

INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP  
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM DIREITO  
MESTRADO PROFISSIONAL EM DIREITO ECONÔMICO E DESENVOLVIMENTO

NATÁLIA DOS SANTOS SILVA

**O ESTELIONATO VIRTUAL E A SUA ESTRUTURA JURÍDICA**

Brasília  
2023

NATÁLIA DOS SANTOS SILVA

## **O ESTELIONATO VIRTUAL E A SUA ESTRUTURA JURÍDICA**

Dissertação submetida ao Programa de Mestrado Profissional em Direito Econômico e Desenvolvimento, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP como parte dos requisitos para obtenção do título de Mestre.

Orientador. Prof. Dr. Alexandre Lima Wunderlich.

Brasília  
2023

NATÁLIA DOS SANTOS SILVA

**O ESTELIONATO VIRTUAL E A SUA ESTRUTURA JURÍDICA.**

Dissertação submetida ao Programa de Mestrado Profissional em Direito Econômico e Desenvolvimento, do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP como parte dos requisitos para obtenção do título de Mestre.

Aprovada em \_\_\_\_/\_\_\_\_/\_\_\_\_

BANCA EXAMINADORA

---

Prof. Dr. Orientador Alexandre Lima Wunderlich

---

Prof. Dr. Avaliador Marcelo Buttelli Ramos

---

Prof. Dr. Avaliador Antônio Carlos Tovo Loureiro

---

## **AGRADECIMENTOS**

Agradeço a elaboração do presente estudo primeiramente a Deus, por sua imensa Sabedoria, amor e bondade de conceder mais essa conquista e pela inspiração de cada dia para a realização deste trabalho.

Agradeço reiteradamente a minha família e amigos pelo carinho e incentivo, a eles dedico esta obra com carinho.

Ao IDP, pela oportunidade singular, pelo ensino e estrutura de excepcional, agradeço ao meu orientador Prof. Doutor Alexandre Wunderlich, pela confiança, conselhos e sua disponibilidade em sempre me ajudar.

## RESUMO

O tema da pesquisa discorrerá sobre os golpes na internet: uma análise do crime de estelionato virtual. Os crimes da internet são uma preocupação internacional, milhares de pessoas sofrem por serem vítimas desses delitos, essas vítimas virtuais, trazem consequências reais em sua vida. A velocidade com que os crimes são cometidos, e a expertise do criminoso fazem com que a internet se torne através dos meios digitais, um local de cometimento de golpes, que antes ocorriam apenas no mundo físico, migraram para o ambiente virtual. Os novos tipos de crime cometidos pela internet produzem prejuízos reais às suas vítimas, com o mundo cada vez conectado, faz-se necessário o estudo desse fenômeno. Todavia, o presente trabalho analisará apenas as leis referentes aos ilícitos criminais, referente ao crime de estelionato virtual, delito este que é o mais recorrente quando se trata de golpes da internet, questionando-se, sumamente, como essa evolução normativa influenciou no combate e punição dos crimes da internet, em especial ao combate ao estelionato virtual, nos últimos anos. A metodologia usada será bibliográfica, documental com dimensão descritiva, pois explica o atual estado das normas que disciplinam os crimes cibernéticos, as leis que tratam sobre crime de estelionato da internet, quais sejam: A Lei n.º 12.737/12 (Lei “Carolina Dieckmann”), o Marco civil da Internet, Lei n.º 12.965/14, que regulam o funcionamento da internet no Brasil, a Lei Geral de Proteção dos Dados (LGPD), n.º 13.709/18. Faremos um levantamento jurisprudencial, nos tribunais superiores brasileiros, para analisar os posicionamentos recentes das cortes, após a Lei n.º 14.155/21 com relação aos crimes de estelionato cometido na internet.

**Palavra-chave:** Estelionato virtual. Crimes virtuais. Lei de proteção aos dados. Direito Penal. Responsabilidade penal.

## ABSTRACT

The theme of the research will discuss scams on the internet: an analysis of the crime of virtual swindling. Internet crimes are an international concern, thousands of people suffer from being victims of these crimes, these virtual victims have real consequences in their lives. The speed with which crimes are committed, and the criminal's expertise make the internet become, through digital means, a place for committing scams, which previously only occurred in the physical world, migrated to the virtual environment. The new types of crime committed over the internet produce real harm to their victims, with the world becoming more and more connected, it is necessary to study this phenomenon. However, the present work will only analyze the laws referring to criminal offenses, referring to the crime of virtual swindling, a crime that is the most recurrent when it comes to internet scams, questioning, in short, if and how this normative evolution influenced the combat and punishment of internet crimes, especially the fight against virtual swindling, in recent years. The methodology used will be bibliographical, documental with a descriptive dimension, as it explains the current state of the norms that discipline cyber crimes, the laws that deal with the crime of internet fraud, that is, the laws of Law 12.737/12 (Law "Carolina Dieckmann"), the Civil Rights Framework for the Internet, Law No. 12,965/14, which regulate the operation of the internet in Brazil, the General Data Protection Law (LGPD), No. 13,709/18, Law No. 14. jurisprudence, in the Brazilian superior courts, to analyze the recent positions of the courts, after Law nº 14.155/21 regarding crimes of larceny committed on the internet.

**Keyword:** Virtual swindling. Virtual crimes. Data protection law. Criminal Law. Criminal liability.

## LISTA DE ABREVIATURAS

CF: Constituição Federal;  
CP: Código Penal;  
CPP: Código de Processo Penal;  
CPC: Código de Processo Civil;  
CC: Código Civil;  
CDC: Código de defesa do consumidor;  
CNJ: Conselho Nacional de Justiça;  
CNMP: Conselho Nacional do Ministério Público;  
CN: Congresso Nacional;  
CL: Câmara Legislativa;  
CD: Câmara dos Deputados;  
PL: Projeto de Lei;  
DEC. LEI: Decreto-lei;  
DOU: Diário Oficial da União;  
PC: Polícia Civil;  
PF: Polícia Federal;  
SF: Senado Federal;  
STF: Supremo Tribunal Federal;  
STJ: Superior Tribunal de Justiça;

## SUMÁRIO

<b>INTRODUÇÃO.....</b>	<b>09</b>
<b>1. INTERNET E O CRIME.....</b>	<b>15</b>
1.1 A criação e o desenvolvimento da internet.....	15
1.2 Convenções internacionais.....	19
1.2.1 <i>Convenção de Budapeste</i> .....	19
1.3 O tratamento jurídico da internet no Brasil: Plano legislativo.....	20
1.3.1 <i>Marco civil da internet</i> .....	22
1.3.2 <i>Lei geral de proteção de dados</i> .....	22
1.4 O cibercrime.....	23
1.4.1 <i>Evolução e conceito</i> .....	24
1.4.2 <i>Educação digital</i> .....	25
1.4.3 <i>Elementos fundamentais</i> .....	26
1.5 Sujeitos dos crimes da internet.....	28
<b>2. A ESTRUTURA JURÍDICA DO CRIME DE ESTELIONATO.....</b>	<b>32</b>
2.1 Figura jurídica do estelionato clássico.....	32
2.2 Elementos subjetivos e objetivos do tipo.....	34
2.2.1 <i>A torpeza bilateral</i> .....	35
2.2.2 <i>Estelionato judicial</i> .....	35
2.2.3 <i>Estelionato contratual</i> .....	36
2.2.4 <i>Estelionato sentimental</i> .....	36
2.2.5 <i>Estelionato e furto mediante fraude</i> .....	37
2.2.6 <i>Estelionato privilegiado</i> .....	38
2.2.7 <i>Estelionato qualificado</i> .....	42
2.3 Fraude aplicada no sistema previdenciário.....	43
2.3.1 <i>Fraude contra pessoa idosa e vulnerável: Reflexos civis e penais</i> .....	45
<b>3. O REFLEXO DOS CRIMES VIRTUAIS EM FACE DO OLHAR JURÍDICO E DA SOCIEDADE NO CONTEXTO ATUAL.....</b>	<b>48</b>
3.1 O estelionato virtual sob à égide penal.....	51
3.2 Elementos do tipo penal.....	52
3.3 A causa de aumento do art. 171, §2º-“b”.....	57

<b>CONCLUSÃO.....</b>	<b>60</b>
<b>REFERÊNCIAS.....</b>	<b>63</b>

## INTRODUÇÃO

A sociedade ao longo dos anos vem se transformando cada vez mais, o mundo se tornou tecnológico, a internet e as tecnologias da comunicação em geral mudaram de analógica para digital, vivemos a cibercultura<sup>1</sup>.

A internet saiu de limitada a um pequeno grupo, para acessível à população em geral, democratizando o seu uso.

Hoje, em um único aparelho temos acesso a inúmeros recursos, além disso, a evolução das tecnologias é benéfica, segundo o sociólogo francês, Lévy, (2012)<sup>2</sup>, as novas tecnologias, possibilitam ao mundo uma nova forma de pensar, ampliando o conhecimento e diversificando a cultura.

A modernidade líquida, denominada pela teoria do filósofo, Bauman, (2001)<sup>3</sup> é uma metáfora referida à sociedade que deixa de ser sólida (definida, duradoura e estável) e passa a se tornar em uma sociedade líquida, ou seja, o líquido assim como a sociedade está em contínua transformação, sua forma líquida proporciona que, seja mais adaptável as mudanças da vida moderna pede a mudança a sociedade sólida para líquida, pós-moderna, Paz, (2017)<sup>4</sup>, a liquidez da sociedade as mudanças se referem a política, tecnologia, meios de comunicação.

