

CENTRO UNIVERSITÁRIO DE GOIÁS – UNIGOIÁS
PRÓ-REITORIA DE ENSINO PRESENCIAL – PROEP
SUPERVISÃO DA ÁREA DE PESQUISA CIENTÍFICA - SAPC
CURSO DE DIREITO

A CRIMINALIDADE NO CIBERESPAÇO E O PAPEL DO DIREITO

ALUNA: ALINE CRISTINA MOURA GABRIEL
ORIENTADORA: CASSIRA LOURDES DE ALCÂNTARA DIAS RAMOS JUBÉ

GOIÂNIA
JUNHO/2022

ALINE CRISTINA MOURA GABRIEL

A CRIMINALIDADE NO CIBERESPAÇO E O PAPEL DO DIREITO

Trabalho final de curso apresentando e julgado como requisito para a obtenção do grau de bacharelado no curso de Direito do Centro Universitário de Goiás – UNIGOIÁS na data de 02 de junho de 2022.



Profa. M.a Cassira Lourdes de Alcântara Dias Ramos Jubé (Orientadora)
Centro Universitário de Goiás - UNIGOIÁS

Prof. M.e. Rogério Pereira Leal (Examinador)
Centro Universitário de Goiás - UNIGOIÁS

A CRIMINALIDADE NO CIBERESPAÇO E O PAPEL DO DIREITO

Aline Cristina Moura Gabriel¹

Cassira Lourdes de Alcântara Dias Ramos Jubé²

RESUMO: Utilizando como referências pesquisas bibliográficas e informações disponibilizadas na internet, o presente artigo tem como objetivo informar e mostrar a problemática de determinados pontos que surgiram com o avanço da tecnologia. A globalização, o surgimento da internet e avanço nas comunicações foram evoluções de extrema importância para nossa sociedade atual, e com isso surgiram também problemas com relação ao ambiente virtual. Se faz necessário analisar os riscos decorrentes disto, dentre eles se encontram a propagação de maior criminalidade devido a facilidade de anonimato nas redes e o aumento das notícias falsas (*Fake news*), dentro do ambiente virtual. Analisando a constante utilização da internet e a exposição que a maioria das pessoas sofre todos os dias seja em aplicativos de conversas pessoais ou para trabalho, é importante expor os problemas do meio virtual e falar da forma que isso se torna essencial para prevenir certos acontecimentos que prejudicam os usuários e a sociedade em geral. Ao final é citado meios de proteção e prevenção que podem ser utilizados pelos usuários para evitar tais delitos e aumentar a segurança ao utilizar a internet cotidianamente e as legislações que realizam o controle sobre tais delitos.

Palavras-chave: Internet. Cibercrimes. Meio Virtual. Evolução Tecnológica.

THE CRIMINALITY IN CYBERSPACE AND THE ROLE OF THE RIGHT

ABSTRACT: Using bibliographic research and information available on the internet as references, this article aims to inform and show the problem of certain points that emerged with the advancement of technology. Globalization, the emergence of the internet and advances in communications were extremely important developments for our current society, and with that, problems also arose in relation to the virtual environment. It is necessary to analyze the risks arising from this, among them are the spread of greater crime due to the ease of anonymity on the networks and the increase in false news (*Fake news*), within the virtual environment. Analyzing the constant use of the internet and the exposure that most people suffer every day, whether in personal conversation apps or for work, it is important to expose the problems of the virtual environment and speak in a way that this becomes essential to prevent certain events that harm users and society in general. At the end, protection and prevention means that can be used by users are mentioned to avoid such crimes and increase security when using the internet on daily basis and the laws that control such crimes.

Keywords: Internet. cybercrimes. Virtual Medium. Technological evolution.

¹Discente do curso de Direito do Centro Universitário de Goiás–UNIGOIÁS. Lattes: <http://lattes.cnpq.br/5443018187861372>. E-mail: alinecrismoura01@gmail.com.

² Professora mestre do Centro Universitário de Goiás – UNIGOIÁS. Graduada em Direito pela Pontifícia Universidade Católica de Goiás; advogada; Especialista em Direitos Humanos pela Academia de Polícia Militar e Docência Universitária pela Universidade Estadual de Goiás; e Mestre em Direitos Humanos pela Universidade Federal de Goiás; Lattes: <http://lattes.cnpq.br/6792979547523586> E-mail: cassiralourdes@gmail.com

INTRODUÇÃO

O intuito deste artigo é a capacidade de ser utilizado como fonte de conhecimento para os profissionais do direito, especialmente no campo do direito penal, para esclarecer e transformar o conceito de crime cibernético, a modernidade trouxe para a sociedade a comodidade da comunicação e da integração social, considerando que vários lugares no mundo as pessoas podem se comunicar por meio de dispositivos eletrônicos na Internet.

O mundo virtual é utilizado em vários campos da sociedade, como educação, política, negócios, ciência e outros. A lei como reguladora não fica ausente, pois o processo de desenvolvimento global é inevitável e, como os grupos acima, a evolução de toda a sociedade é sempre acompanhada pela lei.

Atualmente, a internet possibilita a comunicação rápida entre pessoas em diferentes partes do mundo, o que torna o ambiente virtual um local favorável para várias atividades criminosas. É importante ressaltar as medidas que estão sendo tomadas para minimizar o andamento dos crimes cibernéticos, quais são esses crimes e como a sociedade moderna é uma vítima potencial ao viajar com pacotes de dados contendo informações pessoais e comerciais usando a Internet.

O crime cibernético vem aumentando constantemente, pode-se atribuir a isto o fato que o número de usuários de computadores domésticos aumentou com o passar dos anos e a evolução tecnológica. Nesse contexto, o mundo virtual inicialmente não tem fronteiras ou controles, e os crimes podem ser cometidos sem uma classificação de crime específica. Desde esse período, em decorrência atitude criminosa cometida por meio da internet, também se originou intenção de coibir esses comportamentos.

