CENTRO UNIVERSITÁRIO VALE DO SALGADO
CURSO DE DIREITO

RADAMÉS DOS SANTOS LIMA

ESTELIONATO DIGITAL NO BRASIL: DESAFIOS LEGAIS E PERSPECTIVA À LUZ DA LEI N. 14.155/2021

ICÓ-CE
2023

RADAMÉS DOS SANTOS LIMA

ESTELIONATO DIGITAL NO BRASIL: DESAFIOS LEGAIS E PERSPECTIVA À LUZ DA LEI N. 14.155/2021

Artigo científico apresentado ao Curso de Direito do Centro Universitário Vale do Salgado - UniVS, como pré-requisito para obtenção do título de Bacharel em Direito, sob orientação do Prof. Me. Lucas Vialli Batista Miranda.

ICÓ-CE
2023

RADAMÉS DOS SANTOS LIMA

ESTELIONATO DIGITAL NO BRASIL: DESAFIOS LEGAIS E PERSPECTIVA À LUZ DA LEI N. 14.155/2021

Artigo submetido à disciplina de TCC II do curso de Direito do Centro Universitário Vale do Salgado (UNIVS), como pré-requisito para obtenção do título de Bacharel em Direito.
Aprovado em: 27/06/2023

BANCA EXAMINADORA

_____

Prof. Me. Lucas Vialli Batista Miranda
Centro Universitário Vale do Salgado
Orientador

_____

Prof. Me. José Antônio de Albuquerque Filho
Centro Universitário Vale do Salgado
1º Examinador

_____

Prof. Me. Joseph Ragner Anacleto Fernandes Dantas
Centro Universitário Vale do Salgado
2º Examinador

RESUMO

LIMA, Radamés dos Santos. **ESTELIONATO DIGITAL NO BRASIL: DESAFIOS LEGAIS E PERSPECTIVA À LUZ DA LEI N. 14.155/2021**. 2023. 27f. Trabalho de Conclusão de Curso (Graduação Bacharelado em Direito). Centro Universitário Vale do Salgado, Icó-CE. 2023.

Este artigo científico aborda a análise do contexto do crime de estelionato digital no Brasil, introduzido no Código Penal pela Lei n. 14.155/2021. O objetivo é identificar as principais características desse crime e as medidas preventivas para combatê-lo. A metodologia utilizada foi a pesquisa bibliográfica, com base em dados e informações coletados de diversas fontes. O referencial teórico explora conceitos relacionados ao estelionato digital, suas principais formas de prática no Brasil e as mudanças trazidas pela nova lei. Os resultados evidenciam a importância da prevenção no combate ao estelionato digital, visto que a repressão não é suficiente para inibir sua ocorrência. Nesse sentido, são apresentadas medidas preventivas para usuários e empresas provedoras de serviços, bem como a atuação das autoridades competentes na investigação e punição dos responsáveis. O estudo destaca ainda a relevância da educação e da adoção de medidas preventivas pelos usuários da *internet* para reduzir os riscos desse tipo de crime. Exemplos práticos e sugestões de ações concretas são fornecidos para combater o estelionato digital. Em resumo, este trabalho científico oferece uma análise abrangente sobre o tema do estelionato digital no Brasil, enfatizando a importância da prevenção e do combate a esse crime. O texto é claro, objetivo e respaldado por exemplos práticos e sugestões de ações concretas para mitigar os riscos do estelionato digital. Seu conteúdo é relevante para usuários da *internet*, empresas provedoras de serviços e autoridades competentes que buscam compreender melhor o contexto do estelionato digital no Brasil e como se proteger contra ele.

PALAVRAS-CHAVE: Estelionato digital. Lei n. 14.155/2021. Medidas preventivas. Crimes cibernéticos.

ABSTRACT

LIMA, Radamés dos Santos. **DIGITAL SCREENING IN BRAZIL: LEGAL CHALLENGES AND PERSPECTIVE IN THE LIGHT OF LAW No. 14.155/2021.** 2023. 27f. Completion of course work (Bachelor's Degree in Law). Vale do Salgado University Center, Icó-CE. 2023.

This scientific article addresses the analysis of the context of the crime of digital larceny in Brazil, introduced in the Penal Code by Law n. 14.155/2021. The objective is to identify the main characteristics of this crime and the preventive measures to combat it. The methodology used was bibliographical research, based on data and information collected from different sources. The theoretical framework explores concepts related to digital fraud, its main forms of practice in Brazil and the changes brought about by the new law. The results show the importance of prevention in the fight against digital fraud, since repression is not enough to inhibit its occurrence. In this sense, preventive measures are presented for users and service providers, as well as the performance of the competent authorities in the investigation and punishment of those responsible. The study also highlights the relevance of education and the adoption of preventive measures by *internet* users to reduce the risks of this type of crime. Practical examples and suggestions for concrete actions are provided to combat digital fraud. In summary, this scientific work offers a comprehensive analysis on the topic of digital fraud in Brazil, emphasizing the importance of preventing and combating this crime. The text is clear, objective and supported by practical examples and suggestions for concrete actions to mitigate the risks of digital fraud. Your content is relevant to *internet* users.

KEY WORDS: Digital fraud. Law No. 14.155/2021. Preventive measures. Cybercrimes.

SUMÁRIO

1 INTRODUÇÃO

A criminalidade digital tem se tornado cada vez mais presente na sociedade contemporânea, apresentando desafios ao sistema de justiça criminal e à segurança da informação. Nesse contexto, o estelionato digital destaca-se como uma das principais formas de fraude realizada por meio da *internet* e outros meios eletrônicos.

Este trabalho tem como objetivo estudar o crime de estelionato digital no Brasil, que foi introduzido no Código Penal pela Lei n. 14.155/2021. O objetivo geral é analisar o contexto desse crime, identificando suas principais características e propondo medidas preventivas para combatê-lo.

Para alcançar esse objetivo, foram estabelecidos os seguintes objetivos específicos: apresentar o crime de estelionato previsto no art. 171 do Código Penal; compreender o cenário atual do uso da *internet* e dos meios de comunicação virtuais, bem como o crescimento da criminalidade presente nesses meios; classificar os crimes digitais, considerando o anonimato dos usuários envolvidos e as dificuldades na tipificação de novos comportamentos relacionados à criminalidade digital, com foco específico no estelionato digital; e analisar as estratégias adotadas pelo Estado para combater os crimes digitais, com foco nas atualizações da Lei n. 14.155/2021.

A justificativa para esta pesquisa reside na necessidade de compreender as consequências da nova Lei na sociedade e no sistema de justiça criminal, além da importância da prevenção no combate ao crime. Além disso, este trabalho busca contribuir para o debate sobre o tema, fornecendo informações relevantes para compreender o estelionato digital e adotar medidas preventivas efetivas.

