UNIVERSIDADE DE TAUBATÉ
DEPARTAMENTO DE CIÊNCIAS JURÍDICAS

Gabriela Maia de Gouvêa

CRIMES INFORMÁTICOS À LUZ DA LEI N° 14.155 DE 2021

Taubaté-SP
2022

Gabriela Maia de Gouvêa

CRIMES INFORMÁTICOS À LUZ DA LEI N° 14.155 DE 2021

Monografia apresentada como parte dos requisitos para obtenção do título de Bacharel pelo Curso de Direito do Departamento de Ciências Jurídicas da Universidade de Taubaté.
Professor orientador: Fernando Gentil Gizzi de Almeida Pedroso

Taubaté-SP

2022

Grupo Especial de Tratamento da Informação - GETI
Sistema Integrado de Bibliotecas - SIBi
Universidade de Taubaté - UNITAU

G719c Gouvêa, Gabriela Maia de
Crimes informáticos à luz da lei n° 14.155 de 2021 / Gabriela Maia de Gouvêa. -- 2022.
56f.

Monografia (graduação) - Universidade de Taubaté, Departamento de Ciências Jurídicas, 2022.
Orientação: Prof. Me. Fernando Gentil Gizzi de Almeida Pedroso, Departamento de Ciências Jurídicas.

1. Direito penal. 2. Crimes informáticos. 3. Fraude eletrônica. 4. Estelionato - Competência. 5. Invasão de dispositivo informático. I. Universidade de Taubaté. Departamento de Ciências Jurídicas. Curso de Direito. II. Título.

CDU - 343.2:004

Ficha catalográfica elaborada pela Bibliotecária Regina Márcia Cuba – CRB 8ª/7416

GABRIELA MAIA DE GOUVÊA

CRIMES INFORMÁTICOS À LUZ DA LEI N° 14.155 DE 2021

Monografia apresentada como parte dos requisitos para obtenção do título de Bacharel pelo Curso de Direito do Departamento de Ciências Jurídicas da Universidade de Taubaté.

Direito Penal

Data:_____

Resultado:_____

BANCA EXAMINADORA

Prof. Fernando Gentil Gizzi de Almeida Pedroso Universidade de Taubaté

Assinatura: _____

Prof. _____ Universidade de Taubaté

Assinatura: _____

Dedico este trabalho aos meus pais e meus familiares pelo apoio, e especialmente aos meus saudosos avós maternos, Geraldo Maia e Ana Goret, os quais me deixaram no meio desta caminhada.

AGRADECIMENTO

Agradeço, primeiramente, a Deus por me proporcionar esse dia e me dar forças nesses 05 (cinco) anos de graduação.

Agradeço a todos os meus professores, em especial ao meu orientador pela habilidade, compreensão, dedicação e pelos ensinamentos para que eu concluísse o presente trabalho.

Agradeço ainda aos meus familiares, especialmente aos meus pais, meus avós paternos, meu irmão, meu namorado e meus amigos que estiveram comigo nesta grande caminhada.

Particularmente, agradeço a minha mãe, Patricia, por toda a doçura nos momentos em que pedia seus conselhos e ao meu pai, Fabio, por todo apoio. Ainda, agradeço meus avós paternos, Luiz Gonzaga e Judith, por serem uma fonte de inspiração. Além disso, agradeço o meu irmão, Rafael, pelo encorajamento quando dos momentos de nervosismo, e ao meu amado namorado, Luis Fernando, por todo o carinho e paciência nesse período.

Ademais, agradeço a minha amiga e companheira nessa jornada, Larissa, a qual dividi essa experiência de forma diária e sem igual.

E, finalmente, agradeço a Universidade de Taubaté, por todo o suporte.

“Algumas pessoas não gostam de mudanças, mas você precisa abraçar a mudança se a alternativa for o desastre.”

- Elon Musk

RESUMO

O alvo central deste trabalho está focado em detalhar as alterações realizadas pela Lei n° 14.155/2021 no ordenamento jurídico. Vale ressaltar que a presente alteração legislativa teve como finalidade atualizar o ordenamento jurídico a realidade vivida pelos brasileiros com o avanço tecnológico, ou seja, aumentando o rol de crimes informáticos da Lei n° 12.735/2012 e da Lei n° 12.737/2012. Em síntese, a presente legislação alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais grave os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. O método utilizado para elaboração deste trabalho de graduação esteve focado no próprio texto legal e em várias obras de juristas renomados, conhecidas como doutrina no âmbito jurídico.

Palavras-chave: Direito Penal. Crimes informáticos. Fraude eletrônica. Competência do estelionato. Violação de Dispositivo Informático.

ABSTRACT

This work's main goal is focused in detailing the changes made by the Law nº 14.155/2021 in the juridic system. It is worth highlighting that the present legislative changes had the goal to update the juridic system to the reality experienced by the Brazillians with technological progress, that being, a rise in virtual crimes or cybercrimes, which already worried the past legislator in 2012, with the Law nº 12.735/2012 and Law 12.737/2012. In summary, the present legislation changed the Decret-Law nº 2.848, from december 7, 1940 (Penal Code), to make the crimes that violate a computer device, theft and embezzlement made by electronic or via internet, more severe; and the Decret-Law nº 3.689, from october 3, 1941, (Penal Process Code), to define the competence in modalities of embezzlement. The method that is used to elaborate this graduation paper was focused on the legal text itself and many works of renowned jurists, known as doctrine in the legal scope.

Keywords: Criminal Law. Cybercrimes. Electronic fraud. Scam competence. Computer Device Violation.

SUMÁRIO

INTRODUÇÃO

Esta pesquisa visou analisar os cibercrimes, os quais são entendidos como os delitos cometidos “de maneira virtual, utilizando a Internet como meio, ou envolvendo arquivos ou sistemas digitais/tecnológicos” (D´Urso, 200-), tendo como enfoque as alterações legislativas trazidas pela Lei nº 14.155 de 2021.

O referencial para a pesquisa foi os panoramas histórico-sociais que levaram a esta importante alteração legislativa, a perspectiva doutrinária, legal e jurisprudencial sobre a temática, bem como eventuais divergências quanto à sua aplicação.

Desta forma, cabe indagar-se: quais demandas sociais justificaram a presente alteração legislativa? Como as inovações legislativas trazidas pela Lei nº 14.155/2021 transformaram o cenário de criminalização de atos praticados no ambiente digital? Qual foi a importância da alteração da regra de competência do crime de estelionato? Quais são as primeiras considerações trazidas pela doutrina no tocante a essa inovação legislativa?

O objetivo geral deste trabalho é tratar sobre a nova perspectiva trazida pela Lei nº 14.155/2021 e os reflexos da sua aplicação. Já, os objetivos específicos deste Trabalho de Graduação são demonstrar no que se respaldaram os congressistas para a realização desta importante modificação no Código Penal e no Código de Processo Penal, e expor de forma sistemática as inovações legislativas trazidas pela Lei nº 14.155/2021, criando um paralelo sobre o sistema jurídico anterior e posterior à legislação.

Justifica-se esta temática ante as importantes alterações trazidas pela Lei n° 14.155/2021 para o cenário jurídico-social, visto que ela foi projetada para atacar o aumento extremo, de aproximadamente 70% (setenta por cento), dos números de fraudes cometidas de forma eletrônica no país no ano de 2020, as quais geraram, conforme vislumbra no texto do projeto de lei de autoria do Senador Izalci Lucas, prejuízos estimados em R$ 1.000.000.000,000 (um bilhão de reais), fazendo com

que o Brasil alcançasse o 3º (terceiro) lugar no ranking mundial de registros de fraudes eletrônicas (SENADO, 2020).

Para se ter uma dimensão desta problemática, segundo os dados fornecidos pelo Serasa Experian em agosto de 2021, os brasileiros sofrem uma tentativa de fraude a cada 8 (oito) segundos, sendo que apenas no primeiro semestre de 2021 foram registrados 1,9 milhão de ataques, tornando o maior volume de tentativas já registrado por eles desde o início da coleta de dados, em 2011.

Este aumento é justificado por Jaison Reis, Diretor de Soluções de Identidade e Prevenção a Fraudes da Serasa Experian, como consequência da digitalização causada pela Pandemia de COVID-19:

> [...] Houve uma mudança no comportamento dos brasileiros, que passaram a adquirir bens e serviços online, graças às regras de distanciamento social impostas pela pandemia. Portanto, os oportunistas tinham mais transações para tentar acessar dados e recursos. Por isso a importância de ter plataformas robustas que identifiquem essas tentativas e impeçam a ação dos fraudadores [...] (SERASA, 2021).

Por estas razões, entende-se a necessidade de um estudo aprofundado sobre as mudanças legislativas trazidas pela Lei nº 14.155 de 2021 para compreender a extensão da sua aplicação no caso concreto.

Assim, presente estudo foi focado nas inovações trazidas pela Lei nº 14.155/2021, a qual tipificou alguns atos praticados por meio da rede mundial de computadores ou de qualquer outra forma eletrônica, como crimes cibernéticos, bem como tornou determinados crimes já existentes no ordenamento jurídico mais severos, com o incremento do preceito secundário.

Nessa senda, pretendeu-se demostrar no decorrer deste estudo como esta legislação em específico alterou o cenário dos crimes cibernéticos, se aprofundando nas suas lacunas e em discussão doutrinária acerca desse direito penal virtual e suas conjunturas, tendo como parâmetro as discussões trazidas pelo mundo jurídico e as legislações brasileiras anteriores a Lei n° 14.155/2021.

Nessa conjuntura, o primeiro capítulo deste trabalho visou contextualizar o leitor sobre termos que são aportados pela Lei nº 14.155 de 2021, como, a definição

de crimes informáticos, *malware, vírus, ransomware, spyware, trojan horse,* entre outros. Já, o segundo capítulo explorou a histórico de elaboração da Lei nº 14.155 de 2021, a fim de compreender como o texto foi redigido pelos legisladores e quais alterações foram efetuadas por eles para que o Projeto de Lei nº 4.554 de 2020 se tornasse a lei estudada. Ao final, no terceiro capítulo foi demonstrado quais foram as efetivas mudanças que a legislação estudada realizou no ordenamento jurídico brasileiro de acordo com renomados juristas.

1 DO CRIME

Antes de expor sobre os crimes informáticos à luz da Lei º 14.155 de 2021, é preciso relembrar brevemente o conceito de crime.

O Código Penal entende como crime o fato típico e antijurídico, nos termos do art. 23 do referido diploma[1]. Assim, para que haja um crime é necessário identificar a presença desses dois elementos.

O fato típico é composto pelos seguintes elementos: conduta dolosa ou culposa, resultado, nexo causal e tipicidade (GONÇALVES, 2020, p. 46).

A conduta é, basicamente, a ação ou omissão do ser humano, voluntário e consciente, dirigido a uma finalidade. Os elementos da voluntariedade e da consciência fazem com que o crime só posso ser cometido por seres humanos, uma vez que os animais são irracionais, logo não podem praticar estas condutas (GONÇALVES, 2020, p. 46).

Esta conduta se exterioriza por uma ação, um comportamento positivo, ou por uma omissão, um comportamento negativo (GONÇALVES, 2020, p. 46). Sendo que, a omissão pode ser de suas formas: próprias/puras ou impróprios/comissivas por omissão. A conduta omissiva própria ocorre quando o tipo penal impõe como crime a ausência de conduta, como, por exemplo, no crime de omissão de socorro (art. 135 do CP). Por outro lado, os crimes omissivos impróprios, “são aqueles para os quais a lei impõe um dever de agir e, assim, o não agir constitui crime, na medida em que leva à produção de um resultado que o agir teria evitado” (GONÇALVES, 2020, p. 47).

Além disso, se esta conduta é executada por um único ato, chama-se o crime de unissubsistente; mas se por cometida por um conjunto de atos, o crime será chamado de plurissubsistente (GONÇALVES, 2020, p. 45).

