Discussões jurídicas acerca do estelionato virtual: evolução, características e combate[1]

Carlos Henrique Bassani de Oliveira[2]
Carolina Goulart[3]

Resumo: O presente artigo tem como objetivo analisar os delitos praticados no ambiente virtual, com especial atenção para o estelionato digital. A pesquisa investiga os principais métodos empregados por criminosos online, os quais frequentemente se utilizam de diversos sites e redes sociais, aproveitando-se do constante crescimento de usuários nesses espaços. Além disso, realiza-se uma análise detalhada do crime de estelionato, suas características jurídicas e sua evolução para o meio virtual, especialmente durante o período pandêmico, quando houve um aumento significativo dessas práticas. O estudo também aborda a complexidade da elucidação desses crimes, devido à dificuldade na obtenção de provas durante as investigações policiais, ressaltando a importância da prevenção como a melhor forma de combate. Assim, esta pesquisa busca contribuir para um maior entendimento sobre o delito de estelionato virtual, evolução em números e características jurídicas, buscando o desenvolvimento de estratégias eficazes de prevenção e combate a esse crime.

Palavras-chave: Crimes cibernéticos. Crimes digitais. Estelionato digital. Estelionato virtual.

INTRODUÇÃO

Além do aumento do número de crimes virtuais, a pandemia de Covid-19 também exacerbou outras vulnerabilidades, como a falta de familiaridade de muitas pessoas com as práticas de segurança online e o aumento da dependência de transações financeiras realizadas digitalmente. Isso criou um ambiente propício para a proliferação de esquemas fraudulentos, nos quais os criminosos se aproveitam da ingenuidade, fragilidade ou da distração das vítimas para obter informações pessoais ou financeiras.

Existem inúmeras formas de estelionato virtual, uma das formas mais comuns é o *phishing*, no qual os criminosos enviam mensagens de e-mail ou texto que parecem legítimas, mas na verdade são projetadas para enganar as pessoas a compartilhar informações confidenciais, como senhas ou números de cartão de crédito. Outras táticas incluem a criação de sites falsos que imitam empresas legítimas, a oferta de produtos ou serviços inexistentes e a solicitação de pagamentos adiantados para ganhos fictícios.

A dificuldade em rastrear a identidade dos criminosos virtuais e a falta de legislação específica para lidar com esses crimes representam desafios significativos para as autoridades encarregadas da aplicação da lei. Muitas vezes, os criminosos operam de forma anônima por

---

[1] Artigo científico produzido como requisito obrigatório para conclusão do curso de Direito da Faculdade de Direito da Universidade de Passo Fundo/RS, nos anos de 2023 e 2024.

[2] Acadêmico do Curso de Direito da Faculdade de Direito da Universidade de Passo Fundo – UPF, Campus Soledade. E-mail: 185073@upf.br.

[3] Mestra em Direito pela Universidade de Passo Fundo e Professora da Graduação do curso de Direito na Universidade de Passo Fundo, RS, Brasil. E-mail: carolinagoulart@upf.br.

meio de redes de computadores distribuídas em todo o mundo, dificultando a identificação e a localização de suas atividades.

Além disso, a natureza transnacional da internet e das comunicações digitais torna complicada a atribuição de jurisdição e a coordenação entre as autoridades de diferentes países. Isso muitas vezes resulta em lacunas na aplicação da lei e na impunidade dos perpetradores, incentivando ainda mais a prática de crimes virtuais.

A Lei n° 14.155, promulgada em 2021, é um passo importante na direção certa para combater o estelionato virtual, fornecendo às autoridades brasileiras ferramentas legais mais robustas para investigar e processar os criminosos cibernéticos. No entanto, é necessário um esforço contínuo para fortalecer a cooperação internacional, melhorar a capacidade de resposta das autoridades e educar o público sobre os riscos associados ao uso da tecnologia (Brasil, 2021).

Por meio de uma abordagem multifacetada que combina legislação adequada, cooperação internacional e conscientização pública, pode-se trabalhar para mitigar os riscos do estelionato virtual e proteger os indivíduos contra suas consequências prejudiciais.

Ainda, é crucial reconhecer que o avanço tecnológico continuará a apresentar novos desafios e oportunidades para os criminosos virtuais. Com a rápida evolução das tecnologias digitais, como inteligência artificial e bancos de dados online, os estelionatários estão encontrando maneiras cada vez mais sofisticadas de burlar as defesas e enganar os usuários.

Essa complexidade adicional dificulta ainda mais a detecção e prevenção do estelionato virtual, exigindo uma resposta ágil e adaptável por parte das autoridades e da sociedade em geral. Portanto, é essencial investir em pesquisa e desenvolvimento de tecnologias de segurança, bem como promover a educação contínua sobre segurança cibernética, a fim de enfrentar esses desafios em constante evolução e manter a segurança digital de todos os cidadãos.

1 ESTELIONATO VIRTUAL E SUAS CARACTERÍSTICAS JURÍDICAS

O estelionato é classificado como um crime contra o patrimônio, enquadrado no capítulo VI que aborda o estelionato e outras formas de fraude. Esse delito é descrito no artigo 171 do Código Penal, cujo teor é o seguinte:

> 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).

A origem do termo "estelionato" remonta à palavra grega "*stelio*", que descreve um lagarto capaz de mudar de cor para enganar suas presas. Essa analogia é bastante ilustrativa, pois, no contexto deste crime, a ação típica do criminoso envolve induzir a vítima ao erro, fazendo uso de artifícios fraudulentos para alcançar seu objetivo, que é a obtenção de uma vantagem ilícita, seja para benefício próprio ou de terceiros. O estelionato é classificado como um delito patrimonial que não envolve violência ou ameaça grave, mas sim manipulação por meio de métodos fraudulentos, com o intuito de atingir a integridade do patrimônio alheio (Rodrigues, 2010).

Em resumo, a configuração do crime de estelionato exige quatro elementos essenciais: a obtenção de vantagem ilícita, a causação de prejuízo a outra pessoa, o uso de artifícios ou artimanhas pelo agente e a demonstração clara da intenção do agente de enganar ou induzir a vítima ao erro, de forma a distorcer a percepção dos fatos. No estelionato, o agente manipula, engana e ilude a vítima de tal maneira que ela voluntariamente entrega bens ou objetos, acreditando erroneamente que o estelionatário age de boa-fé (Rodrigues, 2010).

No que diz respeito à expressão "vantagem ilícita", Capez (2020) esclarece que ela se refere ao objetivo material do crime, e se o agente busca uma vantagem legítima, sua conduta é enquadrada como exercício arbitrário das próprias razões, um delito definido no artigo 345 do Código Penal:

> Art. 345 - Fazer justiça pelas próprias mãos, para satisfazer pretensão, embora legítima, salvo quando a lei o permite:
> Pena - detenção, de quinze dias a um mês, ou multa, além da pena correspondente à violência.
> Parágrafo único - Se não há emprego de violência, somente se procede mediante queixa. (Brasil, 1940).

