



LEGISLATIVA NA TIPIFICAÇÃO DOS CRIMES CIBERNÉTICOS E A SUA INTENSIFICAÇÃO COM O AUMENTO DE USUÁRIOS NA INTERNET EM GOIÁS

FUNDAMENTAL RIGHTS OF PEOPLE WITH DISABILITIES IN PENITENTIARY

Maria Laura Cordeiro Da Silva¹, Adenevaldo Teles Junior², Luciângela Ferreira do Brasil³, Maisa Binquine⁴

¹Discente do curso de Direito na Faculdade Evangélica de Goianésia

² Docente na Faculdade Evangélica de Goianésia, Mestre em Direito Agrário pela UFG

³ Docente na Faculdade Evangélica de Goianésia, Mestre em Direito Agrário pela UFG

⁴ Docente na Faculdade Evangélica de Goianésia, Especialista em Direito Público Municipal

Info

Recebido: 06/2021

Publicado: 20/07/2021

ISSN: 2596-2108

Palavras-Chave: Crimes Virtuais.

Internet. Omissão Legislativa.

keywords: Virtual Crimes. Internet.

Legislative Omission.

Resumo

Com o aumento dos usuários de internet no Brasil também houve o crescimento dos crimes realizados de maneira virtual, todavia a legislação não acompanha essa evolução e deixa lacunas para medidas de prevenção e repressão. Com o tema em direito penal, mais especificamente sobre os crimes cibernéticos, o presente artigo tem como objetivo tratar sobre a omissão legislativa a respeito dos cibercrimes, bem como analisar a legislação sobre o tema já existente e aquelas ainda em tramitação como projeto de lei. Ainda, visa a análise de princípios e direitos fundamentais que devem ser respeitados a fim de manter um ambiente virtual seguro. Tem como objetivo geral tratar acerca da omissão

legislativa na tipificação dos crimes cibernéticos, e como objetivos específicos abordar os detalhes e definições dos crimes virtuais; analisar os cibercrimes em uma esfera constitucional; e tratar sobre a omissão legislativa existente, mesmo com a extrema necessidade de tipificação do ilícito em razão de seu aumento devido ao crescimento de número de usuários na internet. Para tanto, foi utilizada metodologia baseada na revisão literária, em que a pesquisa ocorre por meio da seleção de doutrinas, artigos científicos e diplomas legais e constitucionais. Como resultado, foi observado que apesar de já existir algumas leis em vigor versarem sobre a temática, há, ainda, uma grande lacuna legislativa sobre os crimes virtuais.

Abstract

With the increase of internet users in Brazil, there was also an increase in crimes carried out online, however the legislation does not follow this evolution and leaves gaps for prevention and repression measures. With the theme of criminal law, more specifically on cybercrime, this article aims to address the legislative omission regarding cybercrime, as well as analyze the existing legislation on the subject and those still in progress as a bill. It also aims to analyze fundamental principles and rights that must be respected in order to maintain a safe virtual environment. Its general objective is to deal with the legislative omission in the classification of cyber crimes, and as specific objectives to address the details and definitions of cyber crimes; analyze cybercrime in a constitutional sphere; and deal with the existing legislative omission, even with the extreme need to typify the illicit due to its increase due to the growth in the number of internet users. Therefore, a methodology based on literary review was used, in which the research takes place through the selection of doctrines, scientific articles and legal and constitutional diplomas. As a result, it was observed that although there are already some laws in force dealing with the subject, there is still a large legislative gap on virtual crimes.

Introdução

O presente artigo parte da problemática acerca da definição e punição dos crimes virtuais

no Brasil, bem como seu aumento devido ao crescimento de usuários na internet. Com o escopo de facilitar o desenvolvimento da temática

proposta estabelece-se como problemática o seguinte questionamento: como a omissão legislativa contribui para o aumento dos crimes cibernético? Quais medidas vêm sendo tomadas pelo poder legislativo para sanar essas omissões?

Dessa maneira, objetiva demonstrar as omissões legislativas no que tange a temática proposta, bem como a análise das medidas que constitucionalmente devem ser adotadas pelo Poder Legislativo a fim de tipificar condutas criminosas realizadas na internet em território brasileiro. Assim, o artigo tem como dever, durante o seu desenvolvimento, responder e apresentar uma solução para o problema previsto.

Este artigo se justifica pela relevância temática ao tratar sobre os crimes virtuais, haja vista que esse ilícito tem se tornado cada vez mais frequente devido ao crescimento do uso da internet no Brasil. Esse crescimento de usuários foi extremamente significativo, como demonstra Valente (2020) que informa os dados da pesquisa realizada pela Agência Brasil, na qual demonstra que em 2010 o Brasil tinha 37,9 milhões de usuários na internet e esse número passou para 134 milhões no ano de 2020. Nesse interim, busca-se tratar sobre como a legislação prevê medidas repressivas e preventivas para suprimir o aumento dos cibercrimes.

Como forma de possibilitar a solução da problemática, o presente artigo tem como objetivo compreender porque há omissão legislativa a respeito dos crimes virtuais, abordar e analisar as legislações já vigentes e as lacunas legislativas nelas existentes, bem como os projetos de leis. Ainda, analisar-se-á os princípios e direitos fundamentais infringidos pelos crimes cibernéticos, como a

dignidade da pessoa humana e a liberdade de expressão.

Para tanto, o artigo será dividido em três tópicos. O primeiro tópico trata sobre a origem dos crimes virtuais, onde será esmiuçado os conceitos e características dessa modalidade de prática ilícita. Neste tópico, é abordado também, as legislações infraconstitucionais existentes no Brasil, como a Lei Carolina Dieckmann – Lei nº 12.965/14, o Marco Civil da Internet – Lei nº 12.965/14 e a Lei Geral de Proteção de Dados – Lei nº 13.709/18.

No segundo tópico será desenvolvida a noção de constitucionalidade das normas que tratam sobre os crimes cibernéticos, ou seja, quais os princípios constitucionais (dignidade da pessoa humana, liberdade de expressão, entre outros) que respaldam a necessidade de se propiciar um ambiente virtual segura, com leis que tipificam os crimes cometidos virtualmente. Bem como, é abordado a respeito dos prejuízos da omissão legislativa para os direitos fundamentais.

No terceiro tópico é apontado os problemas relacionados à omissão legislativa, ou seja, serão analisadas suas causas. Isto é, se a ausência de normas que tipifiquem as condutas criminosas na internet, podem ser parte de uma estratégia ou apenas morosidade do Poder Legislativo ou, ainda, se o problema está nos operadores do Direito. Ainda, serão observadas as questões socioculturais envolvidas na temática e os projetos de lei em tramitação.

Dessa maneira, o presente trabalho visa contribuir com pesquisas fundadas em dados verídicos sobre os principais cibercrimes, bem como o que leva os indivíduos a incorrerem sobre fraudes na internet, além das facilidades que o

anonimato propicia aos criminosos cibernéticos. Assim sendo, este se justifica na adequação da humanidade aos avanços tecnológicos, de forma que os direitos fundamentais, principalmente a liberdade de expressão, conforme a Constituição Federal Brasileira de 1988 em seu artigo 5º, seja garantida e não violada nos meios digitais.