No tocante ao elemento do resultado, este é entendido como a “lesão ou perigo de lesão de um interesse protegido pela norma penal” (MIRABETE, 2021, p.

---

[1] Art. 23 - Não há crime quando o agente pratica o fato:
I - em estado de necessidade;
II - em legítima defesa;
III - em estrito cumprimento de dever legal ou no exercício regular de direito.

111). Destaca-se que os crimes podem ser classificados pelo resultado que produzem, senão vejamos:

> [...] crimes podem ser materiais (quando o tipo penal descreve uma ação e um resultado, e exige este para o crime estar consumado), formais (quando o tipo penal descreve uma ação e um resultado, mas dispensa o resultado para fim de consumação) e de mera conduta (quando o tipo penal descreve apenas uma ação)" (GONÇALVES, 2020, p. 48).

Já, o nexo causal ou relação de causalidade é o elo existente entre a conduta e o resultado, o qual impõe uma relação de consequência entre estes elementos (ANDREUCCI, 2021, p. 102).

Com relação ao elemento da tipicidade, este é "ao enquadramento da conduta concretizada pelo agente na norma penal descrita em abstrato" (GONÇALVES, 2020, p. 54). Assim, o enquadramento pode ocorrer de duas formas: imediata/direta ou mediata/indireta. A tipicidade imediata ocorre quando há uma perfeita correspondência da conduta ao tipo penal. Por outro lado, a tipicidade mediata ocorre "quando a materialização da tipicidade exige a utilização de uma norma de extensão, sem a qual seria absolutamente impossível enquadrar a conduta no tipo" (GONÇALVES, 2020, p. 54), por exemplo, o uso do art. 29 do CP para enquadrar certa conduta como tentativa de certo crime (GONÇALVES, 2020, p. 54).

No que concerne a antijuridicidade ou ilicitude, esta é a relação de contrariedade que se estabelece entre o fato típico e o ordenamento legal, fazendo com que haja a criminalização do ato praticado. Porém, há casos que seriam perfeitamente criminalizados, pois há o preenchimento dos elementos do fato típico, mas não são, por se enquadrarem em uma causa de exclusão da ilicitude, fazendo com que legalmente a conduta praticada não seja taxada com crime (NUCCI, 2021, p. 223).

Existem quatro causas gerais de exclusão da ilicitude previstas na Parte Geral do CP, são elas: estado de necessidade; legítima defesa; exercício regular de um direito; estrito cumprimento do dever legal. Além do mais, há também causas especiais de exclusão de ilicitude que são previstas na Parte Especial do Código Penal, e que somente são aplicáveis a determinados delitos (MIRABETE, 2021, p. 181/182).

A causa geral de exclusão de ilicitude estado de necessidade está prevista no art. 24 do Código Penal[2], sendo não criminalizada a conduta, dita inicialmente como criminosa, de quem sacrifica um bem jurídico protegido para salvar outro bem jurídico protegido, o qual pode ser próprio ou de terceiro, “desde que outra conduta, nas circunstâncias concretas, não fosse razoavelmente exigível”. (NUCCI, 2021, p. 226).

A legítima defesa é caraterizada, nos termos do art. 25 do CP[3], quando alguém age usando moderadamente dos meios necessários para repelir injusta agressão, atual ou iminente, a direito próprio ou de terceiro (MIRABETE, 2021, p. 188).

Já, o exercício regular do direito, previsto no art. 23, III, do CP, ocorre quando alguém atua dentro dos limites conferidos pelo ordenamento jurídico. Desta forma, o agente não comete qualquer crime, uma vez que está exercendo uma prerrogativa conferida em lei (MIRABETE, 2021, p. 195).

Com relação a não criminalização do ato pelo agente estar em estrito cumprimento do dever legal (art. 23, III, CP), deve-se destacar que este dever deve estar disposto em alguma lei, decreto, regulamento ou ato administrativo fundado em lei e que sejam de caráter geral. Havendo a criminalização do ato, quando o agente extrapolar os limites impostos (GONÇALVES, 2020, p. 96).

Assim, em síntese, é possível rememorar brevemente o conceito do termo “crime” para a melhor analise das alterações trazidas pela Lei nº 14.155 de 2021, a qual é o real enfoque deste Trabalho de Graduação.

---

[2] Art. 24 - Considera-se em estado de necessidade quem pratica o fato para salvar de perigo atual, que não provocou por sua vontade, nem podia de outro modo evitar, direito próprio ou alheio, cujo sacrifício, nas circunstâncias, não era razoável exigir-se.
§ 1º - Não pode alegar estado de necessidade quem tinha o dever legal de enfrentar o perigo.
§ 2º - Embora seja razoável exigir-se o sacrifício do direito ameaçado, a pena poderá ser reduzida de um a dois terços.

[3] Art. 25 - Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual ou iminente, a direito seu ou de outrem.
Parágrafo único. Observados os requisitos previstos no caput deste artigo, considera-se também em legítima defesa o agente de segurança pública que repele agressão ou risco de agressão a vítima mantida refém durante a prática de crimes.

2 DO CRIME DIGITAL

Vislumbrando o conceito de crime dentro do Direito Penal brasileiro, faz-se necessário também frisar o que é Direito Digital e crime informático para uma adequada analise do tema deste trabalho.

O Direito Digital é uma evolução do próprio Direito, respeitando os princípios e institutos fundamentais vigentes na ordem jurídica. Desta forma, não há um Direito da Internet, até porque não se trata de uma área do direito, mas um veículo de comunicação, o qual trouxe desafios para que todas as áreas do Direito solucionassem (PINHEIRO, 2022, p. 26).

Assim, dentro da seara do Direito Penal vinculado ao Direito Digital, é comum que os crimes praticados neste meio sejam nomeados de diversas formas, como: “crime de computador, crime via internet, crime informático, crime praticado por meio da internet, crime praticado por meio da informática, crime tecnológico, crime da internet, crime digital, cybercrimes, infocrimes etc” (TEIXEIRA, 2022, p. 214).

Mas, o doutrinador Tarcisio Teixeira (2022, p. 214) defende como correto o uso do termo “crime de informática” ou “crime eletrônico”, visto que assim é possível contemplar todo o sistema de informática, e não apenas a internet. Neste contexto, esses termos serão os adotados no decorrer deste trabalho.

O crime de informática é, de acordo com o jurista Tarcisio Teixeira, “aquele que, quando praticado, utiliza-se de meios informáticos como instrumento de alcance ao resultado pretendido, e também aquele praticado contra os sistemas e meios informáticos” (TEIXEIRA, 2022, p. 214).

O mencionado jurista classifica esses crimes informáticos como de duas modalidades: atos dirigidos contra o sistema de informática (praticados contra o computador e/ou dados ou programas de computador) e os atos cometidos por intermédio do sistema de informática (TEIXEIRA, 2022, p. 215).

Salienta-se que a Lei nº 14.155 de 2021, a qual será estudada, tem como finalidade a tipificação de alguns atos cometidos por intermédio do sistema de informática, ou seja, cria crimes da segunda modalidade de crime informático

Para compreender os termos que são abordados pelos juristas ao analisar a Lei nº 14.155 de 2021, é necessário explorar os sujeitos ativos e as formas de realização dos crimes informáticos.

Os agentes dos crimes de informática são, em tese, qualquer pessoa, por se tratar de crimes em sua maioria comum (não necessitam de uma qualidade especial do agente) (TEIXEIRA, 2022, p. 229).

Porém, no meio informático a prática de certas condutas faz com que o agente seja conhecido por certas denominações. Por este motivo, mesmo se tratando de crimes comuns, faz-se necessário pontuar alguns sujeitos ativos que, geralmente, praticam esses crimes, quais sejam: *hackers, crackers, insiders, lammers, phreakers, spammers e hacktivist* (TEIXEIRA, 2022, p. 230).

Os hackers são especialistas em informática, capazes de invadir computadores alheios e de impedir que outros os invadam, visto que detém conhecimento sobre informações confidenciais de um sistema de computadores e de redes em particular Já, os crackers, por outro lado, agem de forma obviamente maliciosa, ou seja, com a intenção de prejudicar alguém, tirar proveito ou partido para si da informação obtida (MORAES, 2022, p. 190).

Desta forma, pode-se verificar que os crackers são uma espécie de hackers com intenções deturpadas. Assim, divide-se os hackers em dois grupos: hackers em sentido estrito e crackers (TEIXEIRA, 2022, p. 230).

Nessa senda, os *insiders* são os hackers internos de uma empresa, isto é, são colaboradores que atuam contra a instituição que os empregam, ou algum membro desta entidade (TEIXEIRA, 2022, p. 230). De acordo com Tarcisio Teixeira (2022, p. 230), esses são os causadores dos maiores números de problemas informáticos, visto que por estarem insatisfeitos com o ambiente de trabalho ou estarem em busca de uma promoção com a solução do problema que causaram, realizam as operações e lesam os próprios empregadores.

No tocante aos *lammers*, também conhecidos como *script kiddies* (criança do script), são pessoas que não possuem nenhum ou pouco conhecimento de programação e usam ferramentas desenvolvida por outros, para incomodar usuários (TEIXEIRA, 2022, p. 230).

Em relação aos agentes conhecidos como *phreakers*, estes utilizam de meios de comunicação mediante o emprego de artifícios fraudulentos para que assim não precisem custear pelos serviços (TEIXEIRA, 2022, p. 230). Um exemplo de *phreakers*, é John Draper, conhecido como o “pai dos phreakers”, um hacker americano que descobriu, na década de 70, uma forma de realizar chamadas nacionais e internacionais gratuitamente por meio de um dispositivo criado por ele, nominado como “Blue Box”.

No que se refere aos agentes *spammers,* são aqueles que enviam spam (e-mail não solicitado), que pode ser considerado como um lixo eletrônico, sendo utilizado principalmente para fazer publicidades e propagandas, mas em alguns casos também para enviar vírus e roubar informações (TEIXEIRA, 2022, p. 230).

Por último, os *hacktivistas* são um grupo de hackers que se unem para defender causas sociais ou para ajudar os outros, como o *Anonymous* (TEIXEIRA, 2022, p. 232).

Após compreender algumas espécies de agentes que praticam esses crimes informáticos, deve-se assimilar as formas de ataque e contaminação que realizam.

De antemão, é necessário destacar que as formas de cometimentos de crimes informáticos são incalculáveis, mas os meios mais utilizados e conhecidos são: vírus, trojans, worms, spyware, bot e botnet.

Os vírus são programas desenvolvidos com duas finalidades básicas: atacar e replicar automaticamente. Sendo que, para que eles sejam ativados, é necessário que os arquivos hospedeiros o executem (GRECO, 2022, p. 506). Assim, um vírus é um código malicioso capaz de afetar os dados de um computador, podendo corrompê-los ou destruí-los (MORAES, 2022, 217).

Por outro lado, os *trojans* são conhecidos como cavalos de troia ou *backdoors*, visto que são um legitimo presente de grego, afinal é um programa, por exemplo, um jogo, que abre portas remotas para a invasão de hackers (GRECO, 2022, p. 506). Salienta-se que por não serem virais, muitas vezes não são identificados pelos antivírus contaminado (TEIXEIRA, 2022, p. 233). Nesse contexto, um programa cavalo de troia “não possui capacidade de se duplicar, mas pode possuir um vírus incorporado” (MORAES, 2022, p. 218)

Já, os *worms (writer once read many*) são programas independentes (*standalone*) maliciosos que tem como finalidade replicar mensagens sem o consentimento do usuário. Além disso, a propagação do worms se perfaz por meio da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores, assim não necessita ser explicitamente executado para se propagar e, nem mesmo, embutar cópias de si mesmo em outros programas ou arquivos (GRECO, 2022, p. 506). Um exemplo desse programa foi o Wanna Cry, de 2017, um worms que explorou uma vulnerabilidade do Windows, conhecida como "EternalBlue", para se disseminar.

