FACULDADE EVANGÉLICA DE GOIANÉSIA
CURSO DE DIREITO

CRIMES CIBERNÉTICOS: INVASÃO DE PRIVACIDADE E O OLHAR DA JURISPRUDÊNCIA APÓS A VIGÊNCIA DA LEI N° 14.155 DE 2021

EVA GUSMÃO DA FONSECA
THAYNARA SILVA LIMA

GOIANÉSIA
2023

EVA GUSMÃO DA FONSECA
THAYNARA SILVA LIMA

CRIMES CIBERNÉTICOS: INVASÃO DE PRIVACIDADE E O OLHAR DA JURISPRUDÊNCIA APÓS A VIGÊNCIA DA LEI N° 14.155 DE 2021

Artigo Científico apresentado junto ao Curso de Direito da FACEG – Faculdade Evangélica de Goianésia, como exigência parcial para a obtenção do grau de Bacharel em Direito.

Orientador: Prof. Me. Kleber Torres de Moura

GOIANÉSIA
2023

FOLHA DE APROVAÇÃO

CRIMES CIBERNÉTICOS: INVASÃO DE PRIVACIDADE E O OLHAR DA JURISPRUDÊNCIA APÓS A VIGÊNCIA DA LEI N° 14.155 DE 2021

Este Artigo Científico foi julgado adequado para a obtenção do título de Bacharel em Direito e aprovada em sua forma final pela banca examinadora da Faculdade Evangélica de Goianésia/GO- FACEG.

Aprovada em, 05 de julho de 2023

Nota Final ____

Banca Examinadora

Professor Orientador Me. Kleber Torres de Moura

Professora Convidada Me. Simone Maria da Silva

Professora Convidada Me. Maisa Bianquine Dorneles

AGRADECIMENTOS

Agradecemos a Deus por todas as graças e por nos acompanhar em todos os momentos de nossas vidas, nos dando motivação e perseverança para ultrapassar todos os obstáculos que a vida nos impõe.

Agradecemos com muito amor e carinho as nossas famílias e amigos, sem vocês nossos sonhos não teriam sentido, nossas conquistas são mérito também de vocês. Amamos e somos gratas por nos acompanhar e nos apoiar no cotidiano e nas aflições do dia a dia.

Aos professores da FACEG, nossa sincera gratidão, os senhores são responsáveis por tornar possível vencer este momento ímpar das nossas vidas acadêmicas. Nossas sinceras gratulações!

CRIMES CIBERNÉTICOS: INVASÃO DE PRIVACIDADE E O OLHAR DA JURISPRUDÊNCIA APÓS A VIGÊNCIA DA LEI N° 14.155 DE 2021

"CYBER CRIMES: INVASION OF PRIVACY AND THE PERSPECTIVE OF JURISPRUDENCE AFTER THE EFFECTIVENESS OF LAW N°. 14,155 OF 2021"

EVA GUSMÃO DA FONSECA[1]
THAYNARA SILVA LIMA[1]
KLEBER TORRES DE MOURA[2]

[1]Discente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: evagusmao@outlook.com.br; thaynaralima1579@gmail.com
[2]Docente do curso de Direito da Faculdade Evangélica de Goianésia- e-mail: kleber.moura@yahoo.com.br

Resumo: O presente artigo científico trata acerca dos crimes cibernéticos, levando-se em consideração a invasão da privacidade e o olhar da jurisprudência após a vigência da Lei n° 14.155 de 2021. O objetivo geral do atual estudo pretende analisar o entendimento jurisprudencial após a vigência da Lei n° 14.155 de 2021 e delinear se a sua aplicabilidade é efetivamente eficaz no campo prático. Os objetivos específicos pretendem delinear os parâmetros históricos e conceituais do crime cibernético; analisar os aspectos gerais acerca da cibercriminalidade; observar as legislações brasileiras direcionadas ao combate do crime virtual; indicar os principais aspectos da Lei n° 14.155 de 2021 e; analisar a importância da Lei em garantir a proteção da privacidade e a intimidade do cidadão brasileiro no âmbito virtual. A justificativa da pesquisa em desenvolvimento se dá em virtude da sua relevância jurídica e social. A problemática da pesquisa se dá pelas seguintes perguntas: Qual o entendimento jurisprudencial face aos crimes cibernéticos após a vigência da Lei n 14.155 de 2021? As leis de proteção à privacidade direcionadas ao contexto cibernético são eficazes? A metodologia utilizada foi a pesquisa bibliográfica, pelo viés qualitativo, além de ter sido utilizada a pesquisa descritiva. Os principais autores utilizados foram Silva (2019), Rocha (2018), Santos (2022) e Machado (2019). Conclui-se que o entendimento jurisprudencial dispõe maior rigor contra o cibercrime após a vigência da Lei n° 14.155/21 e que mesmo assim as legislações que tratam acerca desta modalidade delitiva carecem de maior eficácia prática.

Palavras-chave: Cibercrime. Lei n° 14.155 de 2021. Lei Carolina Dieckmann. Jurisprudência. Direito à privacidade.

Abstract: This scientific article deals with cyber crimes, taking into account the invasion of privacy and the view of jurisprudence after the validity of Law No. 14,155 of 2021. Law No. 14,155 of 2021 and outline whether its applicability is effectively effective in the practical field. Specific objectives are intended to outline the historical and conceptual parameters of cybercrime; analyze the general aspects of cybercrime; observe the Brazilian legislation directed to combating virtual crime; indicate the main aspects of Law No. 14,155 of 2021 and; to analyze the importance of the Law in guaranteeing the protection of privacy and intimacy of Brazilian citizens in the virtual environment. The justification for the research under development is due to its legal and social relevance. The problem of the research is given by the following questions: What is the jurisprudential understanding of cyber crimes after the validity of Law n 14.155 of 2021? Are privacy protection laws targeting the cyber context effective? The methodology used was bibliographical research, by qualitative bias, in addition to having used descriptive research. The main authors used were Silva (2019), Rocha (2018), Santos (2022) and Machado (2019). It is concluded that the jurisprudential understanding provides greater rigor against cybercrime after the enactment of Law No. 14.155/21 and that even so, the laws that deal with this criminal modality lack greater practical effectiveness.

Keywords: Cybercrime. Law No. 14,155 of 2021. Carolina Dieckmann Law. Jurisprudence. Right to privacy.

