

## CRIMES CIBERNÉTICOS UMA PONDERAÇÃO SOBRE A LEI 14.155 DE 2021 APLICÁVEL AO CRIME DE ESTELIONATO VIRTUAL

CYBER CRIMES A CONSIDERATION ON LAW 14,155 OF 2021 APPLICABLE TO THE  
CRIME OF VIRTUAL SCAMMER

DELITOS CIBERNÉTICOS UNA CONSIDERACIÓN SOBRE LA LEY 14.155 DE 2021  
APLICABLE AL DELITO DE ESTAFADOR VIRTUAL

Walyson Milhomem de Sousa Gomes<sup>1</sup>  
Lucas Cavalcante Medrado<sup>2</sup>

**RESUMO:** Esse artigo buscou discutir sobre os crimes cibernéticos, fazendo uma ponderação sobre a Lei 14.155 de 2021 aplicável ao crime de estelionato virtual. Este estudo é relevante tanto para a sociedade quanto para o campo do direito, pois oferece uma análise reflexiva e medidas preventivas destinadas a contribuir com a redução do número de vítimas de golpes perpetrados por estelionatários virtuais. O objetivo geral deste trabalho foi analisar a recente alteração suscitada pela Lei 14.155 de 2021 no tocante ao crime de estelionato virtual, adotando a metodologia do trabalho jurídico e o método dedutivo, além da técnica exploratória por meio da análise e revisão de literatura abrangendo pesquisas e estudos associados ao tópico em questão. Com base nos resultados obtidos, pode-se concluir que, as mudanças trazidas pela Lei nº 14.155 de 2021, foram de suma importância para ajudar a combater os crimes virtuais, visto que referida lei atribuiu maior responsabilidade penal para os sujeitos ativos do estelionato virtual. Contudo, é imperativo manter um processo contínuo de revisão das legislações, desenvolvimento de políticas públicas destinadas a combater delitos cibernéticos, implementação de tecnologias de segurança, oferta de treinamentos para os usuários e execução de operações policiais.

1870

**Palavras-chave:** Crimes Virtuais. Estelionato Virtual. Internet. Lei nº 14.155/2021.

**ABSTRACT:** This article sought to discuss cybercrimes, considering Law 14,155 of 2021 applicable to the crime of virtual fraud. This study is relevant both to society and to the field of law, as it offers a reflective analysis and preventive measures designed to contribute to reducing the number of victims of scams perpetrated by virtual fraudsters. The general objective of this work was to analyze the recent change brought about by Law 14,155 of 2021 regarding the crime of virtual embezzlement, adopting the methodology of legal work and the deductive method, in addition to the exploratory technique through analysis and literature review covering research and studies associated with the topic in question. Based on the results obtained, it can be concluded that the changes brought by Law No. 14,155 of 2021 were of paramount importance in helping to combat virtual crimes, as said law attributed greater criminal responsibility to the active subjects of virtual fraud. However, it is imperative to maintain a continuous process of reviewing legislation, developing public policies aimed at combating cyber crimes, implementing security technologies, offering training to users and carrying out police operations.

**Keywords:** Virtual Crimes. Virtual Scam. Internet. Law No. 14.155/2021.

<sup>1</sup>Graduando do Curso de Direito da Faculdade de Ciências Jurídicas de Paraíso do Tocantins (FCJP).

<sup>2</sup> Docente do curso de Direito da Faculdade de Ciências Jurídicas de Paraíso do Tocantins (FCJP).

**RESUMEN:** Este artículo buscó discutir los delitos cibernéticos, considerando la Ley 14.155 de 2021 aplicable al delito de estafa virtual. Este estudio es relevante tanto para la sociedad como para el ámbito del derecho, ya que ofrece un análisis reflexivo y medidas preventivas diseñadas para contribuir a reducir el número de víctimas de estafas perpetradas por defraudadores virtuales. El objetivo general de este trabajo fue analizar el cambio reciente que trajo la Ley 14.155 de 2021 respecto del delito de peculado virtual, adoptando la metodología de trabajo jurídico y el método deductivo, además de la técnica exploratoria a través del análisis y revisión de la literatura que abarca la investigación, y estudios asociados al tema en cuestión. Con base en los resultados obtenidos, se puede concluir que los cambios introducidos por la Ley N° 14.155 de 2021 fueron de suma importancia para ayudar a combatir los delitos virtuales, toda vez que dicha ley atribuía mayor responsabilidad penal a los sujetos activos de la estafa virtual. Sin embargo, es imperativo mantener un proceso continuo de revisión de la legislación, desarrollar políticas públicas orientadas a combatir los delitos cibernéticos, implementar tecnologías de seguridad, ofrecer capacitación a los usuarios y realizar operativos policiales.

**Palabras clave:** Delitos Virtuales. Estafa virtual. Internet. Ley N° 14.155/2021.

## 1 INTRODUÇÃO

A utilidade e o amplo alcance da internet são indiscutíveis. Essa inovação representa o avanço mais significativo e benéfico para a sociedade contemporânea, sendo também o meio de comunicação mais veloz que aproxima o mundo como uma única comunidade global. A população global passa a maior parte do tempo na Internet, seja para fins profissionais ou para atividades de lazer.

1871

No entanto, devido à facilidade de disseminação de dados e informações, indivíduos mal-intencionados têm aproveitado o ambiente virtual para cometer uma variedade de crimes, utilizando aplicativos, sites, e-mails e mensagens com o propósito de ludibriar indivíduos e/ou obter acesso a informações cruciais de suas vidas particulares. Como consequência, houve uma alteração significativa na legislação penal que resultou na promulgação da Lei n° 14.155 de 2021, que introduziu uma nova forma de fraude eletrônica denominada estelionato virtual.

Nesse contexto, tem -se como tema deste trabalho os crimes cibernéticos uma ponderação sobre a Lei 14.155 de 2021 aplicável ao crime de estelionato virtual. O estudo em questão justificativa -se por trata-se de um problema atual e recorrente, uma vez que os crimes cometidos no ambiente virtual afetam milhares de pessoas diariamente e são perpetrados de várias maneiras diferentes.

Consequentemente, de acordo com o que é estabelecido na Constituição Federal de 1988, é responsabilidade do Estado garantir e proteger os direitos à inviolabilidade da vida

privada, à honra, à intimidade e à propriedade, direitos que estão sob ameaça devido a esses tipos de crimes.

Diante disto, o trabalho teve o seguinte problema de pesquisa: com o advento da Lei nº 14.155 de 2021 haverá uma maior punição para quem praticar o crime de estelionato virtual?.

É fundamental ressaltar que o Direito deve constantemente se ajustar às mudanças sociais, destacando assim a relevância do assunto em questão, que teve como objetivo geral, analisar a recente alteração suscitada pela Lei nº 14.155 de 2021, no tocante ao crime de estelionato virtual.

O processo de elaboração deste trabalho foi guiado por objetivos específicos, que delinearão a abordagem metodológica adequada para investigar aspectos críticos e particulares da pesquisa. Estes objetivos incluíram analisar os aspectos gerais do crime de estelionato virtual previsto no art. 171 do Código Penal; demonstrar a carência de uma lei específica para tipificar e penalizar os indivíduos que praticarem o crime de estelionato virtual; verificar quais são os desafios para combater o crime de estelionato virtual no Brasil.

No que se refere aos procedimentos metodológicos, esta pesquisa adota a metodologia do trabalho jurídico, que se concentra em diretrizes práticas para estruturar e compreender o conjunto de técnicas que fundamentam a organização do trabalho jurídico-científico. O método utilizado é o dedutivo, que se caracteriza pela extração argumentativa do conhecimento a partir de princípios amplos aplicáveis a situações específicas, seguindo da análise do geral para o particular. A abordagem técnica selecionada é a revisão bibliográfica. (BITTAR, 2015).