O Direito digital é uma área do direito que surge para suprir a alta demanda de questões que envolvem normas e princípios, para proteger de possíveis violações e da influência do mundo virtual na sociedade e no ordenamento jurídico. Ademais, o direito digital busca a regulamentação e a solução de problemas gerados via de relações que ocorrem na rede, conforme as palavras de Pinheiro, (2021), a saber:

O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.). (PINHEIRO, 2021)<sup>5</sup>.

---

<sup>1</sup>LÉVY, Pierre, apud, CUNHA, Úrsula Nascimento de Sousa, **cibercultura e as identidades líquidas: reflexão sobre a cultura na era das novas tecnologias**, Revista: Pontos de Interrogação: Linguagens, identidades e letramentos - Vol. 2, n. 2, jul./dez. 2012 | 163. Disponível <https://www.revistas.uneb.br/index.php/pontosdeint/article/view/1558>. Acesso em 11 de janeiro de 2023.

<sup>2</sup> Idem.

<sup>3</sup> BAUMAN, Zygmunt. Modernidade Líquida. Tradução, Plínio Dentzien. Rio de Janeiro: Jorge Zahar ed., 2001.

<sup>4</sup> PAZ, E. H. **Literatura líquida: a narração em ambiente digital**. Travessias, Cascavel, v. 11, n. 3, p. 222–234, 2017. Disponível em: <https://e-revista.unioeste.br/index.php/travessias/article/view/18165>. Acesso em: 11 jan. 2023.

<sup>5</sup> PINHEIRO, Patrícia Peck. **#Direito digital**. 7. ed. rev., ampl., atual São Paulo: Saraiva Jur, 2021. E-book. (1 recurso online). ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9786555598438>. Acesso em: 10 jul. 2022, p.26.

A internet está presente no mundo jurídico nos processos e audiências online, nos meios de transporte, na medicina, na educação e no lazer, no meio de comunicação, dentre outros. Esses são exemplos corriqueiros do uso dessa tecnologia, o termo internet está conceituado no Marco Civil da internet, em seu art. 5º, pois:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes. (BRASIL, 2012).

O comércio outro seguimento que se transformou radicalmente ao longo das últimas décadas. Atualmente o comércio eletrônico (*E-commerce*), regulado pelo Decreto n.º 7.962/13 que gerou uma mudança significativa na cultura empresarial e na economia. As transações acontecem inteiramente online: compra e venda de bens e serviços, lojas que antes eram apenas físicas, agora são lojas virtuais, as empresas passam a alcançar novos clientes em vários locais.

Em suma, esse tipo de comércio emerge como um horizonte de novas oportunidades, porem com a grande abundância de dinheiro e informações circulando na rede, os criminosos aperfeiçoaram seus golpes, visando obter vantagem ilícita, praticando assim o estelionato virtual<sup>6</sup>, que vem sendo uma dos principais crimes cometidos na internet, os criminosos usam os meios digitais para cometer golpes, para enganar, para induzir a vítima ao erro, e com isso alcançam a finalidade de obter vantagem ilícita e trazer prejuízo patrimonial, as vítimas.

Questões relacionadas ao roubo de dados, invasões de dispositivos e vazamentos de dados, e os golpes da internet, são preocupações não só dos usuários, mas dos empresários da rede e do Estado, que por meio de leis busca prevenir e punir quem comete esses ilícitos.

A Constituição Federal de 1988, ao consagrar os direitos e as garantias fundamentais em seu Art. 5º, protegem não só o direito ao nome e à imagem, mas os dados que alcançaram, hoje, status de Direito Fundamentais com a Emenda Constitucional nº 115 de 2022, bem como compreendem direitos relacionados à honra, e ao patrimônio todos são alcançados por essa mesma tutela Constitucional.

Nessa senda, a violação desses direitos pode ser constatada a partir de sua propagação de forma velada e maliciosa por meio da prática dos crimes cibernéticos, o que revela a necessidade de maior fiscalização, atuação e responsabilização civil e criminal em face do uso inadequado dos sistemas digitais.

---

<sup>6</sup>GRECO, Rogério. **Código Penal Comentado**. [Digite o Local da Editora]: Grupo GEN, 2021. E-book. ISBN 9786559770700. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559770700/>. Acesso em: 16 nov. 2022, p.545.

Registra-se, ainda, que só no ano de 2020, segundo o levantamento realizado pela Associação Safernet Brasil em parceria com o Ministério Público Federal –MPF –, foram registradas na Central Nacional de Denúncias de Crimes Cibernéticos – CNDCC –156.692 ocorrências de crimes praticados na internet, revelando-se um aumento significativo em relação à prática de infrações penais dessa natureza em comparação com o ano de 2019, cujo total de registros de 75.428 ocorrências.<sup>7</sup>

Nesse sentido, o Anuário Brasileiro de Segurança Pública –ABSP –, lançado no ano de 2022, foram analisados o crescimento do número dos estelionatos cometidos por meio eletrônico, foram analisado o período de 2018-2021, constatou-se que houve um aumento no cometimento desse delito, a análise e feita ao nível nacional e estadual, em ambos o crescimento mais que duplicado, por exemplo, a nível nacional nesse período analisado o crescimento de 495%, o anuário brasileiro é baseado em relatórios e estatísticas das polícias civis, polícias militares, e polícia federal, secretarias de segurança pública, de todos os estados<sup>8</sup>.

Esse cenário se intensificou durante a pandemia do Covid-19, que do dia para noite produziu um “novo normal”, impondo medidas de isolamento, físico e social, e o uso do computador para tudo, desde o trabalho, passando por até compras diárias, até e transações bancárias<sup>9</sup>. O cenário se tornou preocupante, ao ponto de os parlamentares criarem uma iniciativa de lei para a criação de um novo dispositivo legal, surgiu assim PL 4554/20<sup>10</sup>, que posteriormente se tornou a Lei n.º 14.155/21.

A velocidade com que os crimes são cometidos, e a expertise do criminoso fazem como que a internet se torne através dos meios digitais um local de cometimento de golpes, que antes ocorriam apenas no mundo físico, migraram para o ambiente virtual. A dificuldade em provar a materialidade e autoria dos criminosos, isso faz com que a punição dos ilícitos seja difícil, ocorrendo, por vezes, a prescrição do crime, o que transmite à população a percepção de que a internet é uma “terra de ninguém”. Os novos tipos de crime cometidos pela internet produzem prejuízos reais às suas vítimas, com o mundo cada vez mais conectado, faz-se necessário o estudo desse fenômeno.

---

<sup>7</sup> BRASIL, Safernet, **indicadores**. Disponível em <https://indicadores.safernet.org.br/>. Acesso 20/01/2023.

<sup>8</sup> FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública: 2022**. São Paulo: FBSP, p.110-111.

<sup>9</sup> COSTA, Taís Barros Trajano Ribeiro da. **O aumento do crime cibernético durante a pandemia da COVID-19**. Faculdade Damas, Recife-PE, 2020. Disponível em: <https://jus.com.br/> acesso em: 18 de maio de 2021.

<sup>10</sup> CAMARA DOS DEPUTADOS. **Projeto de Lei n.º 4554/20**. Disponível em [https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1947262&filename=PL%204554/20](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1947262&filename=PL%204554/20). acesso em 21/01/2023.

O Estado tem contribuído para o enfrentamento dos chamados crimes cibernéticos<sup>11</sup>. Nesse sentido, as políticas públicas, ações e medidas do Estado para promover e colocar em prática os direitos, e solucionar problemas, surgiu assim: a Lei n.º 12.965/14, denominada Marco Civil da Internet, reguladora sobre o uso e dispõe sobre os direitos e princípios da internet, pune ilícitos civis, tem a tutela do Código Penal, que abrange grande parte dos delitos cibernéticos, em relação ao uso de dados, e o grande fluxo de dados na rede, começou a se proteger com o advento da Lei n.º 13.709/18, LGPD.

Ademais preocupado com penas mais rígidas publicou a Lei n.º 14.155/21 que aumentou a pena dos cibercrimes e criou o tipo penal – fraude eletrônica, conhecido por estelionato virtual, elencado no art. 171, §2º-A do Código Penal. a Lei da 12.737/12, a chamada lei Carolina Dieckmann. Essa é à primeira norma específica a punir os crimes informáticos.

Os crimes eletrônicos vêm crescendo ao longo dos anos, - As fraudes bancárias<sup>12</sup>, conhecidas por estelionato virtual, por exemplo, cresceram cerca de 165% apenas no ano de 2021, segundo dados da Federação Brasileira de Bancos (Febraban)<sup>13</sup>. Esse já elevado crescimento se intensificou durante a Pandemia do Covid-19, notadamente em um contexto no qual a transação bancária passaram a ser feitas feitas sua maioria por meio dos celulares, e com a difusão do Open Bank,<sup>14</sup> os fraudadores usam a dificuldade do Estado em punir, e agem; os ataques podem ser individuais, ou em massa, atingem pessoas físicas ou jurídicas, são uma ameaça a segurança da informação, pois:

Os ataques cibernéticos e as falhas de segurança nas redes, públicas e privadas, e principalmente na web são um problema de constante preocupação para os principais

---

<sup>11</sup> O crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. “Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.” JESUS, Damásio D.; MILAGRE, José A. **Manual de crimes informáticos**. Editora Saraiva, 2016. E-book. ISBN 9788502627246. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502627246/>. Acesso em: 12 nov. 2022, p.20.