Vivemos na Era de tecnologia moderna e de fácil acesso, um grande número de pessoas utiliza os meios tecnológicos para se comunicar de diferentes formas, o que muitas vezes leva a uma exposição inimaginável de suas vidas íntimas. A comodidade que o mundo globalizado nos proporciona, além de trazer algumas vantagens, também pode nos colocar em certa situação de fragilidade.

A primeira seção discute o desenvolvimento histórico da internet e o conceito de crime cibernético, mostrando o caminho dessa evolução. Já a seção dois discute a classificação desses crimes em ambientes virtuais, enfocando as formas mais comuns de ocorrência de tais crimes e apresentando as características típicas juntamente com a implementação desses na prática. Portanto, a seção três trata do direito ao esquecimento e relaciona as leis que já trataram do assunto, bem como os projetos de lei sobre os crimes virtuais.

MATERIAIS E MÉTODOS

Para fazer o estudo sobre o ciberespaço e como o direito atua neste âmbito, foi

adotado o método dedutivo, que é o método próprio da lógica, onde as conclusões são obtidas a partir de princípios gerais com intenção de obter uma conclusão mais específica sobre o tema em questão.

Dessa forma foi feita a pesquisa exploratória que envolve levantamento bibliográfico ou de compilação do tema pesquisado, a partir de material já publicado, constituído principalmente de doutrinas, textos legais e material disponibilizado na Internet.

Tornando possível alcançar um grande número de estudiosos do assunto, com objetivo de compreender e explicar o tema abordado, buscando apresentar do que se trata o ciberespaço e quais acontecimentos da internet se ligam ao direito e a sociedade atual.

1 SURGIMENTO DA INTERNET

No período da Guerra fria, em 1969, se fazia necessário algum meio de realizar a comunicação entre os soldados e os cientistas, uma forma de manter o contato entre eles para obter um melhor resultado nas estratégias. Fruto dessa necessidade foi criado a Arpanet, e nesse ano em questão foi enviado o primeiro e-mail. Em 1982 se popularizou o uso de forma acadêmica nos Estados Unidos. Logo depois se espalhando para outros países, então recebeu o nome de internet (SILVA, 2001).

Em 1990 Tim Berners-Lee, criou a Rede Mundial de Computadores, e foi então que a internet ganhou uma popularidade crescente, e se tornou um mecanismo de comunicação acessível a outras pessoas e não somente para cunho científico como era na década de 60. Com toda essa repercussão veio o surgimento das redes sociais, tudo isso foi um impulso na evolução da tecnologia e da comunicação. (DIANA, 2015)

1.1 BENEFÍCIOS E MALEFÍCIOS DA INTERNET

A era moderna trouxe facilidades e praticidade para o cotidiano, é usual ver as pessoas conectadas em seus aparelhos celulares e computadores. Houve um avanço sobre o uso da tecnologia para o estudo, para trabalhar, para manter relações pessoais e até para o lazer. Em maioria o meio virtual tem muitos benefícios a sociedade em geral, porém é importante se atentar aos riscos que esse ambiente pode oferecer. (QUINELATO, 2017)

Atrás de cada celular ou computador, existe um usuário, uma pessoa exposta a riscos que esse ambiente variado de opções pode proporcionar. Dentre esses riscos estão a exposição de dados pessoais por invasão de vírus, plataformas que podem conter usuários que estão usando informações falsas, hackers, paginas criadas com intenção de subtrair dados importantes de quem a acessar, dentre vários outros riscos que podem estar presentes com um único acesso equivocado por alguém que não conheça o ambiente virtual ou que não saiba os riscos que este oferece. (QUINELATO, 2017)

A superexposição nas redes também facilita a ocorrência de crimes, por ser uma

rede aberta em muitos aspectos, vários usuários podem visualizar ali o conteúdo postado, principalmente por jovens, que gostam de expor e compartilhar seu cotidiano. Apesar de saber do perigo existente, atualmente é comum a exposição da rotina, de lugares frequentados, de viagens realizadas, tudo isso se tornou habitual. (FOLTÝN, 2018)

A maioria das pessoas não se atenta ao risco de partilhar tantas informações, ou não se preocupa o bastante sobre. Com o crescimento dos usuários, pessoas que possuem intenções prejudiciais estão conseguindo realizar cada vez mais crimes utilizando as ferramentas que tem a disposição. A maioria das pessoas conectadas a rede de internet possui uma variedade de redes sociais em seus aparelhos, o que liga diversas informações que podem gerar muitos detalhes de suas vidas íntimas ao acesso de todos. (FOLTÝN, 2018)

1.2 CUIDADOS NECESSÁRIOS PARA NAVEGAR NA INTERNET

Pessoas de todas as idades usam o espaço virtual todos os dias, por ser um ambiente amplo e de fácil acesso, é importante saber como se prevenir e evitar os riscos que existem nesse meio. A maior proteção a disposição de todos é o conhecimento básico sobre a rede de navegação. Buscar saber mais sobre as proteções disponíveis, como os antivírus e como realizar uma navegação de forma segura. (SANTOMAURO, 2014)

Isso implica monitorar o uso de crianças e pessoas que não possuem um conhecimento básico sobre o meio virtual, pois essas pessoas são alvos mais fáceis para usuários com intenções prejudiciais. Explicar os riscos é um método preventivo que evita em grande parte situações perigosas na internet. (SANTOMAURO, 2014)

É complexo limitar os riscos em um ambiente tão aberto como a internet, porém alguns cuidados são de extrema importância para evitar ao máximo os riscos possíveis. Manter em redes sociais somente pessoas que são do conhecimento do usuário, sempre que possível deixar as informações como e-mail, documentos pessoais, ou outras informações de cunho pessoal privadas, ler sobre as ocorrências de delitos virtuais que estão ocorrendo com a finalidade de se precaver sobre isso, se atentar a mensagens com links de acesso ou de pessoas que não são conhecidas, são formas de coibir possíveis práticas criminosas. (FOLTÝN, 2018)