Espera-se que este estudo contribua para o entendimento do crime de estelionato digital no Brasil e para o desenvolvimento de estratégias preventivas que possam ser adotadas por indivíduos e organizações.

2 O CRIME DE ESTELIONATO COMUM

A palavra estelionato origina-se do termo em latim *stellionatu*, o qual, em sua etimologia, deriva do termo *stellio*, uma espécie de lagarto que muda de cor para se camuflar e iludir os insetos dos quais se alimenta (ESTEFAN, 2022).

Segundo Nucci (2022), o estelionato é um crime artístico, uma vez que envolve apresentações, discursos persuasivos e embelezados, bem como todos os artifícios necessários

para enganar alguém com uma história, a qual finda na obtenção de vantagem ilícita em favor do estelionatário.

O Decreto-Lei n. 2.848, de 07 de dezembro de 1940, que disciplina o Código Penal brasileiro, traz em seu Título II os crimes contra o patrimônio, descrevendo a partir do Capítulo VI, art. 171, o crime de estelionato.

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

Para Mirabete (2021), o crime de estelionato então existe quando o agente utiliza qualquer meio fraudulento que induza alguém a erro ou mantenha-o nessa posição, obtendo com essa ação uma vantagem indevida para si ou para outrem.

2.1 OBJETO DO CRIME DE ESTELIONATO

Também conhecido por objeto do crime, se divide em duas categorias: I – objeto jurídico e II – objeto material. O **objeto jurídico** é o bem ou interesse protegido pela norma penal, enquanto o **objeto material** é o bem sobre o qual recai a conduta criminosa (ANDREUCCI, 2021).

O objeto jurídico tutelado, em tom primordial, no crime de estelionato, é a inviolabilidade do patrimônio, destacando-se a repreensão da fraude causadora de dano ao patrimônio da vítima. Já o objeto material é a vantagem ilícita, a qual é obtida em prejuízo alheio e atinge o patrimônio da vítima (CAPEZ, 2022).

Ao abordar o crime de estelionato, Manzini (apud CAPEZ, 2022, p. 245) destaca que esse delito não se limita apenas a uma lesão ao patrimônio da vítima, mas também envolve o uso de fraude para persuadir o ofendido. Assim, o estelionatário é considerado sempre um criminoso, pois suas ações são ilícitas desde o início e violam a moralidade.

Dessa forma, conclui-se, de acordo com Mirabete (2021), que não apenas a inviolabilidade patrimonial é protegida, mas também os princípios da boa-fé, segurança, fidelidade e veracidade nos negócios jurídicos que envolvem um patrimônio. Esses elementos, embora de forma secundária, também são protegidos contra o crime de estelionato.

2.2 SUJEITOS ATIVO E PASSIVO

Os sujeitos de um crime podem ser ativos ou passivos. O sujeito ativo é aquele que pratica a conduta delituosa, costumeiramente chamado de agente do crime, enquanto o sujeito passivo é a vítima da ação delituosa, ou seja, a pessoa que sofre as consequências provocadas pela prática criminosa do agente (ANDREUCCI, 2021).

Uma vez que o crime de estelionato não impõe requisitos específicos para a identificação do autor, qualquer pessoa pode ser considerada como **sujeito ativo**. Da mesma forma, o **sujeito passivo** também pode ser qualquer indivíduo, incluindo tanto o proprietário do patrimônio quanto aquele que sofreu prejuízo devido à conduta criminosa, mesmo que não seja o proprietário (GRECO, 2022).

Greco (2022) destaca que a vítima deve possuir capacidade de discernimento a fim de ser ludibriada. Nesse sentido, caso não a possua, ao invés de caracterizar-se o crime de estelionato, estaria configurado o delito de abuso de incapazes, tipificado no art. 173 do Código Penal.

Ademais, o crime de estelionato exige que o sujeito passivo seja pessoa determinada, visto que a não determinação de pessoas caracteriza crime contra a economia popular ou contra a ordem econômica, previstos, respectivamente, na Lei n. 1.521/1951 e na Lei n. 8.176/1991 (CAPEZ, 2022).

2.3 REQUISITOS PARA CONCRETIZAÇÃO DO ESTELIONATO

A concretização do crime de estelionato, além da obrigatoriedade do dolo, que é quando o agente conscientemente ilude a vítima, passa pela necessidade do adimplemento de três elementos primordiais: fraude, vantagem ilícita e prejuízo alheio (MIRABETE, 2021).

2.3.1 Fraude

A prática da fraude pode ser subdividida em três modalidades, que são o emprego de **artifício** (fraude no sentido material, ou seja, o aparato material ou disfarce utilizado para enganar a vítima); **ardil** (insídia, conversa enganosa, astúcia do agente) ou **qualquer outro meio fraudulento** (podendo ser até mesmo o silêncio, consistindo no estelionato por omissão), cada uma dessas práticas consubstanciada a aptidão de enganar a vítima, uma vez que a incapacidade de persuadir a vítima tornaria o crime impossível, nos moldes do art. 17 do Código

Penal (CUNHA, 2016).

2.3.2 Vantagem ilícita

É o objeto material do crime de estelionato, a razão pela qual o estelionatário se utiliza de meio fraudulento visando enganar a vítima, com a finalidade de obter a dita vantagem ilícita em prejuízo alheio.

Ensina Capez (2022), que tal vantagem, além de ser econômica, uma vez que se trata de crime patrimonial, também deverá ser ilícita, não correspondente a qualquer direito, pois se fosse uma vantagem lícita, restaria configurado o crime de exercício arbitrário das próprias razões, previsto no art. 345 do Código Penal.

2.3.3 Prejuízo alheio

Por último, o prejuízo alheio consiste no dano de natureza patrimonial, ou seja, o prejuízo resultante da obtenção de vantagem ilícita em favor do agente (CUNHA, 2016).

2.4 CONSUMAÇÃO E TENTATIVA

O Código Penal traz em seu art. 14 as definições do crime na modalidade consumada e tentada, sendo:

> Art. 14 - Diz-se o crime:
> **Crime consumado**
> I - consumado, quando nele se reúnem todos os elementos de sua definição legal;
> **Tentativa**
> II - tentado, quando, iniciada a execução, não se consuma por circunstâncias alheias à vontade do agente (BRASIL, 1940).

Por ser um crime material, o estelionato consuma-se, em sua modalidade comum, no momento em que o agente consegue obter a vantagem ilícita, concretando prejuízo à vítima. Com isso, Greco (2022) menciona que para efeitos de reconhecimento de consumação do estelionato há de ser necessariamente observada a afirmação do binômio vantagem ilícita/prejuízo alheio.