Por fim, a pesquisa será enquadrada na modalidade de revisão da literatura, tendo em vista que será realizada por meio de arquivos bibliográficos e levantamento documental, fazendo uso de doutrinas, artigos científicos e dispositivos legais e constitucionais. Para a produção do material de pesquisa cumpre destacar alguns autores que serão essenciais, como Lenza (2019), Nascimento (2019), Senna e Ferrari (2020), Vieira e Brito (2019), Greco (2010), entre outros.

1. ASPECTOS CONCEITUAIS E LEGISLATIVOS DOS CRIMES CIBERNÉTICOS

Como dizia a filosofia de Aristóteles, “o homem é um ser político”, e desde seus primórdios este nasceu para ser sociável, para viver em comunidade e comunicar-se entre os demais homens. Com essa convivência, requer-se um regime que detenha as regras com intuito de uma harmonia social e uma adequada vida em comum, a fim de que conflitos sejam liquidados ou ao menos evitados; e assim surge as primeiras concepções de Direito.

Para Kelsen (1997 apud YOKOHAMA, 1999 p. 22), o direito tem sentido de coação,

expondo que a “coatividade é a característica essencial da própria definição, ou conceituação, do jurídico”; e dessa maneira, trata-se de um sistema impositor que se encarga de regulamentar determinadas condutas humanas.

Com a sociedade em constante mudança é imprescindível a premência em modernizar, adaptar e se enquadrar conforme as modificações forem surgindo. Nesse sentido, o Direito trabalhado por Kelsen traz consigo esse mecanismo de readaptação, sendo um mosaico de possibilidades que se modificam para abranger as inovações. Estas modernizações carecem de leis e intromissão do Estado para regulamentar e assegurar os direitos garantidos a todos, isto em qualquer variante, seja ela física ou digital.

Uma recente pesquisa informada pela Agência Brasil em 2020, demonstra que a cada quatro brasileiros, três deles possuem acesso à internet, o que soma 134 milhões de cidadãos brasileiros no total. Ademais, é considerável a frequência de acesso, porquanto “90% relataram acessar todos os dias, 7% pelo menos uma vez por semana e 2% pelo menos uma vez por mês” (VALENTE, 2020, n.p.). Outra pesquisa apontada pelo Instituto Brasileiro de Opinião Pública e Estatística (Ibope) em 2010, revela que nesta data 37,9 milhões de brasileiros eram ativos na internet.

Isto demonstra e ressalva a importância que a internet possui na vida da hodiernidade, como também o crescimento do interesse pelo mundo virtual, uma vez que é notório que em uma década a quantidade de pessoas com acesso à internet de fato triplicou. Destarte, fica evidente a velocidade em que a população está adquirindo acesso aos meios eletrônicos, e com isso surge a necessidade

de assimilar os atos praticados em âmbito virtual de acordo com as leis vigentes.

É indubitável que as condutas do ser humano em si, nem sempre serão integralmente corretas. Muitas pessoas utilizam ou adquirem certas habilidades que ao invés de maximizar o cotidiano para um mundo melhor, utiliza disso em benefício próprio. Muitas dessas ações são caracterizadas como deslizes judiciais e trazem consigo consequências. É válido mencionar que isso não é uma exclusividade do mundo real, mas também pode acontecer e acontece no mundo virtual, pois é possível considerar que a internet é uma extensão daquilo que acontece na vida real.

Isto posto, verifica-se que é primordial a aprendizagem sobre os crimes cibernéticos, em virtude que, visando o uso correto das ferramentas virtuais, a sociedade começaria a se conscientizar e entender os benefícios que a internet pode oferecer, sem estar cometendo crime algum. Além do mais, torna-se importante destacar a rapidez que a internet possui consigo; e diante disso, o perigo que se tem em compartilhar dados ou praticar atos delituosos no âmbito virtual, uma vez que a velocidade em que a ação é compartilhada e espalhada é alígero, e pode ter consequências quase irreversíveis.

Para que seja possível o melhor entendimento sobre a temática, faz-se necessário o breve apanhado histórico sobre a internet e seu surgimento. Sendo assim, como fala Monteiro (2001, p. 27): “a internet atual surgiu de uma rede idealizada em meados dos anos 60, como uma ferramenta de comunicação militar alternativa, que resistisse a um conflito nuclear mundial”. Com isso, Monteiro (2001) ressalva que havia uma

necessidade de transmitir informações de maneira que o fluxo não fosse interrompido nem corrompido pelos considerados “inimigos” em caso de guerra. Assim, foi tendo-se as primeiras redes de comunicações e a internet se fortalecendo e se adequando cada vez mais com o passar dos anos.

No que tange sobre seu surgimento no Brasil, Monteiro (2001, p. 28) refere-se que “as primeiras iniciativas no sentido de disponibilizar a internet ao público em geral começaram em 1995, com a atuação do Governo Federal”. Não existe muito conteúdo disponível aprofundado sobre o fato, porém relata-se que esta implantação tinha como finalidade estruturar-se para obter estabilidade no País, e assim, posteriormente, determinar a fixação de empresas privadas provedoras de acessos para possibilitar a expansão da quantidade de usuários (MONTEIRO, 2001).

Nesta época do surgimento da internet, a sociedade jamais imaginaria quão longe iria o avanço tecnológico e a facilidade de obtenção para o mesmo. Tendo isto em vista, segundo Colli (2009, p. 6), “apesar de a internet facilitar e ampliar a intercomunicabilidade entre as pessoas, ela pode ter sua finalidade transformada em um meio para a prática e a organização de infrações penais”. Com isso, é possível identificar que muitas pessoas se aproveitaram das ferramentas proporcionadas pela internet, como a de anonimato, por exemplo, para praticarem atitudes ilícitas e fraudar indivíduos.

Perante o exposto, fica evidente que toda invenção traz consigo benefícios e malefícios, ainda mais com uma ferramenta que detém inúmeras possibilidades, que se apresenta inovadora e singularizada. Assim como no mundo real, a liberdade de vivências e acessos que a internet

propõe requer uma legislação documentada para regulamentar os atos praticados neste ambiente virtual, não podendo ficar à cargo de cada indivíduo fazer o seu policiamento pessoal em relação ao que se pode ou não.

Nesse cenário surgem os crimes virtuais ou, como são comumente chamadas as infrações penais praticadas *online*, cibercrimes, que apesar de ter um conceito antigo trata-se de uma expressão relativamente nova, haja vista que surgiu no final da década de 1990, como explica Rocha (2017), em uma reunião do G-8 a respeito das medidas de combate para atividade ilícitas na internet.

Para Colli (2009, p. 9), “a natureza dos cibercrimes insere-os em um contexto no qual a aplicação das normas jurídico-penais internas de um Estado pode ser insuficiente para que se viabilize a instrumentalidade da investigação preliminar”. Isto porque, caso não haja uma tipificação que demonstre que aquela conduta não é permitida, não tem como classificá-la como crime, e conseqüentemente, não é possível que seja justificado um processo penal contra a pessoa que praticou determinada conduta. Portanto, o Direito Brasileiro teve que se adaptar a todas as mudanças que ocorreram com a sociedade no meio virtual.