<sup>12</sup> Nas transferências bancárias pela Internet à revelia dos titulares das contas, o agente, com a intenção de obter uma vantagem patrimonial ilegítima, prejudicando o titular da conta, interfere no resultado de tratamento de dados através da utilização de dados bancários sem autorização. CORREIA, Pedro Miguel Alves Ribeiro; JESUS Inês Oliveira Andrade - **Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas**. REVISTA DIREITO GV | SÃO PAULO | V. 12 N. 2 | 542-563 | MAI-AGO 2016.

<sup>13</sup> MELLO Danilo: **Fraude contra cliente cresce 65% por e 2021**. Agência Brasil, <https://agenciabrasil.ebc.com.br/economia/noticia/2021-10/fraudes-contra-clientes-de-bancos-crescem-165-em-2021>. São Paulo, publicação 29/10/2021. Acesso e 28/08/2022.

<sup>14</sup> LEITE, Luiza; CAMARGO, Matheus. **Open Banking: inovação aberta no sistema financeiro**. Editora Saraiva, 2022. E-book. ISBN 9786553620353. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786553620353/>. Acesso em: 12 nov. 2022.

analistas mundiais e as empresas/profissionais de segurança da informação e web security. (WENDT, 2011)<sup>15</sup>.

Como a legislação penal brasileira vem se aperfeiçoando ao longo da última década para combater, prevenir e punir os crimes de estelionato no âmbito virtual? Foram elaboradas ao longo dessa década algumas Leis, penais e civis, relacionadas à proteção de dados, regulamentação da internet, princípios da internet.

Todavia, o presente trabalho analisará apenas as leis referentes aos ilícitos criminais, referente ao crime de estelionato virtual, delito este que é o mais recorrente quando se trata de golpes da internet, questionando-se e como essa evolução normativa influenciou no combate e punição dos crimes da internet, em especial ao combate ao estelionato virtual, nos últimos anos.

Dar-se-á ênfase à Lei 14.155/21, a referida lei, tornou as penas dos delitos de informática mais grave, e criou qualificadora art. 171 Código Penal, o crime do estelionato virtual, tema central de nossa pesquisa, também conhecido por fraude eletrônica, conforme o recém-criado parágrafo 2º - A do Art.º 171 do Código Penal.

A metodologia usada será bibliográfica, documental com dimensão descritiva, ao explicar o atual estado das normas que disciplinam os crimes cibernéticos, as leis que tratam sobre crime de estelionato da internet, quais sejam: A Lei n.º 12.737/12 (Lei “Carolina Dieckmann”), o Marco civil da Internet, Lei n.º 12.965/14, que regulam o funcionamento da internet no Brasil, a Lei Geral de Proteção dos Dados (LGPD), n.º 13.709/18, a Lei n.º 14.155, e o Código Penal Brasileiro.

Ademais será estudada a ratificação do Brasil à Convenção de Budapeste, que prevê uma cooperação internacional no combate aos crimes cibernéticos. Por fim, será realizado um estudo bibliográfico em livros, artigos científicos, teses e dissertações relacionadas ao tema, de estelionato virtual.

Será utilizado para a elaboração do presente estudo o método hipotético dedutivo, partindo da observação das normas vigentes brasileiras relacionadas aos crimes informáticos, tendo em vista compreender as implicações para o problema de pesquisa. A pesquisa será, ainda, prescritiva, no ponto que indicará os limites do ordenamento jurídico em relação ao tema e prováveis alterações para superá-los.

O presente estudo tem como objetivo analisar a evolução legislativa do crime de estelionato virtual, na legislação brasileira, assim como verificaremos o conceito de crimes da

---

<sup>15</sup> WENDT, E. CIBERGUERRA, INTELIGÊNCIA CIBERNÉTICA E SEGURANÇA VIRTUAL: alguns aspectos. **Revista Brasileira de Inteligência**, n. 6, p. 15-26, 1 abr. 2011.

internet, e quais as legislações existem no Brasil, sobre crimes da internet. Observaremos a estrutura do tipo penal estelionato do art. 171 do Código Penal, com suas características, assim como pesquisaremos sobre a criação do tipo penal estelionato virtual.

O presente estudo está dividido em três capítulos. No capítulo I, será feito um estudo de contextualização do tema proposto, com a história da internet, o conceito de crime, princípios e leis penal no espaço. Ademais, será analisado o conceito de cibercrimes, quais os crimes mais cometidos no Brasil e quais leis vigentes tratam deste tema, ainda no capítulo I abordaremos os conceitos de hackers, usados para disseminar crimes.

Além disso, no capítulo II tratar-se-á do tipo penal Estelionato clássico, seus aspectos jurídicos, suas espécies, com entendimento doutrinário e jurisprudencial. E, por fim, no capítulo III, será realizado um estudo sistematizado do crime Estelionato virtual, também conhecido por *Scamming*, sendo o tema central da pesquisa, estudaremos o seu conceito, e seus elementos jurídicos.

## 1. INTERNET E O CRIME

### 1.1 A criação e o desenvolvimento da internet

A internet surgiu, primeiramente com intuítos militares durante a Guerra Fria<sup>16</sup> (1947-1991), período em que o mundo dividido geopoliticamente em dois blocos, em dois lados, um lado ficou polarizado pelo Socialismo da União Soviética, contra o outro lado o Capitalismo Americano.

Além disso, a internet como meio de comunicação surgiu como canal que transmitisse as comunicações de forma segura, mesmo que ocorresse ataques em locais físicos, a comunicação entre áreas de comando americanos ocorreria, o intuito de possuir um sistema de comunicação que transmitisse as mensagens entre os centros de comando americanos.

Registra-se que a – *Advanced Research Projects Agency* – ARPANET funcionou como a primeira rede de comunicação informática, seu objetivo principalmente era facilitar a comunicação entre órgãos militares americanos, destaca-se que agência pertencia ao Departamento de Defesa Americano<sup>17</sup>.

Com o passar dos anos a internet evoluiu e com o fim da Guerra Fria, a rede despontou do campo militar e passou a ser estudada e desenvolvida no meio acadêmico, o seu uso inicialmente estava restrito apenas aos Estados Unidos, com o tempo a conexão da internet se expandiu a outros países, e no fim da década de 80, o surgimento de grandes empresas provedoras de internet impulsionou a expansão da internet.

Outro fato que tornou popular a internet foi o desenvolvimento do protocolo de hipermídia WWW (*Word, wide, web*), que foi desenvolvido pelo CERN (*European Organization for Nuclear Research*) sistema que interliga documentos de vários formatos como texto, o som, a imagem e vídeo, e possibilitou o alcance da internet ao usuário.

Após o fim da Guerra Fria, o sistema capitalismo prevaleceu de forma econômica, a internet deixou a área restrita militar, desenvolveu-se comercialmente, assim o processo de globalização intenso, com o uso das novas tecnologias desenvolvidas, além desse desenvolvimento ser visivelmente motivado pela grande integração de informações, de cultura e de economias, o grande avanço tecnológico, e maior segurança na transmissão de dados, aproximou às relações comerciais no mundo, a internet diminuiu a distância entre as nações.

---

<sup>16</sup> FERNADES Claudio. **Guerra Fria** – disponível em <https://www.historiadomundo.com.br/idade-contemporanea/guerra-fria.htm>. Acesso 22 de agosto de 2022.

<sup>17</sup> SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva Jur, 2015. E-book. (1 recurso online). (Saberes monográficos). ISBN 9788502229488. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788502229488>. Acesso em: 2 out. 2022, p.14-25.

A ascensão da popularidade da rede, e o elevado volume de digitalização do mundo, em grande parte do referido sucesso, aconteceu com surgimento das grandes companhias do mercado informático conhecidas por *Big Techs*<sup>18</sup>, empresas que são conhecidas como gigantes no mundo corporativo, pois movimentam milhões de dólares em venda e produtos.

As *Big Five*, refere-se ao grupo das cinco maiores empresas do mundo tecnológico: *Microsoft, Apple, Amazon, Facebook e a Google*, possuem valor de mercado altíssimo, tendo em vista que em 2021 alcançou US\$ 9 trilhões de dólares. Tais empresas servem como exemplo no foco em tecnologia, possuindo em conjunto patrimônio equivalente ao PIB mundial de 12%, ficando atrás apenas de grandes economias como os Estados Unidos e China<sup>19</sup>.

Estas companhias trabalharam para o computador deixasse de ser apenas uma máquina, e passasse a oferecer recursos que facilitassem a vida do usuário, além de proporcionar uma elevada popularidade no mercado financeiro em face de todo o envolvimento de produtos digitais, como por exemplo, a milionária indústria dos jogos eletrônicos (*games*), seguimento de entretenimento que movimentou somente em 2021, cerca de US\$ 185 bilhões<sup>20</sup> de dólares.

Os grandes investimentos em bons produtos e serviços, o foco no público jovem, ocasionou o crescimento acelerado da internet e das tecnologias informáticas, com a alta procura e com os preços mais acessíveis para adquirir computadores e seus componentes, inserindo a tecnologia de forma mais presente nos lares e nas empresas.<sup>21</sup>

Contudo, registra-se que a internet não proporcionou apenas benefícios<sup>22</sup> e facilidades, no mundo moderno, existem pessoas que utilizam a rede para praticar atividades ilícitas, reconhecido no meio jurídico e social como crimes virtuais ou *cyber crimes*, segundo as lições de Ferreira, (2001) ao conceituar tais delitos como:

Ações criminosas na área informática, assim entendidas em seu sentido lato, abrangendo todas as tecnologias da informação, do processamento e da transmissão de dados, originaram uma forma de criminalidade que, apesar da diversidade de suas classificações, pode ser identificada pelo seu objeto ou pelos meios de atuação, os

<sup>18</sup> MOROSOV Evgeny. **Big Tech: A ascensão dos dados e a morte da política**: – Edição padrão, editora Ubu, 4 dezembro 2018, p.27.