1.3 DARK WEB E SEUS RISCOS

A internet utilizada pela maioria dos usuários é chamada de *surface Web*, a parte superficial do mundo virtual, existe a *Dark Web*, que é a parte mais desconhecida e possui uma maior dificuldade de acesso. A principal diferença entre a internet convencional e a *Dark Web* são o teor de informações e sites disponíveis. (TIMOCHENCO, 2016)

Existem servidores nessas camadas mais profundas da internet, que contém sites de vendas de produtos ilícitos, como drogas, armas a disposição de quem desejar comprar, além

de conteúdos perturbadores e venda inclusive de órgãos humanos. Todos esses tipos de vendas são de difícil rastreio devido ao pagamento ser realizado por moeda digital não rastreável. (TIMOCHENCO, 2016)

Com a dificuldade de identificar usuários e com a constante criação de novos servidores com ausência de endereço de identificação eletrônica (IP), é praticamente impossível desabilitar os sites ilícitos da *Dark web*, assim deixando essa parte da internet como um local de perigo e propagação da violência e aumento dos crimes em geral no meio digital. (TIMOCHENCO, 2016)

2 CONCEITO DE CIBERCRIME

Na Internet, temos um solo fértil e um ambiente ilimitado para escolhas e oportunidades, nessa falta de restrições que muitas pessoas se deparam com outras que usam ilegalmente a Internet. O cibercrime constitui qualquer irregularidade ou ato ilícito que é cometido por meio do meio virtual, ou algum crime habitual que ocorra através de um facilitador como smartphone ou computador. (NASCIMENTO, 2014).

Segundo Fabrizio Rosa (2002, p.53):

A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

O cibercrime é um tema recorrente atualmente, com o aumento dos computadores, celulares e outros meios tecnológicos, se tornou fácil para qualquer pessoa utilizar a internet para realizar atividades ilícitas sem precisar sair de casa para fazê-lo. Por ser uma forma de crime que não tem um limite de território, ou seja, pode ocorrer em todas as partes do mundo independente da distância entre o criminoso e a vítima, existe um grau maior de dificuldade de identificar o culpado. (NASCIMENTO, 2014).

2.1 CLASSIFICAÇÕES DO CIBERCRIME

Não se fala muito da classificação do cibercrime, haja vista que a constante evolução dos meios tecnológicos dificulta um padrão exato. Porém existem entendimentos sobre uma subdivisão em cibercrimes. São subdivididos em puros, aqueles geralmente praticados por hackers, que tem como intuito atingir as redes de dados que existem, usando os sistemas de empresas por exemplo, e através da informática obter vantagens, seja roubando dados pra suborno ou propriamente realizando a transferência de dinheiro que está na conta virtual. (TATEOKI, 2016)

Os mistos compreendem os crimes que usam a internet como meio para atingir um fim, este diverso de algo relacionado a informática. A caracterização para esse delito se encaixar como cibercrime, é a tecnologia ser necessariamente a forma de realizar a conduta. Existem ainda os comuns que são crimes que já existem e passam a ser realizados por meio da internet, o ambiente virtual se torna um meio para realizar o crime que já existia anteriormente. Como o crime de calúnia, que já é tipificado em lei, mas pode ser realizado através de redes sociais. (TATEOKI, 2016)

2.2 DIFICULDADES EM IDENTIFICAR E PUNIR CIBERCRIMINOSOS

Apesar do aumento recorrente dos crimes pela internet, pouco se fala sobre as formas existentes para combater tais crimes e da dificuldade que existe em punir os delitos cometidos na internet. No ambiente virtual existe uma grande liberdade de expressão para todos os usuários, porém o que gera essa liberdade também facilita que pessoas com intenção de cometer delitos possam realizar essas condutas de forma anônima e sem sair de casa. (ATHENIENSE, 2011)

Apesar de ser complicado identificar a autoria de um crime cometido em ambiente virtual, existe meios de identificar o usuário, como utilizando o endereço IP da rede que foi utilizada para cometer o delito. Dessa forma obtendo dados como a localização e identidade do criminoso. (ATHENIENSE, 2011)

Porém existem meios de alterar esse IP, ou modificar a localização, na maioria das vezes isso que dificulta o processo de punição dos cibercriminosos. Crimes como apologia ao crime, possuem penas menores e que tem uma rápida prescrição. (ATHENIENSE, 2011)

Todos esses fatores inteferem diretamente sobre o quesito punibilidade, e a ação da Lei sobre esses crimes. Além de analisar os fatos do crime, deve-se levar em consideração as condições que ocorreu, os resultados causados, a pena do crime e como identificar o usuário para a punição adequada. (ATHENIENSE, 2011)

2.3 AUMENTO DOS CRIMES DA INTERNET

No período da pandemia houve uma alta significativa com relação aos crimes virtuais, isso em razão da maioria das pessoas começar a utilizar mais o meio virtual para realizar trabalhos e manter contato social. Isso tudo impulsionou os usuários ativos e aumentou as

horas de acesso na internet. (SANTOS, 2021)

Os cibercriminosos conseguiram mais oportunidades de realizar os delitos que já ocorriam anteriormente, dentre eles utilizar as redes para extorsão, roubo de dados bancários, acesso a informações pessoais das vítimas, roubo de cartão, falsos sequestros, e diversos outros crimes. (SANTOS, 2021)

Segundo a ABINC (Associação Brasileira de Internet das Coisas):

Este tipo de crime cresceu cerca de 500% entre 2018 e 2020. Só neste ano, de janeiro até maio, o aumento foi de 116%. O aumento significativo dos valores de resgates também assusta. Os prejuízos deste tipo de ataque devem atingir US\$ 20 bilhões este ano. Isso tem relação com as técnicas de sequestro digital que evoluíram de computadores infectados aleatoriamente nas organizações para sequestro de linhas inteiras de produção de bens ou serviços (ABINC, 2021).

