA INTERNET

Na atualidade sabe-se que grande parte das práticas criminosas na área cibernética ainda não estão positivadas na norma jurídica apropriada. Como se não bastasse a falta de uma norma especifica, temos ainda, como agravante, a grande dificuldade de identificação dos criminosos, o que acaba por causar prejuízo a defesa da vítima por falta de informações suficientes para acusar um infrator responsável. Podemos afirmar que nesse “modus operandi” a única testemunha seria a máquina usada na prática do delito.

Alguns dos princípios jurídicos aplicados ao mundo real, podem ser utilizados no mundo virtual. Apesar de nosso ordenamento jurídico não aceitar todas os tipos de provas como válidas para incriminar o agente infrator, a exemplo as provas ilícitas, ainda assim, a depender do caso em questão, essas provas podem ser aceitas como legítima defesa.

O Art. 25 do (CP) Código Penal Brasileiro defini legítima defesa: *“Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem.”*.

Podemos aplicar também o Art. 23 do Código penal brasileiro, que assegura a excludente de ilicitude, que declara não existir crime quando a conduta do agente estiver amparada pelas três excludentes.

> Art. 23 - Não há crime quando o agente pratica o fato:
> I - em estado de necessidade;
> II - em legítima defesa; (Incluído pela Lei nº 7.209, de 11.7.1984)
> III - em estrito cumprimento de dever legal ou no exercício regular de direito.
> Excesso punível
> Parágrafo único - O agente, em qualquer das hipóteses deste artigo, responderá pelo excesso doloso ou culposo. (Código Penal Brasileiro, 1941)

A legitima defesa busca assegurar o direito de se proteger contra injusta agressão, contra o direito do indivíduo. Não podemos esquecer da situação de vulnerabilidade em que a vítima é colocada nesse tipo de ataque, pois como parte mais fraca não dispõe de meios necessários para sua proteção e defesa.

O que podemos verificar em muitos casos, é a existência de uma legitima defesa feita pela própria vítima ou por terceiros, na tentativa de combater a injusta agressão sofrida. Um caso muito comum que podemos ver são os ataques injuriosos

feitos por redes sociais, aplicativos de comunicação, casos de discussões que são carregados de ofensas que denigrem a imagem da pessoa.

Assim como na vida real e mundo físico, a legitima defesa é aplicável, no mundo virtual também deve ser aplicada porque, nesse ambiente há a ocorrência de crimes que se faz necessário uma intervenção moderada para resolver os crimes.

> "Entende-se por agressão injusta a conduta humana contrária ao direito, atacando (imediatamente mediatamente) bens jurídicos de alguém, seja mediante ação, seja mediante omissão, dolosa ou culposamente, independente da consciência da ilicitude por parte do agressor. Assim, quem se defenda agressão atual e injusta praticada por um inimputável, age em legítima defesa. Agressão atual é a presente. Iminente aquela que está prestes a ocorrer. Não se admite legítima defesa contra agressão passiva (vingança) ou futura (mera suposição)." (Código Penal para Concurso, 2012,p.69)

6.1 ATITUDES PRÁTICAS QUE PODEM GERAR UMA MAIOR SEGURANÇA

A busca por uma melhor proteção contra os ataques cibernéticos é de extrema importância para os dias atuais, onde nosso mundo está cada vez mais digital. Uma segurança total é quase que impossível, porem podemos adotar algumas estratégias que podem fortalecer a segurança online. Vamos ver algumas possibilidades que podem gerar uma maior segurança:

Manter o Software Atualizado: Manter o seu sistema operacional, antivírus, navegadores e outros programas atualizados. Essas atualizações frequentemente corrigem vulnerabilidades de segurança.

Utilizar Senhas Fortes: criar senhas fortes e únicas para cada conta.

Autenticação de dois fatores: muitos usuários não sabem como utilizar, porém a ativação de autenticação de dois fatores é uma ferramenta disponível que adiciona uma camada a mais de segurança, porque exige um segundo método de verificação além da senha.