<sup>19</sup> BIG TECHS: 2021, o ano em que as gigantes de tecnologia se tornaram insuperáveis Isto é Dinheiro <https://www.istoedinheiro.com.br/bigtechs-2021-o-ano-em-que-as-gigantes-de-tecnologia-se-tornaram-insuperaveis/reportagem> 20/12/21. Acesso em 28/09/22.

<sup>20</sup> 2022 promissor: mercado de games ultrapassará US\$ 200 bi até 2023.FORBES. 03 de janeiro de 22 Leia mais em: <https://forbes.com.br/forbes-tech/2022/01/com-2022-decisivo-mercado-de-games-ultrapassara-us-200-bi-ate-2023/> acesso em 21/09/22.

<sup>21</sup> CORREA, Fabiano Simões. **Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da internet**. 2013. Dissertação (Mestrado em Psicologia) - Faculdade de Filosofia, Ciências e Letras de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2013. doi:10.11606/D.59.2013.tde-08102013-162610. Acesso em: 10-08 2022.

<sup>22</sup> HARARI, Yuval Noah. **Sapiens: uma breve historia da humanidade**; tradução Jorio Dauster. 1º ed. São Paulo: Companhia das Letras, 2020.

quais fornecem um denominador comum, embora com diferentes denominações nos vários países ou nos diferentes autores. (FERREIRA, 2001)<sup>23</sup>

Desta feita, os crimes recorrentes no âmbito da internet são os seguintes: estelionato virtual (fraude eletrônica), nos termos do artº171, parágrafo 2º- A do Código Penal<sup>24</sup>, conhecido como o golpe da clonagem do *WhatsApp* em que o autor persuade a vítima a enviar o código de segurança, com o acesso da sua conta, finge ser a vítima com o intuito de obter para si alguma vantagem econômica, além de outras modalidades delituosas como, por exemplo, estelionato sentimental, o falso sequestro, criação de *sites* falsos, etc.

De acordo com a Central Nacional de Denúncias de Crimes cibernéticos,<sup>25</sup> por dia cerca de 2.500 denúncias sobre a prática de crimes virtuais de em face de conteúdo pornográfico, racista, maus tratos aos animais são recebidos na respectiva central. Além disso, o objetivo na criação de canal de denúncias *online* busca amparar as vítimas, além de informar aos órgãos responsáveis sobre tais práticas criminosas.

Além da central, o Ministério Público Federal – MPF, em parceria com outras instituições como a *Ong SaferNet*<sup>26</sup> trabalham em conjunto na prevenção e identificação de crimes virtuais em todo o território nacional, da mesma maneira o fomento de políticas públicas para o enfrentamento a persistência dos autores na prática dos delitos.

Compreende-se, que a globalização e a transformação das tecnologias de comunicação fazem com que a sociedade enfrente uma constante revolução<sup>27</sup>, haja vista as condutas criminosas ocorriam apenas no mundo físico, vindo a ganhar espaço também no ambiente virtual.

Diante da migração na prática de crimes para o ambiente virtual, na mesma maneira da utilização de meios fraudulentos para a obtenção da vantagem, fez nascer a necessidade por parte do Estado, do poder público e principalmente da sociedade na regulamentação das condutas delituosas com maior atenção, dados prejuízos morais, financeiros e sociais suportados pelas vítimas.

---

<sup>23</sup> FERREIRA, Ivette Senise. **A criminalidade informática. Direito e internet: aspectos jurídicos relevantes.** Tradução. Bauru, SP: EDIPRO, 2001. Acesso em: 18 jan. 2023.

<sup>24</sup> **Idem. Greco, (2022).**

<sup>25</sup> BRASIL, **Denúncias de crimes cometidos pela internet mais que dobram em 2020**, Portal G1: reportagem do dia 09/02/2020<https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml>. Acesso em 21/09/22.

<sup>26</sup> A **ONG SaferNet** é uma organização civil, sem fins lucrativos, que tem por objetivos promover o uso seguro das tecnologias e internet, observar se os direitos humanos são tutelados na rede, propõe estudos, e gera relatórios, promove e a interação com governo e sociedade. <https://www.safernet.org.br/site/institucional/quem-somos/dados-institucionais>. Acesso em 21/09/22.

<sup>27</sup> CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva Jur, 2011. E-book. (1 recurso online). ISBN 9788502136663. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788502136663>. Acesso em: 3 ago. 2022, p.12-16.

Ao longo dos anos a internet está cada vez mais presente no cotidiano através de seus vários mecanismos de utilização, como por exemplo, a digitalização da sociedade, realidade alcançada também no meio criminoso, estão se aprimorando cada vez mais para o uso inadequado da internet.

Não obstante, o cenário pandêmico no mundo em face da Covid – 19 contribuiu negativamente para o aumento na prática dos crimes virtuais, principalmente no que se refere a prática de assédio sexual no ambiente de trabalho remoto, além das inúmeras fraudes em contas de usuários para a obtenção de dados sensíveis e vantagem econômica.

Ademais, o crime virtual denominado – *Phishing* – caracteriza-se por ser um ataque cibernético muito popular, em que os criminosos buscam obter informações bancárias ou pessoais de diversas pessoas por meio da fraude virtual, conforme as lições de Crespo, (2011), a saber:

*Phishing scam* ou *phishing/scam*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros. (CRESPO, 2011)<sup>28</sup>

No Distrito Federal, por exemplo, os crimes virtuais cresceram quatro vezes mais durante o período Covid – 19, segundo levantamento da Polícia Civil do Distrito Federal (PCDF), o estelionato é o crime mais praticado no ambiente virtual com maior incidência de registro nos anos de 2020 e 2021, totalizando nove mil ocorrências<sup>29</sup>.

Segundo a Federação Brasileira de Bancos – FEBRABAN – cerca de 70% dos crimes virtuais são praticados por meio da engenharia social, conforme as afirmações de Crespo, (2011) ao definir a engenharia social da seguinte forma:

Engenharia Social é o Método de ataque onde uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. (CRESPO, 2011).<sup>30</sup>

A engenharia social, portanto, é uma técnica que os criminosos observam e investigam as possíveis vítimas fáceis de serem manipuladas ou induzidas ao fornecimento de dados, suas

<sup>28</sup> **Ibidem. Crespo, (2011).**

<sup>29</sup> BRASIL, Sem antivírus: **crimes na internet crescem quatro vezes durante a pandemia**. Correio Brasiliense. Disponível em: <https://www.correiobraziliense.com.br/cidades-df/2022/02/4986608-sem-antivirus-crimes-na-internet-crescem-quatro-vezes-durante-a-pandemia.html>. Reportagem dia 21/02/22. Acesso em 28/09/22.

<sup>30</sup> **Ibidem. Crespo, (2011).**

informações bancárias, senhas de acesso, número de cartão de crédito, etc. por meio do *Phishing* e que tem aumentado desde o início da pandemia no Brasil.

Nesse sentido, a Lei n.º 14.155 de, 27 de maio de 2021 – Lei contra o Estelionato e o furto virtual – foi inserida no âmbito do Código Penal com o objetivo de punir com rigor a prática de invasão a dispositivos eletrônicos e informáticos como um avanço positivo, além de aumentar a pena significativamente do crime virtual, podendo chegar até 08 (oito) anos de reclusão.<sup>31</sup>

## 1.2 Convenções Internacionais

Os países europeus foram os primeiros a legislar sobre o tema em tela, uma vez que a difusão e acesso aos meios eletrônicos em países com maior poder aquisitivo desde a década de 80, tendo a Corte Europeia realizada a Convenção 108<sup>32</sup>, que originou o Tratado de Estrasburgo.

Além disso, o primeiro documento que visava a proteção dos direitos dos usuários em relação ao tratamento de dados pessoais e o acesso no âmbito internacional; um dos pontos importantes abordado no respectivo Tratado refere-se a possibilidade quanto à correção de dados inseridos erroneamente, fazendo com esse Tratado fosse reconhecido pela sociedade da época como um grande marco inicial legislativo<sup>33</sup>.

### 1.2.1 Convenção de Budapeste

O documento normativo mais relevante internacional em que trata de combate a crimes virtuais é a Convenção de Budapeste, convenção essa que fora aprovada pelo Conselho da União Europeia sobre o *Cibercrime*, alcançando um impacto jurídico colossal, dada a importância, e principalmente por não se tratar apenas de uma convenção europeia, tendo sido reconhecido como uma Convenção internacional<sup>34</sup>.

---

<sup>31</sup> BRASIL, FEBRABAN. **Lei endurece penas para crimes eletrônicos, como clonagem do WhatsApp e outros golpes via internet.** FEBRABAN News. 28/05/2021. Disponível em: <https://portal.febraban.org.br/noticia/3631/pt-br/> acesso em 22/09/22.

<sup>32</sup> COUNCIL OF EUROPE. **Details of Treaty No. 108.1981** <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108>. Acesso em 03/10/2022.