No que se refere a definição de cibercrime a Interpol (2015 *apud* NASCIMENTO, 2019) o define como sendo uma atividade ilícita relacionada de maneira direta a qualquer prática ou ação criminosa no ambiente virtual. Sendo assim, o cibercrime nada mais é que uma conduta ilegal realizada por meio da internet, sendo os mais comuns, de acordo com Nascimento (2019, p. 8), são: “pirataria, pornografia infantil, crimes contra a honra, espionagem”, o autor ainda traz uma

definição mais elementar e detalhada de cibercrimes ao afirmar que a expressão engloba “as infrações penais praticadas no âmbito digital ou que estejam envolvidos com a informação digital através dos mais diversos meios e dispositivos conectados à internet, tais como computadores, celulares, *smartphones*, *tablets*, entre outros”.

Tendo definido a expressão “crime” frisa-se que, além das características de crime apresentadas, os crimes virtuais podem ser identificados como aqueles cometidos por meio de aparelhos tecnológicos e com condutas em um ambiente virtual (hardware, software, redes etc.) (ROCHA, 2017). Vale ressaltar, ainda que os crimes virtuais apresentam diversas espécies, como exemplos os crimes contra honra, crimes de invasão de privacidade e intimidade, crimes contra a inviolabilidade do patrimônio e crimes contra a liberdade sexual envolvendo menores de 18 anos (ASSUNÇÃO, 2018). Em razão dessa multiplicidade de espécies, não existe apenas um único tipo de crime, mas sim vários tipos que podem ser cometidos pela internet, sendo que seu diferencial pode ser constatado por meio de análise dos meios utilizados e dos danos causados.

Em pesquisa realizada pela TransUnion (empresa global de análise de informações) observa-se que os crimes virtuais mais comuns no Brasil, em especial durante a pandemia de Covid-19, foi o *phishing*, ou seja, o roubo de dados por meio de iscas falsas, como e-mails de premiações ou cobranças falsas (SAKATE, 2020). Satake (2020, p. 1) observou que “um em cada quatro brasileiros (ou 26% do total de entrevistados) foi vítima de crime envolvendo cartões de crédito”. A pesquisa colacionou dados dos cibercrimes mais

praticados durante a pandemia, e formou o seguinte *ranking*:

1. Phishing (roubo de dados): 27%
2. Golpe de vendedores varejo online: 21%
3. Fraude envolvendo caridade de arrecadação de fundos: 19%
4. Golpe em desempregados: 18%
5. Vacina de Covid-19, curas e testes: 15%
6. Fraude em seguros: 15%
7. Fraude de envio de produtos: 14%
8. Roubo de identidade: 14%
9. Cartão de crédito roubado ou cobrança fraudulenta: 13%
10. Golpe do “benefício do governo”: 12%

Em Goiás, em razão do aumento dos crimes praticados na internet foi criada, em 2017, em Goiânia, a primeira Delegacia Estadual de Repressão a Crimes Cibernéticos (Dercc) do estado. Paulo (2019) cita como exemplo o caso do deputado estadual Diego Sorgatto (PSDB) que foi vítima de crime virtual por meio do Facebook, em que teve sua honra atacada por meio de publicação de mensagens ofensivas. Como desfecho da investigação, a polícia conseguiu identificar dois autores deste crime através da análise dos acessos nos perfis da rede social. Foi possível concluir que ambos eram filiados de partidos políticos rivais, e foram motivados para denegrir a imagem do então deputado estadual Diego Sorgatto (PSDB). Não existe registros divulgados de que estes autores receberam punição devida.

Como outro exemplo de crimes virtuais que ocorreu no Brasil, pode-se citar o fato ocorrido no Hospital de Câncer de Barretos, administrado pela Fundação Pio XII, onde as fichas de seus pacientes foram sequestradas e os autores do crime pediram resgate de quase mil reais em dinheiro virtual (*bitcoins*). O Hospital teve seu sistema desativado por três dias, gerando atrasos de exames; contudo informaram que os dados dos pacientes não sofreram prejuízos, uma vez que o banco de dados foi preservado. O hospital conseguiu regularizar a situação em seis dias após o ataque e informou que não efetuou o pagamento que os *hackers* estavam exigindo. Até onde se tem conhecimento, os autores não foram identificados até os dias atuais. (TOLEDO, 2017 *apud* ROCHA, 2017). Rocha (2017, p. 16) frisa que apesar de a prática do cibercrime estar em evolução,

[...] o Brasil já possui um longo histórico de condutas informáticas danosas. Outro exemplo dessa infeliz estatística é o do ex-prefeito Paulo Maluf, o qual, nas eleições de 2003, foi o primeiro político a sofrer sabotagem digital. Os *hackers* invadiram o site do político espalhou e-mails a todos os eleitores cadastrados, divulgando mensagens de cunho difamatório.

Cumprido tratar acerca dos sujeitos ativos do cibercrime, tendo em vista que a expressão usada para tratar sobre os crimes virtuais evoca a presença dos *hackers*, ou seja, “usuário experiente, exímio programador que invade sistemas computacionais para provar sua capacidade e habilidade computacional, mas sem danificá-los, sem obter

dados ou destruir sistemas”, conforme explica Nascimento (2019, p. 10). O autor frisa que comumente a expressão *hacker* é utilizada de maneira errônea e confundida com o *craker*, que segundo o autor é aquele indivíduo que invade sistemas com intenção de roubar dados e causar danos as vítimas.

Assim como existe a Constituição Federal, o Código de Defesa do Consumidor, o Código Penal etc., houve a necessidade de regimentar os atos que se enquadravam nessas diretrizes, mas que eram praticados no mundo virtual ou que de alguma maneira a internet servia de ferramenta facilitadora para a prática da atividade ilegal. Destarte, o Direito Brasileiro não poderia se ausentar de apresentar respaldo jurídico para tais situações, e assim foi surgindo alguns ordenamentos para normatizar as relações oriundas da internet.

É de bom grado frisar que as leis que surgiram a partir de 2012, que versam sobre a temática em pauta, foram resultado de pressão da mídia sobre o poder legislativo. Nesse cenário, cita-se as Leis nº 12.735/12 e 12.737/12, sendo que a primeira trouxe alteração legislativa do Código Penal, do Código Penal Militar e da Lei de Preconceito, tipificando os crimes realizados na internet, e a segunda dispõe a respeito da tipificação dos crimes informáticos, além de alterar o Código Penal (CRUZ; RODRIGUES, 2018).

A Lei nº 12.737/12 ficou comumente conhecida como “Lei Carolina Dieckmann”, em razão de a atriz brasileira ter sido vítima de crime cibernético quando teve seu computador invadido e imagens furtadas divulgadas e utilizada como meio de extorsão da atriz. Todavia, apesar de ser um avanço legislativo, o referido diploma

normativo recebe diversas críticas, haja vista que, apesar de tipificar crimes informáticos, “não tenha conseguido prever todos os possíveis delitos e também ser tecnicamente frágil”, de acordo com Nascimento (2019, p. 16).