INTRODUÇÃO

O presente artigo científico trata acerca dos crimes cibernéticos, levando-se em consideração a invasão da privacidade e o olhar da jurisprudência após a vigência da Lei n° 14.155 de 2021. Nesse sentido, destaca-se que os crimes perpetuados contra a privacidade no cenário cibernético são fáticos e recorrentes na atualidade, insurgindo na vigência da Lei n° 14.15521 que trouxeram alterações face a Lei Carolina Dieckmann, de modo a efetivar o combate a esta modalidade delitiva no âmbito virtual.

Assim, o objetivo geral do atual estudo pretende analisar o entendimento jurisprudencial após a vigência da Lei n° 14.155 de 2021 e delinear se a sua aplicabilidade é efetivamente eficaz no campo prático. Entretanto, em relação aos objetivos específicos, pretende-se delinear os parâmetros históricos e conceituais do crime cibernético; analisar os aspectos gerais acerca da cibercriminalidade; observar as legislações brasileiras direcionadas ao combate do crime virtual; indicar os principais aspectos da Lei n° 14.155 de 2021 e; por fim, analisar a importância da Lei em garantir a proteção da privacidade e a intimidade do cidadão brasileiro no âmbito virtual.

Deste modo, a justificativa da pesquisa em desenvolvimento se dá em virtude da sua relevância jurídica e social. No que concerne a valoração jurídica da temática, tem-se que ao passo que a Lei n° 14.155 de 2021 alterou as disposições da Lei Carolina Dieckmann, referida análise se torna imprescindível, tendo-se em vista a novação da Lei e a novidade que esta desencadeia no cenário jurídico.

Entretanto, em relação a importância social do tema, considera-se que ao passo que as relações sociais também se desenvolverem na atualidade na seara virtual, referida análise é robustecida de valoração direcionada à sociedade, em que pese ser de interesse da coletividade informações que indicam a proteção do direito à privacidade no cenário cibernético.

Assim, a problemática da pesquisa em fomento se origina a partir das seguintes indagações: Qual o entendimento jurisprudencial face aos crimes cibernéticos após a vigência da Lei n 14.155 de 2021?

Logo, para responder as perguntas acima mencionada a metodologia que se apresentou mais pertinente foi a pesquisa bibliográfica, por meio de conteúdos extraídos da legislação em vigência, doutrinas jurídicas e artigos científicos que

versam sobre o tema. Além disso, a pesquisa se deu pelo viés qualitativo, além de ter sido utilizada a pesquisa descritiva para o levantamento de constatações atinentes ao conteúdo discutido no trabalho em tela, ao passo que os principais autores utilizados para referidas constatações foram Silva (2019), Rocha (2018), Santos (2022) e Machado (2019).

Considera-se, contudo, referente a estruturação da pesquisa, que a ordem dos tópicos segue a ordem dos objetivos acima mencionados, ou seja, o primeiro tópico irá abordar os parâmetros históricos e conceituais do crime cibernético, tendo-se em vista uma análise geral acerca da cibercriminalidade, o tópico dois, entretanto, suscitará um panorama das legislações brasileiras direcionadas ao combate do crime cibernético, apontando os principais aspectos da Lei n° 15.155 de 2021 e, por fim, o tópico três realizará uma abordagem referente ao direito à privacidade e a importância da Lei garantir a proteção da privacidade e a intimidade do cidadão brasileiro no âmbito virtual.

1 PARÂMETROS HISTÓRICOS E CONCEITUAIS DO CRIME CIBERNÉTICO: UMA ANÁLISE GERAL ACERCA DA CIBERCRIMINALIDADE

A tecnologia surgiu no mundo de forma a modificar não somente os objetos e equipamentos que a ela se interliga ou é produto de sua força, tal fenômeno também fez com que a sociedade se modificasse (ROCHA, 2018). Pontua-se que a tecnologia e, de modo específico, a internet, que deu vida ao mundo virtual, operou a nível mundial para que as relações humanas se transformassem e assim pudessem surgir novas interações, compartilhamentos e convivência, por mais que esta se estabelecesse através de logaritmos (SILVA, 2019).

Faz-se imprescindível analisar a evolução e os aspectos históricos que permearam o mundo cibernético desde sua gênese, haja vista ser a partir desta compreensão a possibilidade de se depreender os porquês de os moldes virtuais estarem formatados da maneira que estão nos tempos atuais. Sendo assim, menciona-se, em primeiro plano, segundo Rocha (2018), que os meios tecnológicos dos dias hodiernos: “(...) foi alvo de boicotes e rejeição por muitas pessoas,

geralmente as de baixo padrão educacional, que viviam de trabalho braçal durante a Revolução Industrial" (ROCHA, 2018, p. 9).

Em consonância ao indicado, depreende-se que nos tempos remotos a tecnologia era vista por uma parte da camada social com negatividade, especialmente por compreender que o potencial da inteligência artificial poderia tomar o lugar de muitos trabalhadores, inovando o mercado de trabalho e, ao mesmo tempo, construindo uma nova maneira de se relacionar no trabalho e no meio social (SILVA, 2019).

Todavia, indica-se que os primeiros traços de crimes cibernéticos surgiram justamente no contexto da Revolução Industrial, período considerado entre 1760 e 1840, corroborando Milagre que (2016, p. 22): "Em uma noção bastante rudimentar, os primeiros signos de crimes informáticos seriam os primeiros atos de boicote a essas novas tecnologias implantadas nesse período histórico". A partir desta premissa é possível considerar que o campo cibernético trouxe consigo, desde o seu início, benefícios, mas, de modo pontual, problemas relacionados ao seu uso e às ideias a ela pertencentes.

Esclarece-se, contudo, que os crimes informáticos somente ganharam maior expressão anos após a Revolução Industrial, infere-se que tal situação se deu devido aos avanços tecnológicos que propiciaram maiores funcionalidades e interação "humana-digital" no campo cibernético (SILVA, 2019). Neste interim, referente ao surgimento dos crimes interligados à informática, tem-se que a primeira prática desta modalidade delitiva é incerta (ROCHA, 2016).

É importante considerar os conceitos que caracterizam os crimes cibernéticos, sendo assim, deve-se definir, inicialmente, o que é criptografia, uma vez que os crimes cibernéticos dependerem desta para existir. Destarte, para Silva (2019), criptografia é um mecanismo digital utilizado para mascarar ou esconder informações por intermédio da linguagem codificada.

Neste prisma, retomando o olhar para os aspectos evolutivos e históricos da temática em desenvolvimento, pontua-se que a prática da criptografia é bastante antiga, tendo-se evidências de sua utilização no período de divergências entre a Grécia e a Pérsia entre os anos de 500 a 448 antes de Cristo, conflito este que fez surgir a necessidade de transmitir informações de maneira secreta e oculta, de forma

que seu o destinatário conseguisse entender do que se tratava hipotética informação (ROCHA, 2018).