Para a consecução dos objetivos propostos, o estudo em tela, encontra-se dividido em três capítulos. O primeiro capítulo, busca trazer breves considerações a respeito do que são crimes virtuais e quais são os principais crimes praticados por meio da internet.

No segundo capítulo, aprofundamos ainda mais no âmago deste artigo, abordando de forma detalhada, as disposições sobre o estelionato virtual e as inovações trazidas pela Lei nº 14.155 de 27 de maio de 2021.

Por fim, no terceiro e último capítulo, concentrou-se na problemática da identificação e punição do autor do crime de estelionato virtual.

Diante desses tópicos, este estudo almeja analisar a importância das sanções ocasionadas pela Lei nº 14.155 de 27 de maio de 2021. Para tal, são compartilhadas perspectivas

de notáveis especialistas em Direito Penal, como: Guilherme de Souza Nucci; Victor Eduardo Rios Gonçalves; Paulo Marcos Ferreira Lima, dentre outros.

Por último, é fundamental ressaltar que este estudo não busca abordar exaustivamente todos os aspectos dos crimes virtuais, mas sim, tem como objetivo, contribuir para o combate e conscientização dessas infrações, reconhecendo sua relevância no âmbito jurídico.

## 2 CRIMES VIRTUAIS

A Internet é um canal para comunicação, informação e transferência de dados, que tem substituído muitas ações manuais ou presenciais por atividades digitais e online. Além disso, ela se transformou em um instrumento utilizado para perpetrar ações criminosas, conhecidas como crimes virtuais, informáticos ou cibernéticos.

De acordo com Cassanti (2014, p. 03), crimes virtuais podem ser definidos como:

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

1873

A definição de crime cibernético poderia ser descrita como uma ação que se enquadra nos critérios de tipicidade e ilegalidade, configurando um delito ou violação, intencional ou negligente, de natureza ativa ou passiva. Essa conduta é perpetrada por indivíduos ou entidades jurídicas, envolvendo a utilização da informática, seja online ou offline, e resulta em uma violação direta ou indireta da segurança cibernética. Esse conceito engloba elementos como a integridade, disponibilidade e confidencialidade das informações. (ROSSINI, 2004).

Além disso, os crimes virtuais podem ser cometidos por vários agentes, e vários atos maliciosos podem ocorrer simultaneamente, e esses criminosos podem estar em vários locais do ambiente virtual ao mesmo tempo. Ademais, os agentes também contam com o fato de serem muitas vezes indetectáveis e silenciosos, quando comparados ao crime "real", não possuindo uma localização precisa e concreta que esteja prontamente disponível para as autoridades competentes. (SOUZA, 2021).

Diante disto, criminosos passaram a explorar a internet como meio de transgredir os direitos alheios, sob a presunção de sua imunidade legal para perpetrar variadas

transgressões sem sofrerem consequências legais. Todavia, com o advento da Constituição Federal de 1988 que tornou as questões de informática uma responsabilidade do Estado, algumas medidas foram adotadas para lidar com essa nova realidade, tentando identificar criminosos virtuais aplicando-lhes penalidades no mundo real. (CASTRO, 2021).

Os crimes virtuais abrangem várias categorias. A primeira envolve os crimes puros, que visam acessar sistemas informáticos por meio de atividades de hackers. A segunda foca nos bens da vítima, utilizando a Internet para transferir ilegalmente bens ou valores. Por fim, existem os crimes comuns que usam a Internet para cometer infrações já definidas por lei, como a pornografia infantil tratada na Lei da Infância e Juventude. (SANTANA, 2021).

A segunda classificação inclui tanto os crimes próprios como os crimes impróprios. Sydow (2009) trás a definição de ambos, vejamos:

Delitos informáticos impróprios são delitos comuns, portanto condutas típicas, antijurídicas e culpáveis, e que são perpetradas utilizando-se de mecanismos informáticos como ferramental, sendo que outros meios poderiam ter sido igualmente eleitos para a prática. Por sua vez, delitos informáticos próprios são as condutas típicas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados, precisamente violando sua confidencialidade, sua integridade ou sua disponibilidade. (SYDOW, 2009, p. 75).

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

1874

De acordo Rodrigo Guimarães Colares, existem diversas espécies de crimes praticados na internet, sendo:

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

Ressalta-se que, o presente trabalho discorrerá com mais ênfase sobre os crimes virtuais impróprios, que são aqueles cometidos no ambiente virtual que exigem a ocorrência de um resultado específico para que o crime seja considerado consumado.

Dentre esses, será abordado os mais comuns, sendo: crimes contra a honra (calúnia, difamação e injúria), crimes contra a propriedade intelectual, fraudes virtuais, pornografia

infantil e em especial o crime de estelionato virtual segundo a Lei 14155/2021, o qual será abordado em um tópico próprio.

## 2.1 CRIMES CONTRA A HONRA

À medida que a Internet se expandiu e os sites e redes sociais se tornaram mais sofisticados, indivíduos passaram a enfrentar uma maior exposição pública. Isso resultou em uma crescente divulgação de suas reputações e privacidade, ao mesmo tempo em que suas honras têm sido progressivamente diminuídas. (SOUZA, 2021).

A Constituição assegura a defesa da honra como um direito fundamental, conforme estabelecido no artigo 5º, inciso X da Constituição Federal. Este direito tem como propósito salvaguardar a integridade pessoal de um indivíduo, sua reputação tanto perante si mesmo quanto diante da sociedade em que está inserido. (BARROSO, 2004).

A honra compreende os atributos e traços, tanto físicos quanto morais e intelectuais, de um indivíduo, o tornando valorizado na sociedade. Ela influencia a aceitação de alguém em um grupo social específico ou não, visto que representa um patrimônio pessoal a ser preservado. (CRESPO, 2011).

No código penal, os delitos que atentam contra a honra são categorizados em três modalidades distintas: calúnia, difamação e injúria. A legislação estabelece distinções entre essas categorias em termos de natureza do crime e suas respectivas punições, vejamos de forma detalhada cada um deles:

Calúnia: “Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa”. (BRASIL, 1940).

A calúnia consiste na difamação falsa de alguém, atribuindo-lhe um crime específico. Nesse sentido, a pessoa que a pratica está consciente de sua falsidade ao inventar um crime que não ocorreu ou ao atribuí-lo erroneamente a alguém, mesmo que o crime tenha ocorrido, mas a pessoa acusada não tenha tido envolvimento.

Nas palavras de Gonçalves (2022, p.477) Calunia significa:

Imputar a alguém fato específico definido como crime. Não basta, portanto, dizer que alguém é ladrão, assassino ou estelionatário (hipóteses que configuram injúria), sendo necessário narrar um fato concreto tipificado como roubo, homicídio, estelionato etc. A narrativa tem maior credibilidade perante terceiros e, por tal razão, a calúnia é mais grave do que a injúria. Assim, narrar que determinado professor abusou sexualmente de seus alunos caracteriza calúnia, ao passo que xingá-lo genericamente de pedófilo constitui injúria. Para a configuração do delito em estudo, todavia, não se faz necessária uma narrativa minuciosa do fato

- com detalhes acerca de data, local etc., bastando que seja possível ao ouvinte identificar que o narrador está fazendo referência a um acontecimento concreto.

Nessa perspectiva, no delito de calúnia, o indivíduo imputa a alguém a prática de um crime, sendo essa declaração inverídica e o infrator está ciente da falsidade dessa alegação. Isso resulta em uma afronta à imagem pública da vítima e à sua reputação perante a sociedade. Vale ressaltar que, em um ambiente virtual, esse crime se materializa quando alguém acusa outra pessoa de cometer um crime através de comentários, postagens de fotos e vídeos nas plataformas de redes sociais. (SOUZA, 2021).