A deficiência da lei reside, principalmente, na especificidade do tipo penal acrescentado ao Código Penal na forma do artigo 154-A, *caput*, *in verbis*:

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

O dispositivo legal exige que a violação de dispositivo de segurança para que o crime seja configurado, bem como o simples acesso indevido não é punido, haja vista que o artigo prevê apenas “invasão como ocupação ou conquista pela força e de modo abusivo”, segundo Nascimento (2019, p. 16). Dessa forma, apesar da promulgação das leis supramencionadas, os demais cibercrimes continuam a serem julgados com base nos efeitos dos danos causados. Cruz e Rodrigues (2018) apontam que a maior dificuldade encontrada nos cibercrimes reside nas questões técnica de como chegar no infrator e a quem pertence a competência de julgamento, e não somente na ausência de lei que classifique e puna os crimes virtuais.

A Lei nº 12.965/14, conhecida popularmente como Marco Civil da Internet, faz jus a sua denominação e foi um importante registro de uma regulamentação para o mundo virtual. Devido a crescente funcionalidade que a internet foi adquirindo e seu acesso foi se tornando essencial à vida das pessoas, a lei foi criada com intuito de regularizar essas utilizações e eliminar a ideia de que a internet é uma “terra sem lei”. Nascimento (2019) explica que o Marco Civil da Internet ficou popularmente conhecido como a Constituição da Internet Brasileira e é composto de 10 (dez) princípios elaborados pelo Comitê Gestor da Internet brasileira.

Esse diploma normativo tem como objetivo “definir em lei os direitos oriundos da utilização da internet prevendo o que se pode ou não fazer no âmbito civil, antes de se criminalizar condutas praticadas na internet”, como explica Nascimento (2019, p. 18). Uma diferença da criação desta Lei foi participação do povo brasileiro “que podia comentar os artigos e opinar por meio das audiências públicas ou portais na internet relacionados ao projeto, como e-Democracia e e-Cidadania” (CHC ADVOCACIA, 2019, p. 1).

Os 10 (dez) princípios previstos na Lei do Marco Civil são

[...] liberdade, privacidade e direitos humanos; governança democrática e colaborativa; universalidade; diversidade; inovação; neutralidade da rede; inimizabilidade da rede; funcionalidade, segurança e estabilidade; padronização e interoperabilidade; e ambiente legal e regulatório.

(NASCIMENTO, 2019, p. 18)

Importante esclarecer que se torna necessário, também, a proteção de direitos e princípios fundamentais previstos na Constituição Federal de 1988, como os princípios da razoabilidade e proporcionalidade e os direitos a liberdade de expressão, a privacidade, entre outros (ALENCAR, 2019).

Outra determinação relevante que pode destacar é a Lei nº 13.709, denominada de LGPD (Lei Geral de Proteção de Dados), criada no ano de 2018, contudo só entrou em vigor recentemente no mês de agosto de 2020. Esse dispositivo tem grande destaque, pois tem “o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (GOVERNO FEDERAL, 2020).

Dessa maneira, tem-se que além das legislações específicas, que tratam sobre ilícitos cometidos na esfera virtual, deve-se respeitar os princípios e direitos fundamentais previstos na Constituição Federal de 1988. Sendo assim, no próximo tópico será tratado sobre os direitos a serem resguardados, em destaque para a dignidade da pessoa humana e a liberdade de expressão, bem como a constitucionalidade das normas que versam sobre crimes cibernéticos.

2. OS CRIMES VIRTUAIS E A TUTELA CONSTITUCIONAL

Souza (2018, p.10) fortalece a ideia de que as regras que são aplicadas no mundo real – sejam

elas escritas por meio das leis, ou não-escritas, movidas pelo costume e tradição – devem ser repassadas também ao mundo virtual, visto que os atos praticados em qualquer um desses ambientes pode agredir a sociedade como um todo, a um grupo específico ou a um indivíduo particular. Dessa maneira, essa legislação, a qual o responsável é o Estado através do Poder Legislativo, e o bom senso, responsabilidade própria de cada usuário, devem ser transportados para este campo cuja existência é virtual.

O Estado Brasileiro, detém aquilo que é chamado de “*jus puniendi*”, que é uma expressão latina traduzida como o “direito de punir”. À vista disso, o Direito Penal Brasileiro, segundo Bezerra (2017, [n.p.]), “por meio da aplicação de penas, visa a atingir sua finalidade precípua, na esfera criminal, que é proteger os bens valorados como essenciais à vida social, tornando o convívio entre os homens mais seguro”. Nessa perspectiva, percebe-se que a finalidade do Direito Penal, em geral, é manter a harmonia social. Acrescenta-se que, “o pensamento jurídico moderno reconhece que o escopo imediato e primordial do Direito Penal radica na proteção de bens jurídicos – essenciais ao indivíduo e à comunidade.” (PRADO, 1999, p. 47).

Em contrapartida, “para Jakobs, o que está em jogo não é a proteção de bens jurídicos, mas sim, a garantia de vigência da norma, ou seja, o agente que praticou uma infração penal deverá ser punido para que se afirme que a norma penal por ele infringida está em vigor”. (GRECO, 2010, p. 3). Neste ponto de vista, tem-se que a função não é exatamente proteção dos direitos, mas uma demonstração de poder e garantia de estabilidade

neste, através da propagação de temor nos indivíduos.

Ademais, o Direito Brasileiro, em geral, serve para proporcionar que as garantias fundamentais de cada cidadão brasileiro sejam respeitadas e efetivamente cumpridas. Nesta virtude, aponta a Constituição Federal Brasileira de 1988, que dispõe claramente em artigo 5º que: “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”.

Cabe esclarecer que a livre manifestação de pensamento é classificada como uma das garantias fundamentais, contudo é vedado o anonimato de acordo com o artigo 5º, inciso IV da Constituição da República Federativa do Brasil de 1988. Ou seja, é permitido que qualquer pessoa possa expressar suas opiniões desde que essa manifestação de pensamento tenha a identificação do seu responsável, com o objetivo de resguardar o direito ao contraditório também assegurado pela Constituição (LENZA, 2019). Desta maneira, cabe salientar que ainda por cima essa “preocupação faz-se mais relevante quando levado em conta a possibilidade de qualquer indivíduo se expressar livremente difundindo conteúdos pela internet, mais especificamente o interesse primitivo em estender a liberdade de expressão a discursos de ódio” (VIEIRA; BRITO; TOLARDO, 2019, p. 178).

É interessante apresentar outra garantia constitucional brasileira, que é a dignidade da pessoa humana. Isso requer que “a dignidade da pessoa humana não é uma criação constitucional,

pois ela é um desses conceitos a priori, um dado preexistente a toda experiência especulativa, tal como a própria pessoa humana” (SILVA, 1998, p. 91).

A dignidade da pessoa humana trata-se de “um valor constitucional que irradia luzes sobre todo o ordenamento, em todos os âmbitos [...], orientando todas as atividades estatais [...], bem como de todas as atividades privadas, atuando como piso protetivo mínimo”, como explica Motta (2013, p. 15). Sarlet (2004, p. 52) define da seguinte maneira:

[...] por dignidade da pessoa humana a qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos [...].