<sup>33</sup> LÓSSIO, Claudio Joel Brito. **Manual Descomplicado de Direito Digital:** guia para Profissionais do Direito e da Tecnologia-2. Ed.rev atual. Ampl- São Paulo: editora JusPodivm, 2021, p.174-175.

<sup>34</sup> **Ibidem. LÓSSIO, (2021, p.176-178).**

A citada convenção não se limitou apenas aos países europeus, assim outros países que não fazem parte da União Europeia são signatários, por exemplo, o Japão, Canadá e o Brasil, o objetivo da convenção de estabelecer regras e cooperação entre os estados signatários para se coibir os crimes cibernéticos, em matéria de direito penal material, foram tipificadas condutas criminosas, referentes as fraudes de computadores, crimes de ódio, direitos autorais. Nas matérias de direito processual, há procedimentos que punem os crimes da internet, além de possibilitar um cooperação internacional entre os signatários.

Nesse contexto, O Brasil ratificou ao tratado apenas em 2021, a Convenção internacional de combate aos crimes cibernéticos tendo sido discutida no Congresso Nacional por longos anos, em face do aumento dos crimes virtuais em suas diversas modalidades até os dias atuais.

Diante da necessidade quanto ao enfrentamento aos crimes virtuais de forma crescente, assim como em face da cooperação entre os Estados na coibição das prática criminosa, foi publicado no âmbito do Congresso Nacional, o Dec. Legislativo n.º 37/2021<sup>35</sup> com o objetivo em fomentar a cooperação internacional no sentido de ampliar a coibição dos crimes virtuais, assim como possibilitar a responsabilização dos autores com mais rigor.

### **1.3 O tratamento jurídico da internet no Brasil: plano legislativo**

O tratamento jurídico brasileiro relacionado aos crimes virtuais iniciou com as primeiras ocorrências registradas no âmbito dos delitos digitais. Registra-se que a primeira lei a tratar especificamente de delitos informáticos no Brasil, foi a lei 12.737/2012,<sup>36</sup> conhecida como – Lei Carolina Dieckmann – em face de a atriz brasileira chamada Carolina Dieckmann Worcnman, ter sido vítima de vazamentos de suas fotos íntimas e sido tais fotografias expostas no meio virtual.

Registra-se que o fato teria ocorrido após a atriz levar para a manutenção o seu dispositivo informático e que diante disso, houve a invasão de tal dispositivo e suas fotografias íntimas teriam sido furtadas e divulgadas na internet em razão de a vítima não ter cedido a

---

<sup>35</sup> BRASIL, **Decreto Legislativo 37**. <https://www2.camara.leg.br/legin/fed/decleg/2021/decretolegislativo-37-16-dezembro-2021-792105-publicacaooriginal-164114-pl.html>. acesso em 04/10/2022.

<sup>36</sup> BRASIL, Lei nº 12.737 de, 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm) acesso em: 19 de maio de 2021.

qualquer chantagem por parte do autor ,o fato ganhou notoriedade ampla na mídia e na sociedade.

Diante da repercussão causada pela violação aos direitos da personalidade da atriz, a promulgação da citada lei ganhou um impulso significativo, tendo em vista a existência de diversos projetos de lei sobre o tema em tela, que não ganharam tamanha visibilidade quanto ao fato suportado pela atriz, tendo sido promulgada a Lei Carolina Dieckmann pela Presidente Dilma Rousseff em 2012.

Ante a isso a norma foi aprovada criando três novos crimes<sup>37</sup> a saber: o art.º.154-A do CP invasão de dispositivo, art.º 266 do CP uma manutenção em seu dispositivo, e o crime do art.º 298 do CP falsificação de cartão, que punem condutas do meio digital, a referida lei alterou o Código Penal.<sup>38</sup>

O delito invasão de dispositivo introduzido pelo art.º 154-A do Código Penal é o delito classificado por crime de informática puro, desse modo o delito tem por finalidade atingir o sistema de computador.<sup>39</sup> A conduta punida no artigo 154-A do Código Penal refere-se à invasão de dispositivos informáticos alheios, quebrando os sistemas de segurança ou instalando *malwares*<sup>40</sup>.

A proteção visa tutelar o direito à privacidade e intimidade do usuário nos moldes dos direitos e garantias fundamentais consagrados pela Constituição de 1988 e confere a preservação desses direitos contra qualquer forma de invasão através de qualquer meio, inclusive o virtual, ademais, o art.º 5, inciso X, da CF/88 dispõe que: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Ressalta-se ainda que a lei Carolina Dieckmann foi recentemente alterada pela lei n.º 14.155/21. Nesse sentido, a ação penal em face dos crimes virtuais é condicionada a representação da vítima, salvo se os crimes ocorrerem com a administração pública direta e indireta e em qualquer dos poderes legislativo, executivo e judiciário, cometidos contra qualquer ente federativo: União, estados, DF e municípios.

---

<sup>37</sup> BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm). Acesso em 05/10/2022.

<sup>38</sup> **Idem**.

<sup>39</sup> NUCCI, Guilherme de S. **Código Penal Comentado**: Grupo GEN, 2021. E-book. ISBN 9788530993443. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530993443/>. Acesso em: 12 out. 2022, p.803-804.

<sup>40</sup> CUNHA, Rogerio Sanches, **Código Penal para concursos**: CP. 14. ed., rev., atual e ampl. Salvador: juspodivm 2021, p.574-579.

### 1.3.1 Marco Civil da Internet

É a principal norma federal que regulamenta o uso da internet no Brasil<sup>41</sup>, estão estabelecidos os objetivos, os princípios, garantias e deveres, do uso na internet, o Marco civil especifica diretrizes para a atuação do poder público, incluindo o tema de inclusão digital e educação informática<sup>42</sup>.

O Brasil é um dos primeiros países a normatizar a regulamentação da internet no mundo<sup>43</sup>, o marco civil busca o controle dos conteúdos, seus princípios buscam proteção do usuário, assim como elenca os direitos fundamentais que precisam ser respeitados, protegem os dados, a privacidade do usuário<sup>44</sup>.

Destaca-se que o Marco Civil da internet, não tipifica condutas penais, tendo em vista que as condutas que possam resultar da prática de qualquer modalidade de crime virtual serão observadas o Código Penal, bem como no âmbito da compensação por dano civil ou mesmo no âmbito da responsabilidade civil objetiva, de acordo com o Código Civil vigente.

### 1.3.2 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD)<sup>45</sup>, publicada em 2018, em inspiração por meio da Lei Européia GDPR – *General Data Protection regulation* –<sup>46</sup>, possuindo em sua área de atuação o tratamento de dados, pessoais e no espaço territorial, o seu objetivo na proteção dos direitos fundamentais, da privacidade e da liberdade.

<sup>41</sup> REGINA SIQUEIRA LOUREIRO OLIVEIRA, S. ; GUILHERMINA DE OLIVEIRA, M. Marco Civil da Internet: Uma Questão Tecnológica e Jurídica. **Revista Eletrônica Direito & TI**, v. 1, n. 13, p. 6, 23 jul. 2020. Disponível em <https://www.direitoeti.com.br/direitoeti/article/view/86>. Acesso 08/10/2022.

<sup>42</sup>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,. [Digite o Local da Editora]: Editora Saraiva, 2014. E-book. ISBN 9788502203200. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502203200/>. Acesso em: 06 out. 2022, p.17-30.

<sup>43</sup> **Ibidem. LÓSSIO, (2021, p.140-145).**

<sup>44</sup> LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. [Digite o Local da Editora]: Grupo GEN, 2014. E-book. ISBN 9788522493401. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522493401/>. Acesso em: 06 out. 2022.p.49-59.

<sup>45</sup> GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. [Digite o Local da Editora]: Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555060164/>. Acesso em: 08 out. 2022.

<sup>46</sup> Regulation UE 2016/679. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>. Acesso 08/10/2022.

A referida lei estabelece princípios, direitos dos titulares, controladores e provedores<sup>47</sup>, buscando a transparência, a segurança jurídica e a padronização de leis que proporcionam a proteção uniforme no Brasil e em outras nações.

A LGPD é uma lei recente inserida na sociedade, com grande relevância, tendo em vista que o tratamento de dados pessoais envolve varias questões desde a privacidade, até a informações bancárias e privadas. A referida lei, padroniza o tratamento junto às empresas e órgãos públicos, prevendo penalidade caso seja violada alguma de suas diretrizes.

Além disso, foi criada, no âmbito da respectiva lei a figura da Autoridade Nacional de Proteção de Dados (ANPD)<sup>48</sup> órgão fiscalizador do cumprimento da LGPD, que garante a proteção de dados pessoais, evitar e o vazamento de dados<sup>49</sup>.

#### 1.4 O cibercrime

Os crimes virtuais surgiram de forma contemporânea com o nascimento da própria internet, em meados de 1960 e com os anos essa modalidade criminosa aperfeiçoou-se, tendo em vista que, inicialmente, as práticas de tais delitos consumavam-se através do furto de dados, invasão de sistema, pirataria de programas, etc.

Compreende-se que o estudo do cibercrime<sup>50</sup> tem contribuído positivamente para a sociedade e o mundo jurídico no sentido de possibilitar uma melhor compreensão acerca de suas causas e origens. Ademais, nas ultimas décadas esse cenário se modificou, pois a internet passou a ser vista por muitos criminosos como ‘terra de ninguém’ para o uso sem fronteiras na prática de crimes.