Ademais, os *spywares* são programas tidos como espiões, os quais armazenam e capturam algo do histórico de uso da vítima, como, por exemplo, o programa *screenlogger*, o qual tem a capacidade de capturar telas da área de trabalho do usuário, inclusive armazenando a posição do cursor (GRECO, 2022, p. 506).

No que se refere aos *bots*, “são programas que dispõem de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente” (GRECO, 2022, p. 506).

Com relação ao *botnet*, é “uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos bots etc” (GRECO, 2022, p. 506).

Concluindo, outro termo muito utilizado no meio tecnológico que deve ser abordado é o “*malware”* (códigos/programas maliciosos) que é simplesmente todo programa especialmente desenvolvido para causar prejuízo (GRECO, 2022, p. 550). Assim, verifica-se que os *vírus*, os *worms* e os *trojans* são exemplos de *malware.*

Portanto, com esses conceitos em mente, pode-se analisar de forma mais holística as alterações legais realizadas pelo legislador para combater esse avanço tecnológico malicioso, as quais serão exploradas nos próximos capítulos.

3 ANTES DA LEI N° 14.155/2021

A Lei nº 14.155 de 2021 tipificou condutas frequentes, as quais, porém, não são uma novidade, uma vez que o primeiro ataque cibernético da história ocorreu em 1982, durante a Guerra Fria (ROMANI, 2016).

Na época, o Estados Unidos da América descobriu que a União Soviética estava furtando softwares por meio do seu programa de espionagem Line X, e resolveu se vingar implantando um vírus em um software de controle de gasodutos. O invasor ficou indetectável por alguns meses até ser ativado pelos estadunidenses, fazendo com que o funcionamento das válvulas do gasoduto Transiberiano fosse totalmente alterado sem que os russos conseguissem entender o motivo, até que o gasoduto explodiu em junho de 1982, resultando na maior explosão não nuclear já vista do espaço (ROMANI, 2016).

Assim, mesmo que não seja uma novidade, essas modalidades de furto de dados, fraudes e estelionatos estavam distantes da população em geral, a qual não se preocupava com estas condutas, visto que estavam em um contexto social em que os crimes eram praticados no “mundo real”. Mas, com o avanço da tecnologia nos últimos anos e com a maior acessibilidade da população em geral, este contexto se alterou (D’URSO, 200-).

Preocupado com isso, em 2012, o legislador brasileiro acrescentou ao ordenamento jurídico duas legislações que buscaram tipificar condutas realizadas mediante o uso de sistema eletrônico em específico por meio da Lei nº 12.735/2012 e da Lei nº 12.737/2012, preenchendo uma grande lacuna no ordenamento jurídico.

A Lei nº 12.735/2012, mais conhecida como Lei Azeredo, determinou em seu art. 4° a criação de setores e equipes especializadas no combate à ação delituosa em redes de computadores, dispositivos de comunicação ou sistemas informatizado, nos órgãos da polícia judiciária.

Além disso, essa legislação incluiu um novo inciso para o art. 20, §3°, da Lei n° 7.716 de 1989, a qual define os crimes resultantes de preconceito de raça ou de cor, possibilitando a cessação de transmissões radiofônicas, televisivas, eletrônicas

ou por outra forma de publicação de conteúdos que tenham como finalidade a prática, indução ou incitação à discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

Já, a Lei n° 12.737 de 2012[4], conhecida popularmente como Lei Carolina Dickman, aprofundou-se mais na criação de novos delitos informáticos, introduzindo no Código Penal o crime de invasão de dispositivos informáticos, bem como disciplinou qual ação penal é a competente para este crime (BRASIL, 2012).

Ademais, a presente lei incluiu ainda os §§1° e 2° ao art. 266 do Código Penal[5], aumentando o campo de tipificação do crime que antes era de interrupção ou perturbação de serviços telegráfico ou telefônico, para a inclusão dos serviços informático, telemático ou de informação de utilidade pública (BRASIL, 2012).

Para mais, majorando a pena em dobro quando o crime for cometido por ocasião de calamidade pública. Ainda, a respectiva legislação criou a figura da

---

[4] 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.
§ 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.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
§ 3º 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 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.
Art. 154-B. 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 de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

[5] Art. 266. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

falsificação de cartão de crédito ou débito no parágrafo único do art. 298 do Código Penal[6], a equiparando ao caput (BRASIL, 2012).

O doutrinador Victor Eduardo Rios Gonçalves (2020, p. 332) destaca em sua obra que a aprovação da Lei n° 12.737/2012 marcou o ordenamento jurídico, visto que antes os crimes cibernéticos somente eram passíveis de punição pela legislação comum, uma vez que não havia legislação específica, assim para que “a punição fosse possível, entretanto, mostrava-se necessário algum resultado posterior (a subtração de valores, o dano, a ofensa à honra, etc)” (GONÇALVES, 2020, p. 332).

Mas, como os avanços legislativos não conseguiram acompanhar os tecnológicos, logo com a passagem dos anos e a evolução desenfreada das tecnologias, os referidos artigos foram se tornando brandos para os casos em concreto, conforme o Senador Izalci Lucas (SENADO, 2020) expôs em seu projeto legislativo de n° 4.554/2020, fatos estes que o motivaram a propor em plenário a criação de tipos penais mais completos, com penas mais duras, conforme se verá no próximo capítulo.

[6] Art. 298. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

4 O PROJETO DE LEI Nº 4.554/2020

Em 14 de setembro de 2020, o Senador Izalci Lucas, representante do Distrito Federal, filiado ao PSDB, apresentou o projeto legislativo n° 4554 de sua autoria, o qual inicialmente tinha como enforque combater apenas a prática de fraude eletrônica, através da modificação do art. 155 do Código Penal e a apresentação de hipóteses agravantes, *in verbis*:

> § 8º A pena é de reclusão de 4 a 8 anos se a subtração mediante fraude é cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança, ou com utilização de programa malicioso; ou ainda, se a fraude é cometida valendo-se de dados eletrônicos fornecidos pela vítima ou por terceiro induzido em erro, inclusive por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento.
> § 9º A pena prevista no § 8º aumenta-se de um terço, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e de dois terços se praticado contra pessoa idosa.

Na exposição de motivos do referido projeto, o Senador Izalci destacou diversos dados[7] que enfatizam a importância da apreciação do projeto, como, por

[7] "O Jornal Folha de São Paulo de 26/08/2020 noticia que a pandemia fez aumentar drasticamente o número de fraudes cometidas de forma eletrônica, gerando perdas de aproximadamente R$ 1 bilhão.
Segundo a mesma fonte, a alta foi de 70% e os montantes envolvidos já se apresentam como empecilho à redução de juros ao consumidor, vez que se elevaram os riscos envolvidos.
Esse tipo de crime tem atingindo, inclusive, os beneficiários do auxílio emergencial. Estima-se que 600 mil fraudes foram praticadas somente no pagamento do benefício. São inúmeros os canais de imprensa que vem noticiando a explosão de ocorrências em que criminosos estão lucrando durante a pandemia. Observa-se que tem havido um aumento crescente de crimes dessa natureza nos últimos anos, mas que o número disparou durante a pandemia. A situação agrava-se ainda mais quando os servidores de rede utilizados para o crime estão situados fora do país.
O Banco Central emitiu alerta sobre fraudes durante a pandemia, quando os golpes via WhatsApp ultrapassaram 11 milhões de casos. Bandidos usam inclusive aplicativos de informação sobre o Coronavirus para enganar os cidadãos de bem.
Nosso país alcançou o terceiro lugar no ranking mundial em registros de fraudes eletrônicas. Os criminosos, em função da branda legislação brasileira, estão escolhendo o Brasil como terreno fértil para seguirem impunes. O Jornal O Globo de 14 de julho informa inclusive que os cibercriminosos brasileiros estão expandindo suas atividades aplicando fraudes nos Estados Unidos, Europa e China.
Líderes em segurança contra fraudes lamentam todo o esforço para combater esse tipo de crime enquanto a legislação considerar essa prática como um crime menor, cujas penas são muitas vezes substituídas por penas "alternativas".
O volume de fraudes já começa a afetar a economia do país, gerando perda do poder aquisitivo e também perdas emocionais por parte das vítimas.
Diante do exposto, é medida urgente que aprovemos meios mais rigorosos para punir esse tipo de crime que assola o país" (SENADO, 2020)

exemplo, o fato do Banco Central ter emitido um alerta sobre fraudes durante a pandemia, quando os golpes via *WhatsApp* ultrapassaram 11 (onze) milhões de casos (SENADO, 2020).

Mesmo se tratando de significante temática, o mencionado projeto legislativo só teve sua tramitação agilizada a partir de 23 de novembro de 2020, quando o Senador Lasier Martins, solicitou pelo requerimento nº 2752 de 2020 a tramitação conjunta do referido projeto com a PL 4287/2019, a qual visava disciplinar os crimes cibernéticos (CONGRESSO NACIONAL, 2020).

Assim, em 23 de novembro de 2020, a PL nº 4.554/2020 foi incluída na ordem do dia da sessão deliberativa remota de 25 de novembro de 2020, fazendo com que em dois dias o projeto recebesse 9 (nove) emendas (CONGRESSO NACIONAL, 2020).

A primeira emenda foi proposta pelo Senador Plínio Valério (PSDB/AM), o qual defendeu como necessário uma maior proteção a pessoa vulnerável, assim aplicando também a eles a causa de aumento de pena do §9º (CONGRESSO NACIONAL, 2020), vejamos:

> Art. 155. § 9º A pena prevista no § 8º aumenta-se de um terço, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e de dois terços se praticado contra pessoa idosa **ou vulnerável**.

A segunda emenda que a PL n° 4.554 de 2020 recebeu foi a da Senadora Rose de Freitas (PODEMOS/ES), que visou aumentar o patamar da pena do projeto para 5 (cinco) a 10 (dez) anos e de multa até 1.000 (um mil) salários mínimos (CONGRESSO NACIONAL, 2020), nota-se:

> Art. 155. § 8º A pena é de reclusão de 5 a 10 anos se a subtração mediante fraude é cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança, ou com utilização de programa malicioso; ou ainda, se a fraude é cometida valendo- se de dados eletrônicos fornecidos pela vítima ou por terceiro induzido em erro, inclusive por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, e multa de até 1.000 salários mínimos.

A terceira emenda foi no mesmo sentido que a segunda e foi realizada pelo Senador Jayme Campos (DEM/MT), que teve como objetivo tornar a conduta a ser

tipificada mais severamente punida, para prever expressamente a pena de multa (CONGRESSO NACIONAL, 2020):

> § 8º A pena é de reclusão de 4 a 8 anos **e multa**, se a subtração mediante fraude é cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança, ou com utilização de programa malicioso; ou ainda, se a fraude é cometida valendo- se de dados eletrônicos fornecidos pela vítima ou por terceiro induzido em erro, inclusive por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento.

A quarta emenda foi apresentada pela Senadora Eliziane Gama (CIDADANIA/MA), a qual entendeu tão relevante a matéria tratada que justificou necessário a modificação do tipo penal do estelionato (art. 171 do CP), a fim de aperfeiçoar a qualificante proposta pelo Senador Izalci e prever a qualificadora de fraude eletrônica e uma semelhante causa especial de aumento (CONGRESSO NACIONAL, 2020), senão vejamos:

> Art. 155. § 8º A pena é de reclusão de 4 a 8 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.
> § 9º A pena prevista no § 8º deste artigo **aumenta-se de um terço**, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional, e **de dois terços** se praticado contra pessoa idosa.
> Art. 171 § 4º A pena é de reclusão de 4 a 8 anos e multa, se a fraude é cometida valendo-se de dados eletrônicos fornecidos pela vítima ou por terceiro induzido em erro, inclusive por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento; ou por qualquer outro meio fraudulento análogo.
> § 5º A pena prevista no § 4º deste artigo **aumenta-se de um terço**, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

A quinta emenda foi apresentada pelo Senador Rogério Carvalho (PT/SE), que defendeu a diminuição da pena descrita na PL, por, segundo ele, causar uma desproporcionalidade no ordenamento jurídico, uma vez que se o projeto fosse aprovado e virasse lei daquela forma, o furto cometido por meio eletrônico fora do território nacional, teria pena de 6 (seis) a 13 (treze) anos, maior que a de roubo. Desta forma, essa emenda solicitou a supressão do §9° da PL (CONGRESSO NACIONAL, 2020).

O Senador Randolfe Rodrigues (REDE/AP) apresentou a sexta emenda ao texto da mencionada PL, a fim de resguardar as pessoas com deficiência na causa especial de aumento de pena do §9° (CONGRESSO NACIONAL, 2020), *in verbis*:

> §9º A pena prevista no § 8º aumenta-se de um terço, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional e de dois terços se praticado contra pessoa idosa **ou pessoa com deficiência.**

Ainda, o Senador Paulo Paim (PT/RS) em sua emenda, numerada como sétima, buscou defender a inclusão da majorante também quando o crime for cometido contra pessoas com deficiência, indo de encontro com o defendido na emenda nº 6 (CONGRESSO NACIONAL, 2020).

Além disso, o Senador Jorge Kajuru (CIDADANIA/GO) mesmo sentido do que foi proposto pela Senadora Eliziane Gama (CIDADANIA/MA), defendeu na emenda nº 08 a alteração também do crime de estelionato para prever a qualificante e a causa especial de aumento de pena do cometimento do crime mediante fraude eletrônica (CONGRESSO NACIONAL, 2020), senão vejamos:

> Art. 155. § 8º A pena é de reclusão de 4 a 8 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 análogo.
> § 9º A pena prevista no § 8º deste artigo aumenta-se de um terço à metade, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional, e de um a dois terços se praticado contra idoso.
>
> Art. 171. § 2º-A A pena é de reclusão de 4 a 8 anos e multa, se a fraude é cometida valendo-se de dados eletrônicos fornecidos pela vítima ou por terceiro induzido em erro, inclusive por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento; ou por qualquer outro meio análogo.
> § 2º-B A pena prevista no § 2º-A deste artigo aumenta- se de um terço à metade, se o crime é praticado mediante.

A última e nona emenda proposta é de autoria do Senador Fabiano Contarato (REDE/ES) que seguiu o mesmo entendimento da emenda nº 4 e 8, defendendo a modificação do tipo penal do estelionato (art. 171 do CP), a fim de aperfeiçoar a qualificante proposta pelo Senador Izalci, prever a qualificadora de fraude eletrônica e uma semelhante causa de aumento (CONGRESSO NACIONAL, 2020), vejamos:

> Art. 155. § 8º A pena é de reclusão de 4 a 8 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.
> § 9º A pena prevista no § 8º deste artigo **aumenta-se de um terço à metade**, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional, e de **um a dois terços** se praticado contra pessoa idosa e essa circunstância é sabida pelo autor.
> Art. 171. § 2º-A A pena é de reclusão de 4 a 8 anos e multa, se a fraude é cometida valendo-se de dados eletrônicos fornecidos pela vítima ou por terceiro induzido em erro, inclusive por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento; ou por qualquer outro meio fraudulento análogo.
> § 2º-B A pena prevista no § 2º-A deste artigo **aumenta-se de um terço à metade**, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Em seguida, o Projeto de Lei nº 4.554 foi encaminhado ao Relator Senador Rodrigo Cunha, que se manifestou no sentido da aprovação com o acolhimento das emendas de nº 1, 3, 4, 8 e 9; e pela consequente prejudicialidade do PL nº 4.287, de 2019, e das demais emendas apresentadas, bem como apresentou uma alteração ao art. 70 do CPP, ficando o texto da PL com a seguinte redação (CONGRESSO NACIONAL, 2020):

> Art. 154-A, CP: Invadir dispositivo informático de uso alheio, conectado ou não à 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 – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 3º .....
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
>
> Art. 155, CP:.§ 8º A pena é de reclusão de 4 a 8 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.
> § 9º A pena prevista no § 8º deste artigo, considerando a relevância do resultado gravoso, aumenta-se de um terço a dois terços, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; e de um terço ao dobro se praticado contra idoso ou vulnerável.
>
> Art. 171, CP: § 2º-A A pena é de reclusão de 4 a 8 anos e multa, se a fraude é cometida valendo-se de informações fornecidas pela vítima ou por terceiro induzido em erro, inclusive por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

> § 2º-B A pena prevista no § 2º-A deste artigo, considerando a relevância do resultado gravoso, aumenta-se de um terço a dois terços, se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
> § 4º A pena será aumentada de um terço ao dobro se o crime for cometido contra idoso ou vulnerável, considerando a relevância do resultado gravoso.
>
> Art. 69, CPP:
> II-B - o domicílio ou residência da vítima;
>
> Art. 70, CPP:
> § 4º Quando o crime for cometido pela internet ou de forma eletrônica a competência será determinada pelo lugar de domicílio ou residência da vítima.

Em sessão deliberativa em 25 de novembro de 2020, os membros do Senado Federal decidiram pela aprovação do texto sugerido pelo Relator e por tornar prejudicado o PL nº 4287/2019, que tramitava em conjunto. Após, a matéria foi devidamente encaminhada para a Casa Revisora, no caso a Câmera dos Deputados (CONGRESSO NACIONAL, 2020).

Na Câmera dos Deputados, foi solicitado a apreciação do mencionado projeto de lei com urgência em 14 de dezembro de 2020 pelo Deputado Vinicius Carvalho (REPUBLIC/SP) e outros (CONGRESSO NACIONAL, 2020).

Após diversos tramites internos, em 15 de abril de 2021 o Relator Deputado Vinicius Carvalho (REPUBLIC/SP) apresentou seu parecer realizando alterações no texto da PL e criando texto substantivo, o qual foi submetido a plenário e aprovado na seguinte forma (CONGRESSO NACIONAL, 2021):

> Dê-se ao projeto a seguinte redação:
>
> Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.
>
> Art. 154-A, CP: Invadir dispositivo informático de uso alheio, conectado ou não à 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 – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
>
> § 3º
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

> Art. 155, CP: § 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.
>
> Art. 171, CP:
>
> Fraude eletrônica
> § 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.
> § 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.
>
> Estelionato contra idoso ou vulnerável
> § 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.
>
> Art. 70 § 4º, CPP: Nos crimes previstos no art. 171 do 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.

Retornando a Casa Iniciadora, em 05 de maio de 2021, por unanimidade o texto do PL foi aprovado nos termos acima descritos. Desta forma, em 27 de maio de 2021, o Projeto de Lei nº 4.554 de 2020 foi sancionado integramente pelo Presidente da República se tornando a Lei nº 14.155 de 2021, a qual será aprofundada a seguir (CONGRESSO NACIONAL, 2021).

5 ALTERAÇÕES TRAZIDAS PELA LEI Nº 14.155/2021

A Lei n°14.155/2021 adentrou o ordenamento jurídico alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

Desta forma, divide-se a presente explanação em quatro tópicos, a fim de organizar e sistematizar a questão.

5.1. DA VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO

A Lei n° 14.155 de 27 de maio de 2021 alternou quatro pontos do art. 154-A do Código Penal, o qual tipifica o crime de invasão de dispositivo informático que foi inserido no Código Penal pela Lei nº 12.737, de 30 de novembro de 2012, chamada pela imprensa de “Lei Carolina Dieckmann”, uma vez que a atriz havia sido vítima da conduta que fora tipificada meses antes em maio de 2012.

As quatro significantes alterações no referido artigo, que serão melhores explanadas em subtópicos próprios, são: a) a modificação da redação do *caput*, ampliando a incidência do tipo penal; b) a majoração da pena do crime na sua forma básica; c) a majoração dos limites da causa de aumento de pena do § 2º; e d) a majoração da pena da qualificadora do § 3º.

5.1.1. DA MODIFICAÇÃO DA REDAÇÃO DO *CAPUT* DO ART. 154-A

A modificação da redação do *caput* do art. 154-A do Código Penal feita pela Lei n° 14.155/2021 fez com que a conduta antes tipificada fosse ampliada, uma vez que anteriormente constava que o crime estava em invadir dispositivo informático alheio, ou seja, de propriedade de outra pessoa, e agora, o crime é invadir dispositivo informático de uso alheio.

Dessa maneira, atualmente não é mais necessário que o sujeito passivo, ou seja, a vítima do crime seja proprietária do dispositivo invadido, mas apenas que faça uso deste e por essa invasão o criminoso consiga acessar indevidamente os dados ou informações da vítima que fora armazenado no dispositivo invadido. Assim, é possível verificar que houve uma ampliação do tipo penal, a fim de proteger pessoas que sofriam essa invasão, mas não eram proprietárias dos dispositivos invadidos, fazendo com que não pudessem ser respaldadas pela legislação penal vigente (ESTEFAM, 2022, p. 498).

Para melhor entender o tipo penal, é necessário analisar as elementares deste, quais sejam: o núcleo “invadir”, o substantivo “dispositivo informático”, o advérbio “de uso alheio”, e a frase “conectado ou não à rede de computadores” (GRECO, 2022, p. 504).

Quanto ao verbo “invadir”, frisa-se que este introduz a ideia de que o autor do crime irá penetrar, ingressar sem autorização, em determinado local, o qual fica dentro do dispositivo informático (GRECO, 2022, p. 503), ou seja, o sujeito passivo desconhece esse ingresso (ESTEFAM, 2022, p. 501).

No tocante, ao substantivo “dispositivo informático”, que diz respeito a um *hardware* que pode ser utilizado para armazenar *softwares* ou para ser conectado a outros equipamentos, fornecendo uma funcionalidade. Assim, os dispositivos informáticos são, por exemplo, *tablets*, *smartphones*, computadores de mesa, entre outros (NUCCI, 2022, p. 633).

Com relação ao adjetivo “de uso alheio”, visa qualificar que o dispositivo informático invadido deve ser de uso de terceiro, ou seja, não cabe a tipificação no caso de invasão em dispositivo de uso próprio.

Além disso, quanto à frase “conectado ou não à rede de computadores”, o legislador esclarece que a referida invasão pode-se ser realizada por meio da *internet* ou não (NUCCI, 2022, p. 633). O jurista Mário Cavalcante, exemplifica esse não uso da *internet* com o seguinte exemplo: um “indivíduo que, na hora do almoço, aproveite para acessar, sem autorização, o computador do colega de trabalho” (CAVALCANTE, 2021). No entanto, deve-se destacar que de acordo com o jurista André Estefam, o legislador ao tratar de rede de computadores não está versando apenas sobre a internet (rede mundial de computadores), mas toda rede de

computadores, seja privada, pública, ou ainda, com acesso exclusivo a rede interna (intranet) (ESTEFAM, 2022, p. 501).

Com a referida explicação é possível entender a primeira ampliação realizada no tipo penal, mas essa ampliação foi muito mais significativa, tendo em vista que o legislador ainda aboliu a exigência de violação indevida de mecanismo de segurança, ou seja, violação indevida de um *firewall*, antivírus, *anti-malware*, *antisptware,* entre outros mecanismos de segurança. Um bom exemplo para compreender como essa alteração é o do jurista Mário Cavalcante (2021), vejamos:

> [...] imagine que um funcionário encontrou o pen drive (não protegido por senha) de seu colega de trabalho e decidiu vasculhar os documentos e fotos ali armazenados. Pela redação anterior, não haveria crime. Pela redação atual, o delito restará configurado.
> Houve, portanto, a correção de uma falha da Lei. Isso porque, mesmo sem a violação de mecanismo de segurança, a privacidade estava sendo violada e, portanto, merecia reprimenda penal. [...] (CAVALCANTE, Márcio André Lopes, 2021).

No mesmo sentido o jurista Cezar Bitencourt (2022, p. 346), alerta que, antes da alteração legislativa trazida pela Lei n° 14.155/2021, a inexistência de mecanismo de segurança era um empecilho para a tipificação da referida conduta. Mas, após a Lei n° 14.155/2021, se tornou irrelevante a eventual existência ou inexistência de "um mecanismo de segurança, acionado ou não", para a adequação típica da conduta (BITENCOURT, 2022, p. 346).