Portanto, a constituição apenas garante um direito que é inerente a cada pessoa, que o único critério para ter acesso a essa garantia é ser humano. Sendo que este direito é a base de todos os demais, e ao ser garantido resguarda a proteção aos direitos de liberdade, igualdade, em especial, assim como os demais direitos e garantias

fundamentais resguardados no artigo 5º, da Constituição Federal de 1988 (MOTTA, 2013).

Apesar de toda lei, expressa ou tácita, existente no País é indubitável que se encontram pessoas que cometem infrações perante essas regras, e assim entra o Estado com o direito de punir o que é considerado como crime. De acordo com o artigo 1º da Lei de Introdução do Código Penal (decreto-lei n. 2.848, de 7-12-1940):

“Considera-se crime a infração penal a que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativamente ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.”

Não obstante, ressalva-se que a motivação que as pessoas têm para cometerem infrações no mundo real, também é encontrada para que esses delitos sejam ampliados para o âmbito virtual. Com isso, nota-se que o avanço da internet trouxe consigo não apenas facilidades de comunicação e acesso à informação, mas também oportunidade de novos crimes surgirem e serem praticados pelos usuários desta; ou seja, ocasionou o que é chamado de crimes cibernéticos.

Segundo Chaves (apud SILVA, 2003, p. 19), cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação”. Assim, por meio do conceito analítico de crime, pode-se chegar à conclusão de que “crimes cibernéticos” são todas as condutas

“típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática” (SCHMIDT, 2014, [n.p.]). Percebe-se que a internet tem sido utilizada para cometer crimes que não são devidamente investigados e punidos, isso devido à ausência de determinações legais.

A Convenção de Budapeste versa sobre Crimes Cibernéticos, foi criada em 2001 da Hungria pelo Conselho da Europa, e ofereceu convite para o Brasil recentemente, em 2019, e trata-se do único instrumento internacional vinculante sobre o tema, como explica Senna e Ferrari (2020). A Convenção tem como objetivo tipificar os principais crimes cometidos na esfera virtual, e seu texto engloba tantos os cibercrimes “próprios” quanto os “impróprios”, ou seja,

[...] respectivamente, aqueles que possuem como objeto de tutela os bens informáticos (crimes voltados contra a inviolabilidade e uso devido dos dados e informações cibernéticas em si, como, por exemplo, o acesso não autorizado ou *hacking*) e crime contra bens jurídicos diversos, mas que utilizam da informática enquanto instrumento para sua execução (como, por exemplo, crimes contra honra na internet, armazenamento de imagens de pedofilia, violação a direitos autorais online etc.).

Vale ressaltar, que a ampliação da legislação que versa sobre o tema com a adesão da Convenção de Budapeste pode garantir um arcabouço jurídico mais robusto na luta contra os crimes virtuais, haja vista que a legislação brasileira existente ainda apresenta várias lacunas, como foi

demonstrado no tópico anterior na análise das Lei nº 12.965/14 (Lei Carolina Dieckmann) e a Lei Geral de Proteção de Dados, e o Marco Civil da Internet.

Há algumas noções de estudos criminológicos que apontam alguns atributos dos elementos dos crimes em meio virtual, “dentre elas: (a) a enorme velocidade de trabalho e rapidez nas operações; e (b) a flexibilidade e possibilidade de aplicação diversas, inclusive com relação às falhas na segurança dos sistemas de operação mais vendidos no mercado” (SILVA, 2019, p. 9). Isso demonstra o risco que cada pessoa está exposta com a internet em relação a seus direitos.

Ângelo (2002, p. 1) aponta algumas das principais causas para o aumento das ações criminosas na internet, dentre elas: “a proliferação de ferramentas gratuitas para ataques, as poucas leis para a prevenção dos crimes digitais e o crescente índice de grupos organizados para explorar oportunidades para o cibercrime”. Importante pontuar que devido a essa ausência às condutas lesivas que são cometidas por meio da internet, existem muitos casos que não são devidamente conceituados, que não existem medidas eficazes de investigação e que esse cenário torna atrativo o cometimento desses crimes.

Em relação à aplicação e direcionamento da legislação para esta recente modalidade de crime, de acordo com Filho e Silva (2017, p. 7): “quanto a competência dos cibercrimes a disciplina legal é escassa no ordenamento jurídico brasileiro, ante a isso muito do pensamento sobre a competência dos crimes digitais é ditada pelo pensamento jurisprudencial”. Vale demonstrar que a utilização dos termos “crime virtual” e “cibercrimes” são

apenas colocados como sinônimos na estruturação do texto.

Ademais, fortalecendo a ideia dos empecilhos encontrados para aplicação da punição devida, acrescenta que “é possível compreender, nesse contexto, que há uma grande dificuldade de localização das condutas ilícitas, além da facilidade do agente em esconder o produto do crime, mesmo que este represente altas quantias” (SILVA, 2019, p. 9). Além do mais, há um considerável déficit no país de agentes capacitados para julgar, investigar e até minimizar os cibercrimes, visto que pouco se tem de regulamentos, isto considerando que ainda não é reconhecido pela doutrina majoritária o ramo do Direito Cibernético ou Direito Digital (COLLI, 2009).

Perante o que foi exposto, percebe-se que o Direito Brasileiro ainda está em fase de adaptação a todas as mudanças que ocorreram com o surgimento dos crimes virtuais. Por isso, a estrutura que o Direito do Brasil propõe para tal assunto, ainda possui lacunas que precisam ser preenchidas. Apesar de algumas emendas constitucionais ajudarem no direcionamento dos julgamentos de alguns casos, muitos ainda carecem de lei positivada.

3. PROBLEMÁTICA DA OMISSÃO LEGISLATIVA NOS CRIMES CIBERNÉTICOS

Como foi tratado nos tópicos anteriores, apesar de existir alguns diplomas normativos que versam sobre os direitos digitais e os crimes

virtuais, a legislação brasileira sobre o tema é cravada de várias omissões que serão apresentadas. Contudo, de acordo com Cruz e Rodrigues (2018, p. 13)

A grande dificuldade encontrada para punir os infratores dos crimes praticados na internet conforme já foi mencionada não ocorre pela falta de normas que caracterizam os crimes e os classifica em uma ordem. O real problema se presencia em detalhes como a falta de tecnologia e de mão de obra especializada para o combate aos cibercrimes.

Isso se deve ao fato de que desde a implementação da rede mundial de computadores, em 1988, não foram realizados preparos e investimentos para combater os crimes que começaram a existir nos países que implementaram a internet primeiro, como Estados Unidos Inglaterra e França (DIANA, 2011). Vale ressaltar, que outro problema encontrado na repressão e investigação dos crimes cibernéticos é que o Código de Processo Penal, prevê em seu artigo 386 a exigência de que haja certeza da prática do crime para que se possa aplicar a sanção penal.

Sendo assim, é necessário comprovar a autoria e a materialidade do delito, ou, ao menos, fortes indícios de sua existência, caso contrário poderá ocorrer a absolvição do réu, como expresso no dispositivo supramencionado, *in verbis*:

Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça:

- I - Estar provada a inexistência do fato;
- II - Não haver prova da existência do fato;
- III - Não constituir o fato infração penal;
- IV - Estar provado que o réu não concorreu para a infração (...)
- V - Não existir prova de ter o réu concorrido para a infração penal;

encontro do criminoso virtual. Nota-se que o sistema jurídico não está totalmente preparado para coibir tais condutas, portanto se as normas que tratam de determinado assunto fossem, talvez, aperfeiçoadas, poderíamos ter a esperança de que os índices de criminalidade virtual reduziriam devido a eficácia de suas respectivas leis.

No entanto, a implementação de novas leis para suprir as omissões legislativas existentes não são dispensadas, uma vez que devem ser consideradas de grande importância no combate e penalização dos crimes virtuais. Porém, como explica, Assunção (2018), as sociedades contemporâneas se caracterizam pelo nível acelerado de inovação e adaptação social, principalmente em razão da velocidade de transmissão e compartilhamento de dados pela internet, dificultando, assim, que a norma aborde todos os detalhes dos cibercrimes, sendo essencial “a permanente necessidade de avaliação e aprimoramento legislativo” (ASSUNÇÃO, 2018, p. 35).

Essa perspectiva serve como incentivo para as casas legislativas desenvolverem cada vez mais projetos de lei. Nesse sentido, Siqueira (2017, p. 128) assevera que

Seria um grande avanço se fosse elaborado um novo código especificando crimes virtuais, adentrando em todos seus aspectos e criando uma área policial especializada no assunto, com nível de conhecimento em computadores avançado para que possa se resolver o conflito de forma mais habilidosa, facilitando o

Em razão do aumento dos crimes virtuais e do crescimento do número de usuários na internet, como apresentado no primeiro tópico, tanto o Senado Federal quanto a Câmara dos Deputados, têm dedicado esforços para a produção legislativa que versa sobre os cibercrimes. Assunção (2018) demonstra que o Senado Federal, na Revista “Em Pauta – O processo legislativo do Senado à Serviço da Cidadania”, em sua edição de setembro de 2012, apontou que há vários projetos de lei em tramitação, podendo dar destaque aos seguintes:

Projeto de Lei do Senado nº 427, de 2011, apresentado pelo Senador Jorge Viana (PT-AC), o Projeto de Lei da Câmara (PLC) nº 35, de 2012, de autoria do Deputado Federal Paulo Teixeira (PT-SP), atualmente pronto para votação em Plenário no Senado Federal após ter sido aprovado nas comissões temáticas desta casa e ainda o PL do SENADO nº 236, de 2012, de autoria do Senador José Sarney (PMDB-AP) (ASSUNÇÃO, 2018, p. 36).

O Projeto de Lei nº 236/2012, elaborado pelo Senado Federal, tramita no Congresso Nacional, e tem como objetivo instituir um artigo no Código Penal Brasileiro, haja vista que grandes mudanças ocorreram na sociedade desde 1940, quando o Código Penal atual foi criado (NASCIMENTO, 2019). Sendo assim, surge a necessidade de inovação legislativa para acompanhar a evolução da sociedade, como exemplo, conter a tipificação dos cibercrimes.

Frisa-se que os crimes virtuais pertencem a pauta do referido projeto de lei, prevendo 07 (sete) artigos (artigos 213 a 219) que tratem a respeito da temática em estudo. Nascimento (2019, p. 18) explica que

No que se refere a tais correções, o art. 214 do projeto prevê o crime oriundo do “acesso indevido”, ao contrário do que preceitua a Lei Carolina Dieckmann, que diz “invasão”, retirando, ainda, a exigência de que o sistema informático deva ser protegido, o que nos dias atuais prejudica a tipificação, pois desqualifica o computador de um usuário comum, que pode não ter medidas de segurança adequadas em sua máquina.

Outro ponto do Projeto de Lei 236/2012 que merece destaque se refere a obtenção de dados privados e sua divulgação. Apesar de este ter sido o caso ocorrido com Carolina Dieckmann, a lei popularmente conhecida com seu nome não trouxe a conduta tipificada de maneira abrangente, como explica Nascimento (2019). Haja vista que, a Lei Carolina Dieckmann prevê apenas a invasão de

dispositivo alheio protegido com objetivo de obter dados ou informações, como dispõe seu artigo 2º. Dessa maneira, constata-se que a parte dedicada aos crimes cibernéticos tipifica diversas condutas que serão de extrema importância no combate e na repressão da demanda de crimes praticados na esfera virtual.

O Projeto de Lei do Senado nº 427, de 2011, também está em tramitação e versa sobre crimes virtuais, e sugere uma alteração no Código Penal em vigência a fim de incluir e tipificar a seguinte conduta “atentar contra a segurança de meio de comunicação informatizado mediante acesso não autorizado” (SENADO FEDERAL, 2011). Contudo, o referido projeto de lei ainda aguarda relatoria para que possa ser apreciado pela Comissão de Constituição e Justiça do Senado Federal, como explica Assunção (2018).

Na Câmara dos Deputados também pode-se encontrar alguns projetos de lei em tramitação decorrentes dos debates que ocorreram na CPI de Crimes Cibernéticos instituída em 2016. Dentre as propostas destaca-se algumas, como exemplo o Projeto de Lei da Câmara que trata sobre a apreensão dos instrumentos (computadores, celular, dispositivos eletrônicos) usados nos crimes virtuais. Outra proposta objetiva ampliar o campo de abrangência do crime de invasão de dispositivo informático, previsto na Lei Carolina Dieckmann (CÂMARA DOS DEPUTADOS, 2016).

O Relatório da CPI dos Crimes Cibernéticos propôs a alteração do Marco Civil da Internet – Lei nº 12.965/2014, a qual determina “a indisponibilidade de cópia idêntica de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e nova norma que

possibilite o bloqueio a aplicações de internet por ordem judicial, nos casos em que especifica” (ASSUNÇÃO, 2018, p. 37).

Todos os projetos de lei mencionados encontram-se em tramitação, juntamente com inúmeras outras propostas. É notável que o Poder Legislativo tem se esforçado nas produções de dispositivos que, se aprovados, serão de grande contribuição na luta contra os crimes virtuais. Todavia as várias propostas de lei se deparam com dificuldades para sua aprovação, sendo justificadas pelas questões corriqueiras do trâmite legislativo.

O Congresso Nacional sofre com morosidade no processo legislativo, o que, especialmente nos casos de necessidade legislativa de interesse social, “acaba postergando a consolidação de direitos cidadãos que há muitos anos já deveriam estar em vigor” (VALENTE, 2014, p. 1). Valente (2014) explica que,

Na prática, a aprovação dos projetos está sujeita a um jogo de pressões exercido de forma absolutamente desigual. De um lado, estão os interesses do poder econômico, geralmente atendidos em tempo recorde. É o caso das desonerações de tributos de diversos setores econômicos e dos refinanciamentos de dívidas (Refis) dos que deixam de pagar impostos, como os relativos à Previdência Social e outros. De outro lado, há os interesses da sociedade. Na maioria das vezes, engavetados por uma maioria parlamentar que se tornou representante dos interesses empresariais que financiam suas campanhas eleitorais.

No entanto, o autor ainda afirma que a morosidade do Poder Legislativo é seletiva e responde simplesmente a interesses próprios, justificando-se assim a demora e a omissão legislativa presente na temática, apesar de sua grande relevância social. Os cibercrimes apesar de relativamente novos, estão presente desde 1988 com a instalação de Rede Mundial de Computadores, no entanto, apesar de precedentes existentes nos países de origem, no Brasil há poucos diplomas normativos nacionais e internacionais que versem sobre a temática.

Como se pode observar, o tempo de votação está relacionado à natureza dos projetos e à força dos interesses a eles vinculados. No Parlamento, o ritmo das votações é ditado pelos interesses econômicos mais fortes. Razão pela qual um dos projetos que continua engavetado por anos a fio é a da reforma política, mantendo intactas as atuais regras do jogo que permitem, por exemplo, o financiamento privado das campanhas eleitorais e a violenta incidência de poder econômico nas eleições. (VALENTE, 2014, p. 5)

Essa omissão legislativa, como demonstrada no desenvolvimento do artigo contribui para o aumento da prática dos crimes virtuais, bem como o crescimento de usuários na internet. A ausência de normas punitivas e preventivas, assim como a ausência de meios e instrumentos para auxiliar nas investigações e nas identificações de autoria, resultam no alto índice de crimes virtuais observado nos dias atuais.

Outro ponto importante a ser ressaltado, é o fato de que com a pandemia de Covid-19 e o lockdown instituído pelos governos estaduais, os comércios precisaram encontrar uma nova maneira de sobreviver, haja vista que suas atividades habituais foram restritas. Relatório E-commerce no Brasil, da agência *Conversion*, mostrou que o comércio online teve um crescimento de 40% em comparação ao ano de 2019, tendo registrado 1,66 bilhão de acessos em março de 2021. (E-COMMERCE BRASIL, 2021).

Sendo assim, com base nos dados apresentados, depara-se com a necessidade de implementação de leis em outros ramos do direito que versem sobre direito virtuais e regulamente esses direitos na internet. Logo, a omissão legislativa se faz flagrante não apenas na esfera criminal, mas em todas as esferas que regem a vida da sociedade nos meios virtuais.

CONSIDERAÇÕES FINAIS

Ao se considerar o tema proposto e sua relevância jurídica, tem-se que os cibercrimes não podem ser analisados somente pelo simples conceito, no entanto, sua definição é essencial para a compreensão da temática. Dessa maneira, os crimes virtuais (cibercrimes, crimes cibernéticos ou crimes informáticos) são atividades criminosas relacionadas diretamente a qualquer ação ou prática ilícita na internet. Assim, os crimes cibernéticos podem ser condutas comuns já tipificadas, mas praticadas por meio da internet, como exemplo crimes contra a honra, privacidade, roubo, estelionato, que desde que praticados por

meios virtuais se enquadram nos crimes informáticos.

No Brasil é possível encontrar alguns dispositivos legais que versam sobre o tema, como a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados, Lei nº 12.965/2014 – Marco Civil da Internet, que tem como objetivo estabelecer direitos oriundos da utilização da internet, trazendo previsões para a esfera civil, antes das condutas serem tipificadas e se tornarem de competência do Direito Penal, haja vista esse ramo do direito ter competência residual.

A Lei nº 12.737/2012 – Lei Carolina Dieckmann, que apesar de ser considerada um avanço da legislação brasileira, é eivada de omissões legislativas. Esse diploma normativo se derivou do “ataque” que a atriz Carolina Dieckmann recebeu ao ter suas fotos íntimas roubadas e usadas como forma de chantagem para receber recompensa. Devido ao caso sofrido pela atriz, a Lei nº 12.737/2012 foi editada e publicada, todavia ao tipificar a conduta, houve a restrição de sua consumação, ao exigir que o dispositivo alvo da invasão deveria ser protegido.

Ao se tratar da esfera internacional, pode-se citar a Convenção de Budapeste que, assim que foi aprovada no Brasil, contribuiu de maneira significativa com o tratamento dos crimes virtuais. O diploma internacional também frisa a proteção aos princípios e direitos fundamentais inerentes a toda e qualquer pessoa, como a dignidade da pessoa humana, a privacidade, a honra e a liberdade de expressão.

Tanto no Senado Federal quanto na Câmara dos Deputados é possível encontrar diversos Projetos de Lei que vão desde pequenas

alterações em dispositivos já existentes, à inclusão de artigos em diplomas normativos com a tipificação dos cibercrimes, até a criação de novos diplomas que versem de maneira específica sobre o tema, como exemplo o Projeto de Lei do Senado nº 236/2012 que propõe a criação de um novo Código Penal, no qual dedica 07 (sete) artigos aos crimes cibernéticos.

Contudo, a morosidade do Poder Legislativo é uma barreira para a aprovação dos projetos de lei, justificado pela complexidade do trâmite legislativo. Todavia, restou demonstrado que essa morosidade responde a interesses, sendo que prioriza os interesses econômicos sobre os interesses sociais. Logo, apesar de se tratar de tema extremamente relevante e que sofre para aplicar medidas repressivas e preventivas, se caracteriza pelas grandes omissões legislativas e, muitas vezes, se demonstra incapaz de punir e identificar os autores das condutas ilícitas praticadas na internet.

REFERÊNCIAS

- ALENCAR, Morgana. **Tire as suas dúvidas sobre o Marco Civil da Internet**. 2019. Disponível em: <https://www.aurum.com.br/blog/marco-civil-da-internet/>. Acesso em: 16 mai 2021.
- ANGELO, Fernanda K. **Brasil lidera ranking mundial de hackers e crimes virtuais**. Folha Online, 2002. Disponível em: <https://www1.folha.uol.com.br/folha/informatica/ult124u11609.shtml>. Acesso em: 13 set. 2020.
- BEZERRA, Rayan Vasconcelos. **O direito penal: finalidades e sanções**. Revista Âmbito Jurídico. São Paulo, setembro de 2017. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/o-direito-penal-finalidades-e-sancoes/>. Acesso em: 15 abr. 2021.
- BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Palácio do Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 set. 2020.
- BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Brasília. Palácio do Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 17 mai. 2021.
- CÂMARA DOS DEPUTADOS. Deputada Mariana Carvalho; Deputado Esperidião Amin; Deputado Sandro Alex; Deputado Rafael Motta; Deputado Daniel Coelho; e Deputado Rodrigo Martins. **Câmara dos Deputados CPI – Crimes Cibernéticos – Relatório Final**. Brasília; 04 de maio de 2016.
- DIANA, Daniela. **História da Internet**. 2011. Disponível em: <https://www.todamateria.com.br/historia-da-internet/>. Acesso em: 26 mai. 2021.
- CHC ADVOCACIA. **Marco Civil da Internet: o que é e o que muda para o seu negócio**. 2019. Disponível em: <https://chcadvocacia.adv.br/blog/marco-civil-da-internet/>. Acesso em 01 mai. 2021.
- COLLI, Maciel. **Cibercrimes: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos**. Porto Alegre, 2009.
- CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade**. Revista Científica Eletrônica do Curso de Direito. 13ª ed. Garça-SP, 2018.
- E-COMMERCE BRASIL. **E-commerce brasileiro cresceu 40% após um ano de pandemia, revela Conversion**. 2021. Disponível em: <https://www.ecommercebrasil.com.br/noticias/e-commerce-brasileiro-cresceu-coronavirus/>. Acesso em: 26 mai. 2021.

- EGEWARTH, Arthur Bernardo. **Os crimes cibernéticos e a ineficácia da lei “Carolina Dieckmann”**. Três Passos-RS, 2019. Disponível em: [Arthur Egewarth.pdf \(unijui.edu.br\)](http://unijui.edu.br). Acesso em 21 nov. 2020.
- FILHO, E. G.; SILVA, G. V. da. **Reflexões sobre os cibercrimes e sua competência**. Centro Universitário Antônio Eufrásio de Toledo. v. 13, n. 13. Presidente Prudente, 2017. Disponível em <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/6354/6053>. Acesso em 14 nov. 2020.
- FRANCESCO, W. **O que você precisa saber sobre a Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann”**. 2014. Disponível em: <https://wagnerfrancesco.jusbrasil.com.br/artigos/152372896/o-que-voce-precisa-saber-sobre-a-lei-12737-2012-conhecida-como-lei-carolina-dieckmann>. Acesso em: 19 nov. 2020.
- GOVERNO FEDERAL. **Proteção de Dados – LGPD**. 2020. Disponível em: <https://www.gov.br/defesa/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd>. Acesso em: 01 mar. 2021.
- LENZA, Pedro. **Direito Constitucional Esquematizado**. 23ª ed. São Paulo: Saraiva, 2019.
- MISSE, Michel. **Crime, sujeito e sujeição criminal: aspectos de uma contribuição analítica sobre a categoria “bandido”**. Lua Nova: Revista de Cultura e Política - no.79 - São Paulo, 2010. Disponível em: <https://doi.org/10.1590/S0102-64452010000100003>. Acesso em: 15 mar. 2021.
- MONCAU, Luiz Fernando; LEMOS, Ronaldo; BOTTINO, Thiago Amaral. **Projeto de Lei de Cibercrimes: há outra alternativa para a internet brasileira?** Revista de Direito Administrativo, 2008. Disponível em: [4102-9270-1-PB.pdf \(fgv.br\)](http://4102-9270-1-PB.pdf). Acesso em: 18 nov. 2020.
- MONTEIRO, Luis. **A internet como meio de comunicação: possibilidades e limitações**. Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação - XXIV Congresso Brasileiro da Comunicação – Campo Grande /MS – setembro 2001. Disponível em: <http://www.portcom.intercom.org.br/pdfs/62100555399949223325534481085941280573.pdf>. Acesso em: 15 mar. 2021.
- MOTTA, Artur Francisco Mori Rodrigues. **A dignidade da pessoa humana e sua definição**. Disponível em: <https://ambitojuridico.com.br/cadernos/direitos-humanos/a-dignidade-da-pessoa-humana-e-sua-definicao/>. Acesso em 26 mai. 2021.
- NASCIMENTO, Samir de Paula. **Cibercrime: conceitos, modalidades e aspectos jurídicos-penais**. 2019. Disponível em: <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em 16 mai. 2021.
- PAULO, Ton. **Em alta, crimes cibernéticos devem ser denunciados**. 2019. Disponível em: <https://www.jornalopcao.com.br/reportagens/em-alta-crimes-ciberneticos-devem-ser-denunciados-228474/>. Acesso em: 26 mai. 2021.
- ROCHA, Adriano Aparecido. **Cibercriminalidade: os crimes cibernéticos e os limites da liberdade de expressão na internet**. Disponível em: <https://www.fae.br/userfiles/files/23%20-%20CIBERCRIMINALIDADE%20E%20OS%20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20NA%20INTERNET.pdf>. Acesso em 01 dez. 2020.
- SARLET, Ingo Wolfgang. **Dignidade da pessoa humana e os direitos fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2004.
- SATAKE, Marcelo. **Conheça as fraudes digitais mais comuns na pandemia e veja como**

- evitar.** 2020. Disponível em: <https://invest.exame.com/mf/conheca-as-fraudes-digitais-mais-comuns-na-pandemia-e-veja-como-evitar>. Acesso em 26 mai. 2021.
- SCHMIDT, Guilherme. **Crimes Cibernéticos.** Jus Brasil, Artigos, 2014. Disponível em <https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>. Acesso em: 15 nov. 2020.
- SENADO FEDERAL. **Projeto de Lei do Senado nº 236,** de 2012. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/106404>. Acesso em 20 mai. 2021.
- SENADO FEDERAL. **Projeto de Lei do Senado nº 427,** de 2011. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/101252>. Acesso em: 20 mai. 2021.
- SENNA, Felipe; FERRARI, Daniella. **Convenção de Budapeste e crime cibernéticos no Brasil.** 2020. Disponível em: <https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil>. Acesso em: 18 mai. 2021.
- SILVA, Ana Laura Rossi. **Ciber Crimes: uma análise sob a perspectiva da aplicação do direito internacional.** Minhas Gerais, 2019. Disponível em: [CiberCrimesAnalisePerspectiva.pdf \(ufu.br\)](https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-ciberneticos-no-brasil). Acesso em: 12 nov. 2020.
- SILVA, José Afonso da. **A dignidade da pessoa humana como valor supremo da democracia.** Revista de Direito Administrativo, v. 212, p. 84-94, abr./jun. 1998. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/47169/45637>. Acesso em: 12 abr. 2021.
- SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático.** Editora Revista dos Tribunais, 2003. ISBN 8520324126, 9788520324127. Num. págs. 141 páginas.
- SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira.** (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017). Disponível em <http://local.cneesan.edu.br/revista/index.php/direito/article/view/468>. Acesso em: 19 mai. 2021.
- SOUZA, Juliane Silva de. **Crimes Virtuais.** Porto Velho – RO 2018. Disponível em: <http://repositorio.saolucas.edu.br:8080/xmlui/bitstream/handle/123456789/2836/Juliane%20Silva%20de%20Souza.%20-%20Crimes%20virtuais.pdf?sequence=1&isAllowed=y>. Acesso em 19 nov. 2020.
- VALENTE, Ivan. **Morosidade do Legislativo e seletiva e responde a interesses econômicos.** Disponível em: <https://noticias.uol.com.br/opiniaocolumna/2014/07/25/morosidade-do-legislativo-e-seletiva-e-responde-a-interesses-economicos.htm>. Acesso em: 20 mai. 2021.
- VIEIRA, Priscila Santana; BRITO, Igor Toneti de; TOLARDO, Isabella Fernanda Semprebon. **Direito digital: da regularização de um novo ambiente ao limite da liberdade de expressão.** Revista Jurídica da UniFil, [S.l.], v. 16, n. 16, p. 174-183, out. 2019. ISSN 2674-7251. Disponível em: <http://periodicos.unifil.br/index.php/rev-juridica/article/view/1152>. Acesso em: 22 nov. 2020.
- GRECO, Rogério. **Curso de direito penal – Parte geral.** 12. ed. Rio de Janeiro: Impetus, 2010, 1 v.
- PRADO, Luiz Regis. **Bem jurídico-penal e Constituição.** São Paulo: Revista dos Tribunais, 1999.
- YOKOHAMA, Alessandro Otávio. **A eficácia como condição de validade da norma jurídica em Kelsen.** Florianópolis: dissertação de mestrado, UFSC, 1999.