A falsa sensação de impunidade e de anonimato, assim como a dificuldade de se provar a autoria e materialidade, traduz o reflexo negativo quanto ao crescimento da prática de crimes virtuais na atualidade, assim como acarreta as preocupações por parte do Estado, do poder público e da própria sociedade no enfrentamento a tais crimes que surgem a cada dia com

---

<sup>47</sup> LIMA, Cíntia Rosa Pereira D. **Comentários à Lei Geral de Proteção de Dados**. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935796/>. Acesso em: 08 out. 2022.p.280-298.

<sup>48</sup> BRASIL, **Lei nº 13.853 de, 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/113853.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm) acesso em: 19 de maio de 2021.

<sup>49</sup> **Ibidem. PINHEIRO, (2021, p.15).**

<sup>50</sup> Cibercriminalidade- termo criado por Jaishankar. Apud VIANA, Eduardo- **criminologia**, 9. ed. rev. atual. e ampl. Salvador: Juspodivm, 2021, p.519-525.

mais novidades; tais persistências fazem justiça na aplicação de um trabalho em conjunto para coibir essa cultura fraudulenta no meio virtual.

Uma das medidas importantes e já referendada no presente estudo é a Convenção de Budapeste sobre o cybercrime de 2001, sendo este um tratado internacional que objetiva a cooperação internacional no combate ao crime informático.

#### **1.4.1 Evolução e Conceito**

A celeridade com que as tecnologias da informação se modificam e se transformam a cada momento, bem como a forma com que cada vez atinja vários bens jurídicos distintos, trouxe um olhar mais atento para o poder público em face da proteção jurídica da segurança do usuário e dos dados inseridos no ambiente virtual com prioridade no período de 2012 -2022 por parte do Governo Federal.

Os Crimes virtuais possuem natureza transnacional ou mundial, ou seja, ultrapassam fronteiras territoriais de quaisquer pais; a prática dos delitos atinge todas as classes sociais no mundo, de modo que as vítimas são aleatórias e com o mesmo objetivo para os criminosos – a obtenção da vantagem ilícita, nesse contexto:

Verificam-se, pois, várias denominações, dentre as quais crimes de computador, infrações cometidas por meio de computador, crimes por meio da informática, fraude informática, delinquência informática; crimes digitais, *computer-related crimes*, *cybercrimes* ou crimes cibernéticos. (CRESPO, 2011).<sup>51</sup>

Segundo as lições de Viana, (2021) <sup>52</sup> o Cybercrime é definido como: “[...] qualquer comportamento que utilize uma máquina para a manipulação digital de dados, bem como qualquer comportamento desviante.” O cybercrime, portanto, é toda ação criminosa que usa a internet ou um dispositivo para cometer crimes.

Corroborando as afirmações da autora citada, Sydow, (2022) ao conceituar o cibercrime afirma que se trata de uma: “[...] conduta típica, antijurídica e culpável cometida através de recursos informáticos contra bens jurídicos e/ou cometido em face de bem informático”.

Assim sendo, os crimes virtuais são praticas delituosas que se utilizam da rede mundial de computadores, bem como de dispositivos eletrônicos, como ou sem internet, cuja finalidade consiste na violação de dados sensíveis ou complexos para a prática de outras modalidades de

---

<sup>51</sup> **Ibidem. CRESPO, (2011, p.20).**

<sup>52</sup> **Ibidem. VIANA, (2021, p.523).**

crimes sem que haja a exposição direta dos criminosos, mas a utilização do ambiente virtual para a obtenção da vantagem ilícita a qualquer custo.

#### ***1.4.2 Educação Digital***

A importância da evolução da tecnologia em seus variados níveis, sem a abordagem quanto o papel que os usuários de tais mecanismos para a sua utilização de forma adequada, nesse sentido o usuário se caracteriza por qualquer pessoa que utilize a rede mundial de computadores ou dispositivos informáticos.

Além disso, o Conselho Nacional de Justiça – CNJ, por meio da Resolução n.º 332/20, em seu art. 3º, inciso IV, conceitua o usuário da seguinte forma: “[...] pessoa que utiliza o sistema inteligente e que tem direito ao seu controle, conforme sua posição endógena ou exógena ao Poder Judiciário, pode ser um usuário interno ou um usuário externo<sup>53</sup>”.

Para tanto, o papel do usuário nos crimes virtuais possui relevância por ser a parte mais vulnerável, ademais, a falta de cuidado e prudência do usuário pode contribuir para a ocorrência de tais crimes; é preciso que o usuário utilize qualquer sistema com muito cuidado e observância quanto o recebimento de links ou mensagens suspeitas que possam conter algum vírus<sup>54</sup>.

Com uma sociedade cada vez mais digital e conectada, é fundamental que se trate do tema educação digital. A forma com que os usuários da internet se comportam, com relação a segurança, a responsabilidade e a ética, de acordo com as lições de Pinheiro, (2022) ao afirmar que: “[...] devemos formar cidadão que tenha uma educação digital, o cidadão digital deve dominar não só a máquina e os comandos, mas também deve aprender sobre segurança sabendo identificar e-mails ou *softwares* maliciosos”.

Sendo assim, a educação digital precisa ser ensinada e fomentada juntamente com a inclusão social, pois o contato com o mundo digital deve/deveria facilitar a interação social do homem com a máquina; esse contato precisa ser inclusivo em que todos os indivíduos possam ter o acesso e a oportunidade de estudo, assim como na realização de cursos na área da informática através do seu uso consciente, tendo a capacidade e a perícia para agir com ética, responsabilidade e segurança, pois:

Acreditamos, portanto, que a educação digital deve ser promovida simultaneamente à inclusão digital dos usuários, seja dos indivíduos que estão tendo o primeiro contato

---

<sup>53</sup> CNJ, **Resolução N° 332 de 21/08/2020**. <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em 10/10/2022.

<sup>54</sup> **Ibidem. LÓSSIO, (2021, p.59-62).**

com as máquinas somente no ambiente de trabalho, seja da nova geração que já nasceu dentro de uma sociedade totalmente informatizada. Este último grupo necessita de orientação especial, já que crianças e adolescentes estão passando pelo amadurecimento de seus conceitos éticos, morais e de cidadania. É extremamente necessário que pais e escolas invistam na educação digital de seus filhos. Já não basta apenas orientá-los a não abrir a porta de casa para estranhos. Eles precisam saber também que não é seguro abrir e-mails de estranhos. Esse tipo de ensinamento deve ser aplicado em atividades lúdicas e escolares para, no futuro, ser adotado também no ambiente profissional. (PINHEIRO, 2022).<sup>55</sup>

Nesse mesma linha de pensamento, investir na educação digital e na ética durante o uso da internet pode ser considerado como um caminho positivo para possibilitar o melhor conhecimento e preparo do usuário, bem como o investimento em segurança dos dispositivos informático, e por fim, na proteção de dados com maior atenção e transparência.

### ***1.4.3 Elementos Fundamentais***

A doutrina brasileira costuma classificar os crimes virtuais em crimes impróprios e crimes próprios.<sup>56</sup> Os crimes informáticos Impróprios, também são conhecidos por Crimes Informáticos Comuns; são aqueles que ocorrem mesmo sem a existência do dispositivo eletrônico, ou seja, já existem no mundo físico.

As modalidades criminosas têm sido aprimoradas e modernizadas no ambiente virtual de forma ampla através do uso da internet em níveis catastróficos na esfera mundial, pois os autores acreditam que jamais serão punidos com outro meio de comete-los e propaga-los, as agora com o alcance é global .

São crimes que já possuem tipificação no Código Penal, como, por exemplo, os crimes contra a honra – calúnia, injúria, difamação – que podem ser consumados através da verbalização ou de forma escrita, bem como através do uso do ambiente virtual para a prática de extorsões ou ameaça, nos moldes do art. 147 do Código Penal, pois:

---

<sup>55</sup> **Ibidem. PINHEIRO, (2022, p.185).**

<sup>56</sup> **Ibidem. LÓSSIO, (2021, p.200).**

Os crimes digitais impróprios nada mais são que aqueles já tradicionalmente tipificados no ordenamento, mas agora praticados com auxílio de modernas tecnologias. Assim, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modus operandi*.<sup>57</sup>

Nesse sentido Sydow, (2022) afirma que: “[...] os crimes informáticos impuros é a conduta que visa atingir um bem jurídico que não é informático, diverso do informático, crimes contra honra, por exemplo.”<sup>58</sup> Nota-se que o computador é um dos meios de alcance ilimitado para a prática de crimes.

De acordo com Crespo, (2011) ao analisar a consumação dos crimes virtuais no seu aspecto próprio para a tutela do bem jurídico, afirma que as práticas criminosas são: “[...] delitos cujos bens jurídicos atingidos são primordialmente os sistemas informatizados ou de telecomunicações ou dados.”<sup>59</sup>

Conforme já salientado, a invasão de computadores é um dos delitos mais persistente na atualidade, o que de fato ensejou a necessidade quanto às atualizações na legislação e nas políticas de enfrentamento aos crimes virtuais por parte do Estado e do poder público, bem como, no âmbito do próprio Código Penal para garantir a proteção dos usuários no ambiente virtual.

Observa-se, que anteriormente na Lei Carolina Dieckmann, a aplicação da pena era mais branda, agora a nova tipificação possui pena de até 8 anos de prisão, nos termos do art. 154-A do CP, após o advento da Lei nº 14.155 de 2021, que certamente um avanço importante para o enfrentamento aos crimes virtuais no Brasil e no mundo.