Ademais, no crime de calúnia o sujeito ativo pode ser qualquer pessoa, pois trata-se de crime comum. Por outro lado, o sujeito passivo é uma pessoa natural, desde que identificável. Importante notar que uma pessoa jurídica pode ser vítima de calúnia, todavia, somente em casos relacionados a crimes ambientais, conforme estipulado pela Lei n. 9.605/98. Os menores de dezoito anos podem ser vítimas do crime alvos desse crime, mesmo que não cometam um crime, mas sim, um ato infracional. Além disso, é válido destacar que, a calúnia pode ser direcionada até mesmo a uma pessoa falecida, desde que, a vítima seja o cônjuge ou seus familiares, é o que explana o art. 138, § 2º do Código Penal: “Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime. [...] § 2º - É punível a calúnia contra os mortos.” (BRASIL, 1940).

1876

Por afetar a honra objetiva, o crime de calúnia se concretiza no instante em que terceiros tomam conhecimento da falsa imputação, independentemente do momento em que a vítima dela toma ciência. A forma tentada desse delito só é aplicável quando existe a possibilidade de interromper a disseminação da falsa imputação antes que ela atinja outras pessoas. (SILVA; SANTOS, 2021).

A retratação no contexto da calúnia é permitida, visto que o delito envolve a atribuição de fatos. O acusado que se retrata do que afirmou fica isento de pena, desde que o faça antes da prolação da sentença. Em situações em que o crime tenha sido cometido por meio de comunicação, a retratação pode ocorrer pelos mesmos meios utilizados para caluniar o ofendido, caso este assim deseje. (CASTRO, 2021).

Vale destacar, que o Código Penal Brasileiro prevê a chamada 'exceção da verdade', que permite ao acusado provar que a imputação que fez é verídica, ou seja, que o acusador realmente cometeu o crime em questão. Na calúnia, a exceção da verdade é a norma, sendo

excluída apenas em circunstâncias específicas descritas no § 3º do artigo 138 do Código Penal.

*In Verbis:*

Exceção da verdade

§ 3º - Admite-se a prova da verdade, salvo:

I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;

II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;

III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível (BRASIL, 1940).

Para Guilherme de Souza Nucci:

Trata-se de um incidente processual, que é uma questão secundária refletida sobre o processo principal, merecendo solução antes da decisão da causa ser proferida, prevista no § 3.º. É uma forma de defesa indireta, através da qual o acusado de ter praticado calúnia pretende provar a veracidade do que alegou, demonstrando ser a pretensa vítima realmente autora de fato definido como crime. Afinal, se falou a verdade, não está preenchido o tipo penal ('imputar falsamente fato definido como crime'). (NUCCI, 2017, p. 58).

Portanto, é evidente que as restrições relacionadas à aplicação da exceção da verdade estão listadas diretamente no artigo do Código Penal, e é necessário analisá-las devidamente.

Já a difamação está prevista no Art. 139 do Código Penal que cita: “Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa”. (BRASIL, 1940).

1877

Desta forma, difamação envolve imputar um fato prejudicial à reputação de alguém. Semelhante à calúnia, afeta a dignidade pública da vítima, ou seja, sua reputação. Entretanto, ao contrário da calúnia, na difamação, a declaração pode ser verdadeira ou não, resultando em ato ilícito independentemente da veracidade. Importante ressaltar que, de maneira semelhante à calúnia, o crime é cometido quando terceiros tomam conhecimento das declarações do autor. E se a difamação for por escrito, a tentativa também é possível. (JÚNIOR, 2016).

Conforme afirma Gonçalves (2022, p. 497) difamar é:

Provocar má fama, atingir a imagem da vítima perante seus pares. Tal como ocorre na calúnia, a difamação pressupõe que o agente atribua à vítima um fato determinado, concreto, que seja considerado inadequado ou inapropriado. O que distingue os dois delitos basicamente é que, na calúnia, o fato imputado necessariamente deve ser definido como crime, enquanto a difamação é genérica, isto é, abrange a imputação de qualquer outro fato ofensivo à reputação.



Quando se trata da difamação, a exceção da verdade não é a norma predominante, uma vez que a punição da conduta não depende da veracidade ou não do fato imputado. Contudo, em situações excepcionais, a exceção da verdade pode ser válida, especialmente quando o indivíduo difamado é um funcionário público e a difamação está ligada ao desempenho de suas atribuições. (JÚNIOR, 2016).

Vejamos o que explana o art. 139, § 1º do Código Penal. “A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções”. (BRASIL, 1940).

Sendo assim, se o indivíduo difamar um funcionário público, imputando-lhe um fato prejudicial à sua reputação e relacionado ao seu desempenho no serviço público, o autor da difamação poderá demonstrar que está falando a verdade. Isso se justifica pelo interesse público em garantir que o servidor desempenhe corretamente sua função. No crime de difamação, bem como no crime de calúnia, trata-se de um crime bicomum, uma vez que qualquer pessoa pode atuar como agente ativo ou passivo. (CASTRO, 2021).

No tocante a injúria, em contraste com os dois crimes anteriores, esta se concentra na proteção da honra subjetiva, não da honra objetiva. Portanto, a injúria atinge como a vítima se percebe, sua autoestima, em vez de como terceiros a veem. O autor comete injúria ao proferir declarações que atribuam à vítima características negativas que possam ferir sua dignidade ou decoro. Não envolve, portanto, a imputação de um fato específico, mas sim de qualidades depreciativas. (SOUZA, 2021).

O crime de injúria está previsto no art. Art. 140 do Código Penal com a seguinte redação: “Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa” (BRASIL, 1940).

Com efeito, Gonçalves (2022, p. 509, 510) explica que:

O crime de injúria tutela a honra subjetiva, isto é, a autoestima da vítima, o sentimento que cada pessoa tem em torno de seus próprios atributos físicos, morais ou intelectuais.

[...]

Tal como nos demais crimes contra a honra, a injúria pode ser cometida de forma verbal, por escrito, por gesto ou qualquer outro meio simbólico.

A injúria pode se apresentar de duas formas: direta ou indireta. A manifestação direta ocorre quando é realizada pessoalmente pela pessoa que deseja insultar, enquanto a forma

indireta acontece quando essa pessoa utiliza um intermediário para ofender a vítima. (ASSIS, 2019).

Na esfera online, essa infração é cometida por meio de comentários, mensagens e publicações feitas pelo agente, nas quais são direcionados insultos à vítima, incluindo referências desfavoráveis a suas características morais, físicas e intelectuais. (SOUZA, 2021).

A injúria se concretiza no instante em que a vítima toma conhecimento das declarações prejudiciais feitas pelo autor a seu respeito. Quando a injúria ocorre verbalmente, não permite a tentativa, uma vez que é um delito praticado em uma única ação, sendo unissubsistente. (CASTRO, 2021).

A injúria é um delito comum, passível de ser cometido por qualquer indivíduo. A vítima também pode ser qualquer pessoa desde que natural (física). Destaca-se também que no crime em estudo, diferentemente da calúnia e da difamação, os mortos e as pessoas jurídicas não detêm honra subjetiva e, por esse motivo, não podem ser sujeito passivo. (GONÇALVES, 2022).

Diferente da calúnia e da difamação, não existe exceção da verdade na injúria, porque não há fato na injúria, e a exceção da verdade visa provar fato. (CASTRO, 2021).

1879

## 2.2 CRIMES CONTRA A PROPRIEDADE INTELECTUAL

A violação de direitos autorais é criminalizada no ordenamento jurídico brasileiro. O art. 184 Código Penal trata do delito de violação de direitos autorais e se apresenta do seguinte modo: “violar direitos de autor e os que lhe são conexos: Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa”. (BRASIL, 1940).