O aumento em ocorrências de crimes virtuais se torna um problema maior a medida que os usuários aumentam e seus acessos em aplicativos e sites disponíveis na internet se tornam ferramentas para que criminosos possam exercer condutas prejudiciais, como roubar informações de cartões de crédito e senhas. (SANTOS, 2021)

3 O POSICIONAMENTO LEGAL COM RELAÇÃO AOS CRIMES DA INTERNET

Para que exista o entendimento de crime na legislação brasileira, é necessária clareza na definição do bem jurídico que é tutelado nos delitos, bem como os critérios existentes para tal definição. Fernando Capez (2017) relata que não se fala em crime se a ação não apresentar perigo concreto, ao bem jurídico tutelado.

O Art. 1º do Código Penal Brasileiro, dispõe: “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal” (Brasil, 1940), portanto o crime é a violação de uma norma expressa em Lei. Pode ainda ser definido como uma transgressão das normas sociais estabelecidas, ou seja, legalmente instituída por uma autoridade política. (DIAS, 2010)

O Direito Penal tem sua aplicação realizada quando existe uma conduta que fere o que esta no regulamento legal, assim ofendendo o interesse social e legal, pois o Código Penal, utiliza como base princípio da ofensividade, que é a análise da ofensa ao bem jurídico e a partir disto ocorre a punição penal contra o individuo que realizou tal conduta delitiva. (CAPEZ, 2017).

O Código Penal, é feito de normas coercitivas, assim, tem por objetivo impedir os delitos antes da ocorrência destes, por meio de sanções penais, que não são arbitrárias, e devem estar em sintonia com direito constitucional. Como relata Callegari (2018, p.20): “As normas proibitivas devem também cumprir uma finalidade socialmente justificada, segundo assim se delibere no campo da política criminal. Essa função, modernamente, em tempos

mais recentes, é a de prevenção de novas infrações”.

Existe uma dificuldade em classificar e identificar os crimes virtuais, uma vez que, a tecnologia evolui de forma recorrente, assim, as definições de doutrinadores mudam constantemente, em decorrência disto existe a Perícia Forense Computacional, destinada aos crimes na esfera digital.

Segundo Augusto Rossini (2004, p.113):

[...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Se houvesse atualização nas normas que tipificam atualmente crimes virtuais com o objetivo de amplificar as classificações destes, seria uma forma de diferenciar e facilitar a punição e identificação de padrões, pois muitos possuem características específicas, como um sujeito determinado, forma de execução do crime e consumação igual, como relata Roberto Chacon de Albuquerque (2006).

Ainda com entendimento do mesmo autor, os novos doutrinadores tem a capacidade de contribuir com ideias para combater a impunidade com relação a alguns crimes virtuais, além de reduzir o número de criminosos na internet, e com isso os crimes virtuais, pois faria valer a ideia de prevenção por penas coercitivas em casos de crimes cibernéticos.

3.1 LEGISLAÇÃO PERTINENTE AOS CRIMES CIBERNÉTICOS

No Direito Penal, identificar os autores de tais contravenções é uma tarefa complexa, existem no Brasil algumas delegacias especializadas em crimes virtuais, em algumas capitais brasileiras. Até por volta de 2012, não existiam legislações específicas para crimes virtuais, portanto a internet acabou se tornando um facilitador para os usuários que utilizavam a rede de computadores para cometer atos ilícitos, já que na maioria dos casos não era necessário o complemento para a consumação de ameaças ou agressões a outros bens jurídicos, apenas o conhecimento informático era suficiente para as práticas ilícitas. (VIANNA et al, 2013).

Ainda segundo o mesmo autor, a promulgação da Lei nº 12.737 em 2012, que ficou conhecida como Lei Carolina Dieckmann, houve a inclusão no Código Penal Brasileiro os artigos 154-A e 143-B, que busca responsabilizar os infratores virtuais, após isso veio então a promulgação da Lei 12.965 de 2014, denominada Marco Civil da Internet.

Os bens de origem informática e informações virtuais foram regulamentados pelo ordenamento jurídico brasileiro, mas a sociedade como um todo está em constante evolução, assim existem condutas que não se encontram elencadas ainda em lei, não

possibilitando a punição devido ao princípio da legalidade que se encontra na Constituição Federal, art. 5º, XXXIX “Não há pena sem lei anterior que o defina, nem pena sem prévia cominação legal”. (BRASIL, 1988)

A Lei nº 12.737/2012, é de extrema importância para a proteção das vítimas de crimes virtuais, pois aplica punição com relação a quebra de segurança de qualquer aparelho informático, isso tem por objetivo impedir a conduta delituosa do criminoso em tentar utilizar da rede de informação pessoal de algum usuário na internet para obter informações sem o consentimento do titular, o que viola diretamente a privacidade e gera diversos prejuízos. (JUNIOR, 2013)

Para a aplicação da legislação é necessário que o dispositivo informático tenha meios de segurança, sejam eles senhas, ou algum antivírus, pois, o caput do artigo 154-A, conceitua expressamente a necessidade de existir um programa de proteção para a configuração do crime de violação, caso não exista tal recurso, acaba por se tornar uma conduta atípica, por diferir do texto legal. (BRASIL, 2014)

O entendimento doutrinário tem divergências com relação a diferença entre os aparelhos que possuem ou não proteção, já que legalmente falando, todos os dispositivos deveriam ser protegidos pelo direito. Além do fator que as penas existentes para cobrir tais delitos acabam por ser desproporcionais ao que os criminosos praticam em suas condutas. Por se tratar de uma pena menor, ocorre a rápida prescrição, e isso dificulta a punibilidade do autor do crime. (SOUZA, 2015)

A Lei 12.737/2012 se tratou de avanço significativo no ordenamento jurídico brasileiro pois existia uma falha no referente a matéria de crimes informáticos, já com relação ao Marco Civil da Internet, Lei nº 12.965/2014, significou um implemento na Lei já existente, pois definiu critérios para maior proteção da privacidade dos usuários da rede, os aplicativos e sites existentes na internet deveriam se atentar mais a privacidade, não mais permitindo a troca de informação entre as redes existentes sem que o usuário possuísse conhecimento de tal fato, assim a violação da proteção dos dados pessoais somente seria passível de violação com decisão judicial.