Notabiliza-se, entretanto, que o conceito de criptografia se evoluiu e continua a se evoluir de acordo com os avanços científicos-tecnológicos, atraindo para si olhares de estudiosos para que seus aspectos se evoluíssem (SILVA, 2019). Pontua-se, também, que foi a partir do conceito de criptografia que se teve noção da aparição da internet, na sua forma mais básica e rudimentar, sendo constatável que tal ferramenta também obteve grandes evoluções (ROCHA, 2018).

Após a Guerra Fria, ou seja, após o ano de 1991, principalmente devido aos aspectos que necessitavam do uso da tecnologia e insurgisse preceitos evolutivos face à internet, ocorreu uma profunda revolução tecnológica (SILVA, 2019). Nesse sentindo, de acordo com a perspectiva da atualidade, observa-se que a internet se tornou em uma verdadeira necessidade para a sociedade, estando intrinsicamente ligada ao trabalho, estudos ou lazer do homem moderno, corroborando D'urso que (2017, p. 36):

> Seja para trabalho, estudo ou entretenimento, a internet tornou-se uma necessidade na vida das pessoas, alterando os meios acessá-la, bem como as formas de invadir dispositivos através desta. Seja em notebooks, tablets ou smartphones, a frequência com que as pessoas se mantêm conectadas aumenta a cada dia, os aparelhos, especialmente o celular, tornarem-se essenciais e prevalentes na vida das pessoas.

Logo, superada a conceituação de criptografia e as devidas indicações de sua evolução junto à internet, torna-se consentâneo realizar indicações referentes ao conceito de crimes cibernéticos. Deste modo, o termo "cibercrime" teve surgimento no final dos anos 90, delineada em uma reunião do G-8 que tratava acerca da batalha contra as práticas ilícitas através da internet, de forma a estabelecer critérios punitivos e preventivos para tais práticas (JESUS E MILAGRE, 2016).

Assim, pode-se mencionar que com os avanços das funcionalidades que a internet passou a propiciar, possibilitando que as pessoas pudessem compartilhar dados, imagens, opiniões, além de realizar transações de valores econômicos, trabalhar e ter a internet como meio de obtenção de lucro, fez com que a criminalidade nesta seara se progredisse (TOLEDO, 2017).

Logo, retomando o conceito de cirbercrimes, pode-se defini-lo como qualquer prática delituosa a partir da utilização da internet, podendo-se citar, como exemplo, a consumação de crimes de pedofilia, estelionato, crimes contra a honra, dentre outros, que se consumam via digital (TOLEDO, 2017). Desta maneira, em relação ao contexto brasileiro, pode-se mencionar como um evento marcante da efetivação de um cibercrime, resultando em um forte impacto, o que considera Toledo ao destacar que (2017, p. 25):

> Aqui no Brasil, o Hospital do Câncer de Barretos, e outros administrados pela Fundação Pio XII, tiveram as fichas de seus pacientes sequestradas e o resgate pedido era de quase mil reais por computador em bitcoins (dinheiro virtual). O Hospital ficou com seu sistema desativado por três dias, trabalhando manualmente, o que gerou atrasos e prejuízos a muitos pacientes.

Assim sendo, frente a realidade fática do cirbercrime no Brasil, a legislação pátria passou a se movimentar para tipificar crimes e estabelecer regulamentações quanto ao uso da internet. Mediante ao exposto, considera-se que o Código Penal Brasileiro sofreu alterações que inseriu modalidades delitivas em seu aparato legal com a finalidade de punir eventuais autores de crimes consumados com uso de dispositivo eletrônico ou mediante a utilização da internet (SANTOS, 2022).

Menciona-se que existem crimes perpetuados contra direitos básicos do indivíduo, isto é, existe a violação de direitos do cidadão via internet que são consagrados constitucionalmente, como lesividade ao direito à honra, à isonomia, à privacidade e à intimidade (SILVA, 2019). Isso resplandece que o potencial lesivo dos crimes cibernéticos alcança impactos consideráveis, ao passo que tais violações podem impactar direitos e garantias fundamentais do homem esculpidos no artigo 5° da Constituição Federal de 1988.

Neste interim, destaca-se que foi inserido no artigo 184 do Código Penal o parágrafo terceiro, que faz referência à violação de dados autorais se valendo da internet, tratando-se de uma qualificadora para referido crime de forma a majorar a pena base estabelecida no artigo supracitado (BRASIL, 1940). Nesta perspectiva, estabelece-se o parágrafo terceiro do artigo 184 do Código Penal que (BRASIL, 1940, *online*):

> Art. 184. Violar direitos de autor e os que lhe são conexos: (...) § 3° Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente.

Ademais, deve-se constatar que o aparato legal brasileiro que se movimenta para a punição e prevenção do cibercrime conta com a contribuição do Marco Civil da Internet, estabelecida pela Lei n° 12.965 de 2014, legislação responsável por dispor acerca de normas cibernéticas, positivando algumas garantias, princípios, deveres e direitos em relação a utilização da internet no Brasil, além de indicar diretrizes referente a atuação dos entes federados face ao crime cibernético (ROCHA, 2018).

Entretanto, considera-se que o Marco Civil da Internet não positiva nenhuma espécie delitiva de crimes consumados a partir da utilização da internet, o que reverbera o entendimento que o Brasil carece de maiores regulamentações frente a matéria ainda na atualidade. Destaca-se, além disso, que existem outras leis brasileiras que regulamentam o uso da internet, todavia, nenhuma destas legislações estabelecem crimes e suas correspondentes punições, deixando, até mesmo, de positivar acerca de condutas mais graves exaradas na modalidade online (ROCHA, 2018).

Nesse aspecto, estabelece-se que os aspectos evolutivos e conceituais dos crimes cibernéticos obtiveram momentos cruciais como os mencionados, resultando, pela sua capacidade de impactar as relações humanas, políticas e econômicas, na movimentação legislativa e judiciária do Brasil para tentar regulamentar e punir tais práticas. Assim sendo, torna-se indispensável, em seguida, estabelecer indicações acerca das legislações vigentes no Brasil que combatem o crime cibernético, especialmente quanto a Lei Geral de Proteção de Dados e da Lei n° 14.155 de 2021, legislações mais atuais que versam acerca da presente temática e corrobora para a resposta levantada pela problemática do atual trabalho.