Ainda, segundo Sydow, (2022) compreende-se que os crimes virtuais próprios: “[...] são aqueles que são realizados necessariamente no meio informático e que queira atingir bem jurídico lesivo”. Além da violação dos direitos fundamentais e a intimidade das vítimas, a prática dos crimes virtuais maculam a segurança da informação e principalmente os direitos humanos<sup>60</sup>.

Destarte, o Direito Penal informático é um ramo do Direito Penal, que não se enquadra como uma novidade no mundo jurídico, mas possui a mesma importância na tutela dos bens jurídicos dos usuários que utilizam a rede mundial de computadores para a realização de quaisquer tarefas do dia a dia; o alcance da pena penal em face dos crimes virtuais busca a

---

<sup>57</sup> **Ibidem, CRESPO, (2022, p.25).**

<sup>58</sup> **Ibidem, SYDOW, (2022, p323-324).**

<sup>59</sup> **Ibidem, CRESPO, (2022, p.25).**

<sup>60</sup> **Ibidem, SYDOW, (2022, p.276).**

amplitude na proteção dos direitos que já ultrapassaram a esfera física para o ambiente virtual e não poderia ser diferente.

O Conceito Legal de crimes virtuais possui interface com a mesma definição dos crimes praticados fora do ambiente virtual, e que segundo as lições de Reale, (2020) os crimes virtuais possuem os três substratos na tipificação de qualquer outro crime, quais sejam: fato típico, ilícito e culpável, pois:

A estrutura tripartida compreende o fato típico ou ação típica, a antijuridicidade objetiva e a culpabilidade. Na verdade, esta divisão tripartida constituiria uma necessidade de cunho analítico com finalidade explicativa, antes do que um retrato do fenômeno delituoso em sua substância. (REALE, 2020)<sup>61</sup>

Corroborando as afirmações do autor citado, Nucci, (2021) ensina que:

Trata-se de uma conduta típica, antijurídica e culpável, vale dizer, uma ação ou omissão ajustada a um modelo legal de conduta proibida (tipicidade), contrária ao direito (antijuridicidade) e sujeita a um juízo de reprovação social incidente sobre o fato e seu autor, desde que existam imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme o direito (culpabilidade). (NUCCI, 2021).<sup>62</sup>

Desta feita, a tipificação dos crimes virtuais funciona como a extensão da proteção e da preservação dos direitos e garantia de todos os indivíduos poderem ter um acesso às inovações tecnológicas com segurança e dignidade, pois a persistência de crimes já existentes não pode/poderiam ser tolerados também no ambiente virtual.

## 1.5 Sujeitos dos crimes da internet

Nos crimes da internet, o sujeito passivo pode ser qualquer pessoa, caso ocorra o crime é necessário que seja feita uma ocorrência junto a autoridade policial, bem como a apresentação de provas que possam contribuir para a elucidação do crime virtual praticado, como, por exemplo, *prints* de conversas, links suspeitos recebidos, número de IP, etc.

O autor do crime virtual também pode ser cometido por qualquer usuário, que possua ou não possuir conhecimentos informáticos, mesmo sabendo que existem delitos que precisam de um grande domínio da arquitetura digital para a sua consumação, assim como outros crimes que não necessitam de nenhum conhecimento específico.<sup>63</sup>

---

<sup>61</sup> JR., Miguel R. **Fundamentos de Direito Penal**: Grupo GEN, 2020. E-book. ISBN 9788530991609. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530991609/>. Acesso em: 13 jan. 2023.

<sup>62</sup> **Ibidem**, NUCCI, (2021, p.98).

<sup>63</sup> BIOLCATI, Fernando Henrique De O. **Internet, Fake News e Responsabilidade Civil das Redes Sociais. (Coleção Direito Civil Avançado)**. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2022. E-book. ISBN

Quando os crimes virtuais são abordados na sociedade, logo a figura dos hackers surge como protagonistas na autoria e materialidade dessa modalidade criminosa, tendo em vista a perícia com o uso dos sistemas e programas para propagar a invasão de dados e informações bancárias de qualquer usuário no mundo.

Os *hackers* são identificados pela facilidade na utilização de sistemas e programas de diferentes níveis informáticos para a investida na prática de crimes virtuais, possuindo um domínio significativo no âmbito da segurança da informação que dificulte a sua localização por parte das autoridades, ou mesmo de suas vítimas.

Nesse sentido, Crespo, (2011)<sup>64</sup> ao estudar o conceito de um usuário *hacker*, afirma que: “[...] a tal palavra é no sentido daquele que invade sistemas em benefício próprio, obtendo dados e informações alheias (documentos, programas, músicas etc.), mas sem danificar nada”.

Os *Crackers* por sua vez, são os verdadeiros *ciber* piratas, pois possuem amplo conhecimento e habilidade na invasão de sistemas informáticos. De acordo com Sydow, (2022) os *hackers* se classificam como: *White Hats* – chapéus brancos –, o *Gray Hats* – chapéus cinza – e os *Black Hats* – chapéus negros.<sup>65</sup>

Ainda por cima, os chapéus brancos são os *Hackers* propriamente ditos, tendo em vista que agem apenas por curiosidade, não tendo qualquer intenção de provocar lesão a patrimônio, ou provocar qualquer dano, tais figuras no ambiente virtual trabalham para detectar alhas no sistema, melhorar programas.

Já o “*Black Hats*”, chapéus negros, também conhecidos por *Crackers* são os usuários que utilizam a rede para cometer delitos, e trazer prejuízo.

Nesse sentido, Crespo, (2011)<sup>66</sup> afirma que: “[...] O cracker é aquele que, basicamente, “quebra” um sistema de segurança, invadindo-o, fanáticos pelo vandalismo, também adoram “pichar” páginas da web deixando, na maioria das vezes, mensagens de conteúdo ofensivo e racista”.

Por fim, existe a figura dos “*Gray Hats*” ou chapéus cinza, que são os usuários que podem usar o seu conhecimento para o bem ou usam tais habilidades para o mal. Ademais, os hackers não atacam apenas pessoas físicas, mas também através dos *ciberataques*, que são ataques realizados por grupos terroristas, voltados para através do mundo digital.

---

9786556276410. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786556276410/>. Acesso em: 08 out. 2022, p.178.

<sup>64</sup> **Ibidem, CRESPO, (2011, p.26).**

<sup>65</sup> **Ibidem, SYDOW, (2022, p.330).**

<sup>66</sup> **Idem. Ibidem. p. 330-331.**

Os dados são formados por conjunto de algoritmos, que contem registros, informações processadas que geram conteúdo informativo, além do grande volume de dados circulando na rede conhecido pela ciência da *Big Data*<sup>67</sup>, que estuda, analisa e processam grandes conjuntos de dados, sua proteção destes é uma preocupação mundial.

O art. 3º, I da Resolução 332 do CNJ conceitua Algoritmo por: “[...] sequência finita de instruções executadas por um programa de computador, com o objetivo de processar informações para um fim específico<sup>68</sup>”. Hoje, os dados possuem valor inestimável, pois quem os controla possui mais poder; a crescente preocupação não é apenas do governo, mas também da população.

Além disso, grandes empresas do ramo informáticos denominadas *Big Techs*, possuem a hegemonia do mercado tecnológico, além de sedes no Vale do Silício na Califórnia; as empresas de tecnologia movimentam milhares de dólares por ano, bem como são versáteis em seus produtos, desde aplicativos de armazenamento na nuvem, ate grandes redes sócias como o *Facebook*.

Demandas envolvendo as *Big Techs*, são cada vez mais comuns devido ao grande volume de dados circulando na rede; violam direitos do consumidor, de livre concorrência, da privacidade de dados e vazamento de dados.

Observa-se ainda que, juntas, as empresas possuem um patrimônio valiosíssimo, além do controle de milhares de dados de inúmeros usuários. No que se refere ao tratamento de dados, registra-se que todas as operações são realizadas com os dados pessoais, desde a coleta, o armazenamento, e o descarte dos mesmos.

O Marco Civil da internet, em seu art. 3º, bem como através da aplicação de seus princípios norteadores, expressa uma preocupação na preservação dos direitos fundamentais, sobretudo com a intimidade, privacidade e liberdade de expressão, e o tratamento dos dados.<sup>69</sup>

---

<sup>67</sup> Big Data refere-se a situações em que as tecnologias digitais são utilizadas para lidar com grandes e diversas quantidades de dados e às várias possibilidades de combinação, avaliação e processamento desses dados por autoridades privadas e públicas em diferentes contextos. Cinco características são frequentemente utilizadas para identificar Big Data: Os cinco “Vs”. As possibilidades de acesso a enormes quantidades de dados digitais (High Volume), de diferentes tipos e qualidade, assim como diferentes formas de coleta, armazenamento e acesso (High Variety), e a alta velocidade do seu processamento (High Velocity). O uso da inteligência artificial em particular torna possível novas e altamente eficientes formas de processamento de dados, bem como a verificação de sua consistência e garantia de qualidade (Veracity). Além disso, os Big Data são objeto e base de novos modelos de negócios e de possibilidades para diversas atividades de valor agregado (Value). WOLFGANG, Hoffmann-Riem. **Teoria Geral do Direito Digital**. [Digite o Local da Editora]: Grupo GEN, 2021. E-book. ISBN 9786559642267. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559642267/>. Acesso em: 11 out. 2022, p. 44.

<sup>68</sup> **Ibidem**. CNJ, (2020).

<sup>69</sup> **Art.º 3 do Marco Civil**. A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

Compreende-se, por tanto, que a inteligência artificial são bases de dados que reproduzem comportamentos humanos tanto físicos como sentimentais do usuário, fazendo escolhas pré-selecionadas previamente programadas, gerando um padrão de acordo com o perfil.