O jurista André Estefam esclarece ainda que por se tratar de alteração *in pejus* os fatos cometidos até o dia da publicação da Lei n° 14.155 de 2021, ou seja, até 27 de maio de 2021, não haverá criminalização se inexistir mecanismo de segurança na máquina, visto que é vedada a retroatividade *in pejus* no direito brasileiro (ESTEFAM, 2022, p. 501).

Ainda, o legislador acrescentou que a referida invasão tem que ter uma destas duas finalidades: a) obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo; ou b) instalar vulnerabilidades para obter vantagem ilícita (ESTEFAM, 2022, p. 502).

Sendo assim, o jurista Rogério Greco (2022, p. 504) salienta que este crime tem uma finalidade especial de agir, a qual muito além da simples invasão do

dispositivo informático, que consiste na obtenção, adulteração ou destruição de dados ou informações sem a autorização expressa ou tácita do titular do dispositivo.

No tocante a finalidade especial de instalar vulnerabilidades para obter vantagem ilícita, o doutrinador Rogério Greco (2022, p. 506), destaca que se trata de códigos maliciosos (*malware*).

Evidencia-se que se trata de fins especiais alternativos, ou seja, ambos não precisam existir ao mesmo tempo. Um deles é suficiente para que a estrutura típica possa se completar. Por outro lado, nada impede a coexistência de dois elementos subjetivos especiais do ilícito, em particular, ainda que nenhum deles se concretize, ou se concretize apenas um deles (ESTEFAM, 2022, p. 346).

O jurista Guilherme Nucci, realça em sua obra que o legislador ao equiparar a preparação com a execução do delito para fins de criminalização, consequentemente fez com que o autor que apenas instala vulnerabilidade no dispositivo informático para que, no futuro, se valha disso comete um só crime. Porém, se o autor instala, mas outra pessoa invade, cada qual cometerá o seu delito distinto, ambos tipificados no art. 154-A. Ainda, se duas pessoas, mancomunadas, uma instalando, outra invadindo, tratar-se-á de crime único, em concurso de agentes (art. 29, CP) (NUCCI, 2022, p. 633).

Além disso, o referido doutrinador ainda verifica uma causa legal de excludente de ilicitude que é o consentimento do ofendido, o qual pode ser realizado de forma expressa ou tácita (GRECO, 2022, p. 504).

Com relação aos aspectos doutrinadores do crime em questão, é importante destacar que o bem jurídico protegido é, segundo o doutrinador Cezar Bitencourt (2022, p. 345), a liberdade individual, uma vez que o crime está situado no capítulo do Código Penal que trata desta temática.

Quanto ao objeto jurídico tutelado, ele é múltiplo, sendo que cada doutrinador entende como um ou mais, por exemplo, Guilherme Nucci (2022, p. 632) elenca um rol exemplificativo de objetos, sendo eles: “à intimidade, à vida privada, à honra, à inviolabilidade de comunicação e correspondência e à livre manifestação do pensamento, sem qualquer intromissão de terceiros” (NUCCI, 2022, p. 632) e o patrimônio da vítima. Já André Estefam (2022, p. 500) diz que os objetos são a intimidade e a segurança informática.

No tocante ao objeto material é “dispositivo informático alheio, conectado ou não à rede de computadores, bem como os dados e as informações nele armazenadas” (GRECO, 2022, p. 507).

O sujeito ativo deste delito pode ser qualquer pessoa, sendo assim um crime comum (NUCCI, 2022, p. 632), e o sujeito passivo é a sociedade, na qualidade de titular da segurança informática “e, em especial, o detentor da informação ou dado obtido e o responsável ou controlador do dispositivo informático” (ESTEFAM, 2022, p. 503), que podem ser sujeitos distintos.

Ressalta-se que os sujeitos podem ser distintos, pois o sujeito passivo do crime não se confunde com prejudicado, ainda que sejam geralmente idênticos. O sujeito passivo do delito é sempre o titular do bem jurídico protegido. Já o sujeito prejudicado é qualquer pessoa que, em razão do crime, sofre prejuízo ou dano material ou moral. Portanto, o primeiro como vítima da relação processual-criminal é o titular do direito de representar criminalmente contra o sujeito ativo, além de ter o direito da reparação *ex delicto*, e o segundo será testemunha, a qual resta-lhe ainda o direito de postular a reparação do dano sofrido (BITTENCOURT, 2022, p. 345).

O elemento subjetivo do tipo penal é o dolo, haja vista que o legislador não quis tratar de punir a forma culposa (NUCCI, 2022, p. 634).

Concluindo, o desembargador Guilherme Nucci classifica o presente crime em comum; formal; comissivo; instantâneo, em regra, pois pode assumir a forma de instantâneo de efeitos permanentes, quando a invasão ou instalação de vulnerabilidade perpetua-se no tempo; unissubjetivo; plurissubsistente; admitindo tentativa, em regra, porém, inaceitável no tocante à figura do § 1º, pois se cuida da preparação do crime previsto no caput.

No entanto, o jurista Rogério Greco (2022, p. 508) possui entendimento diverso ao de Nucci, vez que destaca a possibilidade de o delito ser praticado omissivamente de forma imprópria, quando o agente, garantidor, nos termos do art. 13, § 2º, do Código Penal, devendo e podendo agir para impedir o resultado, nada o fizer.

5.1.2. DA MAJORAÇÃO DA PENA DO CRIME NA SUA FORMA BÁSICA

No tocante a majoração da pena do crime na sua forma básica, verifica-se que o legislador aumentu a pena imposta para a conduta descrita no *caput* do art. 154-A de 3 (três) meses a 1 (um) ano de detenção para de 1 (um) ano a 4 (quatro) anos de reclusão. Com isso, a conduta deixou de ser um crime de menor potencial ofensivo sujeito à jurisdição do Juizado Especial Criminal, conforme o art. 61 da Lei n° 9.099/95. Porém, ainda é cabível o instituto da suspensão condicional do processo, nos termos do art. 89 da Lei n° 9.099/95 e o acordo de não-persecução penal, à luz do art. 28-A do CPP.

5.1.3. DO PARÁGRAFO 1° DO ART. 154-A

O §1° do art. 154-A do Código Penal não sofreu qualquer alteração pela Lei n° 14.155/2021, desta forma sua redação permanece a da inclusão pela Lei n° 12.737/2012, qual seja:

> § 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 n° 12.737, de 2012)

Assim, é possível verificar que o presente parágrafo trata de figura equiparada ao crime disposto no *caput* e tem como finalidade tipificar o ato de desenvolver um *malware*, programa malicioso, o qual serve, nas palavras de Mário Cavalcante (2021), como “cavalo de troia” (trojan horse), uma vez que aquele programa irá criar uma vulnerabilidade no sistema para que possa ocorrer uma invasão ao equipamento.

Destaca-se que a presente equiparação tem como finalidade punir à preparação do crime principal, portanto não há sujeito passivo definido, assim a sociedade ocupa esse espaço, fez que ela tem interesse de preservar a intimidade e a vida privada (NUCCI, 2022, p. 635).

Para melhor entender a equiparação, o jurista Rogério Greco (2022, p. 510), relembra que o art. 1º da Lei nº 9.609, de 19 de fevereiro de 1998, traduz o conceito de programa de computador, vejamos:

> Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados.

5.1.4. DA MODIFICAÇÃO DA PARAGRAFO 2° DO ART. 154-A

O parágrafo 2° do art. 154-A do Código Penal traz uma causa especial de aumento de pena ao referido crime quando a invasão gera prejuízo econômico. Com a alteração pela Lei n° 14.155/2021, essa causa de aumento de pena se tornou mais gravosa, tendo em vista que antes era de 1/6 (um sexto) a 1/3 (um terço), e atualmente, é de 1/3 (um terço) a 2/3 (dois terços) (ESTEFAM, 2022, p. 505).

Por visar o aspecto econômico, nota-se que o autor da conduta que provoca prejuízo exclusivamente moral não incide a ele essa causa especial de aumento de pena, sendo que sua sanção apenas deve ser elevada na fixação da pena-base (art. 59, *caput*, do CP) (ESTEFAM, 2022, p. 505).

Deste contexto, verifica-se que o grau de elevação da pena está vinculado ao montante do prejuízo causado (NUCCI, 2022, p. 635).

5.1.5. DA ALTERAÇÃO DA PENA DO PARÁGRAFO 3° DO ART. 154-A

O parágrafo 3° do art. 154-A do Código Penal prevê uma qualificadora pelo resultado ao crime de invasão de dispositivo informático, vejamos:

> § 3º 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: (Incluído pela Lei n° 12.737, de 2012)
>
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei n° 14.155, de 2021)

Deste modo, conclui-se que haverá a incidência da qualificadora pelo resultado quando o agente conseguir obter um destes conteúdos: a) comunicações eletrônicas privadas, como, por exemplo, mensagens trocar pelo *WhatsApp;* b) segredos comerciais ou industriais, como fórmulas ainda não patenteadas; c) informações sigilosas, sendo que é necessário que o sigilo seja definido em lei, por causa do princípio da legalidade que rege o Direito Penal; ou d) na realização do controle à distância não autorizado do dispositivo invadido (ESTEFAM, 2022, p. 506).

O doutrinador Carlos Bittencourt (2022, p. 350) defende em sua obra que a incidência da qualificadora pelo resultado de obtenção de conteúdo por comunicações eletrônicas privadas diz respeito a um tipo penal aberto, dependendo de valoração, sendo valorado por ele que o tipo penal refere "*a qualquer conteúdo e de qualquer comunicação eletrônica*, independentemente de sua relevância ou natureza, desde que distinto das demais hipóteses elencadas" (BITTENCOURT, 2022, p. 350).

Já Rogério Greco defende que no tocante as informações sigilosas definidas por ele cuidam-se de norma penal em branco, uma vez que, para efeitos de reconhecimento das informações sigilosas, haverá necessidade de definição legal. Sendo que, a definição está precisa no inciso III do art. 4º da Lei nº 12.527, de 18 de novembro de 2011, vejamos:

> Art. 4º Para os efeitos desta Lei, considera-se:
>
> [...]
>
> III – informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

Ressalva-se ainda que o acesso ao teor de arquivos privados que não constituam comunicação com terceiros, como textos pessoais, ainda que de cunho particular, não se inclui na qualificadora, sendo que este caso aplicar-se-á o *caput* do art. 154-A (ESTEFAM, 2022, p. 506).

No tocante a qualificadora por obtenção de segredos comerciais ou industriais, segundo o jurista Carlos Bittencourt, o legislador incluiu uma hipótese de qualificadora específica diferente da hipótese explicada anteriormente (BITTENCOURT, 2022, p. 351).

Neste caso, envolve somente os segredos comerciais ou industriais, sendo irrelevante para essa hipótese o fato de esses segredos constarem de documento escrito, se são orais, por exemplo, gravação de voz, ou ainda, desenhados, o importante é que se encontrem armazenados no dispositivo informático (BITTENCOURT, 2022, p. 351).

Nessa senda, independe se são capazes de produzir ou se produziram dano ou prejuízo a alguém, o que, se ocorrer, representará somente o exaurimento do crime, que é capaz de majorar o crime, conforme o § 2º, o qual é aplicável somente às figuras do *caput* e do § 1º (BITTENCOURT, 2022, p. 351).

Ademais, é irrelevante também o fato de se tratar de segredo temporário ou condicionado ao advento de determinado fato, em ambos os casos há a qualificação do crime (BITTENCOURT, 2022, p. 351).

Aliás, é importante relembrar que para a configuração do tipo penal de invadir dispositivo informático de uso alheio que consta no caput do art. 154-A do CP não é necessário a obtenção de vantagem ilícita, e quando ocorre essa obtenção há apenas o exaurimento da ação. Porém, no caso das referidas qualificadoras há uma exceção a essa regra, visto que há consequências quando cumpridas uma dessas finalidades que é o agravamento da penalização. Assim, extraísse desse entendimento que quaisquer outras consequências, que porventura ocorram, que não qualificam o crime, representarão efetivamente apenas exaurimento deste (BITTENCOURT, 2022, p. 351).

Esses resultados, por causarem maior dano à privacidade, o legislador por meio da Lei n° 14.155 de 2021 aumentou a pena desta qualificadora de reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constituir crime mais grave, para pena de reclusão de 2 (dois) a 5 (cinco) anos.

Com efeito, o § 4º acrescenta ainda causa especial de aumento de pena as condutas que normalmente representem o simples exaurimento do crime qualificado

descrito no § 3º, ou seja, divulgar, comercializar ou transmitir a terceiro os dados ou informações obtidas pelo sujeito ativo (BITTENCOURT, 2022, p. 352).

Para entender a causa de aumento de pena por divulgação deve-se conceituá-la, para o doutrinador Carlos Bittencourt (2022, p. 352) a divulgação é tornar público ou do conhecimento de um número indeterminado de pessoas. Desta forma, a divulgação pode produzir-se por qualquer meio, o qual pode ser legítimo ou ilegítimo, por exemplo, imprensa, rádio, internet, etc. (BITTENCOURT, 2022, p. 352).

No tocante a causa de aumento de pena pela comercialização do fruto da invasão realizada, o doutrinador Carlos Bittencourt (2022, p. 352) salienta que a comercialização do produto do crime é natural, sempre que há valor econômico, sendo um *post factum* impunível, em regra. Porém, na situação tipificada, o legislador viu necessidade de punir esse ato (BITTENCOURT, 2022, p. 352).

Com relação a causa especial de aumento de pena pela transmissão a terceiro, o jurista Carlos Bittencourt defende que há redundância no texto do §4°, visto que, nas palavras dele, "*comercializar* é uma forma de transmitir a terceiros, e a *transmissão* a terceiros não deixa de ser uma modalidade de *comercializar"* (BITTENCOURT, 2022, p. 352).

Ao final, destaca-se que o texto § 5º não foi alterado pelo Lei n° 14.155/2021, desta forma contínua prevendo mais uma majorante quando praticado contra determinadas pessoas. Destaca-se que, de acordo o Carlos Bittencourt, essa majorante, deve ser aplicada somente e diretamente ao tipo penal qualificado do § 3° (BITTENCOURT, 2022, p. 352).

5.2. DO FURTO MEDIANTE FRAUDE

A Lei n° 14.155 de 2021 criou mais uma qualificadora para o crime de furto ao inserir o parágrafo 4°-B no art. 155 do CP, a qual incide quando o crime for cometido por meio de dispositivo eletrônico ou informático. Ainda, a citada Lei incluiu também

o §4°-C no art. 155 do CP, o qual introduziu no ordenamento jurídico brasileiro duas causas especiais de aumento de pena para a qualificadora do §4°-B[8].

Segundo André Estefam (2022, p. 555), com a inclusão este parágrafo o legislador tornou a qualificadora presente no art. 155, §4°, II do CP[9] uma modalidade genérica de fraude e, a estudada, uma modalidade específica.

Assim, quem "se faz passar por prestador de serviço para ingressar na residência da vítima e, aproveitando-se da facilidade obtida com esse ardil, subtrai do imóvel algum objeto de valor" (ESTEFAM, 2022, p. 555), comete a furto qualificado mediante fraude na modalidade genérica (art. 155, II, do CP). Já, quem "obtém a senha bancária e os dados de login da vítima e realiza transferência bancária não autorizada, subtraindo os valores correspondentes da conta corrente do ofendido" (ESTEFAM, 2022, p. 555), comete furto qualificado mediante fraude na forma específica (art.155, §4°-B, do CP)

Desta forma, antes da inclusão do parágrafo 4°-B, quem cometia segunda conduta citada, cometia o crime de furto mediante fraude do art. 155, §4°, II do Código Penal. Mas, atualmente, como vimos, com a alteração da Lei n° 14.155/2021 o legislador criou um tipo penal específico para essa conduta que está disposto no art. 155, §4°-B do Código Penal.

Ocorre que, como o direito penal brasileiro não admite retroatividade de lei mais gravosa e a pena do crime de furto mediante fraude comum é menor que a de furto cometido mediante dispositivo eletrônico ou informático, aplica-se ainda pena

---

[8] Art. 155 (...) § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido: II - com abuso de confiança, ou mediante fraude, escalada ou destreza.

[9] Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
Pena - reclusão, de um a quatro anos, e multa.
§ 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. (Incluído pela Lei nº 14.155, de 2021)
§ 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021)
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; (Incluído pela Lei nº 14.155, de 2021)
II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (Incluído pela Lei nº 14.155, de 2021)

do furto mediante fraude comum para os delitos cometidos antes de 27 de maio de 2021, data da entrada em vigor da Lei n° 14.155/2021 (GONÇALVES, 2022, p. 401).

Dito isso, para melhor entender quando ocorre a tipificação do crime no art. 155, §4°-B, do CP, é necessário compreender o conceito de dispositivo informático e dispositivo eletrônico e do termo “meio fraudulento análogo”.

De acordo com o jurista André Estefam (2022, p. 556), dispositivo informático é todo “mecanismo físico ou virtual capaz de reunir informações ou dados digitalizados em ambiente eletrônico, por meio da linguagem característica dos computadores e mecanismos equivalentes”, como exemplo, um *tablet,* um *smartphone* ou um *pendrive.*

Por outro lado, o dispositivo eletrônico é, para o doutrinador, um “aparato eletrônico que não trabalhe com informações ou dados digitalizados” (ESTEFAM, 2022, p. 556).

E, ainda, conforme André Estefam (2022, p. 556), o termo “meio fraudulento análogo” deve-se ser interpretado como o uso de todo meio fraudulento análogo ao dispositivo informático ou eletrônico, vez que, caso não seja, será aplicada a qualificadora do art. 155, §4°, II, do CP.

Salienta-se ainda que para incidência dessa qualificadora (art. 155, §4°-B, do CP) o dispositivo eletrônico ou informático pode ou não estar conectado à rede de computadores[10], bem como é irrelevante o fato de haver ou não violação de mecanismo de segurança (*firewall,* por exemplo) ou utilização de programa malicioso (*malware*), de acordo com a imposição legal (GRECO, 2022, p. 550).

Outrossim, o doutrinador Vinícius Gonçalves (2022, p. 401) destaca em sua obra que o legislador não informa que a fraude deve ser perpetrada por meio eletrônico ou informático, mas que o furto deverá ser cometido por um desses meios para a incidência dessa qualificadora.

---

[10]“Por expressa disposição legal é irrelevante para a existência da qualificadora se o dispositivo estava ou não conectado à rede de computadores. O furto cometido com o emprego do aparato conhecido popularmente como “chupa cabra” se enquadra nessa hipótese. Trata-se de um mecanismo eletrônico instalado pelo agente, não conectado à internet, na entrada dos terminais de autoatendimento bancário que, uma vez inserido o cartão da vítima, copia todos os dados sigilosos. É o que ocorre, também, com dispositivos instalados em máquinas de pagamento de cartão bancário (na modalidade crédito ou débito) que armazenam ilicitamente as informações do usuário, permitindo que o agente realize, posteriormente, transferências ou saques da conta bancária do sujeito passivo.” (ESTEFAM, 2022, p. 556).

Por este motivo, ele defende que um indivíduo que “emprega algum tipo de fraude para obter o cartão bancário da vítima e, em seguida, faz saques não autorizados em caixas eletrônicos, utilizando o cartão da vítima e a respectiva senha obtidos fraudulentamente” (GONÇALVES, 2022, p. 401), responderá pela figura do furto mediante fraude na modalidade específica (art. 155, §4°-B).

Além do mais, o legislador acrescentou que se esta conduta é praticada mediante a utilização de servidor mantido fora do território nacional, contra pessoa idosa (art. 1°, Lei n° 10.741/2003) ou pessoa vulnerável (art. 217-A, caput e § 1º, do CP) haverá a incidência de uma causa especial de aumento de pena, conforme art. 155, §4°-C, do Código Penal (GRECO, 2022, p. 550).

Porém, para incidência dessa causa especial de aumento de pena, o jurista Rogério Sanches Cunha alerta que é necessário que o agente saiba dessa condição, *in verbis*:

> [...] Note-se, por fim, que a majoração da pena pressupõe a ciência das circunstâncias referidas no § 4º-C. O autor da subtração deve ter conhecimento de que sua conduta se vale de conexão internacional. Ou deve saber que a vítima é idosa ou vulnerável, o que nem sempre ocorrerá, em razão das circunstâncias dos crimes cibernéticos, nos quais muitas vezes o criminoso não tem nenhum contato – nem mesmo remoto – com sua vítima. (CUNHA, 2021).

Deste contexto, faz-se necessário destacar que é irrelevante para incidência da majorante do inciso I do §4°-C o fato do sujeito ativo estar ou não em território nacional, sendo relevante apenas a utilização de um servidor fora do país (ESTEFAM, 2022, p. 557).

Com relação a majorante disposta no inciso II do §4°-C, o doutrinador André Estefam (2022, p. 557/558), defende que os demais vulneráveis mencionados no § 1º do art. 217-A do Código Penal também são alcançados por essa proteção, mas com ressalvas, uma vez que se deve realizar uma interpretação finalística, ou seja, visar o ponto de vista patrimonial, já que a norma está no Título II do CP.

Desta forma, ao avaliar essa falta de discernimento que torna a pessoa vulnerável deve-se analisar a patrimonial, por exemplo, “alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para o ato cometido pelo furtador” (ESTEFAM, 2022, p. 558).

Nessa senda, deve-se interpretar ainda a causa especial de aumento de pena no tocante a vítimas que não podem oferecer resistência (art. 217-A, §1°, do CP vislumbrando o sentido patrimonial, por exemplo, “a vítima encontrar-se embriagada a ponto de não discernir a natureza do ato praticado pelo autor da subtração realizada com emprego de dispositivo eletrônico ou informático” (ESTEFAM, 2022, p. 558).

5.3. DAS ALTERAÇÕES NO CRIME DE ESTELIONATO

A Lei n° 14.155/2021 ainda efetuou três significantes alterações no art. 171 do Código Penal[11], quais sejam: a) inseriu o § 2º-A, prevendo a qualificadora do estelionato mediante fraude eletrônica; b) acrescentou o § 2º-B, com uma causa de aumento de pena relacionada com o § 2º-A; c) modificou a redação da causa de aumento de pena do § 4º-A.

Nota-se que essas alterações promovidas no Código Penal pela Lei n° 14.155, de 27-5-2021 foram mais gravosas, logo não podem ser aplicadas a fatos cometidos antes do início de sua vigência, ou seja, antes de 28 de maio de 2021 (ESTEFAM, 2022, p. 693).

Ainda, destaca-se que em contramão das demais espécies de estelionato (art. 157, caput e §2º do CP), que admitem a suspensão condicional do processo e o

[11] 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:
Fraude eletrônica
§ 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. (Incluído pela Lei nº 14.155, de 2021)
§ 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. (Incluído pela Lei nº 14.155, de 2021)
§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.
Estelionato contra idoso
~~§ 4º Aplica-se a pena em dobro se o crime for cometido contra idoso. (Incluído pela Lei nº 13.228, de 2015)~~
Estelionato contra idoso ou vulnerável (Redação dada pela Lei nº 14.155, de 2021)
§ 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)

acordo de não persecução penal, o estelionato mediante fraude eletrônica, na forma consumada, não admite a incidência desses institutos, afinal a sua pena mínima é de 4 (quatro) anos (ESTEFAM, 2022, p. 696).

5.3.1. DO ESTELIONATO MEDIANTE FRAUDE ELETRÔNICA (§2°-A)

A primeira alteração realizada no texto do art. 171 do Código Penal foi a criação de uma nova qualificadora ao crime de estelionato com a inserção do §2-A, a qual tem como finalidade tipificar especificamente a conduta do indivíduo que obtém vantagem ilícita por meio de informações conquistada de forma eletrônica, dadas pela vítima ou por um terceiro que foram induzidos ao erro.

Conforme o jurista Guilherme Nucci (2022, p. 699), essa alteração no texto legal se fez necessária pelo avanço da internet como um todo, que possibilitou que os estelionatários migrassem para novas modalidades de fraude.

O jurista Rogério Greco (2022, p. 750) informa que esta qualificadora tem incidência quando “a vítima ou o terceiro são induzidos a erro, e o agente se utiliza das informações por eles fornecidas, através: a) das redes sociais b) contatos telefônicos; c) envio de correio eletrônico fraudulento; d) ou por qualquer outro meio fraudulento análogo”.

No mesmo sentido, o doutrinador Victor Gonçalves, expõe que para a incidência da qualificadora em estudo é necessário a presença de dois requisitos cumulativos, quais sejam:

> a) que o agente empregue fraude com a utilização de informações fornecidas pela vítima ou por terceiro;
> b) que as informações referidas no item anterior tenham sido obtidas pelo agente, da vítima ou de terceiro, por meio de rede social, contato telefônico, envio de correio eletrônico fraudulento ou qualquer outro meio fraudulento análogo. (GONÇALVES, 2022, p. 158)

Assim, esses dois requisitos devem estar presentes para a configuração do estelionato mediante fraude eletrônica, sendo que a ausência de um desses requisitos gere a tipificação apenas do crime de estelionato na sua figura simples, no qual a pena é menor (GONÇALVES, 2022, p. 159).

Nessa senda, é necessário relembrar que no estelionato, em contramão ao furto, é a que vítima fornece as informações que possibilitam a prática do crime e, no caso estudado, a vítima irá fornecer estas informações porque foi levada a erro por meio de uma fraude eletrônica (GRECO, 2022, p. 750).

Um exemplo da prática desse estelionato, o qual está muito presente em nosso cotidiano, é o conhecido “golpe do Whatsapp”, que ocorre, por exemplo, quando o agente liga para a vítima com o pretexto de entrevistá-la para uma pesquisa e, ao final, roga que ela forneça um código que ele enviou por SMS, que será usado para clonar sua conta do aplicativo WhatsApp; após, o agente então começa a enviar mensagens para os contatos da vítima, fingindo ser ela e pedindo que o empreste dinheiro, pois está com dificuldades financeiros (GONÇALVES, 2022, p. 159).

Outro exemplo muito conhecido da incidência da qualificadora, é quando o agente cria um site falso, no qual a vítima fornece as informações de seu cartão, possibilitando que o agente tome conhecimento e, posteriormente, faça compras usando os dados do cartão da vítima (GONÇALVES, 2022, p. 529).

Destaca-se ainda que para a configuração de estelionato mediante fraude eletrônica é essencial que a fraude seja praticada por algum meio eletrônico ou informático que implique iludir a vítima ou terceiro a fornecer informações. Por este motivo, o doutrinador André Estefam afirma que, no seguinte exemplo, não há o estelionato mediante fraude eletrônica, mas sim estelionato simples:

> [...] o indivíduo mantém página na rede social Facebook anunciando empréstimos a juros baixos e independente de restrições em cadastros de crédito, e, quando o sujeito passivo faz o contato, o convence, mediante ardil, a realizar um depósito prévio, relativo a supostas taxas administrativas, mas, depois de realizado o pagamento mencionado, o(s) estelionatário(s) – obviamente – não honra(m) com o empréstimo e deixa(m) de fazer qualquer contato com o ofendido. Note-se que o agente não induziu a vítima a fornecer qualquer dado a ele, mas convenceu-a, mediante expediente fraudulento, a realizar o depósito em dinheiro na conta do criminoso. (ESTEFAM, 2022, p. 694/695).

Concluindo, o jurista André Estefam explica ainda que a consumação deste crime se dará com o prejuízo financeiro da vítima em favor do agente, assim, no caso do exemplo do “golpe do Whatsapp”, o dono das informações utilizados não teve prejuízo financeiro, não sendo vítima do delito de estelionato mediante fraude;

mas os contatos que fizeram a transferência bancária são as vítimas, cada uma de um delito, os quais serão punidos em concursos de crimes. Já os que não realizaram a transferência, mas foram contatados, serão vítimas de tentativa de estelionato mediante fraude eletrônica (ESTEFAM, 2022, p. 694).

5.3.1. DA CAUSA ESPECIAL DE AUMENTO DE PENA NO ESTELIONATO MEDIANTE FRAUDE ELETRÔNICA (§2°-B)

A segunda alteração efetuada pelo legislador, conforme já visto, foi acrescentar ao texto uma causa especial de aumento, quando o crime de estelionato mediante fraude eletrônica for praticado com a utilização de servidor mantido fora do território nacional.

Esta causa de aumento demonstrou que o legislador tem conhecimento da dificuldade de identificação do sujeito ativo nos crimes virtuais ainda mais os que são realizados no exterior, por causa da questão territorial (GONÇALVES, 2022, p. 530).

Para a aplicação desta causa especial de aumento de pena o julgador irá analisar a relevância no caso concreto e como essa utilização de servidor mantido fora do território nacional dificultou a investigação dos fatos ocorridos, para então fixar o patamar da majoração (GRECO, 2022, p. 571).

Verifica-se uma divergência doutrinária quando a valoração do quantum da causa especial de aumento de pena. Para Victor Gonçalves e André Estefam, quantum de aumento deve guardar proporção com o prejuízo causado ao patrimônio da vítima (GONÇALVES, 2022, p. 530; ESTEFAM, 2022, p. 694). Já, para o jurista Guilherme Nucci, “o aumento deve basear-se no grau de dificuldade da apuração do caso” (NUCCI, 2022, p. 699).

Além disso, frisa-se que para a incidência da estuda majorante o agente não precisa necessariamente estar no estrangeiro, mas que utilize de servidor que está (ESTEFAM, 2022, p. 695)

5.3.1. DA CAUSA ESPECIAL DE AUMENTO DE PENA NO ESTELIONATO (§4°)

A última alteração que foi realizada pela Lei nº 14.155/2021 no art. 171 do Código Penal foi a ampliação da causa especial de aumento de pena do §4º, fazendo com que haja a incidência da majorante também quando delito for praticado contra pessoa vulnerável (GRECO, 2022, p. 753).

Desta forma, atualmente há a incidência da majorante quando crime for cometido contra idoso, pessoa com idade igual ou superior a 60 (sessenta) anos (art. 1º da Lei nº 10.741/2003), ou vulnerável (GRECO, 2022, p. 753).

O doutrinador Rogério Greco (2022, p. 573) destaca em sua obra que para a aplicação dessa causa especial de aumento de pena é necessário que o agente tenha efetivo conhecimento da idade da vítima, senão poderá ser reconhecido o erro de tipo.

Já, com relação as pessoas vulneráveis, o referido jurista enfatiza que para entender este termo é necessário aplicar o art. 217-A do Código Penal, ou seja, para ele são pessoas vulneráveis as menores de 14 (quatorze) anos e as que por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do crime (GRECO, 2022, p. 753).

Além dessa alteração, o legislador alterou também a pena da majorante, introduzindo no ordenamento uma *novatio legis in mellius* (nova lei mais branda), visto que a pena anteriormente deveria ser dobrada e agora pode ser aumentada de 1/3 até o dobro (CAPEZ, 2022, p. 254).

Ademais, o desembargador Guilherme Nucci (2022, p. 699) em sua obra assevera que o grau de aumento a ser aplicado pelo magistrado deverá ser proporcional à relevância do resultado gravoso, ou seja, “quanto maior o prejuízo causado à vítima, mais deve ser o aumento imposto ao agente” (NUCCI, 2022, p. 699).

5.3.2. DA COMPETÊNCIA DE JULGAMENTO NO ESTELIONATO

Uma outra preocupação do legislador que ficou evidenciada com a edição da Lei n° 14.155 de 2021 foi com relação à competência de julgar os crimes de

estelionato. Este tema gerava uma grande discussão doutrinária e jurisprudencial, e consequentemente, insegurança jurídica.

Por este motivo, a Lei n° 14.155 de 2021 incluiu o §4° no art. 70 do Código de Processo Penal, senão vejamos:

> Art. 70. (...) § 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.

Anteriormente, a competência para julgar o estelionato praticado por meio da emissão de cheque sem fundos (art. 171, 2º, VI, do CP) era do local da recusa do cheque, nos termos da Súmula n° 244 do Superior Tribunal de Justiça e Súmula n° 521 do Supremo Tribunal Federal (GONÇALVES; REIS, 2022, p. 182), *in verbis*:

> Súmula 244-STJ: Compete ao foro do local da RECUSA processar e julgar o crime de estelionato mediante cheque sem provisão de FUNDOS.
>
> Súmula 521-STF: O foro competente para o processo e julgamento dos crimes de estelionato, sob a modalidade da emissão dolosa de cheque sem provisão de FUNDOS, é o do local onde se deu a RECUSA do pagamento pelo sacado.

Porém, com o advento da referida legislação, a competência de julgar passou a ser do local do domicílio da vítima, nos termos do art. 70, §4° do Código de Processo Penal, superando as mencionadas Súmulas e criando uma exceção à regra do caput do art. 70 do CPP [12](GONÇALVES; REIS, 2022, p. 182).

Sendo que se entende como o domicílio da vítima para a fixação da competência, de acordo com o jurista Guilherme Nucci (2022, p. 319), “o lugar onde a pessoa mantém o seu centro principal de atividades, negócios e, principalmente, sua família”, nos termos do art. 70 do Código Civil. Assim, aplica-se a regra do

[12] Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.

Direito Civil para a identificação do domicílio da vítima, ou seja, os artigos 70 a 73 do CC[13] (NUCCI, 2022, p. 319).

A exceção de competência prevista no art. 70, §4° do CP, deve ser aplicada também para o estelionato praticado mediante cheque com pagamento frustrado, que é quando no momento da emissão há fundos disponíveis, mas após o agente emite uma contraordem à instituição bancária, a qual determina que não seja pago aquele cheque (CAVALCANTE, 2021).

Além disso, o §4° do art. 70 do CPP aplica-se também no crime de estelionato mediante depósito ou transferência bancária, o qual está tendo muita incidência atualmente. O jurista Mário Cavalcante explica esse crime da seguinte forma:

> [...] Carlos, morador de Goiânia (GO), viu um anúncio na internet que oferecia empréstimo "rápido e fácil". Ele entrou em contato com a pessoa, que se identificou como Henrique.
>
> Carlos combinou de receber um empréstimo de R$ 70 mil, no entanto, para isso, ele precisaria depositar uma parcela de R$ 1 mil a título de "custas" para a conta bancária de Henrique, vinculada a uma agência bancária localizada em São Paulo (SP).
>
> Carlos efetuou o depósito e, então, percebeu que se tratava de uma fraude porque nunca recebeu o dinheiro do suposto empréstimo.
>
> Quem será competente para processar e julgar este crime de estelionato: o juízo da comarca de Goiânia (onde foi feito o depósito) ou o juízo da comarca de São Paulo (local onde o dinheiro foi recebido)? [...] (CAVALCANTE, 2021).

A resposta para essa pergunta irá depender de quando este crime foi cometido. Se anterior a Lei n° 14.155 de 2021, o Juízo competente será o da comarca de São Paulo, pois o entendimento jurisprudencial era no sentido de que a vantagem indevida ocorreu quando o dinheiro adentrou a conta bancária do

[13] Art. 70. O domicílio da pessoa natural é o lugar onde ela estabelece a sua residência com ânimo definitivo.
Art. 71. Se, porém, a pessoa natural tiver diversas residências, onde, alternadamente, viva, considerar-se-á domicílio seu qualquer delas.
Art. 72. É também domicílio da pessoa natural, quanto às relações concernentes à profissão, o lugar onde esta é exercida.
Parágrafo único. Se a pessoa exercitar profissão em lugares diversos, cada um deles constituirá domicílio para as relações que lhe corresponderem.
Art. 73. Ter-se-á por domicílio da pessoa natural, que não tenha residência habitual, o lugar onde for encontrada.

estelionato, tendo como fundamento direto o art. 70, *caput*, do CPP. Se o caso ocorreu após a Lei n° 14.155 de 2021, a competência será do domicílio da vítima, ou seja, no caso, no Juízo de Goiânia, nos termos do §4° do art. 70 do CPP (CAVALCANTE, 2021).