O artigo 7º da lei acima citada, se atenta a privacidade do usuário, informando a inviolabilidade com relação as informações pessoais, e proteção com relação a sua vida privada, gerando mais segurança. Expressa também a importância do sigilo de comunicações privadas e direitos do usuário com relação ao ambiente virtual. (BRASIL, 2014)

O artigo 19 trata da questão da liberdade de expressão, que deve ser assegurada pois se encontra expresso em texto constitucional, assegura também os provedores de internet, que só serão responsabilizados pela conduta de terceiros em caso de neutralidade, quando não tomarem as devidas providências dentro do prazo estabelecido. Ainda relata nesse

artigo, a impossibilidade de existir distinção entre provedores de internet, pois os dados devem possuir um tratamento semelhante, deixando a escolha do usuário qual provedor ele irá utilizar. (BRASIL, 2014)

O Marco Civil da Internet, juntamente com outras legislações e projetos de Lei, tem por objetivo assegurar a privacidade do usuário, protegendo os dados pessoais, e especificando os direitos e deveres, incluindo dos provedores de internet, para que o ciberespaço seja um lugar seguro e possa ser utilizado por todos de forma adequada. (BRASIL, 2014)

4 FAKE NEWS NA SOCIEDADE CONTEMPORÂNEA

Com relação a comunicação em geral, houve avanços significativos que proporcionaram um progresso maior a sociedade em geral. A internet quebrou barreiras de comunicação e trouxe a possibilidade de interação entre várias pessoas ao mesmo tempo independente da distância. O mundo virtual conseguiu aproximar as pessoas, facilitou o acesso a informação em geral, porém também existem desvantagens dessa mesma evolução, a facilidade de espalhar notícias e o acesso de várias pessoas de forma rápida e contínua, também possibilitou a propagação de notícias falsas, e isso se tornou um problema preocupante. (PEREIRA, 2018)

Com relação ao grande fluxo de notícias que circulam na internet todos os dias, é ressaltado a falta de instrução dos usuários que estão utilizando o meio virtual, pois com a falta de informação adequada e a praticidade de espalhar conteúdo na internet, propicia a propagação de notícias falsas e que causam prejuízos a outros usuários e gera manipulação de conteúdo muitas vezes já disponível no mundo virtual. Com esse contexto existe um conflito direto entre a liberdade de expressão, que é um direito garantido a todos, e o problema com as chamadas *Fake News*. (FALCONI E SOBREIRO, 2018).

As *fakes news*, como já sugere o nome, é a disseminação de notícias falsas, com o objetivo de distorcer ou manipular informações para gerar tumulto ou causar uma vantagem, seja política ou econômica, independente da finalidade, causando tumulto e problemas no âmbito social em geral dependendo do alcance e da gravidade da informação que foi alterada. (PEREIRA, 2018).

4.1 CONSEQUÊNCIAS DAS FAKE NEWS

As matérias que são divulgadas com conteúdo alterado, mesmo que parcialmente real, que foi modificado para causar uma outra percepção sobre a notícia, chega a vários usuários, e gera conflito, pois tem o poder de confundir, isso se torna ainda mais complicado quando se trata pessoas com menos instrução sobre o meio tecnológico, pois esta tem mais dificuldade em identificar informações modificadas e com conteúdo falso, isso acaba por

espalhar mais as informações, e a dificuldade em corrigir a informação fica maior. (MORONI, 2019)

Os usuários que acabam modificando e espalhando essas notícias alteradas, por vezes tem por objetivo favorecer a si mesmo ou a alguém, em razão desse objetivo, pegam matérias verdadeiras e alteram pontos específicos que mudam o contexto deixando estas notícias semelhantes a real informação. Um exemplo que ocorre bastante, são modificações ou criação de *fake news* sobre informações políticas, onde alterar o conteúdo pode gerar vantagem a determinado político ou prejudicar um adversário, com base em informações distorcidas ou falsas. (LOBO; et al, 2018)

Ao contrário do que muitos pensam, as *fakes news*, não são um problema recente, mas se popularizou agora devido a facilidade e aumento dos casos, na Rússia em 1990, houve a criação de um canal em uma emissora de televisão que alterava a visão sobre situações em relação a política, na época a comunicação era mais limitada, e não possuía tantos recursos de propagação de informação, a televisão era um meio de informar e criar opiniões para quem acompanhava, portanto as notícias expressas ali possuíam um grande poder para gerar opiniões e alterar o posicionamento social. (PENA, 2018)

É preocupante o aumento dos casos de notícias falsas, visto que a maioria da população possui acesso as mídias digitais, atrelado com a facilidade existente de manipular dados e informações, e as consequências que essas percepções podem gerar em escala maior devido a globalização das informações, se torna um grave problema que precisa de maior atenção. (MORONI, 2019)

A internet não foi o que ocasionou a criação das *fake news*, como já foi relatado é um problema que acontecia anteriormente, porém com a criação da internet se tornou mais simples realizar essa conduta de alteração de informações. O problema é a ampliação da gravidade desse meio. As *deep fake news*, são um conceito de notícias falsas que são mais graves, se tratam de uma modificação em proporção maior, como utiliza da tecnologia disponível para criar imagens e vídeos que não existem, para espalhar informações de forma a parecer mais real e confundir ainda mais os usuários. (ALMEIDA ET AL, 2018)

4.2 POSICIONAMENTO LEGAL SOBRE AS *FAKE NEWS*

É importante discorrer sobre formas possíveis de impedir tais condutas que ocasionam tantos problemas e acabam gerando um tumulto que poderia ser evitado. A internet é um ambiente que a maioria das pessoas tem acesso e utiliza no cotidiano para conversar, trabalhar, se manter informado, por ser um meio de comunicação global, grandes líderes políticos, utilizam também para controlar e tomar decisões importantes sobre a forma de governar. A União Europeia, buscou meios de regulamentar a propagação de notícias, de modo que fosse possível aumentar a veracidade de informações que seriam publicadas,

buscando conferir as fontes antecipadamente, uma forma de controle para diminuir as *fake news* e ainda sim manter o direito de expressão dos cidadãos. (ALMEIDA ET AL, 2018)

A Alemanha alterou a Lei sobre redes Sociais que estipula que os fornecedores de dados, teriam um prazo de vinte e quatro horas para realizar a correção ou excluir notícias falsas ou incompletas, esse prazo se faz valer a partir de informação judicial sobre o erro da notícia ou de reclamação feita por algum usuário que se sentiu prejudicado. (CARVALHO, 2018)

Analisando a postura de demais países com relação a coibir as *fake news* utilizando a lei e métodos coercitivos para essa redução e controle, o Brasil deveria adotar a mesma postura com relação a tomar providências mais reguladoras e uma postura mais rígida, pois isso influencia diretamente sobre os atos sociais, sejam eles políticos ou sobre um usuário em particular, e por vezes isso poderia ser evitado de forma mais simples. (PAESANI, 2014)

Ainda com posicionamento do mesmo autor, observa-se que o direito penal é uma resposta a atos sociais, conforme a Teoria da Tridimensionalidade de Miguel Reale, onde regulamenta que uma lei surge a partir de um conflito social, o direito surge para regular uma conduta prejudicial e buscar meios de evitar que ela se torne recorrente.

O fato, valor e a norma são os componentes existentes sobre a teoria tridimensional do Direito. O fato em si é a conduta que ocorre em sociedade, isso tem um peso, esse seria o valor. Onde aquela conduta afeta a vida em conjunto e como isso causa prejuízos a um todo. Para sancionar e impedir nova ação igual surge a norma que é a forma reguladora que o direito utiliza. Uma teoria que interliga diretamente a ocorrência do fato, ao valor que isso resultou e a norma que surgiu em decorrência da ação. (REALE, 2003)

Nesse viés tem-se os projetos de Lei nº 6.812/2017 e o 7.604/2017 que possuem a intenção de punir as notícias de cunho inverídico e responsabilizar quem propagou a notícia em questão. Visto que a incidência de notícias falsas pode inclusive levar as pessoas a agirem errado imaginando estar em conformidade com a lei, por acreditar em uma afirmação equivocada.

Um exemplo de regulamentação presente no Projeto de Lei nº 6.812/2017 é:

Art. 1º Constitui crime divulgar ou compartilhar, por qualquer meio, na rede mundial de computadores, informação falsa ou prejudicialmente incompleta em detrimento de pessoa física ou jurídica. Penal- detenção de 2 a 8 meses e pagamento de 1.500 (mil e quinhentos) a 4.000 (quatro mil) dias-multa.
Art. 2º Os valores decorrentes da imposição da multa a que se refere o artigo primeiro serão creditados à conta do Fundo de Defesa dos Direitos Difusos – CFDD. (BRASIL, 2017)

Um obstáculo para a aprovação ou sugestão de mais normas sobre esse assunto em questão, é que diversos projetos de lei que já foram apresentados não podem ser aprovados por entrar em conflito direto com a Constituição que garante a todos a liberdade de

expressão. O limite entre regular o que é divulgado todos os dias por meio de perfis sociais e aplicativos na internet e a censura, é uma linha tênue que acaba por dificultar uma regulamentação mais rígida sobre as notícias falsas. (GRIGORI, 2018)

Os doutrinadores também dividem opiniões com relação a sancionar ou não as *fake news*. O fato de ser necessário analisar os direitos de cada usuário sem restringir o acesso a informação, ou deixar de ferir a liberdade em utilizar das redes para se comunicar e expressar o que desejar e ainda conciliar isso ao interesse público de punir os criminosos cibernéticos que utilizam das redes para tumultuar e gerar problemas é um grande desafio. (LIMA, 2013)

Não existe ainda uma lei exata que fale sobre as *fake news* de forma específica, visto que como já citado, depende de uma adequação entre punir o delito e não ferir a norma constitucional que trata sobre a liberdade individual de cada um. Pode ocorrer uma confusão com relação aos artigos do Código Penal que tratam sobre calúnia e difamação, essa regulamentação depende que o nome da pessoa prejudicada esteja diretamente ligado a informação distorcida, isso que tipifica o crime para a legislação, assim não inclui a sociedade em geral, pois depende de especificar a pessoa prejudicada para a imposição de uma sanção. As *fake news* atingem um grupo social em grande parte das ocasiões, e em decorrência da notícia propagada, tem efeitos sobre a política, saúde e outras áreas vitais da sociedade. (BURG E GREGGO, 2018)

O que acaba por julgar a maioria dos projetos de Lei serem inconstitucionais, e impede em parte a punição maior sobre as notícias falsas, é o artigo 220 da Constituição Federal, que relata:

Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição. § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV. (BRASIL, 1988)

Existem jurisprudências que por entender que se tratava de liberdade de expressão, aplicou sentença negando provimento de recurso sobre a *fake news*, por um entendimento majoritário sobre o assunto. Um exemplo é uma decisão proferida pelo Tribunal Regional Eleitoral do Amapá (TRE-AP):

ELEIÇÕES 2018. AGRAVO INTERNO. REPRESENTAÇÃO ELEITORAL. REMOÇÃO DE CONTEÚDO DA INTERNET. FAKE NEWS. AUSÊNCIA. NÃO PROVIMENTO. 1. Não observada a ocorrência de postagem de conteúdo ofensivo e sabidamente inverídico, não configura propaganda negativa a ensejar reprimenda pela justiça eleitoral, na medida em que consiste em mero exercício da liberdade de expressão. 2. Recurso a que se nega provimento. (TRE-AP - RP: 060158873 MACAPÁ - AP, Relator: RIVALDO VALENTE FREIRE, Data de Julgamento: 25/04/2019, Data de Publicação: DJE - Diário da Justiça Eletrônico - TRE/AP, Tomo 71, Data 03/05/2019, Página 9).