Consciência de Phishing: manter atenção dobrada com e-mails, mensagens e links suspeitos. Não clique em links ou baixe anexos de remetentes desconhecidos. É necessário verificar a legitimidade de todas as solicitações recebidas.

Firewalls e Antivírus: a utilização de firewalls e software antivírus confiáveis irão proteger seu dispositivo contra malware e ameaças online.

Backup Regular de Dados: Fazer backup com regularidade de dados importantes, se acontecer um ataque ou houver perda de dados, conseguirá recuperar as informações.

Redes Wi-Fi Seguras: além de proteger a sua rede Wi-Fi utilizando senhas fortes e criptografia WPA3, se disponível. Procure sempre evitar o acesso de informações sensíveis em redes Wi-Fi públicas.

Controle de Privacidade em Redes Sociais: Revise e ajuste regularmente as configurações de privacidade em suas contas de redes sociais. Limite as informações compartilhadas publicamente.

Monitoramento de Contas Bancárias e Transações: Monitore regularmente suas contas bancárias e transações. Relate atividades suspeitas imediatamente ao banco.

Segurança em Dispositivos Móveis: Proteja seus dispositivos móveis com senhas, PINs ou biometria. Instale apenas aplicativos de fontes confiáveis.

Educação contínua: Mantenha-se informado sobre as últimas ameaças cibernéticas e práticas de segurança. A educação contínua é essencial para se manter protegido.

Use Conexões Seguras (HTTPS): Sempre que possível, utilize conexões seguras (HTTPS Hypertext Transfer Protocol Secure, ou Protocolo de Transferência de Hipertexto Seguro.) ao navegar na web. Isso ajuda a proteger suas informações durante a transmissão.

Controle de Dispositivos IoT(Internet das coisas): Se você usa dispositivos da Internet das Coisas (IoT), altere as senhas padrão e mantenha-os atualizados para evitar vulnerabilidades.

Limpeza de Dispositivos Antigos: Antes de descartar dispositivos antigos, faça uma limpeza completa, removendo todos os dados pessoais.

Seguro Cibernético: Considere a possibilidade de adquirir um seguro cibernético para ajudar a cobrir possíveis danos em caso de violação de segurança.

Quando tomamos essas atitudes práticas, podemos melhorar significativamente a segurança online, reduzindo o risco de se tornar vítima de um ataque criminoso online.

7 CONCLUSÃO

A histórica evolução da tecnologia gerou novas possibilidades que trouxeram a melhoria da vida em sociedade. As facilidades geradas pelos avanços tecnológicos influenciam até o trabalho judiciário, gerando maior celeridade na maioria dos atendimentos, porém novas tecnologias não geram apenas facilidades, surgem também dificuldades de adaptação a nova realidade, surgem novas dificuldades na apuração de crimes que nascem na mesma toada das inovações tecnológicas. Destaca-se ainda o fato de que as normas penais não acompanham essa evolução, o que resulta em dificuldades para combater os crimes surgidos dessas inovações, o que evidencia a necessidade de uma norma penal contemporânea.

A constituição federal de 88, traz a previsão de normas que auxiliam na criação de uma camada de proteção, porém a base do nosso ordenamento jurídico ainda é muito vaga, carecendo da criação de leis mais especificas, que tipifiquem os novos crimes ou novas modalidades de práticas criminosas que vão surgindo com a evolução tecnológica.

Infelizmente nossa constituição ao mesmo tempo que permite a criação de novas leis, também acaba por gerar uma possibilidade de isenção das práticas delituosas, uma vez que traz dentro dos princípios constitucionais um rol de benefícios para os agentes criminosos, como já relacionado anteriormente o da legalidade. Não há que se punir uma conduta se não houver uma lei anterior que o defina, o que acaba por permitir que muitas ações criminosas fiquem impunes, se utilizando dessa brecha existente na legislação, muitas pessoas mal intencionadas se utilizam da internet para a prática de delitos.

O direito constitucional da privacidade garante a inviolabilidade da honra, da vida privada e da sua imagem, mas infelizmente é o direito constitucional mais atingido pela ação de ciber criminosos. Situação causadora de grande desconforto para as vítimas, além de prejuízos emocionais, materiais e físico.