2 PANORAMA DAS LEGISLAÇÕES BRASILEIRAS DIRECIONADAS AO COMBATE DO CRIME CIBERNÉTICO: PRINCIPAIS ASPECTOS DA LEI N° 14.155 DE 2021

Devido aos avanços que os crimes no âmbito cibernético vêm alcançando, especialmente no contexto brasileiro, a legislação nacional passou a se preocupar em dispor normas para que tais criminosos sejam devidamente punidos e processados (ROCHA, 2018). Deste modo, salienta-se que atualmente o Brasil possui Leis que tratam exclusivamente dos crimes que ocorrem no mundo virtual, possuindo como uma de suas principais finalidades à proteção da privacidade.

Nesse sentido, deve-se destacar que a Lei n° 12.737 de 2012, conhecida também como Lei Carolina Dieckmann, foi a primeira legislação brasileira a tipificar crimes concretizados nos meios digitais, estabelecendo em seus dispositivos punição para indivíduos que invadem computadores, celulares, dentre outros dispositivos, e violam dados do usuário sem a sua devida anuência (MACHADO, 2019). Quanto a Lei n° 12.732 de 2012, considera Santos que (2022, p. 15):

> A lei ficou conhecida por esse nome devido ao caso ocorrido com a atriz Carolina Dieckmann, quando teve suas fotos íntimas expostas na internet, através de um e-mail infectado, e surgiu para classificar como crime a invasão, sem o consentimento e autorização da vítima, de celulares, tablets, e computadores, que estão ou não conectados à internet, a fim de coletar, eliminar ou adulterar dados ou informações de pessoas físicas ou jurídicas.

Sendo assim, menciona-se que a base legislativa que trata dos crimes cibernéticos se originou, especialmente, devido a ataques perpetuados face ao sistema financeiro, sendo que em tais ações os invasores coletavam dados do indivíduo para realizar transações econômicos sem a devida autorização (MACHADO, 2019).

Além disso, considera-se que outros eventos como, por exemplo, a invasão na rede social *LinkedIn*, que expôs os dados pessoais de mais de 117 milhões de usuários, além de permitir o acesso a senhas, resultando no vazamento que expôs dados pessoais como endereço de e-mail e nome de usuários, fez com que a

legislação voltada para o âmbito virtual também se evoluísse ainda mais após a vigência da Lei Carolina Dieckmann (MACHADO, 2019).

Considera-se também que o ataque face ao Banco do Estado de Sergipe, em outubro de 2021, por meio da técnica de engenharia social, fez com que cerca de 395 mil chaves do sistema de pagamento instantâneo PIX que estavam sob a tutela do Banco do Estado de Sergipe (Banese), fossem obtidas por hackers, bem como o vazamento de dados em 2022 do Twitter, se comporam como fatores relevantes para que a legislação cibernética se expandisse posterior à Lei Carolina Dieckmann (MACHADO, 2019).

Assim, no relatório divulgado pelo Centro de Recursos de Roubo de Identidade (ITRC) indicam que em 2022 mais de 421 milhões de pessoas tiveram suas informações pessoais roubadas por cibercriminosos, corroborando para que os aspectos legais deste seguimento ainda carece de maiores regulamentações e efetividade face a aplicação das legislações existentes e em vigência (SILVA, 2018).

Considera-se, contudo, que a Lei Carolina Dieckmann traz em seu bojo punições consideravelmente brandas, resultando em críticas quanto às suas disposições, principalmente no que tange em o que a legislação considera como crime, em que pese para se enquadrar na tipificação legal o invasor de dispositivos ter que, necessariamente, passar por alguma barreira antes de chegar aos dados ou informações da vítima (SANTOS, 2022). Sendo assim, caso o invasor acesse os dados e informações de hipotética vítima de maneira livre como, à título de exemplo, um celular sem senha, essa ação não é considerada crime, neste aspecto, a Lei n° 14.155 de 2021 destaca que (BRASIL, 2021, *online*):

> 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.

Desta maneira, em relação a Lei n° 14.155 de 2021, deve-se indicar que ela se configura como a legislação mais atual no que concerne disposições referentes aos crimes cibernéticos. Indica-se, no entanto, que referida legislação trouxe, como

acima destacado, alterações face ao Código Penal, tornando o cenário de combate aos crimes virtuais mais severos no que tange a violação de dispositivo informático, furto e estelionato pela internet ou mediante outra forma eletrônica (LIMA, 2021).

Além disso, destaca-se que a Lei n° 14.155 de 2021 também estabeleceu alterações no Código de Processo Penal, definindo nova competência em casos de estelionato cometido na esfera virtual, ou seja, nos casos das modalidades de estelionatos definidas pela própria Lei (SILVA, 2019). Nesta perspectiva, estabelece o § 4° da Lei n° 14.155 de 2021 que foi inserido ao artigo 70 do Código de Processo Penal (BRASIL, 2021, *online*):

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

Nesse aspecto, observa-se uma maior facilidade para que as vítimas de estelionato cibernético ingressem com a devida ação penal, restando o autor do crime a jurisdição pertencente ao lesado, valorando-se, neste caso, o benefício jurídico face às vítimas. Não obstante, em relação ao Código Penal, assinala-se que além da modificação do tipo penal do crime de invasão de dispositivo informático ou eletrônico, criou-se forma majoradas e qualificadas no tocante ao crime de estelionato (SANTOS, 2022).

Nesta perspectiva, torna-se possível identificar a maneira mais gravosa que o ordenamento jurídico brasileiro atual trata os crimes cibernéticos. Assim, com a inovação trazida pela Lei em análise, a modalidade de fraude eletrônica, ou estelionato eletrônico, teve sua pena majorada, sendo que a reclusão prevista é de quatro a oito anos de reclusão e multa se a fraude é consumada com o uso de informações fornecidas pela vítima ou por terceiro induzido ao erro por intermédio da utilização de redes sociais, envio de correio eletrônico fraudulento ou pela uso de contatos telefônicos, estendendo-se tal penalidade ao uso de qualquer outro meio fraudulento análogo para a obtenção de vantagem indevida, como estabelecido pelo

§ 2°-A do artigo 171 do Código Pena introduzido pela Lei n° 14.155/21 (BRASIL, 2021).

Além disso, face à majoração das penas trazidas pela nova Lei ao Código Penal nos casos de estelionato eletrônico, pontua-se que o § 2°-B do artigo 171 do diploma legal mencionado, indica que face ao enquadramento das ações estabelecidas pelo § 2°-A, como já destacas acima, a pena será aumentada de um a dois terços se considerada a relevância do resultado gravoso, cuja a ação se dá mediante a prática delitiva praticada mediante o uso de servidor mantido fora do território brasileiro (BRASIL, 2021).