Destaca-se que caso houvesse mais de uma vítima no exemplo, essa competência seria decidida por prevenção, à luz do art. 83 do CPP, vejamos:

> Art. 83. Verificar-se-á a competência por prevenção toda vez que, concorrendo dois ou mais juízes igualmente competentes ou com jurisdição cumulativa, um deles tiver antecedido aos outros na prática de algum ato do processo ou de medida a este relativa, ainda que anterior ao oferecimento da denúncia ou da queixa (arts. 70, § 3º, 71, 72, § 2º, e 78, II, c).

Ademais, os doutrinadores Victor Gonçalves e Alexandre Reis destacam que mesmo que a conduta descrita no tipo penal seja a emissão do cheque sem fundos, o entendimento consolidado pelos Tribunais Superiores é que só há a consumação do delito com a devolutiva do banco sacado informando o não pagamento do título por insuficiência de fundos (GONÇALVES; REIS, 2022, p. 182)

Por fim, é importante salientar que, pelo entendimento do jurista Mário Cavalcante (2021), por força do princípio da *perpetuatio jurisdictionis* (perpetuação da jurisdição), previsto no art. 43 do CPC e que pode ser aplicado ao processo penal, nos termos do art. 3º do CPP, não cabe a alteração da competência dos processos penais já em andamento quando a entrada em vigor da Lei n° 14.155/2021.

CONCLUSÃO

Por meio do levantamento bibliográfico e documental, foi possível compreender que a Lei nº 14.155 de 2021 foi um meio no qual o legislador encontrou para demonstrar sua intolerância com condutas que estavam sendo cada vez mais praticadas com os avanços tecnológicos.

Para tanto, no primeiro capítulo foi introduzida toda a temática, informando a sua relevância, a metodologia que seria adotada e o que seria abordado neste Trabalho de Graduação.

Após, no segundo capítulo foi relembrado sobre o conceito do termo “crime” no sistema jurídico brasileiro, desta forma foi possível entender que crime é, em síntese, o fato típico e antijurídico.

Nessa senda, no terceiro capítulo foi inserida a ideia do que seria o Direito Digital e crimes informáticos, bem como outros termos frequentemente utilizados para atos criminosos realizados no mundo virtual. Com isso, foi possível compreender que o Direito Digital não é um ramo do Direito, mas uma evolução deste que deve ser contemplada por todas as áreas do Direito. Além disso, verificou-se que o termo “crime informático” é o mais adequado para ser utilizado aos crimes estudados.

No quarto capítulo foi abordado sobre o ordenamento jurídico antes da Lei nº 14.155 de 2021, em virtude disso entendeu-se que em 2012 o legislador brasileiro notou a necessidade de tipificar condutas realizadas mediante o uso de sistema eletrônico de forma específico por meio da Lei nº 12.735/2012 e da Lei nº 12.737/2012, preenchendo assim uma grande lacuna no ordenamento jurídico. Porém, com o passar dos anos e o avanço desenfreado da tecnologia a eficiência dessas tipificações foram progressivamente diminuídas.

Por este motivo, no quinto capítulo foi exposto sobre o Projeto de Lei nº 4.554 de 2020, o qual foi cunhado pelos legisladores brasileiros para alinhar o ordenamento jurídico penal a realidade enfrentada pelos cidadãos. Isto posto, foi possível compreender que inicialmente o texto base do referido projeto de lei tinha como enforque combater apenas a prática de fraude eletrônica, através da modificação do art. 155 do Código Penal e a apresentação de hipóteses agravantes,

mas após diversas alterações realizadas pelas Casas legislativas e sanção presidencial o citado projeto de transformou na Lei nº 14.155 de 2021.

Ao final, no penúltimo capítulo, foi tratado especificamente sobre a Lei nº 14.155 de 2021, demonstrando as alterações que ela realizou no Código Penal para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; bem como a modificação no Código de Processo Penal para definir a competência em modalidades de estelionato. À vista disso, entendeu-se que estas alterações legislativas como um todo, vislumbrando os detalhes de cada alteração, a sua finalidade e sua aplicabilidade.

Concluindo, cumpra-se destacar que os objetivos traçados no primeiro capítulo foram devidamente atingidos, uma vez que o presente Trabalho de Graduação conseguiu tratar sobre a nova perspectiva trazida pela Lei nº 14.155/2021 e os reflexos da sua aplicação; bem como demonstrou no que se respaldou os congressistas para a realização desta importante modificação no Código Penal e no Código de Processo Penal, e expôs de forma sistemática as inovações legislativas trazidas pela Lei nº 14.155/2021, criando um paralelo sobre o sistema jurídico anterior e posterior a legislação.

REFERÊNCIAS

ANDREUCCI, Ricardo A. **Manual de Direito Penal**. São Paulo: Editora Saraiva, 2021. 9786555598377. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598377/. Acesso em: 13 jul. 2022.

BITENCOURT, Cezar R. **TRATADO DE DIREITO PENAL 1 - PARTE GERAL.** São Paulo: Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555590333/. Acesso em: 02 mai. 2022.

BITENCOURT, Cezar R. **Tratado de Direito Penal: Parte especial: crimes contra a dignidade sexual até crimes contra a fé pública - arts. 213 a 311-- Vol. 4.** São Paulo: Editora Saraiva, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555597141/. Acesso em: 06 mai. 2022

BRASIL. **Decreto-Lei n° 2.848 de 07 de dezembro de 1940**. Código Penal. Brasília: DF: Presidência da República, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm#art266 Acesso em: 29 set. 2021.

BRASIL. **Lei n° 7.716 de 05 de janeiro de 1989**. Define os crimes resultantes de preconceito de raça ou de cor. Brasília: DF: Presidência da República, 1989. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7716.htm Acesso em: 29 set. 2021.

BRASIL. **Lei n° 12.735 de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília: DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm Acesso em: 29 set. 2021.

BRASIL. **Lei n° 12.737 de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília: DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm Acesso em: 29 set. 2021.

BRASIL. **Lei n° 14.155 de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de

violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília: DF: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm Acesso em: 29 set. 2021.

CAVALCANTE, Márcio André Lopes. **Lei n° 14.155/2021 promove alterações nos crimes de violação de dispositivo informático, furto e estelionato.** Dizer o Direito, 2021. Disponível em: https://www.dizerodireito.com.br/2021/05/lei-141552021-promove-alteracoes-nos.html Acesso em: 02 mai. 2022.

CAPEZ, Fernando. **Curso de direito penal: parte especial – arts. 121 a 212. v.2**. São Paulo: Editora Saraiva, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596045/. Acesso em: 06 mai. 2022.

CONGRESSO NACIONAL (Brasília, DF). **Projeto de lei n° 4.554 de 2020.** Disponível em: https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-4554-2020. Acesso em: 06 jul 2022.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital: primeiras impressões e reflexos no CP e no CPP**. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/ . Acesso em: 12 mai. 2022.

D'URSO, Luiz Augusto Filizzola. **Cibercrime:** Perigo na Internet!. [s.n.], [S.l.], Disponível em: https://www.oabsp.org.br/comissoes2010/gestoes-anteriores/acao- social/artigos/Artigo%20Cibercrime%20-%20Luiz%20Augusto%20DUrso.pdf . Acesso em: 06 out. 2021.

GONÇALVES, Victor Eduardo Rios. **Direito Penal**: parte especial. 10. ed. São Paulo: Saraiva, 2020

GONÇALVES, Victor Eduardo R. **CURSO DE DIREITO PENAL V 1.** São Paulo: Editora Saraiva, 2021, p. 45. 9786555595666. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555595666/. Acesso em: 02 mai. 2022.

GONÇALVES, Victor Eduardo R.; LENZA, Pedro. **Esquematizado - Direito Penal - Parte Especial**. São Paulo: Editora Saraiva, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555597738/. Acesso em: 06 mai. 2022.

GONÇALVES, Victor Eduardo R.; REIS, Alexandre Cebrian A. **Esquematizado - Direito Processual Penal.** São Paulo: Editora Saraiva, 2022. 9786553623101. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623101/. Acesso em: 05 jul. 2022.

GRECO, Rogério. **Curso de Direito Penal: artigos 121 a 212 do Código Penal. v.2**. São Paulo: Grupo GEN, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 06 mai. 2022.

MIRABETE, Julio F. **Manual de Direito Penal - Parte Geral - Vol. 1**. São Paulo: Grupo GEN, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597028102/. Acesso em: 02 mai. 2022.

MORAES, Alexandre Fernandes **D. REDES DE COMPUTADORES: FUNDAMENTOS**. São Paulo: Editora Saraiva, 2020. 9788536532981. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536532981/. Acesso em: 09 jul. 2022.

NUCCI, Guilherme de S. **Curso de Direito Penal - Parte Geral - Vol. 1.** São Paulo: Grupo GEN, 2021, p. 161. 9788530993658. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993658/. Acesso em: 02 mai. 2022.

NUCCI, Guilherme de S. **Curso de Direito Processual Penal**. São Paulo: Grupo GEN, 2022. 9786559644568. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559644568/. Acesso em: 05 jul. 2022.

NUCCI, Guilherme de S. **Manual de Direito Penal**. São Paulo: Grupo GEN, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559642830/. Acesso em: 06 mai. 2022.

NUCCI, Guilherme de S. **Manual de Direito Penal**. São Paulo: Grupo GEN, 2021. 9788530993566. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993566/. Acesso em: 13 jul. 2022.

PINHEIRO, Patrícia P. **Direito Digital**. São Paulo: Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 05 mai. 2022.

PRADO, Luiz R. **Curso de Direito Penal Brasileiro - Volume Único**. São Paulo: Grupo GEN, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994136/. Acesso em: 02 mai. 2022.

ROMANI, Bruno. 6 casos de ataque hacker. **Super Interessante**, [S. l.], p. Não paginado, 8 jun. 2015. Disponível em: https://www.serasaexperian.com.br/sala-de- imprensa/analise-de-dados/brasileiros-sofrem-uma-tentativa-de-fraude-a-cada-8- segundos-revela-levantamento-da-serasa-experian/. Acesso em: 10 set. 2021

SENADO FEDERAL (Brasília, DF). Senador Izalci Lucas. **Projeto de lei n° 4.554/2020. 04 de outubro de 2020**. Combate a prática de fraude eletrônica, modifica o art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e apresenta hipóteses agravantes. Projeto de Lei n° 4.554 de 2020, [*S. l.*], p. 01-05, [2020?]. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8889876&ts=1630441295245&disposition=inline.Acesso em: 10 set. 2021.

SERASA EXPERIAN. **Brasileiros sofrem uma tentativa de fraude a cada 8 segundos, revela levantamento da Serasa Experian**. [S. l.]: [s. n.], 30 ago. 2021. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/analise-de- dados/brasileiros-sofrem-uma-tentativa-de-fraude-a-cada-8-segundos-revela- levantamento-da-serasa-experian/. Acesso em: 10 set. 2021.

STEFAM, André. **Direito penal, v. 2: parte especial: arts. 121 a 234-C**. 9. ed. São Paulo: Saraiva Jur, 2022. Livro. (1 recurso online). ISBN 9786555596564. Disponível em: https://integrada.minhabiblioteca.com.br/books/9786555596564. Acesso em: 29 jun. 2022.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. São Paulo: Editora Saraiva, 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555591484/. Acesso em: 05 mai. 2022