Segundo o artigo 171 do Código Penal, o estelionato pode ser cometido por meio de artifícios, ardil ou qualquer outro meio fraudulento. Em relação ao termo "artifício", o renomado doutrinador Júlio Fabbrini Mirabete oferece a seguinte explicação:

> O artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc. (Mirabete, 2021, p. 325).

Segundo Ataíde (2017), “os crimes virtuais, em síntese, são ataques criminosos em que o autor realiza o ato ilícito por meio de um ambiente virtual, utilizando-se de equipamentos eletrônicos e acesso à rede”. Pode-se afirmar, de forma inicial, que o estelionato virtual é o

crime em que determinado criminoso, utilizando-se da internet, pratica, em seu benefício ou no benefício de outrem, mas em prejuízo alheio, a atitude de induzir ou manter determinada pessoa em erro, utilizando-se de meios fraudulentos e almejando vantagem econômica ilícita.

Diante disso, destaca-se a importância de compreender e enfrentar os crimes virtuais, uma vez que representam uma ameaça significativa para a segurança e o bem-estar das pessoas na era digital. É fundamental também estar ciente dos riscos e adotar medidas de proteção, como o uso de sistemas de segurança atualizados. Além disso, é crucial que sejam desenvolvidas medidas de conscientização, leis e regulamentos eficazes para responsabilizar os criminosos cibernéticos e promover um ambiente online mais seguro para todos (Ataíde, 2017).

Destaca-se que recentemente o crime de estelionato, previsto no art. 171 do Código Penal, foi alterado pela Lei n° 14.155/2021, a qual introduziu nos § 2°-A e 2°-B a figura da "fraude eletrônica". Conforme Andreucci (2021), essa mudança trouxe maior severidade na punição quando se tratar de crimes de violação de dispositivo informático, furto e estelionato cometidos por meio eletrônico ou pela internet.

A ênfase dada aos crimes de violação de dispositivo informático, furto e estelionato cometidos por meios eletrônicos ou pela internet sugere que essas condutas são consideradas especialmente danosas e merecem uma punição mais rigorosa. Isso provavelmente está relacionado à complexidade e ao alcance desses delitos, que muitas vezes envolvem o acesso indevido a informações pessoais, financeiras ou confidenciais das vítimas, resultando em prejuízos significativos (Monteiro, 2019).

Ao introduzir maior severidade na punição para esses casos, a Lei n° 14.155/2021 busca desencorajar a prática desses crimes e proteger os cidadãos contra as fraudes eletrônicas. É importante notar que a atualização legislativa reflete a necessidade de adaptar a legislação aos desafios impostos pelas novas tecnologias e de fornecer uma resposta adequada a um tipo de crime em constante evolução (Monteiro, 2019).

Na visão de Pereira (2023), visando responder à altura do dano causado pelos criminosos virtuais, a novíssima Lei criou a qualificadora, § 2º-A, do artigo 171 do Código Penal:

> § 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)

Estabelecendo uma pena de reclusão de 4 (quatro) a 8 (oito) anos, além de 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.

O legislador, ao incluir ao final da qualificadora a frase "qualquer outro meio fraudulento análogo", visa abranger todo e qualquer novo tipo de golpe, aplicado pelos estelionatários, que a cada dia evoluem em seu *modus operandi*.

Conforme exarado em nota, o Supremo Tribunal Federal, faz uso do conceito jurídico de *modus operandi*, adotando o seguinte significado: "Maneira de agir, operar ou executar uma atividade seguindo os mesmos procedimentos" (STF, 2024).

A pena de reclusão, aliada à aplicação de multa, demonstra a intenção de impor uma sanção proporcional à gravidade desses crimes e ao dano causado às vítimas. A ampla abrangência das condutas fraudulentas mencionadas, como o uso de informações obtidas por meio de redes sociais, contatos telefônicos e correio eletrônico fraudulento, ou qualquer outro meio fraudulento análogo, visa garantir que diferentes formas de fraude sejam abarcadas pela legislação.

Como se observa, a pena em abstrato da nova qualificadora não permite a concessão do benefício das medidas despenalizadoras da Lei nº 9.099/95, nem mesmo a suspensão condicional do processo, conforme previsto no artigo 89 da Lei dos Juizados Especiais. Não se pode cogitar, a propositura do Acordo de Não Persecução Criminal, conforme estabelecido no artigo 28-A do Código de Processo Penal, com redação dada pelo Pacote Anticrime. Essa ferramenta, introduzida em 2020, é cabível apenas na modalidade simples do estelionato, entretanto, com a qualificadora não é possível a aplicação dessa medida alternativa ao não ser o processo judicial.

Com a entrada em vigor da lei 13.964/19, conhecido como Pacote Anticrime, o crime de estelionato foi alterado para crime de ação pública condicionada à representação da vítima, exceto nos casos descritos no §5º:

> § 5º Somente se procede mediante representação, salvo se a vítima for: (Incluído pela Lei nº 13.964, de 2019)
>
> I - a Administração Pública, direta ou indireta; (Incluído pela Lei nº 13.964, de 2019)
> II - criança ou adolescente; (Incluído pela Lei nº 13.964, de 2019)
> III - pessoa com deficiência mental; ou (Incluído pela Lei nº 13.964, de 2019)
> IV - maior de 70 (setenta) anos de idade ou incapaz. (Incluído pela Lei nº 13.964, de 2019)

A representação e ação penal no contexto do estelionato virtual são aspectos fundamentais para garantir a responsabilização dos criminosos e a aplicação da lei. A representação é o ato pelo qual a vítima expõe o desejo à autoridade policial durante o registro da ocorrência do crime, solicitando a instauração do procedimento investigatório. No caso do estelionato virtual, muitas vezes a vítima pode não ter pleno conhecimento de que foi enganada até que ocorra algum prejuízo tangível, como a realização de transações financeiras fraudulentas ou a divulgação indevida de informações pessoais. Portanto, é essencial que as autoridades incentivem a denúncia e ofereçam canais acessíveis para que as vítimas possam reportar os crimes e optar pela representação.

Após a norma inserida no § 5º do art. 171 do Código Penal pela Lei 13.964/2019, trazendo a necessidade de representação da pessoa ofendida no crime de estelionato, a qual foi aplicada a todos processos em curso, conforme jurisprudência do egrégio Superior Tribunal Federal, durante julgamento no agravo regimental, com votos da segunda turma[4].

Após a representação, a autoridade policial expede a portaria para proceder com a investigação do crime, sendo o andamento, por meio de Inquérito Policial. Isso envolve a coleta de evidências, como registros de acesso a sistemas eletrônicos, análise de comunicações eletrônicas, extratos das movimentações bancárias e identificação de possíveis suspeitos, para fins de apuração de autoria e materialidade. No entanto, investigar crimes cibernéticos pode ser desafiador devido à natureza complexa e transnacional desses delitos, exigindo cooperação internacional e expertise técnica especializada (Brasil, 2017).