O que ajuda na correção de notícias falsas atualmente, é a imprensa realizar retratações sobre as informações incorretas que circulam na mídia, além de emitir alertas por meio da internet sobre os riscos de acreditar em todas as notícias sem buscar saber a veracidade da informação ali presente. (GRIGORI, 2018)

CONCLUSÃO

Como exposto anteriormente no decorrer do texto, os crimes virtuais se tornaram um problema com maior ocorrência, e a utilização em grande escala por pessoas de todo o mundo facilitam os delitos que ocorrem no ciberespaço, isso interfere diretamente na legislação, que tem por dever acompanhar e oferecer proteção as pessoas que utilizam a internet para meios de comunicação e trabalho, além de vários outros recursos que facilitam o cotidiano.

Com a globalização os meios virtuais tornaram-se indispensáveis no cotidiano dos brasileiros, assim como de toda a população mundial, principalmente pelo fácil acesso e pela praticidade em armazenamento e para a própria comodidade, isto porque, o usuário da rede mundial de computadores pode realizar as mais diversas condutas. Assim, surge aqueles indivíduos que utilizam tal facilidade cibernética como meio de realizar atividades delituosas.

Durante tempos após o advento da internet, as condutas realizadas virtualmente não sofriam punição por falta de uma legislação que realizasse essa regulamentação específica. Pois em relação ao princípio da legalidade, só pode existir o crime com prévia cominação legal. Com a criação Lei nº 12.737, a internet passou a ter mais restrições sobre crimes quanto as legislações específicas.

Existe ainda uma dificuldade em processar e julgar tais crimes, visto que a pena muitas vezes é pequena e de rápida prescrição. O que acaba por impedir muitas vezes a execução legal do processo sobre crimes virtuais, além disso, é escasso as Delegacias de Repressão aos Crimes de Informática (DRCI).

É necessária maior especialização de profissionais sobre essa área de crimes da internet e uma maior base para realizar a aplicação adequada da lei, para reduzir os delitos ocorridos e consequentemente tornar o ambiente virtual um meio mais seguro para seus usuários. Impedindo assim a criação de perfis falsos, a disseminação de *fake news*, e a redução de problemas como o *ciberbullying* e outras variáveis que ocorrem por não existir uma punibilidade adequada.

As legislações apresentadas, Lei n. 12.737/2012 e Lei n. 12.965/14 são um marco importante visto a evolução constante da tecnologia no mundo todo. Esse avanço necessita ser acompanhado por mais legislações que possam regular e se adequar aos novos

problemas que podem surgir sobre a esfera virtual. Incluindo legislações mais específicas sobre as fakes news, e uma forma de reduzir essa prática que está cada vez mais comum nas redes em geral.

Conclui-se, que o Brasil, assim como diversas partes do mundo, realizou avanços na tecnologia em geral, e com esses avanços vieram facilidades e usuários que utilizam dessa facilidade para a prática de condutas criminosas. A Lei Carolina Dieckmann, e a Lei n. 12.965/14, considerada o Marco Civil da Internet, além dos projetos de lei existentes, são de grande avanço para redução das atuações dos cibercriminosos, porém necessitam de mais complementos e especificações que possam auxiliar o judiciário na punição efetiva de tais condutas e assim realizar de forma eficiente a proteção aos usuários da internet e obter um controle maior da cibercriminalidade.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006.

ALEXANDRE, Luana. **Como identificar usuário na internet?** Disponível em: <<https://advluanaalexandre.jusbrasil.com.br/artigos/1167302217/como-identificar-usuario-na-internet#:~:text=Cada%20m%C3%A1quina%20tem%20um%20registro,identifica%C3%A7%C3%A3o%2C%20definido%20segundo%20par%C3%A2metros%20internacionais>>. Acesso em: 15 abr 2022.

ATHENIENSE, Alexandre. **Falta de lei sobre crimes virtuais leva à impunidade, diz especialista**. Disponível em: <<https://alexandre-atheniense.jusbrasil.com.br/noticias/2530003/falta-de-lei-sobre-crimes-virtuais-leva-a-impunidade-diz-especialista>>. Acesso em: 11 abr 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 02 mar 2022.

_____. **Decreto-Lei No 2.848, de 7 de dezembro de 1940**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 29 fev 2022.

_____. **Lei N° 12.737, de 30 de novembro de 2021**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 02 mar 2022.

_____. **Lei N° 12.965, de 23 de abril de 2014**. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 02 mar 2022.

_____. **Projeto de lei N.º 6.812, de 2017**. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=7A9EB8D0E28DCD9F0C65C29832FBF82A.proposicoesWebExterno1?codteor=1562966&filename=Avulso+-PL+6812/2017>. Acesso em: 15 mar 2022.

_____. **Projeto de lei N.º 7604, de 2017**. <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2136633>>. Acesso em: 17 mar 2022.

BURG, Daniel; GREGGO, Marcela. **Criminalização das Fake News pede um novo tipo penal**. Disponível em: <<https://www.conjur.com.br/2018-fev-27/opiniao-criminalizacao-fake-news-tipo-penal>>. Acesso em: 27 mar 2022.

BURKE, Gabriela. **Perfil Fake nas redes sociais e crimes virtuais**. Disponível em: <<https://burke.com.br/publicacoes/perfil-fake-nas-redes-sociais-e-crimes-virtuais>>. Acesso em: 26 fev 2022.

CALIFORNIA, AB. 1104 **Lei de Redução da Fraude Cibernética Política da Califórnia**. Disponível em: <https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1104#:~:text=AB%201104%2C%20Chau.->

,The%20California%20Political%20Cyberfraud%20Abatement%20Act.,of%20political%20cyberfraud%20as%20defined>. Acesso em: 14 mar 2022.