O anonimato na internet ainda é o fator preponderante na prática dos crimes cibernéticos, a dificuldade ou até a falta de identificação dos criminosos. A liberdade de expressão direito assegurado em nossa Constituição Federal, está relacionado a expressão do pensamento, que deve de fato ser livre, porém esse mesmo princípio traz a vedação do anonimato. Apesar da vedação constitucional, ainda não existem ferramentas necessárias e suficientes para garantir o cumprimento desse princípio, o

que acaba proporcionando o acobertamento das práticas de crimes cibernéticos. O envolvimento de pessoas munidas de alta capacidade técnica nas invasões de dispositivos eletrônicos é outro fator que contribui

As identidades desses criminosos muitas vezes estão interligadas para a prática de crimes virtuais. Dentre a grande variedade de formas de ataques existentes a finalidades é sempre a mesma: cometer os crimes para obter vantagens para si ou para outra pessoa, lembrando que existe diferença em cada um dos agentes, que elencamos anteriormente.

Os crimes cometidos na internet causam um devastador impacto social e psíquico, em muitos casos, expõe a vítima ao ridículo e ao julgamento social. Quando levamos em conta que essa espécie de prática criminosa é feita nas redes sociais que promovem a interação de pessoas do mundo todo, a dispersão dos efeitos do crime toma proporções gigantescas. Em especial quando esses crimes ferem o direito fundamental da liberdade. Quando o direito à liberdade é afetado num contexto mais ameno e especifico de casos como crimes de estelionato, fraude e pedofilia, buscam atingir uma pessoa ou grupo de pessoas, nesses casos a repercussão não alcança volumoso destaque na divulgação, esses crimes ocorrem de forma mais silenciosa, sem alarme.

Devido ao fato de serem práticas criminosas que na grande maioria, é difícil de ser identificada, acaba tornando a vítima vulnerável pois não tem como se defender. A legítima defesa tem um papel essencial para trazer um contrapeso nessa batalha desigual dos crimes cibernéticos.

Um ordenamento jurídico deficiente e fraco ante a essa prática criminosa, junto com uma polícia investigativa com falta de meios e ferramentas para combater os crimes cibernéticos, a tendência é a descrença no sistema de justiça brasileiro. Um pouco mais de investimento nas câmaras legislativas, criando uma legislação especifica para o combate dessa prática se faz necessário.

Os crimes cibernéticos, vêm num crescente e alarmante aumento, devido a fragilização das vítimas em não conseguirem preservar os seus direitos, em muitos casos.

Por esse motivo precisamos entender que é de extrema importância o avanço das normas legais para o combate, assim como o preparo e especialização de uma polícia mais preparada. Neste momento nosso país não uma segurança efetiva contra as práticas criminosas praticadas. Precisa-se de mudança urgente. Há uma eminente

necessidade de uma adaptação ou atualização de nossa legislação, com a criação de uma previsão específica de determinados tipos penais que somente acontecem através da internet ou sistemas informatizados. Apesar de grande parte dos casos ser possível dizer que o crime virtual cometido se amolda à um dos tipos penais existentes, há ainda uma grande quantidade de outras práticas que configuram crime, porém podem ficar impunes devido a dificuldade no combate e prevenção.

A natureza sem fronteiras da rede mundial de internet, nos mostra a necessidade e importância de uma cooperação jurídica internacional, para combater esses delitos, por isso há a necessidade de uma uniformização na tipificação penal e no sistema investigatório, para facilitar a rapidez na cooperação. Um passo importante foi a assinatura de adesão à Convenção de Budapeste.(23 novembro 2021)

Ante ao exposto podemos concluir que o Direito Digital, os crimes cibernéticos e todas a suas variantes formam um ramo muito complexo do direito, o que por si só nos leva a crer que esse ramo do direito não será para muitos. É necessário que os operadores do direito que queiram atuar nessa área, busquem conhecimento técnico necessário na área de internet e informática. Caso contrário não conseguirá atuar em processos envolvendo o Direito Digital, lembrando ainda que, no direito, o juiz está sujeito aos pedidos realizados pelas partes.