A tentativa também é admita no crime de estelionato, uma vez que se trata de crime plurissubsistente, onde é possível o fracionamento do *iter criminis*. Nas palavras de Capez

(2022), quando o agente não logra êxito na obtenção da vantagem indevida por circunstâncias alheias à sua vontade, há a ocorrência do estelionato na forma tentada, ressaltando que também deve ser observado o meio empregado pelo agente para tentar persuadir a vítima, tendo este que ser eficaz, porém também frustrado por circunstâncias alheias à vontade do autor.

Assim, Estefam (2022), delimita as três hipóteses onde restará configurado o estelionato tentado, sendo: 1ª) quando o agente inicia a fraude, mas não consegue ludibriar a vítima; 2ª) quando o agente consegue empregar a fraude e enganar a vítima, porém não consegue obter a vantagem ilícita e 3ª) quando o agente consegue empregar a fraude, enganar a vítima, obter a vantagem, outrossim a vítima não sofre nenhum prejuízo.

2.5 AÇÃO PENAL

Anteriormente classificado como crime de ação penal pública incondicionada, em virtude das alterações resultantes da Lei n. 13.194, de 24 de dezembro de 2019, conhecida por Pacote Anticrime, o estelionato passou a ser crime de ação penal pública condicionada à representação da vítima, ou seja, somente se procede com o desejo da vítima de representar criminalmente contra o autor.

O §5º, que foi incluído no art. 171 do Código Penal, além de trazer a classificação da ação penal *suso* mencionada, também resguardou as hipóteses onde é dispensada a representação para que se proceda o processo penal, nos casos onde a vítima for: I – a Administração Pública, direta ou indireta; II – criança ou adolescente; III – pessoa com deficiência mental; ou IV – maior de 70 (setenta) anos de idade ou incapaz.

3 DIFUSÃO DO USO DA *INTERNET* NO BRASIL

De acordo com dados da Pesquisa Nacional por Amostra de Domicílios, em 2021, houve um aumento no número de residências com acesso à *internet* no Brasil, alcançando 90% dos lares brasileiros. Em números absolutos, a pesquisa revelou que existem 65 milhões de domicílios conectados, representando um acréscimo de 5,8 milhões em relação a 2019 (BRASIL, 2022).

O número de lares brasileiros conectados à *internet* também reflete na quantidade de pessoas que utilizam esse meio, alcançando um total de 155,7 milhões de indivíduos. Um dado relevante é que o uso da *internet* para realizar chamadas de voz ou vídeo pela primeira vez na história ultrapassou o uso de envio e recebimento de mensagens de texto, voz ou imagens por

meio de aplicativos distintos dos endereços eletrônicos, atingindo uma porcentagem de 95,7% dos usuários, em comparação com 94,9% deste último (BRASIL, 2022).

Dito isso, os dados demonstram que a população brasileira está cada vez mais conectada, preferindo utilizar a *internet* para se relacionar com outras pessoas. Por esse motivo, é cada vez mais necessário tomar cuidado com mensagens mal-intencionadas e contatos de desconhecidos.

Uma pesquisa realizada pela Federação Brasileira de Bancos - FEBRABAN mostrou que sete em cada dez operações bancárias feitas no Brasil em 2021, de um total de 119,5 bilhões de transações, foram realizadas por meio da *internet* e de dispositivos móveis. De acordo com o mesmo estudo, esse resultado foi impulsionado por um crescimento de 28% nas operações realizadas por *smartphones*, totalizando 67,1 bilhões de transações e representando 58% do total. O presidente da FEBRABAN, Issac Sidney, destacou que os consumidores estão passando por uma grande mudança em seus hábitos financeiros, preferindo realizar suas transações por meios eletrônicos em vez de se deslocarem até uma agência bancária (OLIVEIRA; ZANATTA, 2022).

Uma das principais inovações no campo das transações financeiras, o *Pix*, também registrou um grande aumento. De acordo com a FEBRABAN, no período entre março de 2021 e março de 2022, o número de usuários que realizaram mais de 30 *Pix* por mês teve um crescimento impressionante de 809%, enquanto os usuários que receberam mais de 30 *Pix* por mês aumentaram em 464%. Essas porcentagens mostram que as pessoas estão cada vez mais optando por realizar transações financeiras de maneira rápida e descomplicada, o que também ressalta a importância de tomar precauções ao utilizar esse método de pagamento (OLIVEIRA; ZANATTA, 2022).

3.1 AUMENTO DA CRIMINALIDADE NOS MEIOS DIGITAIS

Jesus e Milagre (2016) abordaram a *internet* como um ambiente rico, observando que onde há riqueza, também existe crime. Dessa forma, a globalização possibilitou aos criminosos romperem barreiras no que diz respeito aos métodos utilizados para persuadir pessoas, devido à ampla capacidade de troca de informações na nova sociedade moderna, conhecida como sociedade da informação.

Acompanhando o aumento do uso da *internet* no Brasil, a criminalidade também cresceu significativamente nos últimos anos, principalmente durante a pandemia do COVID-19, quando houve um aumento de 175% no número de crimes cometidos por meio da *internet* (PROFISSÃO REPÓRTER, 2022).

Conforme dados da FEBRABAN, observou-se um aumento de 165% nos casos de golpes de engenharia social no primeiro semestre de 2021 em comparação ao segundo semestre de 2020. Esses golpes envolvem a manipulação psicológica das vítimas, levando-as a fornecer informações pessoais e senhas de seus cartões aos criminosos (EXTRA, 2021).

4 CONCEITUAÇÃO DE CRIMES DIGITAIS / CYBERCRIMES

Embora nem todos os crimes listados no Código Penal ou em outras leis tenham disposições específicas para sua prática em meios digitais, a disseminação do uso da *internet* proporcionou aos criminosos novas maneiras e oportunidades de prejudicar bens protegidos legalmente. Patrícia Pinheiro esclarece que:

> O crime eletrônico é, em princípio, **um crime de meio**, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não. A maioria dos crimes cometidos na rede ocorre também no mundo real. A *Internet* surge apenas como um facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como à necessidade de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio (PINHEIRO, 2021, p. 133).

Jesus e Milagre (2016), por sua vez, definem os crimes cibernéticos como a conduta típica e ilícita realizada por meio da tecnologia da informação ou contra ela. Portanto, os crimes cibernéticos não apenas são crimes cometidos usando meios digitais, mas também podem ter como objetivo causar danos diretos à própria tecnologia da informação.

A conclusão é que, em geral, o ambiente virtual é propício para a ocorrência de crimes, tanto aqueles direcionados especificamente a sistemas, dispositivos informáticos e redes de computadores, quanto para a prática de crimes comuns que já estão definidos em nossa legislação penal.