CANÁRIO, Pedro; SENNA, Carlos. **Não importa existir liberdade de imprensa se a sociedade não confia nos jornais**. Disponível em: <<https://www.conjur.com.br/2018-ago-19/entrevista-david-mccraw-advogado-new-york-times>>. Acesso em: 01 abr 2022.

CAPEZ, Fernandes. **Curso de Direito Penal: Parte Especial – Arts. 121 a 212**. Saraiva, 2017.

CARVALHO, Gustavo Arthur Coelho Lobo de. **O Tratamento Jurídico das Notícias Falsas (fake news)**. 2018

DIANA, Daniela. **História da Internet**. Disponível em: <<https://www.todamateria.com.br/historia-da-internet/>>. Acesso em: 14 fev. 2022.

DIAS, Reinaldo. **Introdução à Sociologia**. 2 ed. São Paulo: Pearson Prentice Hall, 2010.

FABIANO, Célio. **Endereço IP: o que é e 5 coisas que você precisa saber**. Disponível em: <<https://blog.hosts.green/endereco-ip/>>. Acesso em: 09 abr 2022.

FALCONI, Clarissa; SOBREIRO, Talita. **Liberdade de expressão na era das notícias falsas e manipuladas de conteúdo político-eleitoral**. Disponível em: <<http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/7014>>. Acesso em: 10 mar 2022.

FOLTÝN, Tomas. **Entenda como a superexposição em redes sociais pode trazer problemas**. Disponível em: <<https://www.welivesecurity.com/br/2018/06/29/entenda-como-superexposicao-em-redes-sociais-pode-trazer-problemas/>>. Acesso em: 20 fev 2022.

GRIGORI, Pedro. **Projetos de lei no Congresso pretendem criminalizar fake news**. Disponível em: <<https://apublica.org/2018/05/20-projetos-de-lei-no-congresso-pretendem-criminalizar-fake-news/>>. Acesso em: 19 mar 2022.

LIMA, Marcia. **O estatuto teórico epistemológico do direito à informação no contemporâneo: das dimensões aos limites**. Disponível em: <<https://periodicos.ufpb.br/index.php/pbcib/article/view/22389>>. Acesso em: 21 mar 2022.

MENESES, João. **Como as leis estão a definir (e a criminalizar) como notícias falsas**. <Disponível em: <https://journals.openedition.org/cp/5423?lang=en>>. Acesso em 19 mar 2022.

MORONI, Juliana. **Possíveis impactos de fake news na percepção da ação coletiva Complexivas**. Revista de Filosofia Temática, v. 3,2019.

NASCIMENTO, Anderson **O que é cibercrime?** Disponível em: <<https://canaltech.com.br/seguranca/O-que-e-cibercrime/>>. Acesso em: 22 fev 2022.

NAZARETH, Rodrigo Trisoglino. **Saúde e mídia social: As fakes news que matam**. Unisanta Law and Social Science, v. 7, n. 3, 2019.

ONU. **Declaração dos direitos humanos**. Disponível em: <<http://www.dhnet.org.br/direitos/deconu/textos/integra.htm>>. Acesso em: 05 abr 2022.

PACELLI, Eugênio. **Manual de Direito Penal: Parte Geral**. 5 ed. Grupo Editorial Nacional, 2018.

PAESANI, Liliana Minardi. **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil**. 7. Ed. São Paulo: Atlas S.A, 2014.

PENA, Lara. **Fake news: uma breve análise acerca de sua trajetória internacional, consequências políticas e perspectiva jurídica**. Disponível em: <<http://www.periodicos.ufc.br/dizer/article/view/39923>>. Acesso em: 11 mar 2022.

PEREIRA, Rodolfo Viana. **Direitos políticos, liberdade de expressão e discurso de ódio: volume I**. 2018.

QUINELATO, Rosangela. **Benefícios e Malefícios da Internet**. Disponível em: <<https://www.blogdovestibular.com/atualidades/beneficios-e-maleficios-da-internet.html>>. Acesso em: 17 fev. 2022.

QUINTINO, Eudes. **A nova lei Carolina Dieckmann**. Disponível em: <<https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann>>. Acesso em: 05 mar 2022.

REALE, Miguel. **Teoria Tridimensional do Direito**. 5ª ed., Editora Saraiva, São Paulo, 2003.

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

SANTOMARO, Beatriz. **Cuidados na internet**. Disponível em: <<https://novaescola.org.br/conteudo/1525/cuidados-na-internet>>. Acesso em: 19 fev 2022.

SCHMIDT, Guilherme. **Crimes Cibernéticos**. Disponível em: <<https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>>. Acesso em: 22 fev 2022.

SILVA, Leonardo. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA**. Disponível em: <<https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml>>. Acesso em: 12 fev. 2022.

SOUZA, Larissa Anne de Moraes. **A dificuldade da repressão aos crimes virtuais**. 2015.

TATEOKI, Victor. **Classificação dos Crimes Digitais**. Disponível em: <<https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais>>. Acesso em: 25 fev 2022.

TIINSIDE. **Crimes cibernéticos triplicam em 2021 e extorsão digital entra na rotina do brasileiro**. Disponível em: <<https://tiinside.com.br/26/08/2021/crimes-ciberneticos-triplicam-em-2021-e-extorsao-digital-entra-na-rotina-do-brasileiro/#:~:text=%E2%80%9CEste%20tipo%20de%20crime%20cresceu,US%24%2020%20bilh%C3%B5es%20este%20ano>>. Acesso em: 26 fev 2022.

TIMOCHENCO, Longinus. **Deep web e dark web: Os perigos da web profunda e obscura**. Disponível em: <<https://infranewstelecom.com.br/deep-web-e-dark-web-os-perigos-da-web/>>. Acesso em: 20 fev 2022.

VIANNA, Túlio. **Crimes informáticos**. Túlio Vianna; Felipe Machado – Belo Horizonte: Fórum, 2013.