Uma vez reunidas as evidências suficientes, o Ministério Público tem a prerrogativa de oferecer a denúncia contra os acusados, dando início à ação penal. Nesse momento, é crucial que os promotores estejam bem informados sobre as leis e regulamentos relacionados a crimes cibernéticos e possuam o conhecimento necessário para apresentar um caso sólido em juízo.

---

[4] Agravo regimental no recurso extraordinário com agravo. 2. Direito Penal e Processual Penal. 3. Estelionato. 4. Art. 171, caput, c/c os Arts. 29 e 71, todos do Código Penal. 5. Em conformidade com a jurisprudência do Supremo Tribunal Federal sedimentada na interpretação de modificações semelhantes anteriormente realizadas pela Lei 9.099/1995, a norma inserida no § 5º do art. 171 do Código Penal pela Lei 13.964/2019 (necessidade de representação da pessoa ofendida no crime de estelionato) deve ser aplicada a processos em curso, ou seja, ainda não transitados em julgado quando da entrada em vigor da citada Lei 13.964/2019. 6. Em analogia ao art. 91 da Lei 9.099/1995, deve-se intimar a vítima para que, no prazo de 30 dias, ofereça, se quiser, a representação, sob pena de decadência. 7. No caso, não houve inequívoca manifestação de vontade da vítima, perante o Juízo de origem, no sentido do interesse na persecução criminal, nos termos dos precedentes desta Segunda Turma, sendo ainda certo que não existiu intimação judicial para esse fim. 8. Precedentes. 9. Agravo regimental não provido. (STF - ARE: 1.370.525 - PR, Relator: GILMAR MENDES, Data de Julgamento: 13/12/2022, Segunda Turma, Data de Publicação: PROCESSO ELETRÔNICO, PUBLIC 06-01-2023)

Durante o processo penal, é importante que as vítimas sejam devidamente assistidas e informadas sobre o andamento do caso. Além disso, é essencial que haja uma coordenação eficaz entre as autoridades sendo a Polícia Judiciária, o Ministério Público e o Poder Judiciário necessários para garantir uma resposta rápida e eficaz aos crimes virtuais (Ferraz, 2015).

Em suma, a apuração e ação penal desempenham um papel crucial na responsabilização dos autores de estelionato virtual e na proteção da sociedade contra esses crimes. É necessário um esforço conjunto e coordenado entre todas as partes envolvidas para enfrentar os desafios apresentados pela crescente complexidade do cenário cibernético e garantir a aplicação efetiva da lei (Ferraz, 2015).

Além das medidas legais e judiciais discutidas anteriormente, é crucial também investir em educação e conscientização da população sobre os riscos do estelionato virtual. Promover campanhas de segurança cibernética e fornecer orientações claras sobre como identificar e evitar golpes online podem ajudar a reduzir o número de vítimas desses crimes.

Ainda assim, é importante incentivar o desenvolvimento de habilidades digitais, capacitando as pessoas a protegerem suas informações pessoais e financeiras de forma mais eficaz. Essa abordagem preventiva, combinada com a aplicação rigorosa da lei e a cooperação entre os setores público e privado, pode contribuir significativamente para mitigar os impactos negativos do estelionato virtual e construir um ambiente digital mais seguro e resiliente para todos.

2 A INTERNET E O CRIME: A EVOLUÇÃO DO ESTELIONATO DIGITAL

Para o Juiz Barbagalo (2022), a inovação legislativa chegou com algum atraso, pois as condutas que se enquadram em sua definição, assim como as equivalentes ao furto mediante fraude eletrônica, causam intranquilidade há algum tempo. Sendo necessária discussão e aperfeiçoamento da lei penal em relação ao crime de Estelionato Virtual e até mesmo outros crimes, que tanto causam prejuízos à população.

A opinião expressa pelo juiz é de que a inovação legislativa chegou com atraso, pois as condutas abrangidas pela nova qualificadora, assim como os equivalentes ao furto mediante fraude eletrônica, têm causado intranquilidade por um período significativo. Essa observação indica que, na visão do juiz, o problema dos crimes de estelionato virtual e outros delitos similares não foi abordado de forma adequada anteriormente, o que resultou em prejuízos para a população (Barbagalo, 2022).

Essa posição destaca a importância de uma discussão e aperfeiçoamento da legislação penal em relação aos crimes cibernéticos, especialmente o estelionato virtual. Reconhece-se a necessidade de atualizar a lei para lidar com as complexidades e desafios trazidos pelo avanço tecnológico e as consequências desses crimes para a sociedade (Barbagalo, 2022).

O Brasil passou a tratar e se preocupar com o tema nas últimas duas décadas. Hoje, o país é o quarto do mundo com o maior número de ameaças virtuais. A web permite que os criminosos tenham acesso a muitas vítimas, logo, estamos a falar da escalabilidade do crime virtual, o que se torna cada vez mais comum. Além disso, técnicas são utilizadas e hackers recrutados para ocultar atividades de criminosos. As invasões às estruturas críticas dos países crescem a ritmo inimaginável e no Brasil não é diferente (Araújo; Maia, 2019).

Enquanto no Brasil pouco se faz em termos de estrutura investigativa, nos Estados Unidos o FBI convoca especialistas em segurança para o que anuncia ser uma "Guerra Cibernética", já que o crime informático estaria se tornando uma ameaça maior do que o próprio terrorismo. Crime informático não é apenas uma questão de segurança pública, mas também de defesa nacional (Araújo; Maia, 2019).

Quando tratamos da macrocriminalidade, o Brasil se destaca como o quarto principal alvo dos crackers em ataques de *phishing* (roubo de senhas) no mundo, figurando entre os cinco países com mais empresas hackeadas. Estima-se que cerca de 38 milhões de usuários tenham sido lesados (Araújo; Maia, 2019).

A sociabilidade do brasileiro pode ser identificada como propiciadora dos crimes digitais, especialmente em uma era marcada por aplicativos falsos, que muitas vezes não são verificados pelos usuários antes da instalação. E o risco aumenta, uma vez que os cibercriminosos passam a focar na Internet das Coisas, como TVs, geladeiras e carros conectados. Cinquenta e sete por cento dos usuários de smartphones brasileiros foram vítimas de crime virtual móvel (Gonzaga, 2013).