4.1 O ANONIMATO DOS CRIMINOSOS VIRTUAIS

A *internet*, como mencionado nas seções anteriores, traz benefícios para a sociedade, mas

também apresenta elementos que favorecem a prática do mal. Uma das principais razões pelas quais a criminalidade se desenvolve no ambiente digital é a facilidade com que os criminosos podem se esconder no mundo virtual, utilizando informações falsas ou de terceiros ao se cadastrarem em provedores digitais. Isso muitas vezes torna impossível identificar o verdadeiro autor dos crimes (ESTRELA, 2003).

Embora haja possibilidades de identificação dos criminosos digitais, a sensação de anonimato e o conhecimento da falta de preparo das autoridades para investigar crimes de natureza digital levam esses criminosos a se interessarem por práticas criminosas que não realizariam no mundo físico. Não é possível traçar um perfil específico dos criminosos cibernéticos, porém, no Brasil, é evidente que eles são mais criativos do que técnicos. A maior parte dos crimes cometidos no ambiente digital decorre da falta de conhecimento dos usuários e da disseminação de técnicas e ferramentas para aplicação de golpes (JESUS; MILAGRE, 2016).

4.2 CONCEITO DO CRIME DE ESTELIONATO PRATICADO EM AMBIENTE VIRTUAL

A estratégia de conceituar o crime de estelionato comum na primeira parte deste artigo, juntamente com a explicação do conceito de crimes cibernéticos, foi adotada para uma compreensão simplificada do crime de estelionato praticado em ambientes digitais.

Considerando que os crimes virtuais geralmente envolvem a prática ilícita realizada pelo agente através da *internet*, utilizando-se de dispositivos que favorecem sua ação, pode-se afirmar que o estelionato virtual é o crime no qual o agente, por meio da *internet*, induz ou mantém uma pessoa em erro, manipulando meios fraudulentos com o objetivo de obter vantagem econômica ilícita para si ou para terceiros, em detrimento de outrem (ATAÍDE, 2017).

A diferença fundamental entre o conceito mencionado acima e o estabelecido no *caput* do art. 171 do Código Penal está no uso de dispositivos conectados à *internet*, como *smartphones*, computadores ou *tablets*, para a consumação do crime. No entanto, é importante considerar que o Código Penal foi promulgado em 1940, quando a *internet* nem mesmo existia no país. Isso apenas reforça a necessidade de o Direito atualizar-se em relação às questões relacionadas às novas tecnologias da sociedade, a fim de combater as facilidades encontradas pelos criminosos para violar a lei (DINIZ; CARDOSO; PUGLIA, 2022).

Diniz, Cardoso e Puglia (2022) destacam que a diferença entre o estelionato comum e aquele praticado na *internet* é clara em relação ao *modus operandi*. O estelionato comum ocorre

no mundo físico, geralmente envolvendo contato pessoal direto com a vítima, enquanto o estelionato virtual ocorre em um ambiente facilitado pelo uso de computadores ou outros dispositivos conectados à *internet*, onde não há esse tipo de contato. De forma mais enganosa, o agente consegue ludibriar a vítima, resultando em consequências que provavelmente seriam mais facilmente percebidas no mundo físico.

5 A LUTA DO ESTADO CONTRA OS CRIMES CIBERNÉTICOS

Ao longo dos anos, foi necessário adaptar o sistema jurídico brasileiro para garantir maior segurança nos meios virtuais, por meio de medidas repressivas, ou seja, após a ocorrência dos crimes. No entanto, ainda há muito a ser feito para alcançar um ambiente verdadeiramente seguro na *internet*. Muitos desafios ainda precisam ser enfrentados para garantir a proteção adequada dos usuários e combater efetivamente as práticas criminosas no ambiente virtual.

Um dos exemplos mais marcantes foi a promulgação da Lei n. 12.737 em 2012, conhecida como Lei Carolina Dieckmann. Na ocasião, o computador da atriz foi invadido por *hackers* e dados pessoais e íntimos foram acessados. Com a entrada em vigor dessa nova lei, foram adicionados ao Código Penal os artigos 154-A e 154-B, que estabelecem o crime de invasão de dispositivos informáticos (SANTOS; MARTINS; TYBUCSH, 2017).

No ano de 2014, como consequência da evolução da nossa sociedade e em resposta à imersão digital vivida pelos brasileiros, foi promulgada a Lei n. 12.965, o Marco Civil da *Internet*, que estabeleceu princípios, garantias, direitos e deveres para o uso da *internet* no Brasil.

Jesus e Oliveira (2014) destacaram que, até então, no Brasil não havia uma lei específica que tratasse dos deveres dos provedores de acesso e aplicações, bem como dos direitos dos usuários. Como resultado, questões relacionadas a esses temas eram frequentemente tratadas pelo Judiciário, resultando em decisões controversas baseadas na interpretação do Código Civil, Código de Defesa do Consumidor e outras leis existentes.

Dessa forma, a criação do Marco Civil da *Internet* teve como objetivo proporcionar segurança jurídica, fornecendo ao Poder Judiciário mecanismos legais atualizados para a correta resolução de conflitos relacionados à *internet*, evitando decisões contraditórias (JESUS; OLIVEIRA, 2014).

No ano de 2021, foi sancionada a Lei n. 14.155, que promoveu alterações no Código Penal em várias de suas disposições, ampliando as penas secundárias de diversos crimes quando estes são cometidos com o auxílio ou uso da *internet*, bem como com base em fatores

relacionados às facilidades proporcionadas por ela.

Um dos crimes que sofreu alterações significativas foi o estelionato, devido ao seu crescimento no uso de dispositivos eletrônicos. No entanto, a paz nos ambientes virtuais não pode ser alcançada apenas por meio de medidas repressivas, e a luta contra a criminalidade digital ainda terá um longo caminho pela frente.

5.1 A LEGISLAÇÃO APLICADA AO CRIME DE ESTELIONATO DIGITAL

No tópico 2, foi abordado o conceito padrão do crime de estelionato comum, expresso no art. 171 do Código Penal. Agora, é de grande importância compreender a sua pena para que seja possível observar o verdadeiro impacto das alterações trazidas pela Lei 14.155/2021.

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

Em sua obra Dos Delitos e das Penas, Cesare Beccaria, ao refletir acerca da moderação das penas conclui que:

> O rigor das penas deve ser relativo ao estado atual da nação. São necessárias impressões fortes e sensíveis para impressionar o espírito grosseiro de um povo que sai do estado selvagem. Para abater o leão furioso, é necessário o raio, cujo ruído só faz irritá-lo. Mas, à medida que as almas se abrandam no estado de sociedade, o homem se torna mais sensível; e, se se quiser conservar as mesmas relações entre o objeto e a sensação, as penas devem ser menos rigorosas (BECCARIA, 1764).

Estefam e Gonçalves (2022) conceituam a pena como uma retribuição imposta pelo Estado, consistente na privação ou restrição de determinados bens jurídicos, determinados pela lei, com o objetivo de corrigir o condenado e reintegrá-lo à sociedade, visando, assim, prevenir a prática de novos crimes.

Nesse sentido, a atuação do Estado também sofre, ainda que indiretamente, quando um crime é cometido, uma vez que a prática criminosa demanda a aplicação da devida pena para evitar a reincidência do infrator. Isso se configura como o efeito preventivo especial da pena. Além disso, busca-se evitar que outras pessoas tomem o delinquente como exemplo, o que é conhecido como efeito preventivo geral da pena. Essas duas formas de prevenção têm o objetivo único de evitar que outros indivíduos se envolvam em atividades criminosas devido à sensação

de impunidade gerada quando aqueles que transgrediram a lei penal não são devidamente punidos (GRECO, 2018).

Com base nas conceituações e reflexões expostas acima, juntamente com a previsão legal do art. 59 do Código Penal, que estipula que a pena aplicada deve ser necessária e suficiente para reprovação e prevenção do crime, e no art. 1º da Lei n. 7.210/1984 (Lei de Execução Penal - LEP), pode-se observar que o sistema jurídico brasileiro adotou a Teoria da União. Essa teoria atribui à pena duas funções principais: I) caráter preventivo (geral e especial); e II) caráter retributivo (DINIZ; CARDOSO; PUGLIA, 2022).

Retomando o crime de estelionato, o art. 171, *caput,* do Código Penal, estabelece uma pena de um a cinco anos. Nesse caso, pode-se aplicar a suspensão condicional do processo (*sursis* processual), prevista no art. 89 da Lei n. 9.099/1995. Essa medida legal permite a suspensão do processo mediante o cumprimento de condições específicas, expressas no art. 89, §1º da mesma Lei. Se as condições forem cumpridas, o processo é encerrado sem condenação penal.

No entanto, devido ao aumento da prática desse crime e ao surgimento de novos métodos que facilitam sua ocorrência, tornou-se evidente a necessidade de adequação do Direito, incluindo a criação de uma nova qualificadora para o delito (DINIZ; CARDOSO; PUGLIA, 2022).

Finalmente, com a promulgação da Lei n. 14.155/2021, foram abordadas as práticas de diversos crimes relacionados à invasão de dispositivos informáticos e ao uso da *internet* como meio para cometer crimes. Em particular, em relação ao crime de estelionato, conforme objeto do nosso estudo, o art. 171 do Código Penal recebeu o §2º-A, conhecido como fraude eletrônica, que aumentou a pena do estelionato quando cometido por meios eletrônicos para um período de quatro a oito anos, além de multa.

> 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 (BRASIL, 1940).**

Rogério Greco (2022) explica que o §2º-A introduziu uma qualificadora para o crime de estelionato, relacionada aos meios utilizados pelo agente para cometer o crime. Além disso, fica evidente que, na nova redação legal, a vítima ou terceiros são induzidos ao erro, e o criminoso viola o dispositivo quando se aproveita das informações fornecidas em quatro momentos

distintos, conforme exemplificado por Rogério Sanches Cunha (2021), como:

> **a) por meio de redes sociais:** atualmente são muito comuns os anúncios promovidos em redes sociais como Facebook e Instagram. Não raro, são anúncios fraudulentos, manobras ardilosas para atrair pessoas que forneçam seus dados; **b) por contatos telefônicos:** são também muito comuns as fraudes cometidas por meio telefônico. Uma situação que se vê com certa frequência é o envio de mensagem (por WhatsApp, por exemplo) na qual o estelionatário se identifica como amigo ou familiar da vítima e lhe pede um depósito bancário devido a uma emergência. Sem dar-se conta, a vítima efetua o depósito na conta do criminoso; **c) pelo envio de correio eletrônico fraudulento:** neste caso, a vítima recebe um e-mail fraudulento, muitas vezes imitando os caracteres de empresas ou organizações conhecidas e, a partir do acesso por meio do link disponibilizado, insere dados de cartão de crédito ou efetua pagamentos de compras simuladas, o que proporciona a vantagem ao estelionatário; **d) por qualquer outro meio fraudulento análogo:** nesta fórmula analógica se inserem quaisquer outras práticas fraudulentas cometidas por meios eletrônicos ou informáticos, como páginas na *internet*, por exemplo, em que a vítima não é diretamente abordada pelo estelionatário, como nas modalidades anteriores, mas é induzida em erro por fatores diversos (simulação de um estabelecimento comercial regularmente constituído; cópia de outra página conceituada etc.) (CUNHA, 2021).

Dessa forma, o crime de estelionato é configurado, uma vez que a vítima, ao fornecer suas informações, faz parte diretamente do engodo arquitetado pelo estelionatário para obter vantagem indevida (CUNHA, 2021).

A ação penal no crime de estelionato, tanto na sua forma comum quanto na modalidade praticada por meio de fraude eletrônica, é condicionada à representação. Isso significa que é necessário que as vítimas formalizem uma representação contra os criminosos, a fim de combater o crime de forma repressiva. O caráter preventivo da pena por si só não é suficiente para dissuadir os criminosos de cometer o estelionato (DINIZ; CARDOSO; PUGLIA, 2022).

5.2 A EDUCAÇÃO COMO CHAVE PARA A PREVENÇÃO DOS CRIMES CIBERNÉTICOS

A educação, direito social concretizado pelo art. 6º da Constituição Federal do Brasil, apresenta-se como um dever do Estado, que deve assegurar que todos os brasileiros a recebam com qualidade, visando a formação e desenvolvimento de seres humanos íntegros e capazes de contribuir para o progresso do país com ideias e conceitos sociais, econômicos, culturais e plurais (SOUSA, 2021).

Embora no Brasil prevaleça o caráter repressivo, cabe a cada indivíduo buscar o caminho da prevenção como uma arma de combate à criminalidade. Segundo Sá (apud FARIA, 2007), a prevenção implica capacitar as pessoas para antecipar eventos que possam ocorrer em suas

vidas, permitindo-lhes estar preparadas para enfrentá-los e evitar danos.

Uma medida adequada para combater golpes e outros crimes praticados pela *internet* seria a promoção de disciplinas voltadas para o estudo da informática nas escolas, de modo que desde cedo seja possível aprender sobre o uso seguro da internet e as formas de proteção contra golpistas.

Além disso, não basta apenas inserir uma disciplina de informática nas escolas; é necessário assegurar a efetiva utilização desses conhecimentos, de forma que não apenas os jovens se beneficiem, mas toda a população.

Conforme dados do IBGE, em 2021, cerca de 28,2 milhões de pessoas no Brasil, o que corresponde a 15,3% da população com mais de 10 anos de idade, não utilizaram a *internet*. O motivo mais citado por essas pessoas foi a falta de conhecimento para utilizar a tecnologia. O levantamento também revelou que 98,2% dos estudantes da rede privada de ensino utilizaram a *internet*, enquanto esse índice foi de 87% para alunos da rede pública (SILVA, 2022).

Os dados revelam que uma parcela significativa da população brasileira enfrenta dificuldades no uso da *internet*, o que os torna potencialmente mais vulneráveis a golpes e fraudes por parte de estelionatários.

Ao analisar a situação da educação no Brasil em relação aos estudos da criminologia, é possível observar a aplicabilidade da Teoria do Triângulo do Crime, proposta por Lawrence Cohen e Marcus Felson. Segundo essa teoria, para que um crime ocorra, são necessários três elementos: um infrator motivado, uma vítima disponível e um local apropriado. Ao analisar o contexto das fraudes eletrônicas, é evidente a presença desses três elementos, pois o ambiente virtual oferece uma oportunidade favorável para os estelionatários persuadirem vítimas que não possuem conhecimento para se proteger nesse meio (MARCONDES, 2015).

Conforme apontado por Diniz, Cardoso e Puglia (2022), o Governo Federal já possui programas que se assemelham à proposta de oferta de cursos de aprendizagem, como o Programa Nacional de Acesso ao Ensino Técnico e Emprego - Pronatec, criado por meio da Lei n. 12.513/2011. No entanto, os autores mencionam que devido à redução nos investimentos por parte do governo, não é perceptível uma eficácia significativa na melhoria da sociedade brasileira. Sendo assim, sugere-se o aprimoramento dos investimentos e o desenvolvimento de políticas públicas para a inserção e capacitação dos usuários em relação ao uso da *internet*.

Conclui-se, portanto, que a educação é o melhor caminho para prevenir o crescente crime de estelionato digital. É necessário que os órgãos governamentais invistam na disponibilização de cursos, palestras e campanhas publicitárias em importantes centros de divulgação, com o objetivo de educar a população brasileira sobre o uso seguro da *internet*.

5.3 AS DIFICULDADES DE IDENTIFICAÇÃO E PUNIÇÃO DOS ESTELIONATÁRIOS DIGITAIS

O ordenamento jurídico do país cada vez mais busca punir os criminosos digitais. No entanto, a infraestrutura para investigação dos delitos cometidos no ambiente virtual ainda é insuficiente. A criação de delegacias especializadas desempenha um papel de grande importância para as vítimas, que muitas vezes deixam de procurar as autoridades policiais devido à falta de confiança de que os criminosos serão punidos, ou mesmo de que haverá uma investigação policial adequada (KUNRATH, 2014).

Segundo Patrícia Pinheiro (2021), toda investigação começa com base em evidências e informações coletadas. No ambiente virtual, isso não é diferente do ambiente físico, já que as evidências e informações ainda existem, mas são armazenadas de várias maneiras, como em celulares, discos rígidos ou até mesmo nos códigos-fonte de arquivos maliciosos.

Com base nisso, é evidente que mesmo no ambiente virtual os criminosos podem deixar rastros, o que leva a crer que eles possam ser localizados e punidos. Conforme apontado por Wendt e Jorge (2013), as evidências encontradas no mundo virtual são consideradas provas da ocorrência do crime e podem ser obtidas de várias maneiras, como registros de *login* (*logs*), amostras de registros de sessões e registros de navegação na *internet*.

Um grande desafio surge quando há escassez de tecnologia e mão de obra qualificada para combater os *cybercrimes*. Isso ocorre devido ao fato de que, no sistema jurídico brasileiro, a aplicação da pena penal requer a comprovação da ocorrência do crime, incluindo a autoria e a materialidade, ou fortes indícios de que o acusado cometeu o delito (AMARAL, 2022).

Além disso, Amaral (2022) menciona também que a verdadeira dificuldade na investigação dos crimes cibernéticos nem sempre reside na identificação do computador ou dispositivo em que o criminoso comete o delito; pelo contrário, está na identificação do próprio criminoso. Isso ocorre porque o mesmo dispositivo pode ser utilizado por diferentes pessoas, nem todas com a intenção de prejudicar um bem jurídico alheio.

Wendt e Jorge (2013) relatam que as informações fornecidas pelos provedores de *internet* são de extrema importância. Esses dados podem ser utilizados para determinar o local onde o crime foi cometido, delimitar suspeitos e permitir a realização de novas diligências com o objetivo de identificar os verdadeiros infratores da lei.

Por outro lado, Amaral (2022) destaca novamente que devido à falta de profissionais especializados, à falta de cooperação das empresas de tecnologia da informação e à existência

de leis fundamentais que atrasam as investigações, juntamente com o aumento do número de crimes cometidos por estrangeiros no Brasil, ocorre um conflito de competência para julgar os crimes cibernéticos. Esse conflito é causado pela facilidade de adquirir hospedagens de IP (*Internet Protocol*) em outros países, o que contribui para o aumento da criminalidade.

O art. 5º, III da Lei n. 12.965/2014 define o IP como um endereço de protocolo de *internet*. Trata-se de um código atribuído a um terminal de rede para permitir sua identificação, de acordo com parâmetros internacionais estabelecidos (BRASIL, 2014).

Outro aspecto problemático no âmbito da repressão é o lapso temporal excessivo nos procedimentos judiciais. Um relatório do Conselho Nacional de Justiça - CNJ, que analisou ações que tramitaram de 2015 a 2018 nas Justiças estaduais, constatou que um processo criminal leva, em média, três anos e dez meses para ter sua sentença prolatada (FARIA, 2021).

O art. 5º, LXXVIII da CF/88, estabelece que a todos, no âmbito judicial e administrativo, são garantidos a razoável duração do processo e os meios que assegurem a celeridade de sua tramitação. No entanto, apenas a previsão legal não é suficiente para que esse princípio seja efetivo, sendo necessário adotar medidas que visem à sua aplicação. Caso contrário, ele será considerado um princípio constitucional vazio (DINIZ, CARDOSO, PUGLIA, 2022).

Conclui-se, portanto, que o caráter repressivo de combate aos estelionatários digitais apresenta falhas que podem resultar na impunidade dos crimes praticados por meio da *internet*, tornando-se ainda mais importante o desenvolvimento de métodos de caráter preventivo.

6 METODOLOGIA DA PESQUISA

6.1 TIPO DE PESQUISA

A natureza da pesquisa é básica, tendo como característica principal, nas palavras de Appolinário (2011), uma preocupação menor com a aplicação imediata dos resultados obtidos durante o levantamento de dados. Na verdade, essa pesquisa representa um avanço no conhecimento científico puro.

Como esta pesquisa é exploratória, o levantamento de dados foi realizado por meio de pesquisa bibliográfica, com o objetivo de adquirir maior familiaridade com o problema e estabelecer uma hipótese. Segundo Antônio Carlos Gil (2002), uma pesquisa exploratória tem como objetivo principal o desenvolvimento de novas ideias relacionadas ao tema da pesquisa.

A pesquisa adotou uma abordagem qualitativa, possibilitando a observação das características do fenômeno estudado e enfocando sua dimensão subjetiva. Em suma, buscou-

se compreender e explicar a dinâmica das relações sociais (GERHARDT; SILVEIRA, 2009).

Quanto ao método científico, utilizou-se o dedutivo, classificado por Karina Nunes da seguinte forma:

> O método dedutivo pressupõe que só a razão é capaz de levar ao conhecimento verdadeiro, pois os fatos, por si só, não são fonte de todos os conhecimentos. O raciocínio dedutivo tem o objetivo de explicar o conteúdo das premissas e, por intermédio de uma cadeia de raciocínio em ordem descendente (da análise do geral para o particular), chegar a uma conclusão. Para tanto, utiliza o silogismo, construção lógica que, a partir de duas premissas, obtém uma terceira logicamente decorrente, denominada conclusão (NUNES, 2019, p. 149).

Dessa forma, com base nas informações coletadas e apresentadas, foi possível chegar a uma conclusão lógica, que resultou da análise e adaptação de todas as premissas abordadas ao longo da pesquisa.

7 RESULTADOS E DISCUSSÕES

O presente artigo científico teve como objetivo analisar o contexto do crime de estelionato digital, introduzido no art. 171, §2º-A, do Código Penal, pela Lei n. 14.155/2021, identificando suas principais características e as medidas preventivas que podem ser adotadas para combatê-lo no Brasil.

A partir da análise realizada, foi possível constatar a importância da prevenção no combate ao crime de estelionato digital, uma vez que a repressão não é suficiente para inibir sua ocorrência. Nesse sentido, foram apresentadas medidas preventivas que podem ser adotadas pelos usuários e empresas provedoras de serviços, bem como a atuação das autoridades competentes na investigação e punição dos responsáveis.

Além disso, o estudo também apresentou informações relevantes sobre as características do crime de estelionato digital e sua tipificação pela Lei n. 14.155/2021, contribuindo para o desenvolvimento de métodos mais eficazes no combate a esse tipo de crime.

Dessa forma, os resultados obtidos com todo o estudo abordado são importantes para a conscientização da população sobre os riscos do uso inadequado da *internet* e dos meios de comunicação virtuais, bem como para a adoção de medidas preventivas eficazes no combate ao crime de estelionato digital no Brasil. A atuação conjunta dos usuários, empresas provedoras de serviços e autoridades competentes é fundamental para reduzir a ocorrência desse tipo de crime e garantir um ambiente virtual mais seguro para todos.

8 CONSIDERAÇÕES FINAIS

O artigo científico em questão abordou de forma relevante o estelionato digital e as soluções possíveis para combater esse tipo de crime. A análise realizada, baseada em dados e informações coletadas de diversas fontes, proporciona uma visão abrangente sobre o tema, ressaltando a importância da educação, da adoção de medidas preventivas pelos usuários da *internet*, da atuação das empresas provedoras de serviços e das autoridades competentes na prevenção e combate ao estelionato digital.

Durante a elaboração do texto, foram apresentadas informações obtidas a partir de situações concretas, com sugestões de ações para mitigar os riscos do estelionato digital.

Além disso, destaca-se a necessidade de uma abordagem conjunta, envolvendo todos os agentes interessados na prevenção desse tipo de crime, desde os usuários da *internet* até as autoridades competentes.

Conclui-se, portanto, que o estelionato digital representa uma ameaça significativa, afetando inúmeras pessoas no Brasil. No entanto, é possível adotar medidas preventivas e educacionais para mitigar os riscos desse crime.

Nesse contexto, é fundamental que todos os envolvidos estejam cientes dos perigos inerentes ao uso da *internet* e aos meios de comunicação virtuais, bem como das estratégias mais eficazes para prevenir e combater o estelionato digital.

Sendo assim, recomenda-se a continuidade da conscientização e do desenvolvimento de práticas seguras, em conjunto com a constante atualização de conhecimentos sobre o tema, visando a construção de um ambiente virtual mais seguro para todos.

REFERÊNCIAS

ANDREUCCI, Ricardo A. **Manual de Direito Penal.** São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786555598377. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598377/. Acesso em: 17 nov. 2022.

AMARAL, Jean Carlos Rossafa do. **Crimes cibernéticos e as dificuldades no processo de investigação para os crimes na *internet*.** Conteúdo Jurídico, Brasília-DF: 24 maio 2022. Disponível em: https://conteudojuridico.com.br/consulta/artigo/58454/crimes-cibernticos-e-as-dificuldades-no-processo-de-investigao-para-os-crimes-na-internet. Acesso em: 15 nov. 2022.

APPOLINÁRIO, F. **Dicionário de metodologia científica.** 2. ed. São Paulo: Atlas, 2011.

ATAÍDE, Amanda Albuquerque de. **Crimes virtuais: uma análise da impunidade e dos danos causados às vítimas.** 2017. Trabalho de Conclusão de Curso (Bacharel em Direito) – Faculdade da Cidade de Maceió, Maceió, 2017. Disponível em: http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf. Acesso em: 07 nov. 2022.

BECCARIA, Cesare. **Dos delitos e das penas.** São Paulo: eBooksLibris, 2001.

BRASIL. Casa Civil. **90% dos lares brasileiros já tem acesso à *internet* no Brasil, aponta pesquisa.** Brasília, 2022. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa#:~:text=Usu%C3%A1rios%20%2D%20Entre%20os%20183%2C9,era%20de%2079%2C5%25. Acesso em: 11 nov. 2022.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal.** Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.** Diário Oficial da República Federativa do Brasil. Brasília, Distrito Federal, 2014.

CAPEZ, Fernando. **Curso de direito penal: parte especial – arts. 121 a 212. v.2.** São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555596045. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596045/. Acesso em: 09 nov. 2022.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital - primeiras impressões e reflexos no CP e no CPP.** Meu Site Jurídico (JusPodivm), 2021. 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: 14 nov. 2022.

CUNHA, Rogério Sanches. **Manual de direito penal: parte especial (arts. 121 ao 361)**. Salvador. Editora JusPODIVM, 2016.

DINIZ, Felipe F.; CARDOSO, Jacqueline R.; PUGLIA, Eduardo H. P. **O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via *internet*.** Belo Horizonte: Libertas Direito. Disponível em: http://www.faaiesa.edu.br/aluno/arquivos/tcc/tcc_amanda_ataide.pdf. Acesso em: 14 nov. 2022.

ESTEFAM, André Araújo L**. Direito Penal - Vol. 2.** São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555596564. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596564/. Acesso em: 12 nov. 2022.

ESTEFAM, André; GONÇALVES, Victor Eduardo R. **Esquematizado - Direito Penal - Parte Geral.** São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555596434. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596434/. Acesso em: 13 nov. 2022.

ESTRELA, Kilmara Batista. **Crimes digitais.** 2003. Trabalho de Conclusão de Curso (Bacharelado em Ciências Jurídicas e Sociais) – Direito, Centro de Ciências Jurídicas e Sociais, Universidade Federal de Campina Grande, Sousa, Paraíba, 2003. Disponível em: http://dspace.sti.ufcg.edu.br:8080/jspui/handle/riufcg/13373. Acesso em: 13 nov. 2022.

EXTRA. **Pesquisa revela aumento de 165% nos golpes que envolvem roubo de informações pessoais no primeiro semestre.** G1, 2021. Disponível em: https://extra.globo.com/economia-e-financas/pesquisa-revela-aumento-de-165-nos-golpes-que-envolvem-roubo-de-informacoes-pessoais-no-primeiro-semestre-25260257.html. Acesso em: 08 nov. 2022.

FARIA, Flávia. **Tribunais levam, em média, cinco anos para julgar processos criminais.** Amazonas atual, 2021. Disponível em: https://amazonasatual.com.br/tribunais-levam-em-media-cinco-anos-para-julgar-processos-criminais/. Acesso em: 15 nov. 2022.

FARIA, Marcineli Cristina. **A ação preventiva dos ensinamentos do Programa Educacional de Resistência às Drogas e à Violência (PROERD), junto a seus ex-alunos no Vale do Aço.** Monografia apresentada à Fundação João Pinheiro e à Academia de Polícia

Militar, como requisito parcial de aprovação ao Curso de Especialização em Segurança Pública, Belo Horizonte, 2007.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de pesquisa.** Porto Alegre: UFRGS, 2009.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa.** São Paulo. Editora Atlas, 2002.

GONÇALVES, Victor Eduardo R**. Curso de direito penal: parte especial. v.2.** São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786553622685. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553622685/. Acesso em: 12 nov. 2022.

GONÇALVES, Victor Eduardo R.; LENZA, Pedro**. Esquematizado - Direito Penal - Parte Especial.** São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786555597738. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555597738/. Acesso em: 12 nov. 2022.

GRECO, Rogério. **Curso de direito penal: parte geral, volume I**. 19. ed. Niterói: Impetus, 2017.

GRECO, Rogério. **Curso de Direito Penal - Vol. 2.** São Paulo: Grupo GEN, 2022. E-book. ISBN 9786559771462. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771462/. Acesso em: 12 nov. 2022.

JESUS, Damásio D.; MILAGRE, José A. **Manual de crimes informáticos.** São Paulo: Editora Saraiva, 2016. E-book. ISBN 9788502627246. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 13 nov. 2022.

JESUS, Damásio Evangelista D.; OLIVEIRA, José Antônio M. Milagre D. **Marco Civil da *Internet*: comentários à Lei n. 12.965, de 23 de abril de 2014, 1ª Edição.** São Paulo: Editora Saraiva, 2014. E-book. ISBN 9788502203200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502203200/. Acesso em: 14 nov. 2022.

KUNRATH, Cristina. **A expansão da criminalidade no cyberespaço.** 2014. Dissertação (Mestre em Direito) – Universidade Federal da Bahia, Faculdade de Direito, Universidade Estadual de Feira de Santana, 2015. Disponível em: http://www.progesp.ufba.br/sites/progesp.ufba.br/files/dissertacao-final-josefacristina-tomaz-martins-kunrath-2014.pdf. Acesso em: 15 nov. 2022.

MARCONDES, José Sérgio. **Triângulo do Crime: O que é? Origem, Elementos – Teoria do Crime.** *Blog* Gestão de Segurança Privada, 2015. Disponível em: https://gestaodesegurancaprivada.com.br/triangulo-do-crime-seguranca-fisica/. Acesso em: 14

nov. 2022.

MIRABETE, Júlio F. **Manual de Direito Penal - Parte Especial - Vol. 2.** São Paulo: Grupo GEN, 2021. E-book. ISBN 9788597028010. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597028010/. Acesso em: 12 nov. 2022.

NUCCI, Guilherme de S. **Curso de Direito Penal: Parte Especial. Arts. 121 a 212 do Código Penal. v.2.** Rio de Janeiro: Grupo GEN, 2022. E-book. ISBN 9786559643721. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559643721/. Acesso em: 12 nov. 2022.

OLIVEIRA, Bruno; ZANATTA, Pedro. **7 em cada 10 transações bancárias no país são feitas por canais digitais, mostra Febraban.** CNN Brasil, 2022. Disponível em: https://www.cnnbrasil.com.br/business/sete-em-cada-dez-transacoes-bancarias-no-pais-sao-feitas-por-canais-digitais-mostra-pesquisa/. Acesso em: 14 nov. 2022.

PROFISSÃO REPÓRTER**. Crimes virtuais crescem no Brasil; veja flagrante e histórias de vítimas com o Profissão Repórter.** G1, 2022. Disponível em: https://g1.globo.com/profissao-reporter/noticia/2022/07/27/crimes-virtuais-crescem-no-brasil-veja-flagrante-e-historias-de-vitimas-com-o-profissao-reporter.ghtml. Acesso em: 13 nov. 2022.

PINHEIRO, Patrícia P. **Direito Digital**. São Paulo: Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 28 abr. 2023.

SANTOS, Liara Ruff dos et. al. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo.** Santa Maria, 2017. Disponível em: http://coral.ufsm.br/congressodireito/anais/2017/7-7.pdf. Acesso em: 12 nov. 2022.

SILVA, Victor H. **Em 2021, 28 milhões de pessoas no Brasil não usaram a *internet*, diz IBGE.** G1, 2022. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/09/16/em-2021-28-milhoes-de-pessoas-no-brasil-nao-usaram-a-internet-diz-ibge.ghtml. Acesso em: 13 nov. 2022.

SOUSA, Rafaela. **Educação.** Brasil Escola, 2021. Disponível em: https://brasilescola.uol.com.br/educacao. Acesso em: 13 nov. 2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação.** 2 ed. Rio de Janeiro: Brasport, 2013.