Para os magistrados a necessidade de conhecer os termos técnicos vai mais profundo, isso porque um juiz não tem a opção de escolher entre julgar ou não um litígio. Eles são responsáveis pelo dever de julgar a todo litigio apresentado ao poder judiciário, por mais que seja o advogado que dá o rumo do processo, é o juiz através de requerimentos e diligencias que decidirá, dando a palavra final sobre a lide. Por esse motivo um magistrado sem conhecimento técnico tenderá a cometer erros no decorrer do processo, seja pela decisão não ficar unida a lei, que por muitas vezes é incompatível com o meio digital, ou até por confundir como funcionam as coisas na internet.

Enquanto os operadores do Direito lutam para conseguir se adaptar aos dias contemporâneos, as gerações mais novas não tem grande dificuldade, pois simplesmente se utilizam dos meios digitais disponíveis, compram, vendem, interagem com amigos, namoram, manifestam suas opiniões, expõe a sua vida e intimidade, em alguns casos causam consequências inimagináveis, como "*Revenge porn"* ou pornografia de vingança, as chamadas "*fake news",* entregando nas mãos

de advogados e magistrados um verdadeiro imbróglio, a solução das problemáticas geradas.

Quando voltamos os olhares ao legislativo, que em teoria é quem deveria legislar e trazer maior segurança jurídica na área digital, vemos os parlamentares sempre tentando positivar as manifestações da sociedade, porém esbarram na mesma dificuldade que os operadores do direito: a falta de conhecimento técnico, de como funciona a internet.

Destaca-se que a área do Direito Digital não é uma área simples para os operadores do direito, porém apesar de toda dificuldade a sociedade precisa com urgência de profissionais que tenham domínio da área digital, pelo fato de a internet ter se tornado parte indissociável da vida do ser humano, em especial as gerações mais novas. Outro fato a se pontuar é que em poucos anos um profissional que não tenha um mínimo de conhecimento de rede de internet e meios digitais, se tornará um profissional obsoleto sem destaque no mercado de trabalho.

Por último, mas não menos importante, quero pontuar o baixo número de escritores que pesquisem a fundo o direito digital e escrevam bons livros, e a escassez de doutrinadores do direito digital. Poucos autores se aventuram a estudar um ramo tão complexo e controverso como o direito digital. Essa pesquisa gerou o desejo de em um futuro próximo, fazer um estudo mais profundo, adentrar no mundo dos *hackers* da internet, para conhecer melhor esse ambiente e através de estudos e pesquisa proporcionar uma maior proteção para as pessoas.

REFERÊNCIAS

Ana Paula Barbosa-Fohrmann, Allan Roch..., **Direito digital: direito privado e internet**, ano de edição 2019, 2ª Edição, p. 65.

FERRAZ JUNIOR, Tércio Sampaio. ***Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado***, p. 54.

CHAVES, Antônio. **Direito à imagem e direito a Fisionomia**, 2019, p. 38

CYMBALUK, Fernando. **Fake news apelam e viralizam mais do que notícias reais, mostra estudo**. São Paulo: 08 de março de 2018. Disponível em: https://www.uol.com.br/tilt/ultimas-noticias/redacao/2018/03/08/fake-news-apelam-eviralizam-mais-do-que-noticias-reais-mostra-pesquisa.htm. Acesso em: 25 out. 2023.

WARDLE, Claire. **Fake news. It's complicated.** *[S.l.],* 16 de fevereiro de 2017. Disponível em: https://firstdraftnews.org/latest/fake-news-complicated/. Acesso em: 27 Out. 2023.

BITTAR, Carlos Alberto. **Os direitos da personalidade**, 2015, 8ª edição, p. 87

LILIANA MINARDI PAESANI**, Direito e Internet**, São Paulo, Editora Atlas 2000, p.37.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. **Fake news vs. liberdade de expressão:** uma análise favorável ao PL 2.630/20 do Senado Federal. *[S.l],* 1º de junho de 2020. Disponível em: https://migalhas.uol.com.br/coluna/migalhas-de-responsabilidade-civil/328010/fakenews-vs--liberdade-de-expressao---uma-analise-favoravel-ao-pl-2-630-20-dosenado-federal. Acesso em: 18 out. 2023.