De outra banda, é evidente o aumento dos crimes de estelionato, em sua maioria na forma virtual, diante da mudança e globalização que a pandemia trouxe, em especial o salto de conectividade durante o ano de 2020. Conforme demonstrado pelos dados oficiais da Secretaria de Segurança Pública do Estado do Rio Grande do Sul, de forma evolutiva, comparando a elevação do crime de estelionato com outros delitos, como roubo e roubo de veículo. Os dados são oficiais e tornados públicos pela própria Secretaria de Segurança Pública do RS, atualizados em 2024, em forma de tabelas:

Tabela 1[5] – Indicadores criminais do RS em 2018

Secretaria da Segurança Pública - Departamento de Planejamento e Integração - Observatório Estadual de Segurança Pública

Ocorrências de crimes consumados, no Rio Grande do Sul, no período de 01 de janeiro a 31 de Dezembro de 2018

Mês / Ocorrências	Roubos	Roubo de Veículo	Estelionato
2018/Jan	6.722	1.579	2.058
2018/Fev	6.029	1.426	1.796
2018/Mar	6.249	1.642	1.985
2018/Abr	6.244	1.486	1.836
2018/Mai	6.162	1.275	1.934
2018/Jun	6.221	1.366	1.864
2018/Jul	6.345	1.289	2.016
2018/Ago	6.434	1.280	2.138
2018/Set	5.778	1.201	1.857
2018/Out	6.368	1.366	2.206
2018/Nov	5.408	1.206	2.282
2018/Dez	4.825	1.005	2.087
Total	**72.785**	**16.121**	**24.059**

Fonte: SIP/PROCERGS - Atualizado em 06 de fevereiro de 2024.

Fonte: SSP-RS, 2024.

No ano de 2018 os números dos crimes de roubo e roubo de veículos foram exorbitantemente maiores quando comparados ao delito de estelionato. Evidencia-se que os criminosos cometiam em sua maioria o crime violento, ao invés de utilizar-se da forma ardilosa trazida pelo ramo do estelionato.

Tabela 2[6] – Indicadores criminais do RS em 2019

Secretaria da Segurança Pública - Departamento de Planejamento e Integração - Observatório Estadual de Segurança Pública

Ocorrências de crimes consumados, no Rio Grande do Sul, no período de 01 de janeiro a 31 de Dezembro de 2019

Mês / Ocorrências	Roubos	Roubo de Veículo	Estelionato
2019/Jan	5.765	1.203	2.410
2019/Fev	5.677	1.104	2.206
2019/Mar	5.711	957	2.197
2019/Abr	5.844	1.011	2.308
2019/Mai	6.291	906	2.510
2019/Jun	5.619	865	2.197
2019/Jul	5.575	868	2.474
2019/Ago	5.850	922	2.386
2019/Set	5.092	824	2.351
2019/Out	5.227	808	2.801
2019/Nov	4.905	832	2.708
2019/Dez	4.506	827	2.746
Total	**66.062**	**11.127**	**29.294**

Fonte: SIP/PROCERGS - Atualizado em 05 de janeiro de 2024.

Fonte: SSP-RS, 2024.

[5]Dados ano de 2018, fornecidos pela SSP-RS, Secretaria de Segurança Pública. Rio Grande do Sul. Indicadores Criminais. Disponível em: https://ssp.rs.gov.br/indicadores-criminais Acesso em: 15 de junho de 2024.

[6] Dados ano de 2019, fornecidos pela SSP-RS, Secretaria de Segurança Pública. Rio Grande do Sul. Indicadores Criminais. Disponível em: https://ssp.rs.gov.br/indicadores-criminais Acesso em: 15 de junho de 2024.

Em dados no ano de 2019, conforme números oficias divulgados pela Secretaria de Segurança Pública do Rio Grande do Sul, nota-se diminuição e início de mudança no cometimento dos crimes violentos, para o crime fraudulento.

Nesse viés, Rafael Alcadipani, especialista em segurança pública, diz o seguinte: “O criminoso sempre vai buscar o maior lucro com o menor risco. O estelionato é um crime que depende de representação, a pessoa tem que ir lá e decidir que quer denunciar a pessoa.” As penas não são tão altas quanto um roubo (Miranda, 2023).

Tabela 3[7] – Indicadores criminais do RS em 2020

Secretaria da Segurança Pública - Departamento de Planejamento e Integração - Observatório Estadual de Segurança Pública

Ocorrências de crimes consumados, no Rio Grande do Sul, no período de 01 de janeiro a 31 de Dezembro de 2020

Mês / Ocorrências	Roubos	Roubo de Veículo	Estelionato
2020/Jan	5.515	902	3.294
2020/Fev	5.190	906	3.000
2020/Mar	4.783	866	3.364
2020/Abr	2.880	804	4.301
2020/Mai	3.438	719	5.308
2020/Jun	3.673	671	7.249
2020/Jul	3.666	637	6.636
2020/Ago	3.593	536	6.218
2020/Set	3.421	502	7.556
2020/Out	3.767	480	7.291
2020/Nov	3.526	376	6.967
2020/Dez	3.372	488	6.548
Total	**46.824**	**7.887**	**67.732**

Fonte: SIP/PROCERGS - Atualizado em 04 de dezembro de 2023.

Fonte: SSP-RS, 2024.

Ao analisar os dados de 2020, ano onde se deu início a pandemia de COVID-19, nota-se o aumento exponencial do crime de estelionato, sendo em sua esmagadora maioria na forma digital, em comparação com os crimes de roubo e roubo de veículo, os quais tiveram queda significativa. Os números do crime de estelionato mais que dobraram.

Durante a pandemia global do COVID-19, foram emitidas recomendações pela Organização Mundial de Saúde (OMS), abarcando diversos países que sofreram pelas políticas públicas de *lockdown*, ou seja, uma espécie de confinamento domiciliar com o intuito de desacelerar a propagação do vírus. Consequentemente, a população teve que adaptar suas relações sociais, educacionais e de trabalho à nova realidade, fato pelo qual aumentou muito o fluxo de pessoas que passaram a acessar a internet (Miranda, 2023).

[7] Dados ano de 2020, fornecidos pela SSP-RS, Secretaria de Segurança Pública. Rio Grande do Sul. Indicadores Criminais. Disponível em: https://ssp.rs.gov.br/indicadores-criminais Acesso em: 15 de junho de 2024.

Tabela 4[8] – Indicadores criminais do RS em 2023

Secretaria da Segurança Pública - Departamento de Planejamento e Integração - Observatório Estadual de Segurança Pública

Ocorrências de crimes consumados, no Rio Grande do Sul, no período de 01 de janeiro a 31 de dezembro de 2023

Mês / Ocorrências	Roubos	Roubo de Veículo	Estelionato
2023/Jan	2.974	358	7.558
2023/Fev	2.627	323	6.934
2023/Mar	3.095	409	8.417
2023/Abr	2.972	327	7.290
2023/Mai	3.206	314	8.261
2023/Jun	2.672	299	7.381
2023/Jul	2.767	255	7.333
2023/Ago	2.805	285	6.958
2023/Set	2.557	276	6.663
2023/Out	2.509	262	7.632
2023/Nov	2.181	248	7.443
2023/Dez	2.111	236	6.699
Total	**32.476**	**3.592**	**88.569**

Fonte: PROCERGS/OESP - Atualizado em 03 de junho de 2024.

Fonte: SSP-RS, 2024.

Em último comparativo, vê-se um salto exponencial gigantesco em relação ao ano de 2019, tendo o crescimento de cerca de 300% dos crimes de estelionatos, reportado as autoridades policiais.

Nota-se que no ano de 2021 entrou em vigor a lei 14.155, a qual traz o §2-A, acrescentado ao delito de estelionato. Essa adequação legislativa majora a pena base por considerar mais gravosa a conduta que utiliza do ambiente virtual para consumação, visto que essa prática dificulta a defesa da vítima, e ainda, oferece obstáculos para a investigação policial, já que o criminoso pode estar em qualquer local do globo.