Deve-se considerar também que, junta a Lei n° 12.737 de 2012 (Lei Carolina Dieckmann) e as devidas alterações desta trazida pela Lei n° 14.155 de 2021, ambas inseridas no âmbito do Código Penal e no Código de Processo Penal, existem também outras legislações vigentes no Brasil que se conduzem a estabelecer regras e combater crimes que se dão no ambiente cibernético. Nesse sentido pontua-se as disposições previstas no Estatuto da Criança e do Adolescente (Lei n° 8.069/90), a implementação da Lei de Software (Lei Antipirataria n° 9.609/98), Lei de Racismo (Lei n° 7.716/89), e a Lei Geral de Proteção de Dados (LGPD), construindo-se, deste modo, um aparato legal direcionado a aplicabilidade ao cibercrime.

Sendo assim, quanto a LGPD, Lei n° 13.709 de 2018, menciona-se que esta foi sancionada com a finalidade de regularização das atividades de coleta e tratamento de dados pessoais, sendo estes presentes em meios físicos ou digitais, independentemente se realizados por pessoas físicas ou jurídicas, de direito público ou privado (SANTOS, 2022). Considera-se que referida Lei estabeleceu postulados importantes face à proteção de direitos fundamentais de liberdade e privacidade, bem como assegurou a livre formação da personalidade individual no que se refere ao mundo virtual (LIMA, 2021).

Desta maneira, compreende-se que ao se fazer atividades de tratamento de dados pessoais, o sujeito que realizará tais análises deverá deixar explícita o objetivo da operação e as especificidades da obtenção de informações ao titular dos dados, sendo que o possuidor dos dados deverá permitir que tais operações se consumem (MACHADO, 2019). Nesse sentido, observa-se que a LGPD protege as informações e os dados pessoais do indivíduo também no campo virtual, relacionando-se,

portanto, às proteções de informações e dados no campo cibernético estabelecidas pela Lei n° 12.737 de 2012 no que se refere à proteção de informações oriundas da vida privada (BRASIL, 2012).

Entretanto, no que se refere a Lei de Software (Lei Antipirataria n° 9.609/98), menciona-se que tal legislação protege os direitos de autor e registro, estabelece garantias aos usuários de programa de computador, pontua regras de contrato de licença de uso, comercialização e de transferência de tecnologia, positiva acerca de infrações, bem como as suas respectivas punições, no que concerne a violação de direitos do autor de programa de computador (BRASIL, 1998). Deste modo, percebe-se que a legislação em tela também se conduz a proteger direitos constitucionais exercidos no ambiente cibernético, especificamente, em relação à Lei de Software, os direitos autorais que resultam em um programa de computador (BRASIL, 1988):

Todavia, constata-se que, além das leis mencionadas, o Estatuto da Criança e do Adolescente (Lei n° 8.069 de 1990), também considera dispositivos voltados à proteção de direitos que se desenvolvem no campo cibernético para pessoas com idade inferior dezoito anos (BRASIL, 1990). Logo, o artigo 241-A do Estatuto em análise estabelece punição para quem oferecer, trocar, disponibilizar, dentre outros, inclusive mediante o sistema de informática ou telemático, fotos, vídeos ou outro conteúdo que possua cena de sexo explícito ou pornográfico envolvendo criança ou adolescente (BRASIL, 1990).

Sendo assim, nota-se de modo reiterado que o atual aparato legislativo brasileiro se direciona ao combate dos crimes cibernéticos. Além disso, considera-se que a Lei de Racismo (Lei n° 7.716/89), também preceitua em seu § 2° do artigo 20 que terá a pena majorada quem “praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional” através de “publicação em redes sociais, da rede mundial de computadores ou de publicação de qualquer natureza”, corroborando que as disposições incriminadoras e punitivas referentes a seara cibernética se faz presente no contexto nacional (BRASIL, 1989, *online*).

Mediante ao exposto, verificando o atual cenário legislativo contra os crimes cibernéticos, retoma-se que a Lei n° 14.155 de 2021 trouxe alterações relevantes no que tange à invasão da privacidade e outras modalidades delitivas perpetuados no

campo eletrônico e/ou no âmbito da internet. Nesse contexto, analisa-se, em seguida, os atuais entendimentos dos Tribunais no que tange as modalidades de crimes cibernéticos trazidos pela nova Lei n° 14.155 de 2021, compreendendo-se como a proteção de dados e informações virtuais são asseguradas pelo Poder Legislativo e Judiciário na atualidade brasileira.

3 DIRETO À PRIVACIDADE: A IMPORTANCIA DA LEI GARANTIR A PROTEÇÃO DA PRIVACIDADE E A INTIMIDADE DO CIDADÃO BRASILEIRO NO ÂMBITO VIRTUAL

Reitera-se que a Lei n° 14.155 de 2021 trouxe modificações consideráveis no escopo do Código Penal no sentido de agravar as penalidades inerentes aos crimes de violação de dispositivo informático, estelionato e furto consumados de maneira eletrônica ou pela internet, além disso, alterou também o Código de Processo Penal no tocante a competência face as modalidades de estelionato virtual (BRASIL, 2021).

Entretanto, considera-se que a Lei n° 14.155/21 não reformulou somente a legislação penal no tocante aos crimes com reflexos e efeitos patrimoniais perpetuados na seara eletrônica ou mediante a utilização da internet. Deste modo, deve-se indicar que a legislação em análise também estabeleceu crimes cibernéticos que se consumam devido a violação da privacidade dos indivíduos (BRASIL, 2021).

Nesse sentido, em relação ao mencionado, depreende-se que o direito à privacidade é estabelecido pela Constituição Federal de 1988, dispondo no seu artigo 5°, inciso X que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988, *online*). Neste mesmo seguimento, o Código Civil estabelece em seu artigo 21, o seguinte: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2002, *online*).

Assim, vê-se que a legislação brasileira positiva postulados que se portam como assecuratórios frente ao direito à privacidade, nesse sentido, respectivo bem jurídico tutelado também foi recepcionado pela Lei 14.155/21, cujas disposições estabelecem como crimes e cominam penas para aqueles que invadem a privacidade alheia por meio eletrônico se utilizando ou não da internet (BRASIL, 2021). Destaca-se, contudo, que a vida privada é mais abrangente do que a intimidade, portanto, detentora de parâmetros legais que a defendem no meio eletrônico, especialmente devido os avanços do campo cibernético (SANTOS, 2022).

Sendo assim, deve-se considerar que foram inseridos no arcabouço do Código Penal pela Lei n° 12.737 de 2012 (Lei Carolina Dieckmann), e, posteriormente, modificado pela Lei n° 14.155/21, artigos que possuem a finalidade de proteger os usuários de dispositivos eletrônicos, ao passo que foi positivado pela legislação de 2021 práticas delitivas que se direcionam a combater a prática delitiva contra o bem jurídico “privacidade” no âmbito virtual, estabelecendo-se mediante o artigo 154-A o crime de invasão de dispositivo informático (BRASIL, 2021).

Não obstante, assinala-se que o artigo 154-A foi inserido no Capítulo VI da parte especial do Código Penal em que se é positivado os crimes contra a liberdade individual, na seção IV, estabelecendo-se como um crime contra a inviolabilidade de segredos, o que resultou em modificações da legislação e estabeleceu novos parâmetros à segurança para o Direito Penal informático (SANTOS, 2022). Logo, respectivo artigo inserido pela Lei n° 14.155/21 tem como objetivo proteger os arquivos que se encontram em dispositivos informáticos, sua disponibilidade e a integridade dos dados dos usuários.

Assim sendo, o *caput* do artigo 154-A descreveu quatro condutas típicas, ao passo que a primeira se refere a invadir o dispositivo informático de uso de terceiro, com ou sem conexão à internet, com a finalidade de obter dados ou informações sem a devida autorização, expressa ou tácita, do usuário e/ou proprietário do dispositivo (BRASIL, 2021). Além disso, o artigo em tela também positivou como crime a prática de invadir dispositivo informático de uso de outrem, conectado ou não à rede de computadores, com intermédio de violação imprópria de mecanismo de segurança, com objetivo de adulterar dados ou informações sem a devida autorização, expressa ou tácita, do usuário do dispositivo (BRASIL, 2021).

Ademais, o artigo 154-A também dispôs como crime realizado na seara virtual a invasão de dispositivo informático de uso de terceiros, com conexão ou não a internet, com a finalidade de destruir informações ou dados sem autorização do usuário do dispositivo e a prática de invadir dispositivo informático de uso de outrem, conectado ou não à internet, com o objetivo de instalar programas aptos a estabelecer vulnerabilidades para a obtenção de vantagem ilícita (BRASIL, 2021).

Nesse sentido, o artigo 154-A do Código Penal, estabelecido pela Lei n° 14.155 de 2021, dispõe acerca do crime de invasão de dispositivo informático de uso alheio ou à rede de computadores com a finalidade de adulterar ou destruir dados ou informações sem a devida autorização do usuário do eventual dispositivo, bem como a conduta de instalar vulnerabilidades em tais dispositivos (BRASIL, 2021).

Nesta perspectiva, notabiliza-se que além dos crimes inseridos pela Lei n° 14.155/21, respectiva legislação também trouxe ao artigo 154-A a equiparação da invasão informática com o oferecimento, produção, venda, distribuição e a difusão de programa de computador ou de dispositivo com a finalidade de permitir a prática de conduta estabelecida no *caput* do artigo em tela. Deste modo, o § 1° do artigo 154-A do Código Penal visa punir os intermediadores e criadores de dispositivos ou programas de computador que possam facilitar, resultando em vulnerabilidades, o dispositivo eletrônico ou, que possam permitir maior facilidade face a invasão de dispositivos (BRASIL, 2021).

Entretanto, o § 2° do artigo supracitado fez originar uma causa de aumento de pena específica frente ao crime do *caput* do artigo 154-A, sendo respectiva causa de aumento atrelada a verificação do prejuízo financeiro (BRASIL, 2021). Ademais, o § 3° no artigo em evidência estipulou uma qualificadora para o crime de invasão de dispositivo eletrônico, estabelecendo penas mínimas e máximas superiores as previstas no *caput*, cominando reclusão de dois a cinco anos e multa em ocasiões em que a prática delitiva resultou em consequências especiais (BRASIL, 2021).

Nesse interim, considera resultados especiais a obtenção de conteúdo de comunicações eletrônicas de natureza privada que contenha segredos comerciais ou industriais, bem como informações sigilosas definidas em Lei ou controle remoto desautorizado ao dispositivo objeto de invasão (SANTOS, 2022). Em consonância ao indicado, menciona-se que o § 4° do artigo 154-A dispõe acerca de causo de

aumento de pena específica frente a figura qualificada referida acima (BRASIL, 2021).

Tal causa de aumento de pena face a figura qualificada do crime se dá quando em casos de obtenção de dados, além de se obter as informações, há também a divulgação, transmissão a outrem ou comercialização, a qualquer título, dessas informações ou dados (BRASIL, 2021). Contudo, o § 5° do artigo 154-A menciona o grupo de pessoas que em situações de ataque ou invasão de comunicações privadas, obter segredos, acesso remoto ou informações de cunho sigiloso, irá resultar em maior rigor na aplicabilidade da Lei (BRASIL, 2021).

Nessas situações em que alguma das pessoas mencionadas pelos incisos do § 5° do artigo 154-A do Código Penal forem vítimas de alguma das modalidades delitivas de invasão de dispositivo eletrônico, aumentar-se-á a pena de um terço à metade (BRASIL, 2021). Além disso, destaca-se que a Lei n° 14.155/ 21 alterou o artigo 155 do Código Penal que prevê o crime de furto, estabelecendo-se por meio dos §§ 4° B e C que (BRASIL, 2021, *online*):

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

Mediante ao exposto, notabiliza-se que a Lei n° 14.155 de 2021 trouxe maior rigor também aos crimes contra os patrimônios perpetuados no campo virtual ou face a algum dispositivo eletrônico, estabelecendo causas de aumento de pena em relação a pena cominado pelo *caput* do artigo 155 do Código Penal (BRASIL, 2021). Deste modo, vê-se que há o aumento de pena quando se tem a utilização de programa malicioso para a violação de mecanismos de segurança, além de ser estabelecidos aumentos em casos em que o crime é praticado com uso de dispositivos localizados fora do Brasil ou se praticado contra idoso ou pessoa vulnerável (BRASIL, 2021).

Outrossim, menciona-se que com a vigência da Lei n° 14.155 de 2021 os Tribunais Superiores passaram a exarar novos entendimentos acerca dos crimes relacionados a invasão de dispositivos eletrônicos conforme positivado no artigo 154-A do Código Penal. Nesse sentido, em relação ao § 2° do artigo mencionado, em que se fez originar uma causa de aumento de pena específica frente ao crime do *caput* do artigo 154-A, sendo que respectiva causa de aumento é atrelada a verificação do prejuízo econômico, o Tribunal de Justiça do estado de São Paulo entendeu que (TJ-SP, *online*):

> INVASÃO DE DISPOSITIVO INFORMÁTICO - materialidade – prova oral e documentos acostados aos autos comprovando a invasão do sistema operacional do site da vítima, da obtenção de informações sigilosas e da alteração de dados do sistema. INVASÃO DE DISPOSITIVO INFORMÁTICO – réu que não se desincumbiu de atestar o alegado – não acolhimento – declaração de vítima apontando o réu como sendo o autor do delito – validade – versão da vítima confirmada pelos e-mails e pelo restante da prova documental acostada aos autos. CAUSA DE AUMENTO – art. 154-A, §2º, do CP - e-mail, comprovante de depósito e prova oral indicando o prejuízo econômico suportado pela vítima. (TJSP; Apelação Criminal 3003607-07.2013.8.26.0586; Relator (a): Mens de Mello; Órgão Julgador: 6ª Câmara de Direito Criminal; Foro de São Roque - 1ª Vara Criminal; Data do Julgamento: 24/08/2017; Data de Registro: 29/08/2017).

Assim, compreende-se que respectivo entendimento jurisprudencial ao tratar do crime de invasão de dispositivo eletrônico em que houve a violação de mecanismos de segurança, resultando em obtenção de informações sigilosas da vítima e, ainda, em que o acusado chantageou a vítima financeiramente para que não vazasse as informações, fazendo com que ela contratasse um serviço de segurança e se dispendesse do valor de dois mil reais, restou entendido pelo Tribunal de Justiça de São Paulo que referida situação se enquadra na causa de aumento de pena prevista no § 2° do artigo 154-A do Código Penal, isto é: “Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico” (BRASIL, 2021, *online*).

Além disso, a jurisprudência do Tribunal de Justiça do Distrito Federal realizou entendimento no tocante a procedimentos tendentes a obter elementos que possam instruir futura ação penal que impute a alguém a prática do crime do art. 154-A, do Código Penal. Deste modo, o artigo 154-B do Código Penal estabelece que (BRASIL, 2012, *online*): “Nos crimes definidos no art. 154-A, somente se procede mediante

representação, salvo se o crime é cometido contra a administração pública direta ou indireta (...)". Nesta perspectiva, a jurisprudência do TJ-DF, no tocante a ação penal dos crimes estabelecidos pelo artigo 154-A, firmou que (BRASIL, TJ-DF, *online*):

> (...) 2. Nos termos do art. 4º, caput e parágrafo único, do CPP, é de incumbência das autoridades investigatórias oficiais do Estado (Polícia Judiciária, Ministério Público, Banco Central, CVM, COAF, entre outros) a tarefa de realizar investigações criminais tendentes a obter a responsabilização criminal de alguém. Somente a Polícia Judiciária (ordinariamente) e o Ministério Público (este em caráter excepcional) podem conduzir procedimentos tendentes a obter elementos que possam instruir futura ação penal que impute a alguém a prática do crime do art. 154-A, do CP (TJDF; APC 07170.67-64.2020.8.07.0001; Ac. 135.6381; Quarta Turma Cível; Rel. Des. Arnoldo Camanho; Julg. 15/07/2021; Publ. PJe 30/07/2021).

Paralelamente, o Superior Tribunal de Justiça (STJ) entendeu pela manutenção das medidas cautelares de proibição de acesso à internet face ao cometimento do crime previsto no § 3° do artigo 154-A do Código Penal. Neste aspecto, vê-se que a atuação do Poder Judiciário também está seguindo parâmetros menos brandos quanto a prática de crime de violação de dispositivo eletrônico. Assim sendo, a jurisprudência do STJ menciona que (BRASIL, STJ, *online*):

> A restrição de acesso à internet pode representar a suspensão do exercício da atividade econômica do paciente, assim como ocorre com os servidores públicos, com os advogados, com os médicos e demais profissionais que se valem das suas profissões para o cometimento de delitos, tudo com espeque no art. 319, VI do Código de Processo Penal. A duração de tal medida excepcional deve passar pelo crivo revisional do Juiz da causa, até mesmo de ofício, considerando os princípios e garantias constitucionais pertinentes. (...) (STJ; AgRg-HC 660.315; Proc. 2021/0114159-1; DF; Quinta Turma; Rel. Min. Reynaldo Soares da Fonseca; Julg. 19/10/2021; DJE 25/10/2021).

Desta maneira, corrobora-se que a Lei n° 14.155 de 2021 trouxe modificações consideráveis face ao Código Penal no que tange a violação da privacidade por meio de mecanismos eletrônicos. Assim sendo, as jurisprudências atuais estão seguindo entendimentos que colocam maior rigor àqueles que comentem o crime do artigo 154-A do Código Penal, inferindo-se, a partir das interpretações dos Tribunais Superiores, que os crimes cibernéticos ao passo que aumentam na sociedade

brasileira atual, também sofrem maior represália pelo Poder Judiciário e se torna alvo cada vez mais severo do Código Penal.

Todavia, importa considerar, que devido ao relatório divulgado pelo Centro de Recursos de Roubo de Identidade (ITRC), ao indicar que em 2022 mais de 421 milhões de pessoas tiveram suas informações pessoais roubadas por cibercriminosos, a legislação que trata sobre a proteção do direito à privacidade no âmbito virtual ainda carece de efetividade quanto a sua aplicação (SANTOS, 2022). Assim, menciona-se que após a vigência da Lei n° 14.155 de 2021, mesmo com o seu conteúdo mais severo do que os trazidos pela Lei Carolina Di, no campo prático se deve maiores implementações para o efetivo combate à invasão de privacidade perpetuada na seara virtual.

Assim, como um resolução para referida problemática, pode-se indicar maior criteriosidade no que tange o acesso à informação virtual, sendo que para tal deveria se ter barrreiras de segurança com maior efetividade no que concerne mencionada proteção. Logo, vê-se, embora ainda se tenha que evoluir no que concerne a eficácia da Lei n° 14.155 de 2021 no combate à invasão da privacidade no contexto virtual, que as Leis que se direcionam a este cenário estão tendentes a se especializar e punir os cibercrimes, exemplo disso é a vigência da Lei contra *Fake News,* que estabelece punição para as falsas informações perpetuadas no munda cibernético.

CONSIDERAÇÕES FINAIS

Conclui-se que a Lei n° 12.737 de 2012, conhecida também como Lei Carolina Dieckmann, foi a primeira legislação brasileira a tipificar crimes concretizados nos meios digitais, estabelecendo em seus dispositivos punição para indivíduos que invadem computadores, celulares, dentre outros dispositivos, e violam dados do usuário sem a sua devida anuência.

Arremata-se, contudo, que a Lei Carolina Dieckmann traz em seu bojo punições consideravelmente brandas, o que resultou em críticas quanto às suas disposições, principalmente no que tange em o que a legislação considera como crime, em que pese para se enquadrar na tipificação legal da Lei supracitada o

invasor de dispositivos ter que, necessariamente, passar por alguma barreira antes de chegar aos dados ou informações da vítima.

Além disso, pode-se concluir, em relação a Lei n° 14.155 de 2021, que ela se configura como a legislação mais atual no que concerne disposições referentes aos crimes cibernéticos. Desta maneira, depreende-se que a Lei n° 14.155 de 2021 trouxe alterações face à Lei Carolina Dieckmann, além de também ter estabelecido alterações no Código de Processo Penal, definindo nova competência em casos de estelionato cometido na esfera virtual.

Nesse sentido, contata-se que com a vigência da Lei n° 14.155 de 2021 houve maior facilidade para que as vítimas de estelionato cibernético ingressem com a devida ação penal, restando o autor do crime à jurisdição pertencente ao lesado, valorando-se, neste caso, o benefício jurídico face às vítimas, entendimento este corroborado pela jurisprudência do Tribunal de Justiça do Distrito Federal.

Conclui-se, além disso, que foram inseridos no arcabouço do Código Penal pela Lei n° 12.737 de 2012 (Lei Carolina Dieckmann), e, posteriormente, modificado pela Lei n° 14.155/21, artigos que possuem a finalidade de proteger os usuários de dispositivos eletrônicos, ao passo que foi positivado pela legislação de 2021 práticas delitivas que se direcionam a combater a prática delitiva contra a bem jurídica “privacidade” no âmbito virtual.

Sendo assim, pode-se concluir que o artigo 154-A foi inserido no Capítulo VI da parte especial do Código Penal em que se é positivado os crimes contra a liberdade individual, na seção IV, estabelecendo-se como um crime contra a inviolabilidade de segredos, o que resultou em modificações da legislação e estabeleceu novos parâmetros à segurança da privacidade frente ao Direito Penal informático.

Nesse sentido, conclui-se, no que concerne o entendimento jurisprudencial após a vigência da Lei n° 14.155 de 2021, ao tratar do crime de invasão de dispositivo eletrônico em que houve a violação de mecanismos de segurança, resultando em obtenção de informações sigilosas da vítima e, ainda, em que o acusado chantageou a vítima financeiramente para que não vazasse as informações, fazendo com que ela contratasse um serviço de segurança, que

referida conduta é considerada restou configurada como crime de violação de privacidade na modalidade qualificada, havendo, portanto, a majoração da pena.

Além disso, conclui-se que o Superior Tribunal de Justiça (STJ) entendeu pela manutenção das medidas cautelares de proibição de acesso à internet face ao cometimento do crime previsto no § 3° do artigo 154-A do Código Penal. Outrossim, vislumbra-se que que devido ao relatório divulgado pelo Centro de Recursos de Roubo de Identidade (ITRC), ao indicar que em 2022 mais de 421 milhões de pessoas tiveram suas informações pessoais roubadas por cibercriminosos, a legislação que trata sobre a proteção do direito à privacidade no âmbito virtual ainda carece de efetividade quanto a sua aplicabilidade no campo prático.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL, **Constituição da República Federativa do**. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 e 11 de abr. de 2023.

BRASIL. Decreto Lei n° 2.848 de 7 de dezembro de 1940. **Código Penal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 12, 15, 18 e 20 de mai. de 2023.

BRASIL, **Lei n° 12.965 de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15, 20, 25, 26 e 27 de mai. de 2023.

BRASIL, Lei n° 13.709 de 14 de agosto de 2018. **Lei Geral de Proteção de dados Pessoais**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 e 12 de mai. de 2023.

BRASIL, **Lei n° 12.737 de 30 de novembro de 2012**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 de mai. de 2023.

BRASIL, **Lei n° 14.155 de 27 de maio de 2021**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 15, 16, 17, 20 e 23 de mai. de 2023.

BRASIL, Decreto-Lei n° 3.689 de 3 de outubro de 1941**. Código de Processo Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 10 e 11 de mai. de 2023.

BRASIL, Lei n° 8.069 de 13 de julho de 1990. **Estatuto da Criança e do Adolescente**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 18 e 23 e mai. de 2023.

BRASIL, Lei n° 10.695 de 1 de julho de 2003**. Lei de Software**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.695.htm. Acesso em: 20 e 23 de mai. de 203.

BRASIL, **Lei n° 7.716 de 5 de janeiro de 1989**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 18 e 23 de mai. de 2023.

BRASIL, **Lei n° 10.741 de 1 de outubro de 2003**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Acesso em 10 de mai. de 2023.

BRASIL, Lei n 10.406 de 10 de janeiro de 2002. **Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 02 e 05 de mai. de 2023.

D'URSO, Luiz Augusto Filizzola. **Cibercrime**: perigo na internet. São Paulo: Revista dos Tribunais, 2017.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

JUSTIÇA, Tribunal de. São Paulo. **TJ-SP**. Disponível em: https://www.tjsp.jus.br/. Acesso em 06 e 07 de mai. de 2023.

JUSTIÇA, Tribunal de. **TJDFT**. Distrito Federal. Disponível em: https://www.tjdft.jus.br/. Acesso em: 05 e 09 de mai. de 2023.

JUSTIÇA, Superior Tribunal de. **STJ**. Disponível em: https://www.stj.jus.br/sites/portalp/Inicio. Acesso em: 10 e 12 de mai. de 2023.

LIMA, Cláudio Vieira Guimarães. **Crimes cibernéticos**: o lado obscuro da rede. Goiânia: PUC-GO, 2021.

MACHADO, ANDRÉ. **Especialistas explicam como computador de Carolina Dieckmann foi hackeado**. São Paulo; Saraiva, 2019.

MILAGRE, Antônio Eudes Nunes. **A internet e a globalização**. Rio de Janeiro: Lúmem, 2016.

NOVELINO, Marcelo. **Manual de Direito Constitucional**. 2. ed. São Paulo: Método, 2013.

ROCHA, Adriano Aparecido. **Cibercriminalidade**: os crimes cibernéticos e os limites da liberdade de expressão na internet. São Paulo: FEFI, 2018.

SANTOS, Matheus Cristini Vieira. **Crime cibernético**: invasão de privacidade por meio da internet. São Paulo: IESGAE, 2022.

SILVA, Lindenberg Barros. **Redes de computadores**: guia total. 1. ed. São Paulo: Érica, 2019.

TOLEDO, Marcelo. **Hackers invadem sistema do Hospital do Câncer de Barretos e pedem regaste**. São Paulo: Saraiva, 2017.