A propriedade intelectual é um campo do direito que, por meio de regulamentações legais, assegura aos criadores ou detentores da produção o direito de adquirir, durante um período específico, a titularidade sobre sua criação. (VANIN, 2016).

Explica Gonçalves (2022, p. 1167), sobre o crime contra a Propriedade Intelectual, bem como o caracteriza, vejamos:

O crime consiste em violar direito autoral. Violar é sinônimo de transgredir, ofender. O autor tem direitos patrimoniais e morais sobre sua obra. Assim, caracterizam o crime, por exemplo, o plágio, a utilização indevida de imagem da obra, a sua reprodução não autorizada, a confecção pela editora de número maior

de exemplares de um livro sem o conhecimento do autor a fim de não pagar os direitos autorais sobre o número excedente etc. (GONÇALVES, 2022, p.1167).

De acordo com a explicação de Bitencourt (2016), o interesse protegido por esse tipo de crime é o direito autoral, que, na realidade, abarca um conjunto de direitos morais ou financeiros decorrentes da criação de uma obra. O autor também ressalta que o alvo da proteção penal é a propriedade intelectual. Os direitos autorais englobam os direitos do criador e os direitos relacionados a eles.

Gonçalves (2022) ainda salienta que a extensão do significado de direitos autorais é estabelecida por uma legislação específica (Lei n. 9.610/98), tornando assim o crime em análise uma norma penal em branco. Essa lei mencionada incorpora, de fato, várias definições que aprimoram as formas qualificadas da infração.

É válido dizer, que os direitos relacionados à propriedade intelectual são abrangentes, uma vez que não se limitam somente à posse de objetos físicos, ou seja, bens materiais, mas também se estendem a elementos imateriais. (BARBOSA, 2010).

Evidencia-se que, o ambiente virtual possibilita a rápida circulação de informações, incluindo cópias de obras feitas por terceiros sem manter os direitos autorais da obra original. O cometimento desse crime também é confirmado pela falta de fiscalização ativa. Além da cópia de obras, também é comum a pirataria de softwares e aplicativos pela Internet. (SANTOS, 2021).

1880

Portanto, diante desse panorama, podemos concluir que a propriedade intelectual é um direito respaldado por lei, assegurando ao autor de uma obra específica o privilégio e a exclusividade sobre o resultado de sua criação intelectual.

### 2.3 FRAUDES VIRTUAIS

Fraudes virtuais, também conhecidas como cibercrimes, são práticas delituosas que se valem da tecnologia digital e da internet para enganar e prejudicar indivíduos, empresas e instituições. Esses crimes exploram a facilidade de comunicação e transações online, visando obter ganhos ilícitos às custas de informações, dados pessoais, financeiros ou propriedade alheia. (SILVA; SANTOS, 2021).

O reconhecimento do crime de fraude virtual ocorreu em 2012, quando a conhecida Lei Carolina Dieckmann foi promulgada através do projeto de Lei 12.737/2012. O principal

propósito desta Lei foi atender às longas demandas da indústria financeira, que sofre impactos diretos das fraudes virtuais, resultando em danos consideráveis.

No entanto, devido à aprovação acelerada dessa lei em decorrência dos eventos envolvendo a atriz Carolina Dieckmann, cujas fotos pessoais foram disseminadas em várias redes sociais, a lei tornou-se restrita em comparação a outros projetos em análise no Congresso Nacional. (NOVAIS, 2020).

O delito de fraude virtual acontece quando um indivíduo penetra, corrompe ou altera informações digitais, programas ou uma infraestrutura de processamento de dados. Como exemplo ilustrativo, temos uma situação em que alguém infiltra-se no computador de outra pessoa e compartilha imagens íntimas na esfera online. (SANTOS, 2021).

Nas palavras de Lima (2005, p. 60), fraudes virtuais são definidas como:

Uma invasão de sistemas computadorizados e posterior modificação de dados, que tem como intuito obter vantagem sobre bens, físicos ou não, ou seja, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros.

O modus operandi desses golpes pode variar, mas frequentemente envolvem a criação de sites, mensagens ou anúncios falsos que se assemelham a fontes confiáveis. Isso induz as vítimas a compartilhar informações sensíveis, como senhas, números de cartão de crédito ou dados de conta bancária. (SANTOS, 2021).

1881

Uma das características marcantes das fraudes virtuais é a capacidade dos criminosos de operarem em âmbito global, muitas vezes de forma anônima, dificultando a identificação e punição. Além disso, a constante evolução tecnológica permite que novos métodos de fraude surjam regularmente, desafiando a capacidade das autoridades e das empresas de se manterem à frente dessas ameaças. (SILVA; SANTOS, 2021).

Há duas categorias de fraudes virtuais, a saber, fraude externa e fraude interna. A fraude externa acontece quando o perpetrador do ato fraudulento não possui vínculo direto com o local em que a fraude ocorrerá, enquanto a fraude interna é praticada quando o autor da fraude tem algum tipo de conexão com o local alvo da fraude, podendo ser realizada por um funcionário, residente ou até mesmo por um prestador de serviços que tenha interagido com o local. (NOVAIS, 2020).

A compreensão das fraudes virtuais e a adoção de práticas de segurança cibernética são essenciais em um mundo cada vez mais conectado digitalmente. A conscientização e a

vigilância constante são elementos cruciais para minimizar os danos causados por esses crimes e manter a confiança no ambiente online.

## 2.4 PORNOGRAFIA INFANTIL

Entre as denúncias mais comuns de crimes virtuais estão as relacionadas a pornografia infantil. De acordo com Alves (2020, não paginado) “[...] entre março e julho de 2020, primeiros meses de pandemia, foram registradas 42.931 denúncias de pornografia infantil. Durante o mesmo período do ano passado, haviam sido 20.860”. O autor ainda cita que “o compartilhamento desse tipo de conteúdo criminoso se concentra, principalmente, no Twitter, Facebook e Instagram, além de fóruns anônimos (os “chans”) e sites de troca de arquivos de imagem”.

Os artigos 240 e 241 do Estatuto da Criança e do Adolescente abordam o tema da produção e comercialização de material pornográfico. Esses artigos têm como objetivo criminalizar a divulgação e publicação de fotografias ou vídeos envolvendo crianças e adolescentes, inclusive através de meios de comunicação online, como a Internet.

Nesse sentido, aqueles que mantêm esse tipo de conteúdo em websites e computadores também estão incorrendo no mesmo crime. É essencial salientar que o acesso por parte do usuário a conteúdos pornográficos é irrelevante, uma vez que a mera presença de material de natureza explícita ou pornográfica envolvendo crianças ou adolescentes é suficiente para caracterizar a infração. Além disso, qualquer registro que contenha conteúdo de natureza sexual explícita ou pornográfica, mesmo que a criança ou adolescente esteja vestido, é considerado crime. (CASTRO, 2021).

Nesse cenário, Guilherme de Souza Nucci explana que:

A maneira pela qual o autor do crime adquire, possui ou armazena o material é livre, valendo-se o tipo da expressão “por qualquer meio” Comumente, com o avanço da tecnologia e da difusão dos computadores pessoais, dá-se a obtenção de extenso número de fotos e vídeos pela Internet, guardando-se o material no disco rígido do computador, em disquetes, DVDs, CDs, pen drives, entre outros. (NUCCI, 2018, p. 849).

O artigo 241-A do Estatuto da Criança e do Adolescente aborda o tema das publicações de imagens envolvendo crianças e adolescentes em plataformas de mídia social, mencionando que:

Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou

pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008).

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa (BRASIL, 1990).

É importante destacar, que o Superior Tribunal de Justiça (STJ), entende que, se a publicação ocorreu nas redes sociais e se ela violou o direito da criança e do adolescente, a rede social não precisa ser comunicada, pois deverá o provedor remover a publicação ofensiva, mesmo sem ser notificado.

O Informativo n. 723, do STJ de 7 de fevereiro de 2022 explana que: “Responde civilmente por danos morais o provedor de aplicação de internet que, após formalmente comunicado de publicação ofensiva a imagem do menor, se omite na sua exclusão, independentemente de ordem judicial.” (BRASIL, 2022).

As consequências mais graves advindas da pornografia infantil envolvem danos que persistem ao longo do tempo, permanecendo ativos enquanto o material pornográfico estiver online ou sendo disseminado de outras maneiras. É importante destacar ainda que esse tipo de pornografia tem o potencial de funcionar como um incentivo para que agressores sexuais cometam novos abusos contra crianças ou indivíduos menores de idade em situação de vulnerabilidade. (CARVALHO, 2020).

É evidente que esse tipo de conduta tem se intensificado com o avanço dos recursos eletrônicos e tecnológicos de comunicação, o que proporciona ao indivíduo uma facilidade maior para se engajar na disseminação de pornografia por meio das plataformas virtuais.

1883

### 3 ESTELIONATO VIRTUAL SEGUNDO A LEI Nº 14.155/2021

Os crimes virtuais estão em constante aumento, principalmente devido à rapidez e facilidade de acesso à informação pela Internet. As pessoas estão cada vez mais dependentes desse meio, compartilhando uma variedade de informações. A rápida evolução tecnológica também facilita o acesso a computadores, permitindo a prática de crimes virtuais por indivíduos que exploram a vulnerabilidade das informações para obter vantagens fraudulentas em detrimento de outros. (BASTOS, 2016).

Uma das formas mais frequentes de estelionato no ambiente digital é a invasão do e-mail da vítima, especialmente aqueles indivíduos que têm o hábito de verificar seus saldos e registros bancários por meio do computador. Nesse contexto, o criminoso (cracker) busca maneiras de replicar a página autêntica do serviço de internet banking do usuário, levando-

o a tentar fazer o login, sem perceber que os dados inseridos serão capturados por um terceiro mal-intencionado que os utilizará de maneira imprópria. (FEITOZA, 2012).

Cabe mencionar alguns exemplos bastante frequentes de estelionatos virtuais, como: propostas de empréstimos com juros reduzidos ou inexistentes; oportunidades de emprego online com salários atrativos, porém exigindo pagamento antecipado; websites que vendem produtos que nunca são entregues; e a grande quantidade de mensagens de corrente via WhatsApp. Em essência, o estelionato virtual abrange qualquer método em que ocorra um ganho financeiro ilegítimo, enganando as pessoas e levando-as a acreditar na veracidade dessas vantagens. (SILVA; SANTOS, 2021).

A punição para quem praticava o crime de estelionato virtual era a prevista no caput do artigo 171 do Código Penal. Essa punição podia levar o criminoso a reclusão de um a cinco anos, além de multa. No entanto, essa situação mudou com a introdução da Lei nº14.155, de 27 de maio de 2021 que acrescentou a figura de fraude eletrônica:

#### Art. 171 – 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)

[...]

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). (BRASIL, 2021).

Agora, de acordo com o § 2º-A do artigo 171 do Código Penal, a pena aplicada para quem praticar a ação criminosa de maneira não presencial, envolvendo meios eletrônicos como redes sociais, telefonemas falsos ou envio de e-mails enganosos ou métodos semelhantes, será de 4 a 8 anos.

Porém, ressalta-se que, o parágrafo 2º-A é uma óbvia *novatio legis in pejus*, é uma Lei prejudicial ao réu e por ser uma *novatio legis in mellius*, só tem aplicação a partir do dia 28 de maio de 2021. Se, em 27 de maio de 2021, ou antes disso, alguém tiver praticado conduta idêntica a essa, será responsabilizado pelo artigo 171, *caput*, do Código Penal, pelo crime de

estelionato na sua modalidade simples. Então essa qualificadora, por ser gravosa ao réu, é irretroativa e somente se aplica do dia 28 de maio de 2021 para frente. (CASTRO, 2021).

O parágrafo 2º-B do artigo 171 do Código Penal, também adicionado pela Lei nº 14.155/2021, introduz um elemento de aumento de pena aplicável somente quando a qualificadora do parágrafo 2º-A está presente. A pena é aumentada de um a dois terços se o crime for realizado utilizando um servidor localizado fora do território nacional. Essa punição mais severa é justificada pela maior dificuldade em identificar o autor do crime, devido à complicada localização e punição decorrentes dessa situação. (SILVA; SANTOS, 2021).

Contudo, a aplicação dessa circunstância agravante ao estelionatário depende do seu conhecimento acerca do uso de um servidor localizado fora do país. Se o estelionatário não possui essa ciência, a majorante não se aplica em seu caso. (GONÇALVES, 2022).

O § 4º do artigo 171 do Código Penal também é uma das recentes alterações trazidas pela Lei nº 14.155/2021. Antes da entrada em vigor dessa alteração, publicada em 28 de maio de 2021, o aumento de pena previsto aplicava-se apenas para o crime praticado contra idoso (60 anos ou mais). Além disso, o aumento de pena não variava de 1/3 ao dobro, mas apenas ao dobro, quando praticado contra idoso. (ROCHA, 2021).

1885

Com a nova disposição que permite a ampliação da pena dentro da faixa de 1/3 até o dobro, o acusado de cometer estelionato contra idosos pode ser favorecido. Isso caracteriza uma mudança legislativa positiva, conhecida como *novatio legis in melius*, permitindo que se aplique retroativamente a casos de estelionato contra idosos ocorridos antes da implementação da Lei n. 14.155/2021. (CASTRO, 2021).

A outra alteração trazida pela lei foi a inclusão do vulnerável como vítima para majorar a pena. Nesse caso, trata-se de uma *novatio legis in pejus*, porque cria uma nova hipótese de aumento de pena que não existia antes de 28 de maio de 2021. (GONÇALVES, 2022).

É importante ressaltar que tanto a Lei de 2021 quanto o artigo 171 do Código Penal não estabeleceram uma definição para o termo "vulnerável". Portanto, é necessário recorrer à definição contida no artigo 217-A, parágrafo 1º, do Código Penal, que se refere ao estupro de vulnerável. Isso abrange vítimas menores de 14 anos, indivíduos com doença mental ou aqueles que temporariamente não podem oferecer resistência, como alguém sob efeito de embriaguez. Vamos observar o conteúdo do artigo 217-A, parágrafo 1º:



Incorre na mesma pena quem pratica as ações descritas no caput com alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência. (BRASIL, 2021, não paginado).

É relevante enfatizar que essa circunstância de aumento de pena só é relevante se o perpetrador do crime estiver ciente da condição da vítima, ou seja, se estiver consciente de que a pessoa é idosa ou vulnerável, pois isso está intrinsecamente ligado à intenção da ação. Nesse contexto, podemos observar a explicação de Gonçalves (2022, p. 1073), que aborda essa perspectiva.

Há muitos casos, todavia, em que o agente não tem conhecimento de que a vítima é idosa e, em tais hipóteses, a majorante não poderá incidir, como, por exemplo, em certos golpes perpetrados pela internet nos quais não há qualquer contato entre o autor do crime e a vítima.

Diante do exposto, nota-se que, com a entrada em vigor desta lei, delitos cibernéticos, incluindo invasões de dispositivos, práticas fraudulentas e roubos realizados por meio de aparelhos eletrônicos, como smartphones, computadores, tablets, entre outros, que ocorram no ambiente digital, estão enfrentando sanções mais rigorosas. Isso está proporcionando uma proteção ligeiramente maior aos usuários da internet. (SOUZA, 2021).

Nesse contexto, Luiz Augusto D'Urso, um perito em Direito Digital, esclarece que atualmente, a invasão de um sistema informático (artigo 154-A, CP) resulta em uma sentença de reclusão que varia de um a quatro anos, ao passo que o furto realizado através de fraude na internet e o estelionato pela internet ou por meio de plataformas de redes sociais têm, individualmente, uma pena de reclusão que varia entre quatro e oito anos. (D'URSO, 2017).

1886

#### 4 DIFICULDADE DE IDENTIFICAÇÃO E PUNIÇÃO DOS INFRATORES

Muitos pesquisadores e juristas ainda criticam o direito penal, mesmo com as alterações relativas aos crimes virtuais. Há a opinião de que a legislação não conseguiu se manter atualizada em relação ao aumento dos delitos digitais e à frequência com que são cometidos. (SOUZA, 2021).

SCHAUN (2018) explica que o desenvolvimento legislativo, não consegue acompanhar o dinamismo das tecnologias virtuais, devido a isto, por mais que haja uma lista abrangente de crimes cibernéticos, estes carecem de uma definição precisa, dificultando assim a adequada tipificação.

Adicionalmente, em virtude da complexidade e do anonimato que caracterizam o ambiente virtual, as autoridades de segurança enfrentam desafios consideráveis ao investigar crimes cibernéticos. Sodré (2021, p. 15) aborda as complicações relacionadas à apuração desses delitos, conforme mencionado a seguir:

Ainda que o direito tutele, legislativamente, as práticas ilícitas que se dão pelo meio informático ou contra ele, há ainda muito a se progredir no meio tecnológico para se garantir e proporcionar a tutela jurisdicional. A dificuldade em apurar essas penalidades se dá pela falta de materialidade delitiva, que torna o trabalho investigativo complexo, uma vez que é possível o autor do crime executá-lo em um Estado da Federação, ou até em outro país, e a consumação de ser em qualquer lugar, ainda, podendo utilizar-se de meios que garantam seu anonimato.

Nesse contexto, os crimes virtuais continuam a se proliferar diariamente devido ao desafio de obter recursos adequados para estabelecer os elementos essenciais de autoria e materialidade. Isso ocorre porque há numerosas maneiras pelas quais qualquer indivíduo pode utilizar o anonimato ao navegar na internet, incluindo a capacidade de alterar endereços de e-mail, modificar o endereço IP e a facilidade de esconder evidências do crime. (SOUZA, 2021).

De acordo com Santos, Martins e Tybucsh (2014), um dos desafios identificados está relacionado à ausência de colaboração e intercâmbio de informações entre as autoridades competentes em relação às vítimas de tais delitos, o que gera incerteza quanto à participação no processo penal.

Braga (2018), explica que o estelionato virtual enfrenta desafios significativos na identificação e punição dos infratores devido à sua complexidade e à capacidade dos criminosos de permanecerem anônimos, visto que, os criminosos ocultam sua verdadeira identidade usando pseudônimos, redes de computadores anonimadoras ou técnicas de mascaramento de IP, dificultando o rastreamento. Além disso, a coleta e preservação de provas digitais são complicadas, já que os dados podem ser facilmente manipulados ou ocultados, exigindo conhecimento técnico avançado para coletar, autenticar e apresentar essas provas em tribunal.

Outro desafio na punição dos infratores do crime de estelionato virtual é que, na maioria das vezes, as vítimas não denunciam o crime devido a sentimentos de vergonha, falta de conhecimento ou a percepção de que não haverá consequências. Isso torna difícil para as autoridades rastrear e responsabilizar dos infratores. (SOUZA, 2021).

A falta de compreensão sobre o que constitui um crime de estelionato virtual e como agir em caso de se tornar uma vítima de tais crimes permite que os perpetradores fiquem impunes, como se esses delitos não deixassem vestígios ou não tivessem consequências. Além disso, essa falta de conhecimento cria desafios significativos na área da segurança digital, levando as pessoas a temerem situações em que muitas vezes não deveriam. (ATAIDE, 2017).

Assim, torna-se essencial contar com uma equipe policial altamente especializada e devidamente treinada no campo tecnológico, a fim de conduzir investigações de crimes virtuais de maneira eficaz. Isso é fundamental para garantir e preservar os direitos de todos os cidadãos à privacidade, à intimidade, ao sigilo e à livre manifestação do pensamento nas redes informáticas, considerando essas garantias como pilares constitucionais essenciais. (BRAGA, 2018).

É relevante mencionar que em 12 de abril de 2023, o Governo Federal brasileiro oficializou a adoção da Convenção sobre o Crime Cibernético, celebrada em Budapeste. Ao aceitar o convite do Conselho da Europa para participar desse tratado internacional, o Brasil tornou-se parte de um instrumento multilateral, fortalecendo, conseqüentemente, sua colaboração com parceiros estratégicos no combate aos delitos cibernéticos. (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2023).

1888

Referida Convenção engloba estratégias e recursos colaborativos com outras nações para enfrentar delitos cibernéticos::

Em vigor desde 2004, a Convenção de Budapeste de 2001 é um dos mais importantes instrumentos a lidar com aspectos penais substantivos, processuais e cooperativos no combate aos crimes cibernéticos e envolve mais de 60 países. Por seu caráter multilateral global e específico, ela reconhece o respeito às soberanias dos Estados signatários, preservação dos direitos e garantias fundamentais das partes e interesses das autoridades nacionais de aplicação da lei, em especial quanto ao objetivo de investigação e persecução de crimes praticados na internet e/ou com intermédio de ferramentas de internet e tecnologias digitais. (POLIDO, 2021, não paginado).

A Convenção sobre o Cibercrime foi criada com o objetivo de lidar com essas ameaças digitais em uma escala global, desempenhando um papel crucial no estabelecimento de normas internacionais para a investigação e a punição de crimes cibernéticos. (CONVENÇÃO DE BUDAPESTE, 2001).

A incorporação à Convenção oferece às autoridades brasileiras uma maneira mais ampla e rápida de obter provas eletrônicas e informações relevantes sob jurisdição

estrangeira. Além disso, a adesão torna a colaboração internacional no combate a esses crimes mais eficaz. (VIEIRA, 2023).

Embora tenhamos leis nacionais que tratam de importantes aspectos da repressão de crimes virtuais, é incontestável que a natureza internacional da criminalidade digital transcende fronteiras. Assim, a decisão do Brasil em aderir à Convenção de Budapeste tornou-se fundamental para complementar nossa legislação nacional, que ainda apresenta deficiências nesse domínio, oferecendo diretrizes mais precisas para a investigação e sanção de crimes virtuais. (POLIDO, 2021).

Entretanto, apesar da Convenção representar um avanço notável na luta contra os crimes cibernéticos, é crucial que o Brasil continue empenhado em atualizar sua legislação de forma constante, como evidenciado pela promulgação da Lei nº 14.155 de 2021, que marcou um avanço significativo na repressão ao estelionato virtual. Para tanto, é fundamental ressaltar que a efetividade das sanções depende igualmente da implementação adequada e da cooperação das autoridades competentes.

No entanto, apesar das alterações trazidas pela Lei nº 14.155 de 2021, existem outras ações que se fazem imprescindíveis para enfrentar o estelionato virtual. Isso inclui: investimentos em tecnologia para prevenção e combate aos crimes virtuais, conscientização da população sobre os riscos e cuidados na internet, cooperação internacional para investigação e punição de criminosos cibernéticos, e aprimoramento constante das leis e políticas de segurança digital.

1889

## CONSIDERAÇÕES FINAIS

A presente pesquisa orientou-se por meio de um objetivo geral, que foi o de analisar a recente alteração suscitada pela Lei nº 14.155 de 2021, no tocante ao crime de estelionato virtual.

A trajetória que culminou na conclusão deste estudo foi guiada por objetivos específicos, os quais delinearão o caminho metodológico apropriado para investigar aspectos particulares e fundamentais da pesquisa. Nesse contexto, foram enfatizados os tipos mais frequentes de crimes virtuais, assim como a nova legislação que introduziu penalidades mais substanciais para os autores do estelionato virtual. Além disso, foi examinada a complexidade da identificação e punição dos infratores desse delito.

Pois bem, a partir da pesquisa realizada, pode-se afirmar que o estelionato virtual tem se tornado uma ocorrência bastante comum nos últimos anos, isso se deve em grande parte à habilidade dos criminosos em ocultar dados e informações, tornando conseqüentemente, a identificação e a aplicação de penalidades mais desafiadoras.

Inicialmente, identificou-se que os crimes virtuais são aqueles cometidos no ambiente online, utilizando dispositivos eletrônicos e acesso à internet. Além disso, foi constatado que o estelionato virtual se caracteriza quando uma pessoa, valendo-se de dispositivos tecnológicos e conexão à internet, induz ou mantém alguém em erro, por meio de artifício, ardid, ou qualquer meio fraudulento, com o propósito de obter vantagem ilícita, seja para benefício próprio ou de terceiros, prejudicando a vítima.

Constatou-se também, que no Brasil, a luta contra os crimes virtuais começou tarde, pois somente em 2012 foi sancionada a primeira lei destinada a proteger os direitos patrimoniais e de imagem no meio eletrônico. Já no tocante ao Estelionato Virtual somente em 2021 foi sancionada a Lei nº 14.155 de 2021, a qual inseriu os parágrafos § 2º-A, § 2º-B e modificou o § 4º do artigo 171 do Código Penal, tendo como objetivo fortalecer o arcabouço legal para lidar com os crimes virtuais, tornando as penalidades mais adequadas e específicas para as condutas cometidas no ambiente digital.

1890

Apesar disso, foi evidenciado que existe uma considerável complexidade na identificação e punição dos infratores, revelando que o Brasil ainda precisa de reformas na legislação para reprimir efetivamente a ocorrência desses delitos. Isso se reflete na realidade de que as investigações relacionadas aos crimes virtuais no país frequentemente não alcançam resultados eficazes e substanciais, mesmo diante das mudanças legislativas mencionadas.

Diante disto, conclui-se que, as mudanças trazidas pela Lei nº 14.155 de 2021, foram de suma importância para ajudar a combater os crimes virtuais, visto que referida lei atribuiu maior responsabilidade penal para os sujeitos ativos do estelionato virtual.

Contudo, é imperativo manter um processo contínuo de revisão das legislações, desenvolvimento de políticas públicas destinadas a combater delitos cibernéticos, implementação de tecnologias de segurança, oferta de treinamentos para os usuários e execução de operações policiais. Além disso, é fundamental aumentar a conscientização da população sobre a segurança digital e os procedimentos necessários para prevenir fraudes online.

## REFERÊNCIAS

ALVES, I. **Brasil registra mais de 40 mil denúncias de pornografia infantil**. 2020. Disponível em: <https://observatorio3setor.org.br/noticias/brasil-registra-mais-de-40-mil-denuncias-de-pornografia-infantil/>. Acesso em: 16 ago. 2023.

ASSIS, R. Crime de injúria: descubra o que é e quais as suas peculiaridades. **Jusbrasil**. 2019. Disponível em: <https://www.jusbrasil.com.br/artigos/crime-de-injuria-descubra-o-que-e-e-quais-as-suas-peculiaridades/771246905>. Acesso em: 29 ago. 2023.

ATAIDE, M. A de. **CRIMES VIRTUAIS: UMA ANÁLISE DA IMPUNIDADE E DOS DANOS CAUSADOS ÀS VÍTIMAS**. 2017. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade da Cidade de Maceió. Maceió, 2017. Disponível em: [http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc\\_amanda\\_ataide.pdf](http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf). Acesso em: 09 set. 2023.

BARBOSA, D. B. **Uma Introdução à Propriedade Intelectual**. Segunda Edição. Ed: Revista e Atualizada. 2010. Disponível em: [https://www.dbba.com.br/wp-content/uploads/introducao\\_pi.pdf](https://www.dbba.com.br/wp-content/uploads/introducao_pi.pdf). Acesso em: 17 ago. 2023.

BARROSO, L. R. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista de Direito Administrativo**, Rio de Janeiro, n. 235, p. 1-36, jan.mar/2004. Disponível em: <https://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/45123/45026>. Acesso em: 17 ago. 2023.

1891

BASTOS, J. T. **CRIME CIBERNÉTICO E O ESTELIONATO VIRTUAL**. Erechim, 2016. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Regional Integrada do Alto Uruguai e das Missões – Campus Erechim. 2016. Disponível em: [https://www.uricer.edu.br/cursos/arq\\_trabalhos\\_usuario/4259.pdf](https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4259.pdf). Acesso em: 28 ago. 2023.

BITENCOURT, C. R. **TRATADO DE DIREITO PENAL 3 - PARTE ESPECIAL - DOS CRIMES CONTRA O PATRIMÔNIO ATÉ DOS CRIMES CONTRA O SENTIMENTO RELIGIOS**. 12. ed. São Paulo: Saraiva, 2016. E-book.

BRAGA, D. C. S. Métodos de investigações no âmbito cibernético. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 24, n. 5681, 20 jan. 2019. Disponível em: <https://jus.com.br/artigos/71463>. Acesso em: 08 set. 2023.

BRASIL. **Decreto-Lei nº 2.848 de 7 de dezembro de 1940**. Código Penal Brasileiro. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm). Acesso em: 18 ago. 2023.

\_\_\_\_\_. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Planalto.gov.br. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8069.htm](http://www.planalto.gov.br/ccivil_03/leis/l8069.htm). Acesso em: 16 ago. 2023.

\_\_\_\_\_, 2021. **Lei nº 14.155, de 27 de maio de 2021. Brasília, 27 de maio de 2021; 200º da Independência e 133º da República.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2021/lei/L14155.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm). Acesso em: 27 ago. 2023.

\_\_\_\_\_. Superior Tribunal de Justiça. **Informativo de Jurisprudência nº 723.** 2022. Disponível em: <https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedica o&livre=0723.cod>. Acesso em: 18 ago. 2023.

CARVALHO, L.M. **A PRÁTICA DA PEDOFILIA E CRIMES SEXUAIS A APLICAÇÃO DA LEI EM CRIMES VIRTUAIS.** 2020. Trabalho de Conclusão de Curso (Bacharel em Direito) - Pontifícia Universidade Católica de Goiás-PUCGOIÁS, Goiás, 2020. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/955/1/LUCAS%20MACH ADO%20CARVALHO.pdf>. Acesso em: 18 gos. 2023.

CASSANTI, M. O de. **Crimes Virtuais, Vítimas reais.** Rio de Janeiro: Brasport, 2014.

CASTRO, L. **DIREITO PENAL - PARTE ESPECIAL: Crimes contra a Pessoa - Parte II.** Livro Eletrônico, 2021.

COLARES, R. G. Cybercrimes: os crimes na era da informática. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 7, n. 59, 1 out. 2002. Disponível em: <https://jus.com.br/artigos/3271>. Acesso em: 15 ago. 2023.

1892

**CONVENÇÃO DE BUDAPESTE.** 23 nov. 2001. Disponível em: [http://www.mpf.mp.br/atuacaotematica/sci/normas-elegislacao/legislacao/legislacoes-pertinentes-dobrasil/docs\\_legislacao/convencao\\_cibercrime.pdf](http://www.mpf.mp.br/atuacaotematica/sci/normas-elegislacao/legislacao/legislacoes-pertinentes-dobrasil/docs_legislacao/convencao_cibercrime.pdf). Acesso 08 set. 2023

CRESPO, M. X. F de. **Crimes digitais.** São Paulo: Saraiva, 2011.

D'URSO, L. A. F. **Cibercrime: perigo na internet.** Publicado em 2017. Disponível em: <http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-perigo-na-internet/>. Acesso em :28 de ago. de 2023.

FEITOZA, L. G M de. **Crimes Cibernéticos: O estelionato virtual.** Brasília 2012. Disponível em: <http://repositorio.ucb.br/jspui/bitstream/10869/2819/1/Luis%20Guilherme%20de%20Mat os%20Feitoza.pdf>. Acesso em: 28 ago. 2023.

GONÇALVES, V. E. R. **Curso de direito penal - parte especial - Arts 121 a 183.** 6. ed. São Paulo: Saraiva, 2022. E-book. Disponível em: <https://bibliotecadigital.saraivaeducacao.com.br/epub/785664?title=Curso%20de%20direit o%20openal%20-%20%20parte%20especial%20%20-%20Arts%20121%20a%20183#references>. Acesso em: 17 ago. 2023.

JÚNIOR, A. P. **COLEÇÃO ÍCONES DO DIREITO MANUAL DE DIREITO PENAL.** 2. ed. São Paulo: Saraiva, 2016. E-book. Disponível em:

<https://bibliotecadigital.saraivaeducacao.com.br/epub/604625?title=COLE%C3%87%C3%83O%20%C3%8DCONES%20DO%20DIREITO%20MANUAL%20DE%20DIREITO%20PENAL#references>. Acesso em: 17 ago. 2023.

LIMA, P. M. F. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Convenção de Budapeste é promulgada no Brasil**: Autoridades brasileiras poderão contar com mais um recurso nas investigações de crimes cibernéticos. 2023. Disponível em: [https://repositorio.ufsc.br/bitstream/handle/123456789/248821/A%20ADES%C3%83O%20DO%20BRASIL%20A%20CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE%20E%20A%20CORRE%C3%87%C3%83O%20DAS%20DEFICI%C3%84NCIAS%20LEGISLATIVAS.%20Vers%C3%A3o%20final%20-%20Documentos%20Google%20\(1\).pdf?sequence=1](https://repositorio.ufsc.br/bitstream/handle/123456789/248821/A%20ADES%C3%83O%20DO%20BRASIL%20A%20CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE%20E%20A%20CORRE%C3%87%C3%83O%20DAS%20DEFICI%C3%84NCIAS%20LEGISLATIVAS.%20Vers%C3%A3o%20final%20-%20Documentos%20Google%20(1).pdf?sequence=1). Acesso em: 08 set. 2023.

NOVAIS, L. C. **CRIMES CIBERNÉTICOS E SUA EVOLUÇÃO**. 2020. Trabalho de Conclusão de Curso (Bacharel em Direito) - Faculdade Vale do Cricaré, São Mateus, 2020. Disponível em: <https://repositorio.ivc.br/bitstream/handle/123456789/265/TCC%20FINAL%20-%20LUCAS%20CARDOZO%20NOVAIS.pdf?sequence=1&isAllowed=y>. Acesso em: 15 ago. 2023.

NUCCI, Guilherme de Souza. **Estatuto da criança e do adolescente comentado**. 4a ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.

NUCCI, G. S de. **Manual do Direito Penal**. 7. ed. São Paulo: Revista dos Tribunais, 2017.

ROCHA, J. B. *Novatio legis in mellius* no estelionato contra o idoso a partir da Lei 14.155/2021. **Revista Consultor Jurídico**, 10 de junho de 2021. Disponível em: <https://www.conjur.com.br/2021-jun-10/bheron-novatio-legis-in-mellius-estelionato-idoso>. Acesso em: 28 ago. 2023.

ROSSINI, A. E. S de. **Informática Telemática e Direito Penal**. São Paulo: Memória Jurídica 2004.

SANTANA, R. F. S. **CRIMES CIBERNÉTICOS: ANÁLISE EVOLUTIVA DA LEGISLAÇÃO PENAL BRASILEIRA E SEUS DESAFIOS**. Salvador – BA, 2021. Disponível em: <http://ri.ucsal.br:8080/jspui/bitstream/prefix/4456/1/TCCROQUESANTANA.pdf>. Acesso em: 16 ago. 2023.

SANTOS, L. R dos; MARTINS, L. B; TYBUCSH, F. B. A. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo**. 2014. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf>. Acesso em: 08 set. 2023.

SANTOS, G. D.A dos. **CRIMES VIRTUAIS: tratamento legal e limitações no combate aos crimes cibernéticos**. 2021. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Anápolis – 2021. Disponível em:



<http://repositorio.aee.edu.br/bitstream/aee/18227/1/Gabrielly%20Daianne.pdf>. Acesso em: 14 ago. 2023.

SILVA, F. J; SANTOS, R. J.M dos. **O Estelionato praticado por meio da Internet: uma visão acerca dos Crimes Virtuais.** 2021. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/18080/1/TCC%2001.12.21%20dep%C3%B3sito%20final.pdf>. Acesso em: 03 nov. 2022.

SOUZA, M. **Cibercrimes e os Reflexos no Direito Brasileiro.** 2021. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Pontifícia Universidade Católica de Goiás, Goiânia/GO, 2021. Disponível em: <https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/2659/1/TCC%20-%20MYKAELLY%20SOUZA%20.pdf>. Acesso em: 16 ago. 2023.

SODRÉ, L. G. S da. **Dificuldades na colheita de elementos de autoria e materialidade delitiva dos Crimes Cibernéticos.** 2021. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Centro Universitário do Planalto Central Aparecido dos Santos – Uniceplac. Gama-DF. 2021. Disponível em: <https://dspace.uniceplac.edu.br/bitstream/123456789/1717/1/Ludmilla%20Gon%C3%A7alo%20da%20Silva%20Sodr%C3%A9%20.pdf>. Acesso em: 07 set. 2023.

SCHAUN, Guilherme. Uma lista com 24 crimes virtuais. **Jusbrasil.** 2018. Disponível em: <https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais>. Acesso em: 07 set. 2023.

SYDOW, S. T. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: [http://www.egov.ufsc.br/portal/sites/default/files/delitos\\_informaticos\\_proprios\\_uma\\_abordagem\\_sob\\_a\\_perspectiva\\_vitimodogmatica.pdf](http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf). Acesso em: 15 ago. 2023.

VIEIRA, M. E. P. **A adesão do Brasil a Convenção de Budapeste e a Correção das Deficiências Legislativas quanto os Crimes Cibernéticos.** 2023. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Centro de Ciências Jurídicas da Universidade Federal de Santa Catarina – Florianópolis. 2023. Disponível em: [https://repositorio.ufsc.br/bitstream/handle/123456789/248821/A%20ADES%C3%83O%20DO%20BRASIL%20A%20CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE%20E%20A%20CORRE%C3%87%C3%83O%20DAS%20DEFICI%C3%84NCIAS%20LEGISLATIVAS.%20Vers%C3%A3o%20final%20-%20Documentos%20Google%20\(1\).pdf?sequence=1](https://repositorio.ufsc.br/bitstream/handle/123456789/248821/A%20ADES%C3%83O%20DO%20BRASIL%20A%20CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE%20E%20A%20CORRE%C3%87%C3%83O%20DAS%20DEFICI%C3%84NCIAS%20LEGISLATIVAS.%20Vers%C3%A3o%20final%20-%20Documentos%20Google%20(1).pdf?sequence=1). Acesso em: 09 set. 2023.