Dessa forma, observa-se a tentativa da legislação brasileira em se adequar ás transformações tecnológicas ao impor maior rigidez legislativa ao crime de estelionato, todavia, ainda há muito a ser feito, visto que, principalmente após a pandemia do COVID-19, os casos de golpes virtuais cresceram exponencialmente, sendo que os criminosos continuam encontrando brechas para praticarem seus atos ilícitos, conforme demonstrado na tabela supracitada, com os dados do ano de 2023.

É clara a permissibilidade que o ambiente virtual traz para a prática de crimes cibernéticos, onde as características dessa modalidade criminosa, como o anonimato dos infratores, propiciam sua impunidade. Todavia, o Estado deve estar preparado para garantir a

[8] Dados ano de 2023, fornecidos pela SSP-RS, Secretaria de Segurança Pública. Rio Grande do Sul. Indicadores Criminais. Disponível em: https://ssp.rs.gov.br/indicadores-criminais Acesso em: 15 de junho de 2024.

eficácia de seus dispositivos legislativos, a fim de promover a paz dos indivíduos ofendidos (FELIX, NASCIMENTO, 2023).

A urgência em fortalecer não apenas a legislação, mas também a conscientização pública e a segurança digital são evidentes. A capacitação, tanto dos indivíduos quanto das instituições, para reconhecer, prevenir e responder às ameaças cibernéticas é fundamental para proteger não apenas os cidadãos, mas também a infraestrutura crítica do país. A colaboração entre os setores público e privado se torna essencial para desenvolver estratégias eficazes na luta contra os crimes digitais e na promoção de um ambiente online mais seguro e protegido (Gonzaga, 2013).

O Brasil é frequentemente citado em debates sobre atividades cibernéticas, dada a sua vasta população e o aumento do acesso à tecnologia. Contudo, estabelecer sua posição precisa em um "ranking" de países com maior número de hackers é uma tarefa difícil, devido à clandestinidade dessas atividades e à escassez de dados precisos sobre o tema (Kurtz, 2024).

No Brasil, existe uma comunidade de segurança cibernética dinâmica, abrangendo tanto profissionais legítimos quanto indivíduos envolvidos em atividades maliciosas. Algumas estimativas indicam que o país pode possuir uma presença notável na cena cibernética global, tanto em termos de hackers éticos quanto de criminosos cibernéticos (Kurtz, 2024).

Embora o Brasil não receba a mesma atenção que os Estados Unidos, Rússia ou China nas discussões sobre cibersegurança, ainda pode desempenhar um papel relevante no cenário cibernético global. Como em muitos outros países, as autoridades brasileiras enfrentam desafios significativos na prevenção e combate às atividades cibernéticas ilegais, incluindo o estelionato virtual. Isso ressalta a importância de investir em medidas eficazes de segurança cibernética e cooperação internacional para enfrentar essas ameaças (Kurtz, 2024).

O panorama atual da situação do estelionato virtual, sob a perspectiva da lei, revela um desafio crescente para as autoridades e legisladores. O avanço tecnológico tem proporcionado novas oportunidades para criminosos, que exploram as vulnerabilidades do mundo digital para cometer fraudes e enganar indivíduos desprevenidos. Diante desse cenário, as leis precisam acompanhar de perto as mudanças no ambiente online, buscando manter-se atualizadas e eficazes na prevenção e punição do estelionato virtual (Ataíde, 2017).

A complexidade do estelionato virtual torna essencial a colaboração entre diferentes jurisdições e setores. Muitas vezes, os criminosos operam em âmbito internacional, desafiando as fronteiras tradicionais da aplicação da lei. A cooperação internacional é crucial para a criação de estratégias eficazes de combate ao crime virtual, garantindo que as legislações possam ser aplicadas de maneira efetiva em escala global (Kurtz, 2024).

Além disso, é fundamental que as leis abordem não apenas as consequências do estelionato virtual, mas também os meios pelos quais esses crimes são perpetrados. Isso envolve a definição clara de práticas ilegais, a identificação de lacunas nas leis existentes e a implementação de medidas proativas para prevenir esses tipos de delitos. A sensibilização da população sobre as ameaças online também desempenha um papel crucial na prevenção do estelionato virtual, destacando a importância da educação jurídica e da conscientização digital (Andreucci, 2021).

Ademais, a velocidade com que novas tecnologias emergem exige uma abordagem dinâmica por parte da legislação. As leis precisam ser flexíveis o suficiente para se adaptarem às mudanças rápidas no cenário tecnológico, garantindo que os esforços de prevenção e repressão não fiquem obsoletos diante de inovações criminosas. Incentivar a pesquisa e o desenvolvimento de tecnologias de segurança também se mostra essencial para enfrentar os desafios impostos pelo estelionato virtual (Andreucci, 2021).

A punição efetiva dos criminosos é outra faceta crucial da abordagem legal ao estelionato virtual. A imposição de penas significativas e a aplicação consistente da lei enviam um sinal claro de que tais práticas são inaceitáveis e resultarão em consequências severas. Além disso, a criação de unidades especializadas e o treinamento adequado para profissionais da aplicação da lei são passos importantes para garantir que as investigações sejam conduzidas de maneira eficiente e justa (Andreucci, 2021).

Os crimes de estelionato virtual continuaram a representar uma ameaça significativa em 2023, com um aumento preocupante de incidentes relatados em várias partes do mundo. De acordo com relatórios preliminares, muitos países viram um aumento de até 25% nos casos de fraudes online em comparação com o ano anterior. Esses números alarmantes refletem não apenas a sofisticação crescente dos golpes cibernéticos, mas também a vulnerabilidade contínua dos usuários da internet a essas atividades criminosas (Ataíde, 2017).

Além disso, as mudanças no comportamento online dos consumidores, como o aumento das transações financeiras digitais e o uso generalizado de plataformas de comércio eletrônico, contribuíram para a expansão do cenário do crime virtual. A crescente adoção de tecnologias como a inteligência artificial e a *blockchain* pelos estelionatários também tem complicado a detecção e prevenção desses crimes, representando um desafio adicional para as autoridades e instituições reguladoras. Assim, em 2023, apesar dos esforços para fortalecer as leis e intensificar as medidas de segurança cibernética, os crimes de estelionato virtual continuaram a ser uma preocupação premente em todo o mundo (Ataíde, 2017).

Para Fabiana Greve *et al*, em 2018, a *blockchain* é descrevida como:

> Uma tecnologia emergente que oferece suporte distribuído confiável e seguro para realização de transações entre participantes que não necessariamente têm confiança entre si e que estão dispersos em larga escala numa rede P2P. É considerada uma tecnologia disruptiva, pois cria digitalmente uma entidade de confiança descentralizada, eliminando a necessidade de uma terceira parte de confiança. Dessa forma, pode substituir entidades certificadoras e centralizadoras das transações de negócios, tais como bancos, governos, cartórios, etc. O potencial de transformação é imenso e aplicações estão surgindo a partir desta tecnologia em inúmeros setores: finanças, saúde, artes, governo, além da própria computação: protocolos de redes e nuvem.

Entendida como um banco de dados compartilhado e imutável que facilita o processo de registro de transações e rastreamento de ativos em uma rede de negócios, como por exemplo o *Bitcoin, Ethereum*, entre outras moedas virtuais, onde por diversas vezes, os estelionatários fazem o uso para guardas as vantagens indevidas, em razão do sigilo e privacidade que essas moedas trazem aos usuários. Diversos estelionatários utilizam-se da facilidade que possuem em aprender inovações tecnológicas para o aproveitar-se dentro do mundo do crime, em especial atuação sobre pessoas que não possuem tanto conhecimento.

Em suma, o panorama da atual situação do estelionato virtual sob a perspectiva da lei é desafiador, exigindo abordagens inovadoras e colaboração global. A adequação das legislações, a cooperação internacional, a conscientização pública e a punição efetiva são elementos essenciais para construir um ambiente digital mais seguro e proteger os cidadãos contra os riscos do crime cibernético (Ataíde, 2017).

A colaboração entre os setores público e privado, a conscientização da população e a implementação de medidas proativas são fundamentais para enfrentar essa ameaça em constante mutação. À medida que avançamos, é imperativo que as leis se adaptem às rápidas mudanças tecnológicas, garantindo a eficácia das medidas de prevenção, punição e proteção dos cidadãos. O desafio do estelionato virtual transcende fronteiras, exigindo uma abordagem coordenada para mitigar seus efeitos prejudiciais e construir um ambiente digital mais seguro e resiliente para todos.

3 DAS DIFICULDADES PARA A ELUCIDAÇÃO E COMBATE DOS CRIMES VIRTUAIS

O estelionato virtual, uma forma de crime cibernético cada vez mais comum, apresenta uma série de desafios significativos para as autoridades policiais e organizações de segurança cibernética em todo o mundo. Uma das principais dificuldades reside no anonimato e na transnacionalidade dos criminosos envolvidos. Eles operam por meio de uma série de camadas

de proteção, tornando sua identificação e responsabilização bastante difíceis. Além disso, muitos desses criminosos estão situados em jurisdições estrangeiras, o que torna a cooperação internacional essencial, porém complexa (Andreucci, 2021).

Frequentemente, os estelionatários operam por trás de uma cortina de anonimato, utilizando técnicas avançadas de ocultação de identidade e localização, tornando desafiador rastreá-los e responsabilizá-los.

Outro grande obstáculo é a constante evolução das técnicas e tecnologias utilizadas pelos golpistas. Eles estão sempre buscando novas maneiras de explorar vulnerabilidades nos sistemas e nas pessoas, exigindo uma resposta ágil e adaptativa das autoridades e organizações de segurança. A sofisticação das técnicas de ocultação e evasão também é uma questão preocupante, tornando a investigação ainda mais desafiadora (Granucci, 2024).

Além disso, o estelionato virtual muitas vezes envolve grupos criminosos altamente organizados que operam em escala global. Esses grupos podem compartilhar informações e recursos, ampliando o alcance e a complexidade das atividades fraudulentas. Isso destaca a necessidade de uma cooperação internacional eficaz e coordenação entre diferentes agências de aplicação da lei e jurisdições (Granucci, 2024).

Os golpes baseados em engenharia social exploram os padrões de pensamento e comportamento das pessoas, tornando-os extremamente eficazes. Quando um invasor compreende as motivações por trás das ações de um usuário, ele pode enganá-lo e manipulá-lo com sucesso (Granucci, 2024).

Ademais, os hackers aproveitam-se da falta de conhecimento dos usuários. Com o rápido avanço da tecnologia, muitos consumidores e funcionários podem não estar cientes de certas ameaças, como downloads automáticos ou *phishing*. Além disso, os usuários podem subestimar o valor de seus próprios dados pessoais, como números de telefone, e, como resultado, não entendem completamente como proteger a si mesmos e suas informações (Granucci, 2024).

Proteger as vítimas de estelionato virtual também é uma preocupação importante. Muitas vezes, essas vítimas enfrentam não apenas perdas financeiras, mas também consequências emocionais e psicológicas. Portanto, é crucial garantir que existam recursos disponíveis para oferecer suporte às vítimas e ajudá-las a se recuperarem dos danos causados (Silva; Boeri Junior; Pinto, 2023).

É crucial destacar a importância da prevenção na redução do cibercrime, pois sem a devida atenção a essa questão, a tendência é que esses delitos continuem a crescer. Portanto, é essencial promover a conscientização sobre medidas preventivas, fornecendo orientações e

dicas para evitar ataques virtuais. Isso é fundamental para proteger os usuários e impedir que se tornem vítimas de crimes cibernéticos (Silva; Boeri Junior; Pinto, 2023).

Segundo Meireles (2020) é possível identificar algumas dificuldades dos profissionais envolvidos na abordagem deste problema, especialmente em relação à sua competência tecnológica, o que resulta na ineficiência de suas atividades. Além disso, evidencia-se a carência de ferramentas adequadas para investigação, sublinhando a necessidade de os profissionais terem acesso a recursos fornecidos pela instituição para aprimorar seu desempenho.

Identifica-se ainda, desafios relacionados à obtenção de provas criminais por meio da perícia. Para realizar exames, os peritos precisam acessar os dispositivos eletrônicos do agente, porém muitas vezes são limitados a realizar apenas exames indiretos, utilizando aparelhos semelhantes e requerendo autorização da autoridade competente (Meireles, 2020).

Outro desafio importante é a subnotificação e subdenúncia dos casos de estelionato virtual. Muitas vítimas optam por não relatar o crime por falta de conscientização, vergonha ou descrença na eficácia das medidas de resposta. Isso leva a uma subestimação significativa da extensão do problema e dificulta a alocação de recursos para combatê-lo (Ataíde, 2017).

Questões jurisdicionais e legais também complicam a resposta ao estelionato virtual. As diferenças nos sistemas legais entre países podem dificultar a cooperação entre as agências de aplicação da lei, bem como o processo de extradição e julgamento dos criminosos (Martinelli, 2024).

Existe uma vertente de pensamento popular que o sistema judicial brasileiro é insuficiente para o julgamento eficaz do delito de estelionato. Essa afirmação resulta no sentimento de insatisfação popular ante a persecução penal, principalmente em sua fase pré judicial, ou seja, quanto à investigação criminal. Os casos de estelionato no Brasil se tornaram tão frequentes, que as vítimas passaram a se acomodar e em alguns casos, nem se preocupam em procurar as instituições policiais para representarem a favor da apuração criminal (Miranda, 2023).

Tal fato, associado ao excesso de demanda em virtude do aumento do número de casos, contribui para o recrutamento de novos criminosos, o que agrava exponencialmente a situação vivenciada. Dito isso, este tópico abordará sobre os principais obstáculos da investigação criminal para os casos de estelionato digital. (Miranda, 2023).

Os principais obstáculos existentes no combate aos golpes virtuais, deve-se estudar a realidade das instituições policiais brasileiras, principalmente da Polícia Civil, responsável pela investigação criminal e demais diligências iniciais da persecução penal, dentro do Inquérito Policial.

Mesmo diante dessa realidade de sucateamento, com poucos servidores e muita demanda, a Polícia Civil, em especial a gaúcha, atua de forma a reprimir o criminoso ardil, porém, ainda assim, enfrenta alguns obstáculos como as barreiras territoriais, a impessoalidade dos criminosos, a constante evolução dos golpes digitais e a facilidade na abertura de contas laranja em instituições financeiras.

No tocante as barreiras territoriais, para que haja uma troca de informações entre a instituição de um estado para com outro, é necessário a realização de diligências que, assim como as demais ações processuais, são reguladas por prazos que nem sempre são cumpridos. No caso dos crimes de estelionato digital, em que todas as ações são muito dinâmicas, inclusive quanto a transferências de valores, onde rapidamente o dinheiro se perde em meio a diversas transferências bancárias, essa troca de informações entre as policias estaduais deveria ocorrer em uma dinâmica similar a atividade criminosa, caso contrário a eficácia da investigação sofrerá prejuízos (Miranda, 2023).

Enfrentar o cibercrime é uma jornada contínua, uma vez que os criminosos estão sempre aprimorando suas estratégias para atacar sistemas e usuários. Além disso, a aplicação das leis e a investigação desses crimes podem ser dificultadas por desafios técnicos, como a complexidade de rastrear os responsáveis e a falta de recursos e capacitação adequada das autoridades. No entanto, é crucial reconhecer que a existência de regulamentações específicas para lidar com o cibercrime é um passo fundamental para prevenir e punir esses delitos. A conscientização da população sobre os riscos e as práticas de segurança também desempenha um papel vital na diminuição da incidência desses crimes. É importante estar ciente de que a tecnologia e os métodos empregados pelos criminosos cibernéticos estão em constante evolução, o que pode tornar as regulamentações existentes menos eficazes ou até mesmo ultrapassadas em certos casos (Oliveira e Santos, 2023).

Para combater eficazmente o estelionato virtual, são necessárias estratégias abrangentes e coordenadas. Isso inclui a promoção da cooperação internacional entre agências de aplicação da lei, o investimento em tecnologia e capacitação para lidar com ameaças cibernéticas emergentes, a melhoria das leis e mecanismos de coleta de dados e a promoção da conscientização e educação pública sobre os riscos e melhores práticas de segurança cibernética (Martinelli, 2024).

Diante desses desafios multifacetados, é evidente que a luta contra o estelionato virtual requer uma abordagem holística e colaborativa, que envolva não apenas as autoridades policiais e organizações de segurança cibernética, mas também governos, setor privado, instituições financeiras, organizações da sociedade civil e a população em geral. Somente através de uma

cooperação estreita e coordenada em todos os níveis, podemos esperar fazer progressos significativos na redução e prevenção desse tipo de crime cibernético.

CONCLUSÃO

A sociedade está cada vez mais conectada, e as redes sociais desempenham um papel fundamental nessa interação, uma vez que o ser humano sempre teve a necessidade de conviver socialmente. Essas ferramentas estão presentes na vida de muitos brasileiros e, como destacado, tornaram-se também um ambiente propício para a ocorrência de crimes, seja devido à facilidade de acesso ou ao grande número de usuários.

Nesse contexto, é importante observar que a criação de um perfil falso em uma rede social nem sempre é considerada um crime. É necessário que haja uma intenção real de obter algum benefício com essa conduta, pois muitas vezes as pessoas buscam o anonimato para interagir com outros usuários ou simplesmente têm afinidade com figuras públicas. Além disso, quando essa ação se enquadra no crime de falsa identidade, na maioria dos casos, ela é subsumida por um crime mais grave.

Após uma análise das doutrinas e das alterações introduzidas pela Lei n° 14.155/2021, que acrescentou parágrafos ao artigo 171 do Código Penal e estabeleceu novas regras para julgamento, foi possível traçar um panorama do crime de estelionato. Ficou evidente que a prática do estelionato virtual tem se tornado cada vez mais frequente e, devido à pandemia de Covid-19 vivenciada nos últimos dois anos, o número de vítimas aumentou consideravelmente.

Portanto, as modificações introduzidas por essa lei foram de grande importância no combate aos crimes virtuais. No entanto, ainda há desafios significativos na identificação dos criminosos, o que indica a necessidade de revisões legislativas mais abrangentes no Brasil para conter a ocorrência desses delitos. Isso se reflete no fato de que as investigações de crimes virtuais no país frequentemente não alcançam resultados eficazes e substanciais, mesmo após as mudanças legais mencionadas neste artigo.

Dito isso, a fim de frear o crescimento de casos, as instituições financeiras devem estabelecer métodos mais rígidos de comprovação de identidade para abertura de contas bancárias, com o intuito de diminuir a ocorrência de contas de “laranjas”. Outrossim, pode-se instituir prazos mais rígidos de respostas das instituições privadas de ofícios emitidos pelos órgãos legais, no intuito de tornar as investigações da Polícia Civil e Ministério Público mais dinâmicas.

Em resumo, é evidente que a legislação brasileira tem progredido na tipificação dos crimes cibernéticos, mas as sanções ainda são relativamente brandas, e as normas devem continuar evoluindo para desencorajar a prática de crimes virtuais.

Conforme os dados trazidos e exposto, com números fornecidos pela própria Secretaria de Segurança Pública do Estado do Rio Grande do Sul, é evidente que os criminosos iniciaram uma mudança no cometimento de delitos, para um menos com penas mais brandas e que traga menos risco a sua vida, embarcando no mundo ardiloso e fraudulento do delito de estelionato, o qual cresceu exponencialmente durante e após a pandemia. A legislação que entrou em vigor, tornando mais severas as punições que se mostraram positivas, mas também insuficientes, pois evidenciado claramente em dados do ano de 2023, o constante aumento do estelionato virtual sobre a diminuição dos crimes violentos, como roubo e roubo de veículos.

Somente por meio de uma abordagem integral e colaborativa, envolvendo setores públicos e privados, será possível construir um ambiente digital mais seguro e protegido contra os impactos nefastos do estelionato digital, promovendo, assim, uma sociedade mais resiliente e protegida frente às nuances do cenário tecnológico em constante evolução. Para alcançar esse objetivo, o Estado deve adotar novos métodos de investigação e aprimorar os recursos digitais e tecnológicos disponíveis às autoridades.

Diante de tais considerações, é imperativo que o legislador e as instâncias responsáveis adotem estratégias que aprimorem a legislação existente e fortaleçam os meios de investigação e repressão, a fim de preservar a integridade da sociedade brasileira diante dos desafios impostos pelo avanço tecnológico.

REFERÊNCIAS

ANDREUCCI, Ricardo Antônio. **O crime de estelionato cibernético ou virtual.** 2021. Disponível em: https://emporiododireito.com.br/leitura/o-crime-de-estelionato- cibernetico-ou-virtual. Acesso em: 26 ago. 2023.

ARAÚJO, A. L.; MAIA, F. M. O estelionato virtual no Brasil: aspectos penais e jurídicos. **Revista Jurídica CESUSC**, v. 20, n. 37, p. 75-94, 2019.

ATAÍDE, Amanda Albuquerque de. **Crimes virtuais: uma análise da impunidade e dos danos causados às vítimas**. Maceió, 2017.

BARBAGALO, Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade**. Disponível em: https://www.migalhas.com.br/depeso/367289/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade. Acesso em: 24 jul. 2023.

BRASIL. Presidência da República. **Decreto-lei no 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm. Acesso em: 12 abr. 2024.

BRASIL. Presidência da República. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso e: 22 abr. 2024.

BRASIL. Supremo Tribunal Federal. Jurisprudência: **AG.REG. NO RECURSO EXTRAORDINÁRIO COM AGRAVO 1.370.525/PR**. BRASÍLIA. 2023. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=765089610 Acesso em: 13 de junho de 2024.

BRASIL. Supremo Tribunal Federal. **Vocabulário Jurídico (Tesauro)**. Brasília. 2024. Disponível em: https://portal.stf.jus.br/jurisprudencia/tesauro/pesquisa.asp?pesquisaLivre=MODUS%20OPERANDI#:~:text=NOTA%3A,Maneira%20de%20agir%2C%20operar%20ou%20executar,atividade%20seguindo%20os%20mesmos%20procedimentos. Acesso em: 15 de junho de 2024.

BRASIL. Tribunal Regional Federal da 3ª Região. **Escola de Magistrados Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017

CAPEZ, Fernando. **Curso de Direito Penal**. Editora Saraiva. 2020.

COSTA, C. L.; SILVA, M. C. Aspectos criminais do estelionato na era digital. **Revista de Direito, Estado e Telecomunicações**, v. 8, n. 1, p. 11-31, 2020.

FELIX, Ysmara Padilha. NASCIMENTO, Yris Assíria Alves. A vulnerabilidade dos idosos diante dos crimes cibernéticos. 2023. **Trabalho de conclusão de curso (Graduação em Direito)** - Curso de Direito, Universidade de Potiguar. Natal/RN, 2023.

FERRAZ, J. L. Aspectos penais e processuais do estelionato cibernético. **Revista Brasileira de Ciências Criminais**, v. 121, p. 281-301, 2015.

GONZAGA, Yuri. **"Sociabilidade" do brasileiro propicia crimes virtuais, diz empresa; prejuízo aumenta.** Disponível em: https://m.folha.uol.com.br/tec/2013/12/1385479-sociabilidade-do-brasileiro-propicia-crimes-virtuais-diz-empresa-saiba-se-proteger.shtml Acesso em: 13 abr. 2024.

GRANUCCI, Rapahel. Engenharia Social: O que é e como se prevenir desses golpes. **Minds Digital**, 2024. Disponível em: https://minds.digital/prevencao-a-fraude/engenharia-social/. Acesso em: 18 abr. 2024.

GREVE, Fabíola Greve et al. Blockchain e a Revolução do Consenso sob Demanda. **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)** -

Minicursos, 2018. Disponível em: http://143.54.25.88/index.php/sbrcminicursos/article/view/1770>. Acesso em: 13 abr. 2024.

KURTZ, João. **Registros de ocorrências de crimes virtuais aumentam 70% no país em 1 ano.** Disponível em: http://www.techtudo.com.br/noticias/noticia/2014/10/registros-de-ocorrencias-de-crimes-virtuais-aumentam-70-no-pais-em-1-ano.html. Acesso em: 10 jan. 2024.

MARTINELLI, Guilherme. A Eficácia da Legislação Brasileira na Prevenção de Crimes Digitais. **Jusbrasil**, 2024. Disponível em: https://www.jusbrasil.com.br/artigos/a-eficacia-da-legislacao-brasileira-na-prevencao-de-crimes-digitais/2147918640. Acesso em: 17 abr. 2024.

MEIRELES, Julia. Crimes Virtuais e as dificuldades de combatê-los. **Jusbrasil**, 2020. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-e-as-dificuldades-de-combate-los/876548834. Acesso em: 23 maio, 2024.

MIRABETE, Júlio Fabbrini e FABBRINI, Renato N. **Manual de direito penal: parte especial: Arts. 121 a 234-B do CP – volume 2**, 36° edição, São Paulo, Atlas, 2021.

MIRANDA, Lucas Eller Freitas de Alencar. **Os impactos da falta de punição para o crime de estelionato digital no brasil**. Universidade Federal de Juiz de Fora, Governador Valadares-MG, 2023. Disponível em: https://repositorio.ufjf.br/jspui/bitstream/ufjf/16511/1/lucasellerfreitasdealencarmiranda.pdf Acesso em: 16 de julho de 2024.

MONTEIRO, G. M. Estelionato eletrônico e os desafios da tipificação penal. **Revista de Direito do Consumidor**, v. 125, p. 263-282, 2019.

OLIVEIRA, Matheus Davi de; SANTOS, Mylena Vitória Sales Maia dos**. Crimes cibernéticos: as dificuldades encontradas na Investigação**. 2023, 34p. Trabalho de Conclusão de Curso (Direito) – Universidade Potiguar, Natal-RN, 2023. Disponível em: https://repositorio.animaeducacao.com.br/items/5dc9942d-d65d-41ab-91bd-61c6cf54030f. Acesso em: 12 abr. 2024.

PEREIRA, Emanuela de Araújo. A problemática do tipo penal "fraude eletrônica". **Consultor Jurídico**, 2023. Disponível em: https://www.conjur.com.br/2023-fev-13/emanuela-pereira-problematica-tipo-penal-fraude-eletronica/. Acesso em: 12 abr. 2024.

RODRIGUES, Sérgio. Estelionato, uma palavra que muda de cor. **Veja**, 2010. Disponível em: https://veja.abril.com.br/coluna/sobre-palavras/estelionato-uma-palavra-que-muda-de-cor-2. Acesso em: 12 abr. 2024.

SILVA, Lorany Stefany Souza da; BOERI JUNIOR, Hermes Eomar; PINTO, Edson Pontes. Os mecanismos de combate aos crimes da internet no Brasil. **Revista FT, Ciências Sociais**, Volume 27 - Edição 128/NOV 2023. Disponível em: https://revistaft.com.br/os-mecanismos-de-combate-aos-crimes-da-internet-no-brasil/. Acesso em: 12 maio 2024.

SSP-RS, Secretaria de Segurança Pública do Estado do Rio Grande do Sul. **Indicadores Criminais.** Disponível em: https://ssp.rs.gov.br/indicadores-criminais Acesso em: 15 de junho de 2024.