NOHARA, Irene Patrícia. **Desafios da Ciberdemocracia diante do fenômeno das *Fake News:*** regulação estatal em face dos perigos da desinformação. *In:* RAIZ, Diogo (coord.). **Fake News:** a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. E-book.

ROGÉRIO SANCHES CUNHA, **Código Penal para Concurso 5° Edição**, Salvador, Editora Juspodivm, 2012.

ROGÉRIO SANCHES CUNHA, **Manual de Direito Penal 6° Edição**, Salvador, Editora Juspodivm, 2019.

RAIZ, Diogo; SALES, Stela Rocha. **Fake News, Deepfakes e Eleições.** *In:* RAIZ, Diogo (coord.). **Fake News:** a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. E-book.

ANDRADE, Leonardo. **Cybercrimes na deep web: as dificuldades de determinação de autoria nos crimes virtuais**. ***Jus.com.br***, 2015. Disponível em: <https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicasde-determinacao-de-autoria-nos-crimes-virtuais/2>. Acesso em: 15/11/2023.

CAMILLO, Carlos Eduardo Nicoletti. **O fenômeno das *Fake News* e a sua repercussão na responsabilidade civil no sistema jurídico brasileiro.** *In:* RAIZ, Diogo (coord.). **Fake News:** a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. E-book.

MARCELO NOVELINO, **Curso de Direito Constitucional 12° Edição,** Salvador, Editora Juspodivm, 2017, p. 347

BERGMAN, Michael K. ***The Deep Web: Surfacing Hidden Value.*** 2001. Disponível em:<http://brightplanet.com/wp-content/uploads/2012/03/12550176481deepwebwhitepaper1.pdf>. Acesso em: 15/11/2023.

RAIZ, Diogo; SALES, Stela Rocha. **Fake News, Deepfakes e Eleições.** *In:* RAIZ, Diogo (coord.). **Fake News:** a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2020. E-book.

RUEDIGER, Marco Aurélio. **Os Robôs nas Redes Sociais**. *[S.l.]*, 2017. Disponível em: http://dapp.fgv.br/artigo-os-robos-nas-redes-sociais/. Acesso em: 27 jun. 2020.
SALUTES, Bruno. **O que é IP.** *[S.l],* 21 de outubro de 2019. Disponível em: https://canaltech.com.br/software/o-que-e-ip/. Acesso em: 25 out 2023.

SARAIVA, Raquel. **PL das fakes news: censura? Lei da mordaça? Entenda o que pode mudar:** aprovado pelo Senado nesta terça, projeto de lei, que tem como

objetivo combater notícias falsas, carrega inúmeras preocupações que ferem direitos do usuário. [Entrevista cedida a] NAKAGAWA, Liliane. *[S.l],* 02 de julho de 2020. Disponível em: https://olhardigital.com.br/noticia/pl-das-fakes-news-censura-lei-damordaca-entenda-o-que-pode-mudar/102964. Acesso em: 18 out. 2023.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4451/DF.** Relator: Ministro Alexandre de Moraes, 06 de março de 2019. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur399151/false. Acesso em: 24 out. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm. Acesso em: 02 out. 2023.

https://codebit.com.br/blog/developer/qual-diferenca-entre-hacker-cracker

https://tecnoblog.net/responde/o-que-e-um-crime-cibernetico

MELO, Leonardo Bueno de. Entrevista: Leonardo Bueno de Melo, perito da Polícia Federal. ***Consultor Jurídico,*** Jul. 2008. Disponível em: <http://www.conjur.com.br/2008-jul-20/falta_lei_informacao_beneficiam_cibercrime?pagina=2>. Acesso em: 15/11/2023.

https://www.jusbrasil.com.br/artigos/crimes-virtuais-e-as-dificuldades-de-combate-los/876548834]

https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade