

CRIMES VIRTUAIS: UM OLHAR SOB A ÓTICA DO DIREITO PENAL VIRTUAL CRIMES: A VIEW FROM THE PERSPECTIVE OF CRIMINAL LAW

Victor Valério Medeiros Siqueira de Freitas¹

Waldiney Batista dos Santos²

Leticia Vivianne Miranda Cury³

RESUMO: Introdução: Diante da globalização da informatização, do aumento dos delitos cometidos no cenário virtual e dos relevantes justificativos de ordem pessoal, social e acadêmica, torna-se indispensável a realização da presente pesquisa. A partir da suposição de que é evidente a exigência de investigar a eficácia da legislação brasileira no que refere à aplicação do Direito Penal aos delitos virtuais. Objetivo: o objetivo geral desta pesquisa consiste em examinar o papel do Direito Penal brasileiro no âmbito do combate aos delitos cometidos no ambiente virtual. Então, conceituam-se crimes virtuais, apresentou-se a legislação acerca do tema e identifica-se a importância do Direito Penal brasileiro na luta contra esse tipo de crime. Método: os procedimentos metodológicos foram embasados na pesquisa bibliográfica, utilizando um método de investigação puramente exploratório e descritivo, com abordagens qualitativas e quantitativas. Ao adquirir compreensão sobre o conceito de crime virtual por meio da pesquisa bibliográfica, é possível investigar a representatividade do Direito Penal brasileiro no combate a esse tipo de infração e identificar que a legislação a respeito é ineficaz e insuficiente, tanto pelo fato de não possuir um rol variado de tipificações quanto pela questão das penas brandas. Por fim, pode-se concluir que a legislação brasileira, como um todo, no que se refere aos crimes virtuais, demonstra-se ineficaz na contenção das atividades criminosas, necessitando de revisão e aprimoramento para atender, possivelmente, às demandas atuais.

1285

Palavras-chave: Crimes virtuais. Direito penal. Legislação. Suficiência.

ABSTRACT: Faced with the globalization of computerization, the increase in crimes committed in the virtual scenario and the relevant justifications of a personal, social and academic nature, it is essential to carry out this research. Based on the assumption that the requirement to investigate the effectiveness of Brazilian legislation with regard to the application of Criminal Law to virtual crimes is evident. Objective: the general objective of this research is to examine the role of Brazilian Criminal Law in the context of combating crimes committed in the virtual environment. Then, virtual crimes are conceptualized, the legislation on the subject is presented and the importance of Brazilian Criminal Law in the fight against this type of crime is identified. Method: the methodological procedures were based on bibliographical research, using a purely exploratory and descriptive research method, with qualitative and quantitative approaches. By acquiring an understanding of the concept of virtual crime through bibliographical research, it is possible to investigate the representativeness of Brazilian Criminal Law in the fight against this type of infraction and to identify that the legislation in this regard is ineffective and insufficient, both because it does not have a varied list of typifications and the issue of mild penalties. Finally, it can be concluded that Brazilian legislation, as a whole, with regard to virtual crimes, proves to be ineffective in containing criminal activities, requiring revision and improvement to possibly meet current demands.

Keywords: Virtual crimes. Criminal law. Legislation. Sufficiency.

¹Graduando em Direito pelo Centro Universitário São Lucas – Porto Velho-RO.

²Graduando em Direito pelo Centro Universitário São Lucas – Porto Velho-RO.

³Professora titular do curso de Direito pelo Centro Universitário São Lucas – Porto Velho-RO.

I.INTRODUÇÃO

A sociedade tem sofrido intensas mudanças em virtude do processo de globalização. Em razão disso, o ordenamento jurídico mundial precisou se ambientar à realidade imposta pela informatização. Diante dessa situação, considerando o notável aumento do número de crimes que o uso de computadores, rede de computadores ou dispositivos conectados para causar danos a pessoas e bens, seja através da extorsão de recursos financeiros, de estresse emocional ou danos à reputação, o Direito brasileiro, principalmente pela necessidade social e pelas situações corriqueiras, viu-se pressionado a agir.

São mais comuns do que se imagina, muito embora não tenham a mesma repercussão, exemplos como o incidente envolvendo a atriz Carolina Dieckmann em maio de 2011 são ilustrativos. Nesse caso, um criminoso virtual invadiu o computador pessoal da atriz, obtendo acesso a diversas fotos pessoais e íntimas, com o fim de obter vantagem financeira (o invasor exigiu certa quantia em dinheiro para não publicar as fotos).

Como tentativa de proteger o indivíduo dos crimes praticados no âmbito virtual, assim como punir os delituosos, foram aprovadas leis, no Brasil, que fizeram a tipificação criminal de delitos informáticos e agravaram-se determinados crimes, tais como violação de dispositivo informático, furto e estelionato quando praticados de maneira eletrônica ou através da internet.

1286

Nessa toada, o Direito Penal assumiu seu papel de regulamentar esse tipo de crime, cometido virtualmente. Essa tipificação representa, aparentemente, um esforço do legislador em adequar o Direito brasileiro à realidade da era da informatização advinda do processo de globalização. Nesse contexto, surge o seguinte problema: a legislação penal brasileira vigente é suficiente para combater os crimes virtuais?

No intuito de acompanhar a evolução do sistema normativo, a legislação brasileira buscou implementar novos tipos criminais referentes aos, assim denominados, delitos informáticos. Nessa perspectiva, e considerando a diversidade de tipificações e as penas brandas, a hipótese definida consiste na ideia de que a legislação não se mostra suficiente, haja vista que o rol de crimes disciplinados pela lei está distante de compreender a realidade prática desse tipo de delito. Ademais, a maior evidência da insuficiência da legislação está disposta na parte das punições, que não se mostram com a força necessária para assumir o papel preventivo e sancionador.

Assim, analisar o papel do Direito Penal brasileiro na esfera de combate aos crimes praticados no ambiente virtual constitui o objetivo geral desta pesquisa. Como objetivos específicos, anotem-se os seguintes: apresentar conceitos e outras informações pertinentes

relativas aos crimes virtuais; identificar a representatividade do Direito Penal brasileiro no combate aos crimes virtuais; e investigar a suficiência da legislação brasileira nesse cenário.

Esta pesquisa justifica-se, a princípio, pela necessidade pessoal de adquirir conhecimentos diversos sobre este tema tão contemporâneo e dinâmico que tem sido bastante presente na realidade da sociedade brasileira. Um aprofundamento de estudos acerca da temática faz-se indispensável à formação intelectual dos pesquisadores. Ademais, por se tratar de questão que tem ganhado destaque na comunidade, principalmente àquela que mais utiliza o mundo virtual como ferramenta de sobrevivência cotidiana, o tema possui relevância notável no âmbito social.

Na prática, essa investigação, como qualquer outra, contribui para a expansão da literatura sobre os crimes virtuais e fomenta o desenvolvimento de novas análises que abordem outros e/ou estes mesmos aspectos. Portanto, é valoroso falar sobre algo que faz parte da rotina do indivíduo, pois ajuda a comunidade a compreender melhor a matéria, contribui para a bibliografia e comunidade acadêmico-científica; e, é claro, acrescentar informações e discutí-las sob outras perspectivas, pelo fato de valorizar a questão, é sempre apreciável.

Os procedimentos metodológicos escolhidos fundamentam-se na pesquisa bibliográfica com método de investigação pura. Ideias e fatos serão discutidos através de diálogos com os materiais utilizados: livros, artigos, legislação. Esse levantamento utiliza como base o que já foi 1287 trabalhado por outros estudiosos. Para Porto (2019), a metodologia escolhida para ser utilizada em um trabalho representa a via para sua execução.

O desenvolvimento desta pesquisa, nos itens a seguir, ocorrerá a princípio mediante uma contextualização do objeto central do tema que consiste no crime virtual propriamente dito; conceitos para crimes virtuais serão apresentados no intuito de fazer compreender as bases do assunto.

Posteriormente, a legislação brasileira que dispõe sobre os delitos informáticos será o foco; o contexto jurídico em que a discussão se situa faz-se como indispensável à discussão acerca de sua suficiência, por isso, entender leis como a do Marco Civil e visualizar a evolução da legislação sobre o tema é fundamental. Depois, o objeto de estudo é o papel do Direito Penal em relação ao combate aos crimes virtuais; a conversa se dedica, então, a analisar se a legislação, na figura do Direito Penal, se mostra suficiente para interceptar ou ao menos minimizar o crescimento da prática de crimes no ambiente virtual.

2 HISTÓRICO DOS CRIMES VIRTUAIS

No Brasil, anualmente, milhões de pessoas são vítimas de crimes e ataques cibernéticos. Com a instauração do estado de pandemia que atingiu o mundo, a prática de crimes dessa natureza se intensificou.

Os crimes virtuais configuram-se em consequências negativas e diretas do crescimento desenfreado das novas tecnologias, principalmente do avanço da internet.

Consoante Santos, et al. (2017, p. 5), “à atividade onde um computador ou rede destes é utilizado como base para cometimento de crimes ou facilitação para destes” é atribuída o nome de crime virtual.

Os crimes praticados no ambiente virtual constituem forma de violência, muito embora não caracterizada de forma física, como ocorre nos crimes praticados fora do ambiente virtual.

Ao invés de utilizar, por exemplo, objeto perfuro-cortante ou arma de fogo como instrumento para efetivar a violência contra a vítima, o agente delituoso, que não se apresenta fisicamente, utiliza métodos fundamentados na violência moral, em que predominam ameaças, xingamentos e agressões de cunho moral, via oral. Por isso, é importante aceitar que a violência moral é uma forma de violência tão cruel e expressiva quanto à violência física, ou nunca um crime praticado no meio virtual será considerado equivalente, em termos de danos à vítima, a um crime praticado no mundo real.

1288

De acordo com Meneses (2019, p. 7), os crimes cibernéticos são fruto da utilização dos sistemas computadorizados e constituem “episódios em que as pessoas se aproveitam dessas ferramentas para fazer atos que trazem danos a bens jurídicos de terceiros”.

Nesse tom, entende-se que assim como os crimes praticados no mundo real, os delitos praticados no ambiente virtual também ofendem bens jurídicos protegidos por lei. Bens jurídicos possuem valores inestimáveis e por isso são tutelados por leis e constituem a base do Direito Penal no sentido do estabelecimento de sanções.

“A violência virtual é amparada especialmente pela possibilidade de criação de perfis fakes (falsos), que estabelecem uma falsa noção de anonimato, dificultando a identificação do agressor e a origem da ofensa”, cita Guimarães (2019, p. 33), que afirma, complementando, “que isso é crucial para o aumento do número de situações que culminam em delitos virtuais.”

Como dito, nos crimes praticados fora do ambiente virtual o agente criminoso se apresenta fisicamente, em sua maioria; contudo, nos crimes cibernéticos, raramente esse sujeito se identifica. É essa a principal vantagem, para os criminosos, de praticar crimes no mundo

virtual.

É válido mencionar que existem duas correntes que classificam os crimes virtuais de formas diferentes: a primeira distingue crimes virtuais próprios (violam bens jurídicos novos, não previstos na legislação) de crimes virtuais impróprios (utilizam o meio virtual como ferramenta para prática, mas que não se configuram apenas virtualmente); e a segunda divide os crimes virtuais em puros (utiliza o meio informático para violar o próprio meio informático), mistos (utiliza o meio informático para violar bem jurídico diverso do informático) e comuns (utiliza ferramenta comum para violar o meio informático) (COSTA, 2019, p. 34).

Quanto à diferença entre crimes virtuais próprios e impróprios, explica Salustiano (2021, p. 10): crimes próprios são “aqueles praticados exclusivamente por meio de computadores” e crimes impróprios são os “que atingem o bem comum sendo o meio virtual apenas uma das formas de execução do crime, podendo ser praticado por outros meios”.

Adiante, frisa-se que as primeiras ações criminosas que podem ser chamadas de crimes virtuais foram praticadas por volta de 1980, quando houve um expressivo aumento da criminalidade, sob uma perspectiva geral. Escândalos envolvendo manipulações de caixas bancários, abusos em processo de telecomunicação, aparecimento em grande escala de pirataria de programas e também a pornografia infantil resultaram na ampliação da divulgação dos crimes que ocorriam fora da realidade física social (EGEWARTH, 2019, p. 34).

1289

Daí surgiu a necessidade de conceituar o crime praticado fora da realidade física, atribuindo diversas denominações, inclusive a de crime virtual. Quanto à essa conceituação, somam Azevedo e Cardoso (2021, p. 12) “que um crime virtual é um fato típico e antijurídico que utiliza a tecnologia da informação (informática, internet, computador, celular, etc.) como sujeito passivo ou meio de execução, desde que o ambiente de execução do delito seja o virtual.”

Analisando as explicações de Santos, et al. (2017, p. 31) e Azevedo e Cardoso (2021, p. 38) “acerca de crime virtual, as definições apresentadas são dissemelhantes em sua explicitação, mesmo que a fundamentação basilar seja a mesma, ou seja, é como exposto por Salustiano (2021, p. 9): “o conceito de crimes virtuais diverge conforme cada autor, porém o fundamento resume-se ao meio empregue para o delito ser a internet e o dispositivos que fazem uso da mesma”.

Diariamente são veiculadas notícias pelos diversos meios de comunicação a respeito do aumento do número de crimes praticados no ambiente virtual.

Em 2021, a título de exemplo, matérias foram publicadas em jornais de grande circulação informando que as denúncias anônimas de crimes cometidos pela internet cresceram

desregradamente nos últimos anos – a fundamentação para tal afirmativa encontra-se na lista de milhares de notificações recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos (uma parceria da Safernet Brasil com o Ministério Público Federal) (SALUSTIANO, 2021, p. 19).

Para D’urso (2019, p. 13), “os crimes virtuais são cada vez mais comuns porque as pessoas cultivam a sensação de que o ambiente virtual é uma terra sem leis”. Esse pensamento assola principalmente aqueles que já foram, de uma forma ou de outra, prejudicados com a prática desse tipo de crime.

É difícil, assim, discordar de tais pensamentos consolidados, pelo fato de que considerável número de crimes virtuais continua encharcando as delegacias, mesmo as especializadas, por não encontrarem desfechos positivos.

Praticamente todos conhecem alguém que já foi vítima de um golpe pela internet, dada a imensa variedade de formas pelas quais os crimes podem ser cometidos no ambiente virtual, o que dificulta o trabalho da investigação e fomenta o empenho do criminoso na busca pelo exercício.

A noção de terra sem lei também é admitida por D’urso (2019, p. 14) que acrescenta o seguinte: “por se tratar de um ambiente muito amplo e versátil a internet constantemente teve seus problemas com relação à segurança de seus sistemas, e sempre houve aqueles que exploraram essa fragilidade”.

1290

O autor acredita que a demora em reconhecer o mundo virtual como ambiente propício à prática de crimes foi o que mais dificultou a criação e implementação de legislação específica e que, conseqüentemente, causou o aumento das práticas.

Se por um lado, a expansão da internet viabilizou a globalização do contato entre as nações, por outro, “aumentou a vulnerabilidade das sociedades aos ataques criminosos no âmbito virtual”, proporcionando a prática de diversos tipos de crimes que ofendem bens jurídicos diferentes e praticamente todo e qualquer indivíduo (REIS; VIANA, 2021, p. 24).

A partir da necessidade de conter o avanço desenfreado do número de práticas delituosas ocorridas no ambiente virtual, ordenamentos jurídicos do mundo todo identificaram a imprescindibilidade da criação de legislação específica aplicável. No Brasil, país considerado de terceiro mundo, a legislação apresentou sinais de avanço na década passada, com Leis como a de nº 12.965/2014, conhecida como Marco Civil da Internet e outras.

3 A LEGISLAÇÃO BRASILEIRA

Com a evolução da criminalidade no ambiente virtual, o Brasil resolveu adequar o ordenamento jurídico à nova realidade. Surgiram Leis ao longo dos anos que apresentaram tipificações criminais de delitos informáticos, que tornaram mais rigorosa a punição para certos crimes e que foram estabelecidos no Brasil princípios, garantias, direitos e deveres para regulamentar o uso da Internet.

3.1 O marco civil da internet

A responsabilidade de dispor sobre princípios, garantias, direitos e deveres para o uso da Internet no Brasil é da Lei nº 12.965, de 23 de abril de 2014, que determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (BRASIL, 2014).

Ademais, é importante destacar que é o Decreto nº 8.771, de 11 de maio de 2016, que regulamenta a Lei nº 12.965/14, ao tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, que indicam procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações. Além disso, aponta medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações (NUCCI, 2021, p. 21). 1291

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet no Brasil, traz alguns dispositivos muito importantes para a compreensão da temática:

No artigo 2º, apresenta seus fundamentos (respeito à liberdade de expressão, a pluralidade e a diversidade, a finalidade social da rede, entre outros); no artigo 3º, a Lei elenca um rol exemplificativo de princípios (proteção da privacidade, responsabilização dos agentes de acordo com suas atividades, e mais alguns); no artigo 4º, explica os objetivos da Lei (promoção do direito de acesso à internet a todos, do acesso à informação, ao conhecimento, e outros); e no artigo 5º, que discorre sobre alguns conceitos (por exemplo, explica que internet é o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes) (BRASIL, 2014).

O Marco Civil da Internet ainda destaca os direitos e garantias dos usuários, a forma de atuação do Poder Público e trata de temas relativos à proteção aos registros, aos dados pessoais e às comunicações privadas (os últimos temas também são tratados pelo Decreto que regulamenta o Marco) (BRASIL, 2014).

Mencionam Barreto Júnior e César (2017, p. 84) “O Marco Civil da Internet é uma resposta do Poder Legislativo brasileiro aos conflitos inerentes à sociabilidade humana, surgidos com a disseminação da sociedade da informação”.

Ocorre, no entanto, que, se por um lado esse avanço no ordenamento jurídico representa uma resposta do Direito aos novos desafios, por outro, a velocidade que o Direito age ainda é muito lenta, se comparada à velocidade da evolução digital.

Salientam Cancelier e Pilati (2017, p. 73) “que o Marco Civil da Internet faz partedo que consideram um processo pós-moderno de produção jurídica, que corresponde à nova realidade do desenvolvimento da legislação nacional.”

O que ainda destaca a referida Lei no cenário mundial é a forma como foi construída, haja vista ser fruto de uma política legal que buscou analisar e prever direitos e responsabilidades de todos os usuários da internet (individuais, governamentais e corporativos).

O Marco Civil da Internet é interpretado pelos estudiosos como um dispositivo principiológico.

Como entendem Medeiros e Wachowicz (2018), “a lei tem suas bases na liberdade de expressão, inviolabilidade da privacidade e neutralidade da rede, conceitos bem definidos e abordados pelo dispositivo.” Além disso, o Marco funciona como um reforço do direito de acesso à internet que deve ser garantido a todos e reconhece a importância da garantia desse direito para o exercício da cidadania.

Segundo Teffé e Moraes (2017, p. 56) “explicam que a intenção do legislador era equilibrar os princípios da Lei, com a finalidade de dar liberdade suficiente para que o indivíduo possa desenvolver sua personalidade.” Por isso, para as autoras, a liberdade de expressão é o princípio mais destacável dentre os mencionados na Lei, ganhando uma valorização notável.

Sob outra ótica, Lima (2018, p. 69) assevera que:

A aplicabilidade do Marco Civil da Internet por si só, não representa de forma eficaz a garantia do direito à privacidade nas Redes Sociais”. Em outras palavras, entende que há impossibilidade de assegurar o exercício do direito à privacidade, haja vista a própria dinâmica e velocidade que novas situações fáticas vão acontecendo no contexto virtual.

Nessa perspectiva, recapitule-se aquela ideia de que a internet é uma terra sem lei. Não se trata da inexistência de legislação aplicável aos delitos ocorridos no meio informático, mas da dificuldade que a legislação existente tem de acompanhar a celeridade desmedida do avanço tecnológico.

O próprio Marco Civil da Internet evidencia o retardo legislativo em ratificar normas relativas; ora, a prática dos delitos no meio virtual não teve início apenas em 2014 (ano de aprovação da Lei nº 12.965/2014), então não justifica a homologação da Lei tardia.

O Marco Civil da Internet [...] tem natureza peculiar pela sua idealização, criação e discussão, contando com ampla participação dos cidadãos em fóruns de discussão, na

Internet e em audiências públicas”, por isso é tão importante para a sociedade brasileira, a ponto de receber tal denominação e reconhecimento (COSTA; PENDIUK, 2018, p. 3).

Desse modo, é necessário dar os devidos créditos e reconhecer que, embora a passos lentos, a legislação brasileira tem se mostrado atenta à evolução social e incansável na busca pela adequação do ordenamento jurídico. A Lei nº 12.965/2014 representa uma tentativa louvável, digamos de passagem, de conduzir a normatividade rumo à modernidade.

3.2 A evolução da legislação específica

O Marco Civil da Internet, no Brasil, como o próprio nome sugere, foi o ponto de partida da legislação que passou, a partir de então, a buscar estudar e compreender a importância do processo de evolução da era digital. Assim, novas leis surgiram e hoje regulam a matéria no ordenamento jurídico brasileiro.

Conforme Souza (2021), a promulgação de leis que dispõem sobre os crimes virtuais significa que o Brasil vem caminhando para inibir essa nova modalidade de delitos.

A Lei nº 12.735, de 30 de novembro de 2012, antes mesmo do Marco Civil da Internet, alterou o Código Penal, o Código Penal Militar e a Lei nº 7.716/1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares (BRASIL, 2012). 1293

A Lei nº 12.737, também de 30 de novembro de 2012, tem como objeto dispor sobre a tipificação criminal de delitos informáticos, realizando alterações no Código Penal (tipificando, por exemplo, a invasão de dispositivo informático) e dando outras providências (BRASIL, 2012).

Conhecida como Lei Carolina Dieckmann, a Lei nº 12.737/2012 representou uma imensa inovação na legislação brasileira, ao tipificar o crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal. O núcleo central do delito é “invadir”; o instrumento para efetivação é “dispositivo informático alheio, conectado ou não à rede de computadores”; e o objetivo é “obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita” (BRASIL, 2012).

O referido crime prevê pena de detenção de três meses a um ano e multa e estabelece:

que “quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida” também sofre a mesma penalidade; aumento de pena (de um sexto a um terço) quando resultar prejuízo econômico da invasão (§2º); reclusão (de seis meses a 2 anos; e multa) “se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido” (§3º) e aumento dessa pena (de um a dois terços) “se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos” (§4º); e aumento de pena (de um terço à metade) quando o delito for praticado contra certas autoridades (Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal;

Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal) (§5º) (BRASIL, 2012).

Outras previsões importantes que a lei traz: quanto à ação penal, que “somente se procede mediante representação” (a exceção a essa regra diz respeito aos crimes “contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos”); e quanto à equiparação de cartão de crédito ou débito a documento particular, em relação à falsificação de documento particular, especificamente à falsificação de cartão.

A Lei Carolina Dieckmann (Lei nº 12.737/12) foi a primeira lei específica sobre crimes virtuais. No entanto, como expõe Ferreira (2021, p. 34), sofreu muitas críticas ao não prever a forma de violência moral nas condutas praticadas pelos crimes cibernéticos.”

Em conformidade com Dornelas (2019, p. 33) “a eficiência da Lei 12.737 é questionável, pelos operadores do Direito, já que a ótica da Lei Carolina Dieckmann abrange em grande parte, apenas o desfalque patrimonial sofrido pela vítima”, não considerando outras vertentes, como a lesão às garantias individuais, como a honra, imagem, dignidade.

Considerando essas críticas e o anseio social por Leis mais abrangentes, em 2018 foi sancionada a Lei nº 13.709, de 14 de agosto de 2018, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), que apresenta disposições acerca do tratamento de dados pessoais (com enfoque nos meios digitais), por pessoa natural ou por pessoa jurídica de direito público ou privado (NUCCI, 2021, p. 29). 1294

No intuito de “regular a proteção de dados e reconhecer que a informação, dados pessoais, transformou-se em verdadeiro insumo da produção, adquirindo tanta relevância quanto o capital e o trabalho.”

Segundo Buchain (2021, p. 65). “A Lei Geral de Proteção de Dados Pessoais estabelece como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme escreve o artigo 1º do dispositivo.”

A Lei Geral de Proteção de Dados Pessoais oferece “uma garantia dos direitos que todos os cidadãos possuem na proteção de seus dados nos meios digitais, sendo notória a eficiência e ajuda que a mesma oferece.”

Colaboram Sousa et al. (2022, p. 44). “Assim, representa um enorme avanço no que concerne à legislação brasileira que dispõe sobre os delitos praticados no meio virtual.”

Mostra-se relevante e preocupada em complementar o Marco Civil e fomentar a criação de novos dispositivos que versem no todo ou em parte sobre tipificações e disposições que envolvam os crimes virtuais.

É incontestável que essa Lei Geral, de acordo com Pinheiro (2021, p. 79), representa uma atualização legislativa nacional, pois simboliza a “completa proteção aos dados pessoais em qualquer mídia ou suporte”.

Segundo Buchain, (2021, p. 65) “Desta forma, deve-se reconhecer que, para além da defesa da privacidade, o que se protege e se regula através da LGPD é o poder de acesso e o controle das informações pelo cidadão.”

Para Agostinelli (2018, p. 19) O Marco Civil e a Lei Geral de Proteção de Dados Pessoais representam,então, uma “dinâmica adotada pelo legislador em prol da transparência, liberdade e tutela jurídica em relação aos direitos fundamentais da personalidade.”

Recentemente, outra Lei ganhou destaque no cenário legislativo nacional:

A Lei nº 14.155, a mais recente no ordenamento jurídico brasileiro, de 27 de maio de 2021, também fez alterações no Código Penal ao tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; alterou, ainda, o Código de Processo Penal para definir a competência em modalidades de estelionato (BRASIL, 2021).

1295

A Lei nº 14.155/2021 ampliou as penas cominadas pela Lei Carolina Dieckmann (Lei nº 12.737/2012); penas relativas ao crime de invasão de dispositivo informático, previsto no artigo 154-A do Código Penal. A pena que era de detenção de três meses a um ano e multa agora é de reclusão de um a quatro anos e multa; o aumento previsto no §2º (de um sexto a um terço) agora é de um terço a dois terços; e a pena prevista no §3º (reclusão de seis meses a 2 anos e multa) conservou a multa e aumentou a reclusão para dois a cinco anos. Mudanças foram implementadas também nos artigos 155 (furto) e 171 (estelionato) do Código Penal e no artigo 70 do Código de Processo Penal (para definir a competência em modalidades de estelionato) (BRASIL, 2021).

O que se vê a partir desta breve exposição e análise aos poucos dispositivos legais que dispõem sobre crimes virtuais é que, por mais que o legislador se esforce ao estabelecer tipificações e cominar penas, ainda parece estar longe do mínimo ideal.

De acordo com D'URSO, (2019, p. 34) “Não existem conceitos que representem a real dimensão do que seja um crime virtual; não existem tipificações suficientes, e nem penas compatíveis com o grau de repulsa de cada delito.”

A legislação existente é limitada e visivelmente obsoleta, considerada a época das mais antigas (homologadas em 2012 e 2014).

Muito embora existam essas leis, ressalva Dornelas (2019, p. 25):

Não existe um código específico nem ao menos com uma conceituação jurídica

adequada, e isso se torna bastante preocupante, levando em consideração o crescente número de usuários da informática, e consequentemente as vítimas”. Entende-se, assim, que ainda há uma visível necessidade de uma urgente revisão das normas jurídicas.

Nessa perspectiva, tendo em vista que os crimes praticados em ambiente virtual representam fenômeno jurídico recente, boa parte da doutrina entende que o ordenamento jurídico brasileiro ainda não acompanhou o ritmo dessa evolução, o que seria justificativa para as lacunas legislativas perigosas que precisam ser sanadas.

4 O PAPEL DO DIREITO PENAL BRASILEIRO NO COMBATE AOS CRIMES VIRTUAIS

Como dito, o entendimento majoritário corresponde à tentativa fracassada da legislação de acompanhar a evolução da sociedade e dos crimes por ela praticados. A função do Direito Penal nessa circunstância é simples: estabelecer normas que possam ser efetivadas e que se mostrem eficazes. Mas, afinal, esse papel tem sido cumprido?

Como menciona Capez, (2018, p. 21) “Existe um rol de condicionantes à efetividade da atividade exercida pelo Direito Penal, que consiste em proteger certos bens jurídicos que são reconhecidos como de superior relevância para a sociedade.”

1296

A dificuldade em criar uma legislação íntegra e satisfatória, os obstáculos persistentes quanto à sua efetiva aplicação e o impasse entre o contexto que requer essa legislação e a capacidade de ela ser implementada, são só alguns dos fatores que inviabilizam o exercício do papel do Direito Penal no ordenamento jurídico brasileiro.

No tocante à parte da legislação que versa sobre os delitos praticados no ambiente informatizado, Araújo (2021, p. 508) “afirma que, em que pese haja a tipificação de alguns crimes virtuais feita pelo Código Penal, o dispositivo possui penas brandas e sem suficiência para a coibição da prática desses atos”.

Nesse tom, soma Lócio (2019, p. 17) ao definir o que se pode nominar como solução, a esse problema de tênues punições, “a elaboração de penas mais severas, leis penais mais positivas, melhor fundamentadas e com aplicação devida”.

Apesar de parecer um recurso plausível, a instituição e aplicação de punições mais rígidas aos crimes já tipificados só resolve o problema relacionado aos delitos que já existem. Contudo, outro problema, que consiste na ausência de uma legislação em especificidade ao *cybercrime*, continua sem solução à vista, o que culmina na ideia de que a internet é uma terra sem lei.

A respeito, Lócio (2019, p. 17) explica que a ausência de regulamentação transmite mesmo

essa ideia de terra sem lei atribuída à virtualização e que esse plano legislativo frágil “irá ocasionar lacunas, na qual os criminosos aproveitaram dessa situação para efetuar suas ações delituosas”. De igual modo, Bezerra (2020, p. 55) “afirma que o fato de os crimes virtuais serem desprovidos da devida regulamentação é fundamento mais que suficiente para consolidar essa concepção de que a internet é uma terra sem lei.”

O Brasil sofre inúmeras críticas no que se refere à sua legislação, de modo geral, e mais ainda, haja vista o atual cenário, em relação à legislação específica que trata dos crimes virtuais. O fato de “não haver uma legislação específica à respeito de crimes virtuais ou cibernéticos, ou mesmo com a legislação existente, ainda ser um país que sofre constantemente com a prática de crimes virtuais” é a principal crítica (BARBOSA, 2020, p. 18).

Em concordância com o pensamento acima descrito, daí também surge a noção de que o mundo virtual é uma terra sem lei, que conclui que os criminosos não recebem a punição devida.

Corroborando com esse ponto de vista, Costa (2021, p. 34) acentua a relação direta entre a impunidade e a ausência de um respaldo legislativo forte: “um dos grandes empecilhos e, que no fim, acaba fomentando a impunidade é a falta, ainda, de normas específicas de regulamentação dos ilícitos nesse mundo virtual”.

O autor explica que, muito embora, ao longo dos anos, a legislação tenha apresentado certo avanço, ainda parece estar longe do mínimo ideal, pois não é bem regulamentada, é imprecisa e tímida. 1297

Frise-se que não basta a elaboração da norma propriamente dita, pois, como se tem conhecimento e já fora objeto de discussão neste trabalho, já existem diversas Leis sem apresentações reais de resultados eficazes – destaque-se que embora seja variada, a quantidade mostra-se insuficiente ainda. “O Direito e, conseqüentemente, a legislação devem evoluir para acompanhar de perto a dinâmica social, sob pena de tornar letra morta, sem aplicabilidade aos casos concretos e sem força coercitiva” (CAMPOS, 2018, p. 20).

Importante mencionar que não está aqui sendo defendido o aumento da legislação. O argumento é crescer e expandir o rol de tipificações, o que não necessariamente implica em criar várias novas Leis.

O simples aprimoramento das que já existem, desde que feito adequada e satisfatoriamente, poderia ser suficiente quanto ao problema da falta de norma que tipifique todas as condutas que possuem essência criminosa.

Para Sá e Silva (2020 p. 34) “Ademais, mesmo com a ampliação de algumas punições, através de Lei, ainda existe a sensação, especialmente para os operadores do Direito, de que as penas são brandas e sem capacidade repressiva bem-sucedida.”

Nesse ponto, ainda Sá e Silva (2020 p. 34):

Defendem a ausência de força coercitiva das sanções, ao analisarem que uma pena de detenção de três meses a um ano jamais seria suficiente para inibir e reprimir delitos informáticos – embora sejam considerados de menor potencial ofensivo, a sanção branda ou inexistente não se mostra como uma solução viável, eficaz e suficiente à repressão desse tipo de prática.

Concluem que as punições, que recentemente foram aumentadas, ainda são desproporcionais aos danos causados às vítimas.

É preciso analisar a nova realidade da sociedade que necessita que o Direito acompanhe essa evolução digital.

Conforme Araújo Lima (2020, p. 29), que “há uma descomunal dificuldade em regulamentar as condutas que se originam desta evolução”.

Todavia, adicionam Procópio e Silva (2021, p. 22), “a incumbência de se adequar as evoluções tecnológicas gerindo medidas eficazes ao combate dos crimes virtuais, protegendo o status de ordenamento jurídico brasileiro” não deixa de ser do Direito, em particular do Direito Penal, como protetor dos bens jurídicos.

Cita Rodrigues Costa (2021, p. 34) “O Direito deve acompanhar a evolução da sociedade para que não fique inseguro a utilização dos meios eletrônicos no dia a dia.”

Nessa conjuntura, discorre Macêdo (2020, p. 56):

sobre o papel do Estado em combater os crimes virtuais: a dificuldade de atualização penal, devido a lentatramitação das leis no Senado, não é compatível com a velocidade de ação dos criminosos; assim, o Direito Penal tem o dever de agir na luta pela atualização penal, buscando inovar e amparar a população.

Ao realizar uma análise mais minuciosa das Leis apresentadas anteriormente é possível identificar diversas lacunas que poderiam ser sanadas pelo Direito Penal, mas que ainda não foram.

Procópio e Silva (2019, p. 21) observam e identificam que “mesmo com a criação de normas que versam sobre a matéria e o cumprimento da legislação existente, o ordenamento jurídico brasileiro ainda se apresenta insuficiente para garantir a segurança dos usuários desse meio tecnológico”.

Em compreensão semelhante, Bezerra (2020, p. 17) argumenta que “condutas ilícitas praticadas em ambiente informático podem prejudicar a manutenção dos níveis adequados de segurança”.

Nesse sentido, é notável a imprescindibilidade de uma legislação mais ampla e versátil que venha a versar acerca dos crimes cometidos na internet, com punições mais severas, obedecendo a proporcionalidade, é claro, mas que objetive o controle da prática desses delitos.

Desse modo, é incontestável, para Sá e Silva (2020, p. 24), “a necessidade de uma legislação que abrange como um todo o uso da internet no Brasil, e que sejam preenchidas as lacunas existentes na legislação para uma efetiva punição, e conseqüentemente tornando a lei eficaz”.

Conclui Santos (2021) que já existem diversas decisões de Tribunais contribuindo para o preenchimento de lacunas em relação aos crimes virtuais.”

O próprio Superior Tribunal de Justiça já emitiu decisões, de notória relevância no ordenamento jurídico, nesse sentido. Para alguns, os dispositivos legais atualmente vigentes tipificam grande parte dos crimes cibernéticos. “Entretanto, a mente criminosa não se limita nas condutas já tipificadas, exigindo do legislador estudo específicos das condutas e das tecnologias usadas para, assim, cominar punições relativas às práticas delituosas”, como lembra Souza (2021, p. 11).

Procópio e Silva (2019, p. 21) citam que “uma grande evolução para a sociedade seria a elaboração de um Código específico para crimes virtuais que aprofundassem todos os seus aspectos”. Em consonância, Sá e Silva (2020, p. 23) destacam que “fazem-se necessários mecanismos de prevenção e sistemas de controle da internet, bem como, a redução da impunidade e a imposição de penas mais severas”.

Assim, é axiomático que o Direito Penal, embora mostra-se empenhado em criar normas, continua por não assimilar a necessidade de estar sincrônico com o desenvolvimento social e tecnológico, transmitindo a ideia de que é atrasado e, por conseguinte, viabilizando o aumento da prática de condutas ainda, sequer, tipificadas como criminosas.

1299

CONSIDERAÇÕES FINAIS

Buscando se ambientar à realidade imposta pela informatização, o ordenamento jurídico brasileiro, como tentativa de proteger o indivíduo dos crimes praticados no âmbito virtual e punir os criminosos, estabeleceu leis, no Brasil, que fizeram a tipificação criminal de alguns delitos informáticos e tornaram mais graves alguns crimes.

Leis como a Lei nº 12.965/14 (Marco Civil da Internet no Brasil) e a Lei nº 12.737/12 (Lei Carolina Dieckmann) surgiram em meio ao caos; uma pela necessidade de regulamentação básica sobre o tema dos crimes virtuais e outra como tentativa de mostrar resposta a um crime que envolvia uma celebridade brasileira. Em outras palavras, Leis que nasceram para “tapar buracos”, sem embasamento legal adequado, eficácia suficiente e resultados destacáveis.

Mais recentemente, a Lei nº 13.709/18 e a Lei nº 14.155/21 apresentaram-se de forma mais

dinâmica e, aparentemente, mais elaborada. A primeira, intitulada Lei Geral de Proteção de Dados Pessoais, e a segunda, que agravou certos crimes, se mostraram mais atentas à realidade social e parecem ser mais promissoras que as demais.

O Direito Penal assumiu seu papel de regulamentar esses crimes cometidos no meio virtual. Contudo, essa singela tipificação representa apenas um esforço do legislador em adequar o Direito brasileiro à realidade da era da informatização advindo processo de globalização. Nada mais. Conclui-se, a partir disso, que o Direito Penal brasileiro e a legislação vigente estão longe de mostrar suficiência quanto ao combate dos crimes virtuais.

Considerando a minúscula diversidade de tipificações e a ausência de força repressiva das punições relacionadas aos delitos, é evidente que o Direito Penal brasileiro, embora tenha assumido o papel de combater os crimes mediante proteção dos bens jurídicos, não o exerceu, nem exerce, com eficiência e suficiência. Ao entender o conceito de crime virtual, mediante a pesquisa bibliográfica, foi possível investigar a representatividade do Direito Penal brasileiro no combate a esse tipo de infração e identificar que a legislação a respeito é ineficaz e insuficiente, tanto pelo fato de não possuir um rol variado de tipificações quanto pela questão das penas brandas.

REFERÊNCIAS

AGOSTINELLI, Joice. A importância da lei geral de proteção de dados pessoais no ambiente online. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA**, v. 14, n. 14, 2018.

ARAÚJO, Cláudio Rodrigues. Análise da aplicação do Direito Penal nos crimes virtuais. **Pensar Acadêmico**, Manhuaçu, v. 19, n. 2, p. 494-511, mai./set., 2021.

LIMA, Isaac Araújo. **Cibercriminalidade**: discussões sobre a colisão de direitos fundamentais e a dificuldade punitiva. 33f. Artigo (Bacharelado em Direito) – Centro Universitário Fametro, Fortaleza, 2020.

AZEVEDO, Leticia Silva de; CARDOSO, Thais Mariana. **Crimes cibernéticos**: evolução e dificuldades na colheita de elementos de autoria delitiva. 25f. Artigo (Curso de Direito) – Faculdade de Direito da UNA Bom Despacho, Bom Despacho, 2021. Disponível em: <<https://repositorio.animaeducacao.com.br/handle/ANIMA/13241>>. Acesso em: 09 fev. 2023.

BARBOSA, Mateus Israel Alves Cruvinel. **Crimes virtuais a evolução dos crimes cibernéticos e os desafios no combate**. 24f. Artigo Científico (Bacharelado em Direito) – Escola de Direito e Relações Internacionais, Curso de Direito, Pontifícia Universidade Católica de Goiás, Goiânia, 2020. Disponível em: <<https://periodicorease.pro.br/rease/article/view/2684>>. Acesso em: 11 out. 2023.

BARRETO JÚNIOR, Irineu Francisco; CÉSAR, Daniel. Marco Civil Da Internet e neutralidade da rede: aspectos jurídicos e tecnológicos. **Revista Eletrônica do Curso de Direito da UFSM**, v. 12, n. 1, p.65-88, 2017. Disponível em: <<https://periodicos.ufsm.br/revistadireito/article/view/23288>>. Acesso em: 11 out. 2023.

BEZERRA, Clara Augusta Silva. **A ineficácia da prestação jurisdicional no combate aos crimes virtuais**: a dificuldade da persecução penal. 22f. Artigo Científico (Bacharelado em Direito) – Escola de Direito e Relações Internacionais, Curso de Direito, Pontifícia Universidade Católica de Goiás, Goiânia, 2020. Disponível em: <<https://periodicorease.pro.br/rease/article/view/2684>>. Acesso em: 11 out. 2023.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 11 out. 2023.

_____. Decreto nº 8.771, de 11 de maio de 2016. **Regulamenta a Lei nº 12.965, de 23 de abril de 2014**, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 11 fev. 2023.

_____. Lei nº 12.735, de 30 de novembro de 2012. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989**, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em: 10 fev. 2023.

_____. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 09 fev. 2023.

_____. Lei nº 14.155, de 27 de maio de 2021. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal)**, para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm>. Acesso em: 01 fev. 2023.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 08 fev. 2023.

BUCHAIN, Luiz Carlos. A lei geral de proteção de dados: noções gerais. **Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região**, v. 10, n. 97, p. 51-66, mar. 2021.

CAPEZ, S. P. F. **Código Penal Comentado**. 3. ed. São Paulo: Saraiva, 2018. p. 333- 341.

CAMPOS, Yonara de Vasconcelos. **A evolução do Direito Penal frente às novas tecnologias: um estudo sobre os crimes virtuais de natureza sexual**. 21f. Artigo (Graduação em Direito) – Centro de Ciências Humanas e Sociais Aplicadas do Centro Universitário de Maringá, Maringá, 2018.

CANCELIER, Mikhail Vieira de Lorenzi; PILATI, José Isaac. Privacidade, pós- modernidade jurídica e governança digital: o exemplo do Marco Civil Da Internet na direção de um novo Direito. **Espaço Jurídico: Journal of Law**, Joaçaba, v. 18, n. 1, p. 65-82, jan./abr., 2017. Disponível em: <<https://repositorio.animaeducacao.com.br/handle/ANIMA/13241>>. Acesso em: 09 fev. 2023.

CHIARA, I. D. *et al.* **Normas de documentação aplicadas à área de Saúde**. Rio de Janeiro: Editora E-papers, 2008.

COSTA, Dayara de Oliveira. **Crimes virtuais: uma breve análise da legislação brasileira sobre o tema**. 27f. Artigo científico (Graduação em Direito) – Núcleo de Apoio à Pesquisa e Extensão da Fundação Educacional Jaymede Altavila da Faculdade Cesmac do Agreste, Arapiraca, 2019.

COSTA Rodrigues, LUCCA, Bruno de. **Crimes virtuais: uma análise da falta de tipificação legal dos crimes cibernéticos**. 39f. Monografia (Bacharelado em Direito) – Escola de Direito e Relações Internacionais, Curso de Direito, Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: <<https://repositorio.animaeducacao.com.br/handle/ANIMA/13241>>. Acesso em: 09 fev. 2023.

1302

COSTA, Roberto Renato Strauhs da; PENDIUK, Fábio. Direito digital: o marco civil brasileiro da internet e as inovações jurídicas no ciberespaço. **Revista Publica da Faculdade de Educação Superior do Paraná**, v. 2, n. 1, 2018.

DORNELAS, Natália Alves. **A resposta estatal quanto aos crimes cibernéticos: uma análise direcionada às leis 12.735/2012 e 12.737/2012**. 43f. Projeto de Pesquisa (Curso de Direito) – UniFacig Centro Universitário, Manhuaçu, 2019.

D'URSO, Luiz Augusto Filizzola. **Cibercrime: perigo na internet**. Publicado em 2019. Disponível em <<http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/>>. Acesso em: 08 fev. 2023.

EGEWARTH, Arthur Bernardo. **Os crimes cibernéticos e a ineficácia da Lei “Carolina Dieckmann”**. 35f. Monografia (Bacharelado em Direito) – Universidade Regional do Noroeste do Estado do Rio Grande do Sul, Três Passos, 2019.

FERREIRA, Sarah Pereira. **Crimes cibernéticos: a ineficácia da legislação brasileira**. 31f. Artigo Científico (Curso de Direito) – Escola de Direito e Relações Internacionais da Pontifícia Universidade Católica de Goiás, Goiânia, 2021.

GUIMARÃES, Ana Larissa Gonçalves. **Crimes virtuais e novas modalidades de violação de gênero contra a mulher: a divulgação não consentida de imagens íntimas na internet.** 65f. Monografia (Graduação em Direito) – Departamento de Direito Público da Faculdade de Direito da Universidade Federal do Ceará, Fortaleza, 2019.

LIMA, Luciano de Almeida. Diretrizes para aperfeiçoamento e interpretação da lei do Marco Civil da internet com vistas à garantia do direito à privacidade nas redes sociais. **Prisma Jurídico**, v. 17, n. 1, p. 58-74, jan./jun., 2018.

LÓCIO, Ana Laura Miranda Alencar. **Entraves da aplicação da lei penal nos crimes virtuais.** 21f. Monografia (Bacharelado em Direito) – Centro Universitário Dr. Leão Sampaio, Juazeiro do Norte, 2019.

MACÊDO, Luiz Fernando Belizário. **Cibercrimes: a internet como ferramenta na execução de crimes virtuais e o combate realizado pelo Direito Penal brasileiro.** 41f. Monografia (curso de Direito) – Faculdade Evangélica de Rubiataba, Rubiataba, 2020.

MEDEIROS, Heloísa Gomes; WACHOWICZ, Marcos. Observância de direitos autorais na sociedade informacional: lições do Marco Civil da Internet brasileiro. **RJLB**, a. 4, n. 6, p. 2045-2068, 2018.

MENESES, Sâmia Pereira. **Crimes virtuais: possibilidades e limites da sua regulamentação no Brasil.** 28f. Artigo (Bacharelado em Direito) – Centro Universitário Fametro, Fortaleza, 2019.

NUCCI, Guilherme de S. **Código Penal Comentado.** Grupo GEN, 2021. 9788530993443. Disponível em: <<https://app.minhabiblioteca.com.br/#/books/9788530993443/>>. Acesso em: 07 fev. 2023.

1303

PINHEIRO, Patricia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. **Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região**, v. 10, n. 97, p. 75-87, mar. 2021.

PORTO, Lidianne. **Você já ouviu falar de método?** Saiba o que é a metodologia! 2019. Disponível em: <<https://escolaeducacao.com.br/o-que-e-metodologia/>>. Acesso em: 13 fev. 2023.

PROCÓPIO, Grasielle da Silva; SILVA, Mazukyevcz Ramon Santos do Nascimento. **Os crimes virtuais no ordenamento jurídico brasileiro.** 2019. Disponível em: <https://bdcc.unipe.edu.br/wp-content/uploads/2019/09/CRIMES-VIRTUAIS-NO-ORDENAMENTO-JUR%C3%8DDICO-BRASILEIRO-CD.pdf>. Acesso em: 25 abr. 2023.

REIS, Ariovaldo Nascimento Ribeiro; VIANA, Geraldo Denison. Crimes virtuais: legislações insuficientes ou ineficiência das autoridades competentes?. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 7, n. 10, p. 1607-1626, out. 2021.

SÁ, Daniely Samara Oliveira Lima de; SILVA, Pâmela Peron. **Da ineficácia da lei Carolina Dieckmann na ocorrência de crimes virtuais.** 2020. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/14143/1/Tcc%20definitivo%20enviado%20RUNA.pdf>. Acesso em: 05 fev. 2023.

SALUSTIANO, Daniel Frederick e Silva. **Crimes virtuais no Brasil: elementos configuradores.** 22f. Artigo Científico (Bacharelado em Direito) – Escola de Direito e Relações Internacionais, Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: <<https://periodicos.ufsm.br/revistadireito/article/view/23288>>. Acesso em: 10 fev. 2023.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo. **Anais do 4º Congresso Internacional de Direito e Contemporaneidade**, Santa Maria, p. 1-14, 2017. Disponível em: <<https://repositorio.animaeducacao.com.br/handle/ANIMA/13241>>. Acesso em: 09 fev. 2023.

SANTOS, Gabrielly Dairanne Alves dos. **Crimes virtuais: tratamento legal e limitações no combate aos crimes cibernéticos.** 42f. Monografia (Bacharelado em Direito) – UniEvangélica, Anápolis, 2021. Disponível em: <<https://periodicos.ufsm.br/revistadireito/article/view/23288>>. Acesso em: 11 fev. 2023.

SOUSA, Iara Maria da Silva *et al.* Lei geral de proteção de dados: impactos na vida do cidadão empresas e governo. **Facit Business and Technology Journal**, v. 1, n.33, 2022.

SOUZA, Alexandre Dourado Gomes de. **O avanço dos crimes cibernéticos: um estudo sobre os crimes previstos nas leis 12.737/2012 e 12.735/2012 e a importância da materialidade da prova e seus reflexos no ataque cibernético na rede informática do Superior Tribunal de Justiça em 2020.** 19f. Artigo Científico (curso de Direito) – Centro Universitário FG, Guanambi, 2021. Disponível em: <<https://repositorio.animaeducacao.com.br/handle/ANIMA/13241>>. Acesso em: 09 fev. 2023.

1304

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil, análise a partir do Marco Civil da Internet. **Pensar**,