LUMEN ET VIRTUS
ISSN: 2177-2789

CRIMES CIBERNÉTICOS: A RELEVÂNCIA DAS ALTERAÇÕES PROMOVIDAS PELA LEI 14.155/2021 NO TOCANTE AOS CRIMES PATRIMONIAIS

https://doi.org/10.56238/levv16n47-106

Data de submissão: 25/03/2025 **Data de publicação:** 25/04/2025

Ana Júlia Sousa Evangelista
Acadêmico do 9° período do Curso de Direito do Instituto de Ensino Superior do Sul do Maranhão-IESMA/Unisulma, turno: Noturno.
E-mail: anajuliaeva@gmail.com

Hugo Hayran Bezerra Silva
Orientador
Graduado em Direito/FEST. Pós-graduado em Direito Penal/IBMEC. Mestre em Desenvolvimento Regional/UNIALFA.
E-mail: hugohayra@outlook.com

RESUMO

O presente artigo teve como objetivo apresentar a evolução da legislação brasileira para regular os crimes cibernéticos. Para isso, foi necessário entender como esta espécie de ilícito penal é tipificado na legislação penal, com a finalidade de compreender as consequências jurídicas aplicáveis. Com o propósito de prevenir a execução de crimes cibernéticos, foram promulgadas algumas legislações, entre elas a lei 14.155/2021, a qual é objeto de estudo nesse artigo, trazendo algumas alterações nos crimes patrimoniais cometidos por meio da internet, fazendo um comparativo com a lei 12.737/2012, observando os pontos essências entre ambas, assim causando impactos na sociedade da informação por meio da inserção e alteração de artigos do Código Penal Brasileiro. O presente trabalho utilizou a revisão bibliográfica, fazendo análise e interpretação de materiais teóricos já publicados sobre um tema específico, usufruiu de fontes secundárias, como livros, artigos científicos, dissertações e teses, para explorar o que já foi discutido e descoberto sobre o tema. Esta pesquisa foi fundamentada em contribuições teóricas de diversos doutrinadores, entre eles Cassanti, (2014), Rossini (2004), Lai e Mourão, (2021). Desta forma, este artigo, buscou analisar detalhadamente o texto da lei supramencionada e de outros objetos jurídicos elaborados, assim como as modificações resultantes ao ordenamento jurídico pátrio.

Palavras-chave: Crimes cibernéticos. Crimes patrimoniais. Legislação brasileira. Lei n° 14.155/2021.

1 INTRODUÇÃO

A internet tem inovado a cada a dia a vida do ser humano, e se tornou indispensável na vida dos indivíduos, pois é uma ferramenta que encurta distâncias, e que aproxima as pessoas, tornando o ser humano dependente da informática.

O número de pessoas com acesso aos meios digitais só cresce, facilitando a comunicação e a transmissão de informações em qualquer lugar do mundo, e substituindo muitos atos do cotidiano pelos sistemas informatizados. Essa inovação trouxe grandes progressos e facilidades, no entanto, também se tornou um meio para a realização de condutas ilícitas perigosas, tornando as pessoas vulneráveis à riscos inerentes a tecnologia da informação. Tais condutas são conhecidas como crimes cibernéticos e existem nas mais diversas formas.

Perante o exposto, o trabalho teve o seguinte problema de pesquisa: como as alterações introduzidas pela Lei nº 14.155/2021 contribuem para o aprimoramento da legislação penal brasileira no combate aos crimes patrimoniais cibernéticos, e em que medida tais mudanças atendem à necessidade de proteção jurídica eficaz contra práticas ilícitas no ambiente virtual?

É necessário colocar em destaque que o Direito está constantemente se ajustando às mudanças sociais, ressaltando assim a relevância do assunto em questão, que teve como objetivo geral, analisar a importância das mudanças introduzidas pela Lei nº 14.155/2021 no combate aos crimes cibernéticos, com foco especial nos crimes patrimoniais cometidos por meio de dispositivos digitais. Assim, para a elaboração deste trabalho foram seguidos os objetivos específicos, que delinearam a abordagem metodológica adequada para investigar aspectos críticos e particulares da pesquisa.

Estes objetivos incluíram analisar os impactos jurídicos e sociais das novas disposições no combate aos crimes cibernéticos, principalmente na proteção do patrimônio e segurança dos usuários; estudar as alterações específicas introduzidas pela Lei nº 14.155/2021 no Código Penal, com ênfase nas modificações nos crimes patrimoniais cometidos no ambiente cibernético; comparar as disposições da Lei nº 14.155/2021 com a legislação anterior, especialmente a Lei nº 12.737/2012, para destacar os avanços e as lacunas preenchidas.

Para a finalidade dos objetivos oferecidos, o estudo em tela, encontra-se dividido em três capítulos. O primeiro capítulo, traz um breve histórico do surgimento da internet e a importância dela para a sociedade, e como o Direito penal se conectou a internet, para que seja preservado os direitos dos usuários.

Já no segundo capítulo, estudaremos a essência deste artigo, trazendo o conceito de crimes cibernéticos, e a classificação desses crimes, em tipos e espécies.

E por fim, no terceiro e último capítulo, esse estudo deseja analisar a importância das sanções ocasionadas pela Lei nº 14.155 de 27 de maio de 2021, nos crimes patrimoniais, como a invasão de

dispositivo, furto e estelionato. Para tal, são compartilhadas perspectivas de notáveis especialistas em Direito Penal, como Rossini, Cassanti entre outros.

Além disso, a pesquisa foi inicialmente bibliográfica, buscando em livros, artigos, periódicos e na legislação brasileira, buscando informações que sejam o suficiente para embasar a teoria proposta na presente pesquisa. Vale ressaltar que este estudo não busca abordar exaustivamente todos os aspectos dos crimes virtuais, mas sim, tem como objetivo, contribuir para o combate e conscientização dessas infrações, reconhecendo sua relevância no âmbito jurídico.

2 CONCEITO GERAL DA HISTÓRIA DA INTERNET NO DIREITO

Para que se inicie a argumentação é essencial saber como a internet surgiu e como ela se tornou fundamental na comuicação da sociedade, portanto, nesta tese serão abordados as principais noções sobre o surgimento da internet, e qual a sua conexão com o direito.

2.1 O SURGIMENTO E A IMPORTÂNCIA DA INTERNET NA SOCIEDADE

A internet tornou-se necessária na nossa sociedade, é uma feramenta que veio facilitar a vida das pessoas, pois é um utensílio que encurta distâncias, e que aproxima as pessoas, tornando o ser humano dependente dela.

O número de pessoas com acesso aos meios digitais só crescem, e estão sendo, cada vez mais, aperfeiçoados, facilitando a comunicação e a transmissão de informações em qualquer lugar do mundo, surgindo assim a expressão “sociedade da informação” (WERTHEIN, 2000), assim o desenvolvimento da sociedade do século XVI, acontece de uma forma mundial e não local. Para Castells (2000), toda essa essa comunicação e a reconstrução do capitalismo está ligada ao desenvolvimento informacional da socidade “pós industrial”, sendo assim, uma forma organizacional econômica e social baseada nas novas tecnologias, especificamente ao avanço da Internet.

Mais o que vem ser a internet essa ferramenta que se tornou indispensável na vida das pessoas, a internet é uma extensa rede de computadores interligadas no mundo inteiro e plugadas por meio de cabos, linhas discadas (telefônicas), tecnologia de micro-ondas, satélite de comunicações e outros meios de telecomunicações.

> A internet é um conjunto de redes de comunicações em escala mundial e dispõe de milhões de computadores interligados pelo protocolo de comunicação TCP/IP, que permite o acesso a informações e todo tipo de transferência de dados. A Internet carrega uma ampla variedade de recursos e serviços num espaço virtual também chamado de ciberespaço, daí que, como no mundo real, a segurança digital é um terreno de ferrenha disputa entre defensores e agressores. (CASSANTI, 2014, p. 01)

A internet surgiu durante a Guerra fria no decorrer das décadas de 70 e 80. A partir desse começo, a sua evolução é efêmera comparada a outras tecnologias. Sendo desenvolvida pelos os Estados Unidos da América com a finalidade militar.

Segundo BRITO, Auriney (Saraiva, 2013. p.21).

> "[...] No histórico da internet, a ARPANET figura como a principal fonte de criação da internet, mas não como a única. Paralelamente à ARPA, jovens cientistas trabalhavam em projetos em busca do estabelecimento de comunicação entre computadores, quando, a partir da década de 1970, pode-se verificar que várias outras formas descobertas".

O autor cita que a ARPANET que é Administração de Projetos e Pesquisas Avançados. Projeto desenvolvido para uso exclusivo das forças americanas, o que seria um dos experimentos de onde deu início à internet.

A demora para que essa tecnologia alcançasse outros países foi pouca, o Brasil é um exemplo, pois foi iniciada através da conexão entre centros universitários brasileiros e americanos. A partir desse início, seu avanço foi rápido e contínuo. Assim as novas tecnologias e a necessidade de conquistar cada vez mais usuários, a internet alavancou uma desenfreada produção de vários outros equipamentos eletrônicos que conectam o usuário à rede.

> "[...] a partir do segundo semestre do ano de 2011 acompanhamos um aumento muito expressivo dos chamados dispositivos móveis como celulares, smartphones e tablets. Com isso, os ataques virtuais que antes eram restritos aos computadores estão migrando para as plataformas móveis" (CASSANTI, 2014, p.17)

A tecnologia trouxe consigo a modificação não somente dos objetos e equipamentos que a ela se interliga, mas tal fenômeno fez com que a sociedade se modificasse (ROCHA, 2018). Observa -se que a tecnologia 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).

A internet é um instrumento que tem grande importância no mundo todo, o seu uso trouxe vários benefícios em todas as áreas e atividades tornando-se imprescindível na vida das pessoas. Essa inovação trouxe grandes progressos e facilidades, no entanto, também se tornou um meio para a realização de condutas ilícitas perigosas, tornando as pessoas vulneráveis à riscos inerentes a tecnologia da informação. Tais condutas são conhecidas como crimes cibernéticos e existem nas mais diversas formas.

2.2 CONEXÃO ENTRE O DIREITO E A INTERNET

O Marco Civil da Internet no Brasil, também conhecido como Lei nº 12.965 de 2014, encontrou dificuldades desde o projeto até a sua promulgação, sendo **s**ancionado em 2014, pela então presidente Dilma Rousseff. Porém**,** o início de sua trajetória se deu em 2009 e o projeto de lei tramitou desde 2011 entre as casas legislativas.

Mesmo com todas as dificuldades esta lei possui uma importância enorme para evolução tecnológica o Brasil, pois ela possui o objetivo de regular os direitos, garantias e deveres no uso da internet. Estabelecendo princípios que tornam a internet no Brasil mais segura e democrática. Mas apesar, desse surgimento de nova fase da sociedade no século XXI, o Direito não acompanhou a evolução tecnológicas, sobretudo em relação á prática de crimes virtuais. Dessa forma, o Marco Civil apresenta diretrizes importantes para a utilização da Rede Mundial de Computadores. Mas apesar da criação da Internet e da emergência da Constituição Federal de 1988, vale destacar que:

> Essa Constituição chega em um momento de grande maturidade para a democracia brasileira, em que o país, havendo repelido uma lei de imprensa das mais sombrias origens, encontra-se a trilhar caminhos mais balanceados na ponderação entre a liberdade de expressão e outros direitos e garantias fundamentais. A questão que se apresenta agora é como fazê-lo no ambiente da Internet. Como estruturar os compromissos normativos e tecnológicos que compõe a Internet no Brasil para que ela seja, ainda que um instrumento de destruição criativa, também um espaço para preservação de certos valores essenciais não somente à sua natureza, como meio, mas à nossa dignidade como fim (THOMPSON, 2012, p. 3).

Apesar da regulamentação do Marco Civil, ainda há lacunas que precisam ser preenchidas, pois o Marco Civil da Internet direcionou a forma de realizar negócios na internet e também diversas formas de entretenimento, mas não estabelece sanções penais e sim, orientações acerca das condutas feitas no ambiente virtual. Vale exemplificar, que pretações de serviços por empresas devem apresentar clareza aos usuários da Rede Mundial de Computadores, assim tem a necessidade de proteção de dados cadastrais dos clientes.

Dessa forma, a privacidade, "a intimidade e outros direitos constitucionais previstos na nossa costituição também estão inseridos na Lei 12.965/14" (MARRA,2019, p. 07). Assim, o que tange á liberdade de expressão, que é garantida na nossa Constituição de 1988, precisa se moldar a realidade da internet. Dessa forma, o Marco Civil veio ajustar previsões legais aos usuários da Rede.

A tecnologia trouxe consigo a modificação não somente dos objetos e equipamentos que a ela se interliga, mas tal fenômeno fez com que a sociedade se modificasse (ROCHA, 2018). Observa -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).

Assim, o reconhecimento que temos, direitos garantidos na nossa Constituição Federal de 1988, devemos buscar entender que um ambiente virtual, possui necessidades e demandadas diferentes. Dessa forma, toda a evolução da internet e as novas formas de comunicação, fazem com que o Direito, e especificamente o Direito Penal e Processual Penal, precisam de uma nova dinâmica sobre as ameaças vindas do uso indevido da Internet. E uma das necessidades especifica é a solução dos crimes virtuais, os quais são praticados através dos aparelhos informáticos.

3 CONCEITOS GERAIS DE CRIME CIBERNÉTICO

Para começar uma argumentação é preciso a compreensão de crimes cibernéticos, por isso, neste tópico serão discurtidos os conceitos fundamentais e onde essa espécie de delito se adequa no nosso ordenamento jurídico.

3.1 CRIMES CIBERNÉTICOS

A princípio, é necessário recorrer ao Código Penal Brasileiro, que em seu artigo 1° define crime como a infração penal que a lei comina pena de reclusão ou de detenção, isolada, alternativa ou cumulativamente com pena de multa (BRASIL, 1940).

Suncidamente, crime é toda conduta típica, antijurídica e culpável, ou seja, é tudo aquilo que contraria ao que está disposto na lei e no ordenamento jurídico de um país. Dessa forma os crimes cibernéticos, são atividades ilegais realizadas valendo-se da tecnologia, com o objetivo de acessar ou comprometer sistemas computacionais.

A internet é a via pela a qual há comunicação, trocas de informação e transferência de dados, e com o avanço dessa ferramenta muitas ações manuais ou presenciais, foram substituídas por atividades digitais e online. E ao mesmo tempo, abriu-se uma porta para a prática de ações criminosas, conhecidas como crimes cibernéticos.

Conforme Cassanti (2014), crimes virtuais podem ser definidos como:

> Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital. Crimes virtuais são delitos praticados através da internet que podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão (Cassanti,2014, p. 03)

Para Rossini (2004), a definição de crime cibernético poderia ser descrita como uma ação que se enquadra nos critérios de tipicidade e ilegalidade, configurando um delito ou violação, intencional ou negligente, de natureza ativa ou passiva. Esse conceito engloba elementos como a integridade, disponibilidade e confidencialidade das informações.

Ademais, quanto à definição de crimes virtuais, a Organização para a Cooperação Econômica e Desenvolvimento da ONU, dispõe: "o crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático e dados ou transmissão de dados" (ROSSINI, 2002).

Os crimes cibernéticos abrangem várias categorias e podem ser divididos em duas vertentes, como sendo os crimes cibernéticos puros ou próprios e os crimes cibernéticos impuros ou impróprios. A classificação desses crimes no direito penal não é simples, pois a evolução da tecnologia é constante, por isso as análises e opiniões dos legisladores sobre o assunto mudam frequentemente.

Deduz -se, que crime cibernéticos é a conduta típica, ilícita e culpável que preenche os pressupostos de crime ou de contravenção penal, ocorrida com dolo ou culpa, executada por pessoa física ou jurídica por meio da informática, seja na Rede Mundial de Computadores ou não, e que vai de encontro à segurança do sistema informático, o qual deve observar a integridade, desimpedimento e a privacidade de indivíduos e entidades.(MARRA, 2019)

3.2 ESPÉCIES DE CRIMES CIBERNÉTICOS

Os crimes cibernéticos podem ser classificados em diversas categorias, dependendo do objetivo, das técnicas utilizadas e do impacto. Alguns desses crimes cibernéticos já existiam em meio a sociedade, porém praticado por outros meios, que não fosse a internet. Os crimes cometidos visivelmente, se desenvolvem e se desenvolveram em uma proporção muito grande, acompanhando os avanços da tecnologia. Mas na WEB, identificar o sujeito ativo do crime é um desafio para o direito, pela a liberdade do anonimato que este meio oferece, e acaba se tornando atrativo para os criminosos.

A classificação desses crimes no direito penal não é simples e nem fácil, pois a tecnologia está em constante evolução, por isso as análises e opiniões dos legisladores sobre o assunto mudam frequentemente.

Conforme Colares (2002), existem diversas espécies de crimes praticados na internet sendo:

> calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, escrito ou objeto obsceno, incitação ao crime, apologia de crime ou criminoso, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões, jogo de azar, crime contra a segurança nacional, preconceito ou discriminação de raça-cor-etnia-etc., pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software. (COLARES, 2002, não paginado)

No entanto, podemos apresentar duas divisões acerca da classificação. A primeira divisão que classifica como crimes puros, crimes mistos e crimes comuns. E uma segunda divisão que estabelecem em crimes próprios e crimes impróprios.

3.2.1 Crimes cibernéticos puros, mistos e comuns

Os crimes cibernéticos puros ocorrem exclusivamente no ambiente digital, ou seja, que só podem ser cometidos por meio de sistemas de informática, redes de computadores, ou a internet. São aqueles praticados por computador e se realizam ou se consomem também em meio eletrônico. Neste tipo de crime, a informática, não em si, mas a segurança dos sistemas, a titularidade das informações, a integridade de dados, da máquina e dos periféricos, é que está sob a proteção legal. Essa prática delituosa possui o objetivo de atingir o sistema de um computador, seja a parte física ou de dados, geralmente praticado por hackers. Para Montes (2020), tem como finalidade a invasão do dispositivo informático, uma violação da integridade física ou lógica do computador e seus sistemas.

No entanto, são crimes nos quais é necessário que o agente criminoso precise imprescindivelmente de um computador para realizar os ataques de maneira remota ou direta. Assim sendo, pode-se dizer que não estão envolvidas apenas a invasão e a captura dos dados salvos em massa, mas também a intenção ruidosa de modificar, adulterar ou destruir dados existentes no computador.

3.2.2 Crimes cibernéticos próprios e impróprios

Os crimes cibernéticos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática. DAMÁSIO, (2016).

Portanto os crimes cibernéticos impróprios são que atingem o bem comum sendo o meio virtual apenas uma das formas de execução do crime, podendo ser praticado por outros meios. Dessa forma, são aqueles que utilizam o sistema informático como meio para a prática de condutas ilícito-típicas já existentes, que já estão previstos na legislação penal tradicional brasileira. JUSTINIANO, (2016)

4 LEI Nº 14.155/2021 DOS CRIMES CIBERNÉTICOS

A Lei nº 14.155/2021, sancionada no Brasil em 27 de maio de 2021, altera o Código Penal para agravar as penas para crimes cometidos mediante o uso de meios eletrônicos, como o uso da internet ou outros dispositivos informáticos. O principal foco da lei é endurecer as penas para crimes de invasão de dispositivos informáticos, fraudes eletrônicas, e outras atividades ilícitas digitais.

Esta lei fez inúmeras alterações no Código Penal para tornar mais graves as penas dos crimes de violação de dispositivo informático, de furto e de estelionato (arts. 154-A, 155 e 171), previstos originalmente no texto de 1941, se cometidos de forma eletrônica ou pela internet, além de modificar a competência de certas modalidades de estelionato no art. 70, § 4º do Código de Processo Penal. (LAI E MOURÃO, 2021).

4.1 ALTERAÇÃO NO TIPO SIMPLES E NA CLÁUSULA DE EQUIPARAÇÃO

Dentre as alterações trazidas pela Lei 14.155/2021 deu-se no crime de invasão de dispositivo informático, previsto no art. 154-A do Código Penal.

Com a tipificação do crime de invasão de dispositivo informático previsto no artigo 154-A do CP, a Lei nº 12.737/2012 reconheceu de forma pioneira a tutela de um novo bem jurídico-penal, a segurança informática, ladeando outros valores fundamentais que merecem a proteção do Direito Penal (ESTEFAM, 2020, p. 440).

O artigo 154-A do Código Penal Brasileiro**,** introduzido pela Lei nº 12.737/2012 (conhecida como Lei Carolina Dieckmann**),** tipifica o crime de invasão de dispositivo informático.

Isso se deu quando o computador da atriz famosa Carolina Dieckmann, foi invadido e, logo em seguida as suas fotos intimas foram divulgadas, as quais constavam no aparelho. Esse caso teve uma repercussão grandiosa e, em razão disso, o legislador pátrio agiu para criar um tipo penal que criminalizasse tal tipo de comportamento.

Dessa forma, o legislador alterou o tipo incriminador e, também, previu maior confirmação para o comportamento, pode-se observar através do quadro abaixo, no qual estão destacando as alterações promovidas:

Lei 12.737/2012	**Lei 14.155/2021**
Art. I54-A. Invadir dispositivo informático alheio, conectados ou não á rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:	Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não á rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – detenção, 03 (três) meses a 01(um) ano, e multa.	Pena – reclusão, de 01 (um) a 04 (quatro) anos, e multa.

FONTE: Elaborado pelo autor, 2024

Realmente, quando se verifica o conteúdo do art.154-A, caput do Código Penal não mais exige, que a invasão de dispositivo informático tenha ocorrido através de "violação indevida de mecanismo de segurança". Como consequência, para a prática a delituosa, agora, pouco importa a violação de mecanismo de segurança, o que implica em alteração prejudicial ao acusado e que, portanto, não pode retroagir. E ainda, a figura típica passa a contar com pena significativamente maior, deixando de ser um crime de menor potencial ofensivo, para passar a figurar entre os crimes de médio potencial ofensivo.

Vale ressaltar que o art. 154-A, *caput* tem uma cláusula de equiparação, prevista em seu § 1º, que positiva o seguinte:

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012).

Verifica-se, que o dispositivo em ênfase confirma a intenção do legislador de criminalizar os atos preparatórios concernentes ao crime de invasão de dispositivo. Assim, há uma antecipação da punição, para reduzir as chances de execução efetiva do comportamento subsequente, a qual se representa um ato lesivo.

O art. 154-A, §1º consubstancia tipo misto-alternativo, praticado por quem realiza quaisquer das condutas nele previstas, ou seja, pratica o delito quem "produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*". Note-se que não basta que a conduta delitiva possibilite a invasão, mas que o agente tenha praticado o comportamento com o intuito de permitir que isso aconteça. (LAI E MOURÃO, 2021).

4.2 MODIFICAÇÃO NA CAUSA DE AUMENTO DE PENA: ART. 154-A, § 2º

Uma das alterações que a Lei 14.155/2021, ocorreu no art. 154-A, § 2º, do Estatuto Repressor, de acordo com o quadro abaixo:

Lei 12.737/2012	Lei 14.155/2021
§2° Aumenta-se pena de um sexto a um terço se da invasão resulta prejuízo econômico.	§2° Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulte prejuízo econômico.

FONTE: Elaborado pelo autor, 2024.

Com essa alteração a penalização por invasão de dispositivo informático se tornou mais severa atendendo a necessidade de proteção dos bens patrimoniais em crimes cibernéticos, estabelecendo um aumento de pena específico para quando há invasão ultrapassar a violação de privacidade e atinge

o patrimônio da vítima. Pois o que antes era apenas com detenção e multa, mesmo em casos de prejuízo econômico.

Mas com a nova alteração, se o delinquente invade o aparelho da vítima e, de posse de fotos íntimas suas, ameaça divulgar as imagens, acaso esta não lhe transfira certa quantia, o jurista estará diante de uma hipótese de extorsão e não de simples invasão de sistema informático. Nesse caso, a realização da transação bancária será exaurimento da extorsão e não hipótese de incidência da aludida majorante. A majorante, assim, é um reforço à punição do *caput*, que não desconstitui o fato deste ser residual/subsidiário em relação a outros tipos. (LAI E MOURÃO, 2021)

4.3 INVASÃO DE DISPOSITIVO INFORMÁTICO QUALIFICADA: AUMENTO DA PENA COMINADA

Ao modificar o tratamento penal para a invasão de dispositivo informático**,** fez ajustes principalmente na pena, a Lei 14.155/2021 o legislador elevou a pena cominada para sua figura qualificada, contida no art. 154-A, § 3º, mas manteve os termos do preceito primário da visando fortalecer a punição e a proteção ao patrimônio digital e à privacidade.

Lei 12.737/2012	Lei 14.155/2021
Art.154 -A, §3°. 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.	Art.154 -A, §3°. 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.
Pena - reclusão de 06 (seis) meses a 02 (dois) anos, e multa, se a conduta não constitui crime mais grave.	Pena- reclusão, de 02 (dois) a 05 (cinco) anos, e multa.

FONTE: Elaborado pelo autor, 2024.

O legislador, manteve os termos do preceito primário, garantiu que a conduta típica continuasse claramente delimitada, aplicável tanto a invasões com objetivo de acessar dados quanto a outras ações invasivas, a figura qualificada do § 3º, que passou a prever pena de reclusão de 2 a 5 anos e multa para situações em que a invasão resulta em: acesso a conteúdo sigiloso, privado, segredo comercial, industrial ou informações sigilosas e prejuízo econômico à vítima.

De fato, por via de tal alteração, o legislador pátrio recrudesceu o tratamento dado ao comportamento previsto no art. 154-A, § 3º do Estatuto Repressor, razão pela qual a inovação normativa não retroage. (LAI E MOURÃO, 2021).

4.4 FURTO

Ademais das regras citadas acima, a Lei 14.155/2021 trouxe mais uma modalidade qualificada de furto, a qual se entende por denominar de furto qualificado pela fraude eletrônica. Isso ocorreu pela inserção do art. 155, § 4º-B no Código Penal, com a seguinte redação:

> § 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.(Incluindo pela a Lei n° 14.155/2021)

Anteriormente a Lei 14.155/2021, o furto mediante fraude já estava previsto no Código Penal, mas essa nova norma especificou situações que envolvem fraudes eletrônicas e estabeleceu causas qualificadoras com penas mais altas.

Sabe-se que o furto mediante fraude, na forma do art. 155, § 4º, inciso II, é caracterizado pelo emprego de enganação. Nele, a vítima é submetida a um processo de ilusão, que permite ao delinquente acessar o bem por ele objetivado. Marca, assim, em especial, o furto mediante fraude eletrônica, o fato de a fraude ser realizada por "meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores" ou "por qualquer outro meio fraudulento análogo". (LAI E MOURÃO, 2021)

Dessa forma, o art. 155, § 4º, inciso II se refere ao meio de execução do delito, por outro lado o art. 155, § 4º-B, além de tangenciar o meio para execução, realça a uma especial importância o instrumento empregado. Assim, se alguém acessa uma conta bancária, por via de senha obtida através da invasão do computador da vítima, e dela retira quantias, prática furto mediante fraude eletrônica.

Mas além, de positivar o furto qualificado pela fraude eletrônica, a Lei 14.155/2021 criou causas de aumento específicas para esta modalidade de crime, a teor do art. 155, § 4º-C e seus incisos:

> § 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. (Incluído na Lei n° 14.155/2021)

Percebe-se que o legislador, indicou que a causa de aumento de pena estaria condicionada à "relevância do resultado gravoso", prevendo, na sequência, no inciso I, majoração decorrente da prática do crime por via da utilização de servidor mantido fora do território nacional e, no inciso II, incremento de sanção concernente a características das vítimas.

As majorantes do furto qualificado mediante fraude por meio eletrônico, Art. 155 § 4º -C, a lei em tela ainda acrescentou um aumento de pena que poderá oscilar em decorrência da relevância do resultado gravoso. Primeira hipótese o aumento é de 1⁄3 a 2 / 3 se o crime for praticado com a

utilização de servidor mantido fora do território nacional, pela maior dificuldade de coibição de um servidor fora do território brasileiro. Segunda hipótese: aumento de pena será de 1⁄3 ao dobro se o crime for exercido contra idoso ou vulnerável. (SILVA,2021)

4.5 ESTELIONATO

Assim, como a Lei 14.155/2021 criou a modalidade de furto mediante fraude eletrônica, a Lei 14.155/2021 também positivou o estelionato mediante fraude eletrônica , descrita no art. 171,§ 2° - A. Vale a pena salientar, esse ponto, que o estelionato tem por particular a fraude, mesmo em figura simples, diferente do que acontece no furto. Veja-se o tipo simples, contido no art. 171, *caput* do Código Penal:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis. (Brasil, 1940)

Realmente, no estelionato, o criminoso consegue enganar a vítima, através do emprego de artifício, ardil, ou qualquer outro meio fraudulento, fazendo com que a própria vítima lhe entregue, de bom grado, uma vantagem ilícita. E nesse contexto percebe-se, a diferença entre furto mediante fraude e estelionato, para um melhor entendimento segue um quadro esquemático:

Furto mediante fraude	**Estelionato**
Agente prática a fraude para ele, diretamente, ou comparsa subtrair a coisa	Agente prática a fraude para a vítima lhe entregar a coisa de bom grado

FONTE: Elaborado pelo autor, 2024.

Por sua vez, o novel § 2º-A estabelece sanção mais grave “se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo”. Veja a norma citada:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Redação dada pela Lei nº 14.155, de 2021)

Já §2°-B do art.171, o legislador previu causas de aumento específicas para os casos de estelionato eletrônico, e quais também não retroagem.

> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, 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. (Redação dada pela Lei nº 14.155, de 2021)

Contudo a Lei 14.155/2021, também trouxe mudança no art. 171, § 4° do Código Penal, possibilitando o aumento de pena nos casos de estelionato contra idoso ou vulnerável, fazendo- o nos seguintes termos:

> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso. (Redação dada pela Lei nº 14.155, de 2021)

As condutas atingidas e transformadas pela nova lei, demonstram as transformações sociais que ocorrem de forma tão apressada em nosso meio, principalmente o que se versa sobre o mundo digital e suas consequências. (SILVA, 2021)

Assim essas alterações apresentam uma adequação da legislação penal às novas tecnologias e às vulnerabilidades associadas ao ambiente digital. Sendo o objetivo fortalecer a proteção dos cidadãos contra fraudes eletrônicas e reforçar a responsabilização dos autores desses crimes.

4.5.1 Regra de competência para o estelionato eletrônico

Por último a Lei 14.155/2021 acabou alterando também o artigo 70 § 4º do Código de Processo Penal, sobre a competência para julgamento de algumas modalidades previstas no mesmo artigo. A lei então determinou que a competência para o processamento de crimes de estelionato seja no domicílio da vítima 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". Tal mudança manteve a regra da Súmula 48 do STJ. (SILVA, 2021)

Veja-se a norma citada, art.70, § 4° do CPP:

> § 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. (Incluído pela Lei nº 14.155, de 2021)

Dessa forma, por força do art. 70, § 4º do Código de Processo Penal, nos casos de estelionato eletrônico, a competência será definida pelo local do domicílio da vítima, e, em casos de pluralidade de vítimas, pela prevenção.

Essa alteração visa facilitar o acesso à justiça para a vítima e auxiliar na investigação do crime, já que o autor da fraude eletrônica pode agir remotamente, de qualquer lugar, o que muitas vezes dificulta a determinação da competência territorial. Antes dessa alteração, a competência, em regra,

era estabelecida pelo local onde o ato fraudulento foi cometido, o que tornava mais difícil processar crimes que envolvem golpes digitais. Dessa forma, ao fixar o foro de julgamento no domicílio da vítima, a legislação facilita o trâmite processual em situações em que o autor se encontra em localidade desconhecida ou fora do alcance direto das autoridades locais da vítima.

5 CONSIDERAÇÕES FINAIS

Esse trabalho buscou analisar os delitos cometidos no meio cibernético. Teve como objetivo específico, explorar o conceito e curiosidades diante dos crimes cibernéticos, assim como, averiguar as medidas concebidas pela legislação brasileira no intuito de conter os crimes cibernéticos. A Lei nº 14.155/2021 representa um avanço significativo no enfrentamento aos crimes cibernéticos patrimoniais no Brasil, ao atualizar o Código Penal para refletir a realidade do ambiente digital. Com o aumento das penas para crimes como invasão de dispositivo informático e furto eletrônico, além da criação do estelionato eletrônico, a legislação responde de forma mais rigorosa e proporcional ao impacto dos delitos cibernéticos, que afetam um número crescente de vítimas e atingem uma ampla gama de patrimônios.

Com a evolução tecnológica, os crimes cibernéticos se tornaram uma preocupação crescente, exigindo um sistema legal adaptado às novas modalidades de delitos. Essas mudanças não só reforçam a proteção dos direitos dos usuários e a segurança de seus dados, mas também desencorajam práticas criminosas ao impor sanções mais severas e específicas, assim buscando preencher lacunas legislativas e fortalecer a segurança jurídica, estabelecendo penas mais rigorosas para infratores e aprimorando a proteção dos bens e direitos dos cidadãos no ambiente digital.

Desse modo, a lei visa não apenas responsabilizar de forma mais eficaz os autores desses crimes, mas também atuar de forma preventiva, inibindo ações que possam prejudicar a sociedade da informação e a confiança nos meios digitais. Com o aprimoramento do combate aos crimes cibernéticos, a legislação brasileira reforça a importância da atualização constante frente às novas práticas criminosas, oferecendo uma resposta mais adequada e condizente com a realidade digital atual.

REFERÊNCIAS

BRASIL, **Código Penal de 1840**, disponivel em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em 15 de out. de 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 set. 2024.

BRASIL, **Lei n. 14.155/2021 de 27 de maio de 2021, promove alterações nos crimes de violação de dispositivo informático, furto e estelionato.** Disponivel em : https://www.planalto.gov.br/ccivil_03/_ato20192022/2021/lei/L14155.htm#:~:text=Altera%20o%20Decreto%2DLei%20n%C2%BA,Penal)%2C%20para%20definir%20a%20comp et%C3%AAncia. Acesso em 20 de set. de 2024.

BRASIL**, Lei n. 12.737 de novembro de 2012, promove alterações nos crimes de violação de dispositivo informático, furto e estelionato.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 de set. de 2024.

BRITO, R. G. G**.. Aplicabilidade das Normas Penais nas Condutas Ilícitas de Cyberbullying Cometidas em Redes Sociais na Internet**. Revista Esmat., v. 5, n. 6. 2013.

CASSANTI, Moisés de Oliveira**. Crimes Virtuais, Vítimas reais**. Rio de Janeiro: Brasport, 2014.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura. In: A sociedade em Rede**. São Paulo: Pa e Terra, 2000. v. 1.

COLARES, Rodrigo Guimarães. **Cybercrimes: os crimes na era da informática**, 2002. **In: Jus Navigandi**, Teresina, ano 6, n. 59, out. 2002. Disponível em: http://jus2.uol.com.br/doutrina. Acesso em: 10.04.2016.

DAMÁSIO, José Antônio**. Manual de Crimes Informáticos.** – São Paulo: Saraiva, 2016.

JUSTINIANO, Nara Fernanda**. terminologia e tecnologia: um estudo de termos de crimes cibernéticos.** Disponivel em:< http://icts.unb.br/jspui/bitstream/10482/22977/1/2016_NaraFernandaJustiniano.pdf >. Acesso em 15 de out. de 2024.

MARRA, Fabiana Barbosa. **Desafios Do Direito Na Era Da Internet: Uma Breve Análise Sobre Os Crimes Cibernéticos. Campo Jurídico, v. 7, n. 2, 2019**. Disponível em : < http://fasb.edu.br/revista/index.php/campojuridico/article/view/289 >. Acesso em 10 de outubro de 2024.

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

ROHRMAM, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005.

SILVA, Ana Maria**, a Lei 14.155/2021 dos crimes informáticos e suas implicações no Código Penal**. Disponivel em: < https://www.jusbrasil.com.br/artigos/a-lei-14155-2021- dos-crimes-informaticos-e-suas-implicacoes-no-codigo-penal/1293902850>. Acesso em 28 out. 2024

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

ESTEFAM, André**. Direito Penal, Parte especial: arts. 121 a 234-B**, volume 2**.** 7. ed. São Paulo: Saraiva Educação, 2020.

WERTHEIN, Jorge. Publicação de Artigos Científicos. **A sociedade da Informação e seus Desafios,** maio/ago. 2000. Disponível em: < www.scielo.br/pdf/%0D/ci/v29n2/a09v29n2.pdf >. Acesso em 07 set. 2024