Por fim, a resolução 332 do CNJ, no seu art. 3º, inciso II conceitua a inteligência artificial como um: “[...] conjunto de dados e algoritmos computacionais, concebidos a partir de modelos matemáticos, cujo objetivo é oferecer resultados inteligentes, associados ou comparáveis a determinados aspectos do pensamento, do saber ou da atividade humana.”<sup>70</sup>

---

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

<sup>70</sup> **Ididem. CNJ, (2020).**

## 2. A ESTRUTURA JURÍDICA DO CRIME DE ESTELIONATO

O vocábulo estelionato adveio no Latim- *stelionattu*, sua origem decorre da influência do Direito Romano, estelionato remete a característica do réptil camaleão, animal que como uma de suas características a mudança de cor dependendo da situação.<sup>71</sup> Na linguagem jurídica é um tipo penal que reflete a forma para enganar ou adquirir coisas, via uma fraude, pois:

A ação tipificada é obter vantagem ilícita (para si ou para outrem), em pre-juízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento. A característica fundamental do estelionato é a fraude, utilizada pelo agente para induzir ou manter a vítima em erro, com a finalidade de obter vantagem patrimonial ilícita. (BITENCOURT, 2022).<sup>72</sup>

No ordenamento jurídico brasileiro, a figura do estelionato surgiu com as Ordenações Filipinas no livro 5, Capítulo 65, ao qual buscava punir a conduta de fraude que obtivesse vantagem econômica em negociações, com intuito de fraudar bens alheios, além do mais, a figura típica com as características que o estelionato possui atualmente, surgiu no Código Penal de 1830, ademais nos Códigos brasileiros subsequentes 1981 e no vigente código penal 1940, a figura estelionato permaneceu.<sup>73</sup>

### 2.1 Figura jurídica do estelionato clássico

Segundo as lições Loureiro, (2014) no direito comparado a tipificação da conduta do estelionato baseia-se em dois modelos: o modelo alemão, ao qual descreve a conduta de estelionato por obter vantagem indevida pelo engano da vítima, que gera o prejuízo patrimonial, nesse modelo não se exige qualquer tipo de qualificação típica do engano, o estelionato, portanto busca-se priorizar a objetividade, a saber:

O modelo alemão de Betrug proscreve a conduta daquele que obtém vantagem indevida a partir da criação ou manutenção de um engano da vítima, que provoca a disposição patrimonial induzida por erro. Não há exigência legal de qualquer qualificação específica desse engano, o qual simplesmente deve recair sobre fato. (LOUREIRO, 2014).<sup>74</sup>

<sup>71</sup> BITENCOURT, Cezar R. **Tratado de direito penal: parte especial: crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos - arts. 155 a 212.** v.3. [Digite o Local da Editora]: Editora Saraiva, 2022. E-book. ISBN 9786553622074. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786553622074/>. Acesso em: 13 jan. 2023, p. 152.

<sup>72</sup> **Idem. p.154.**

<sup>73</sup> LOUREIRO, Antônio Carlos Tovo. **Perfil do estelionato contratual no ordenamento jurídico-penal brasileiro.** 2014. Tese (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015. doi:10.11606/T.2.2015.tde-26082015-113642. Acesso em: 2022-10-26, p.9.

<sup>74</sup> **Ibidem. LOUREIRO, (2014, p. 16).**

Ademais, o segundo modelo refere-se ao modelo francês no qual o estelionato exige uma qualificação do erro, que se consolida na realização da fraude, este modelo observa a subjetividade, das ações do sujeito, pois:

*Escroquerie* alicerça-se a partir da enumeração de situações típicas. O tipo penal francês exige uma qualificação do engano, que será cristalizado em manobras fraudulentas, utilização de nome ou de qualidade falsa ou abuso de qualidade verdadeira. (LOUREIRO, 2014).<sup>75</sup>

Ademais, o crime de estelionato está elencado no Código Penal de 1940, em seu art. 17, caput, bem como seguindo o modelo adotado pelo Brasil nos moldes do conceito francês da figura do estelionato. No CP, o estelionato encontra-se, na parte especial do código, no título II, dos crimes contra o patrimônio, cuja finalidade é proteger a inviabilidade do patrimônio, podendo este ser móvel ou imóvel, e tutela as pessoas física ou jurídica.<sup>76</sup>

Nota-se que na ação praticada necessita está presente a conduta – obter para si ou para outrem vantagem ilícita e prejuízo alheio – o binômio vantagem ilícita e prejuízo alheio é imprescindível na conduta do agente, pois o prejuízo pretendido, ou vantagem gerada pode ser qualquer natureza, não precisa ser apenas econômico<sup>77</sup>.

De acordo com Bitencourt, (2019) existe a duplicidade do nexos causal, ou seja, possuía a dupla relação de causa e efeito, a fraude seria a causa, e o engano se caracterizaria o efeito. O Estelionato é, portanto um crime de duplo resultado.<sup>78</sup>

O núcleo do tipo penal está descrito nos verbos: 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.<sup>79</sup>

Induzir significa persuadir, incutir, provocar o engano ou a falsa percepção da realidade, o verbo manter no crime de estelionato tem o sentido permanecer, persistir, na situação em que se encontra enganado, persuadido, e pôr fim a vantagem ilícita abrange qualquer tipo de benefício.

---

<sup>75</sup>**Ibidem.p.16.**

<sup>76</sup>BALDAN, Édson Luís. **Estelionato. Enciclopédia jurídica da PUC-SP.** Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Penal. Christiano Jorge Santos (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/425/edicao-1/estelionato>. Acesso em 26/10/2022

<sup>77</sup> **Ibidem. GRECO, (2021, p.536).**

<sup>78</sup> **Idem. BITENCOURT, (2019, p.845).**

<sup>79</sup> **Grifo nosso.**

Ressalta-se que a vantagem no crime de Estelionato art. 171 do CP, é uma vantagem ilícita, caso a vantagem seja lícita o crime não será estelionato, passando o agente configurar o tipo penal do crime de Exercício arbitrário das próprias razões art. 345 do CP.<sup>80</sup>

O elemento ardid se entende pela astúcia, a conversa enganosa, é a fraude em sentido imaterial, utiliza-se da conversa para enganar a vítima. Por fim qualquer outro meio fraudulento caracteriza por qualquer forma, escrita ou não, falando ou em silêncio, na ação ou omissão.<sup>81</sup>

De acordo com Capez, (2015) existem quatro fases no crime de estelionato: 1) o emprego da fraude pelo agente, 2) o erro que a vítima incorreu, 3) a obtenção da vantagem ilícita pelo autor e 4) a vítima sofre o prejuízo.<sup>82</sup>

## 2.2 Elementos subjetivos e objetivos do tipo

O crime de estelionato possui como elemento subjetivo o dolo, não possuindo a modalidade culposa, pois o delito em tela admite coautoria e participação, ainda quanto as características do delito, compreende-se que o sujeito ativo pode ser cometido por qualquer pessoa, sendo assim, um crime comum, além disso, no tocante ao sujeito passivo este pode ser vítima qualquer pessoa física ou jurídica, com ou sem personalidade, desde que a vítima seja determinada, e que sofra prejuízo patrimonial.<sup>83</sup>

Nota-se que a vítima precisa ter capacidade de discernimento para ser enganada, caso não possua, ocorrerá o crime de Abuso de Incapaz elencado no art. 173 do CP. A forma tentada do crime é possível,<sup>84</sup> e a consumação no crime de estelionato ocorre com a obtenção da vantagem ilícita, ou seja, é quando o sujeito alcança o proveito econômico, provocando prejuízo a vítima.

Nesse sentido, o Superior Tribunal de Justiça – STJ pacificou o entendimento acerca da obtenção da vantagem no crime de estelionato conforme o teor do informativo nº 663, a saber:

Se o crime só se consuma com a efetiva obtenção da vantagem indevida pelo agente ativo, é certo que só há falar em consumação, nas hipóteses de transferência e depósito, quando o valor efetivamente ingressa na conta bancária do beneficiário da fraude. (BRASIL, 2020).<sup>85</sup>

<sup>80</sup> CUNHA, Rogério Sanches, **Código Penal para concursos: CP**. 14 ed. rev, atual e ampl. Salvador: juspodivm 2021, p.667.

<sup>81</sup> CAPEZ, Fernando; Prado, Stela. **Código penal comentado**. 6. ed. São Paulo :saraiva, 2015, p.408-409.

<sup>82</sup> **Idem. ibidem**.p409.

<sup>83</sup> **Ibidem. CUNHA, (2021, p.668).**

<sup>84</sup> **Idem. GRECO, (2021, p. 538).**

<sup>85</sup> BRASIL, Superior Tribunal de Justiça – STJ. **informativo nº 663, 14 de fevereiro de 2020**. CC 169.053-DF, Rel. Min. Sebastião Reis Júnior, Terceira Seção, por unanimidade, julgado em 11/12/2019, DJe 19/12/2019. <https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisarumaedicao&livre=0663.cod.acesso> em 13/10/2022.

Dadas as contribuições acerca da identificação do estelionato em sua essência para o mundo jurídico e seus efeitos na sociedade, à luz do entendimento no âmbito do STJ, merece destaque uma análise sucinta a respeito de algumas espécies de estelionato para a elaboração do presente estudo.

### **2.2.1 A torpeza bilateral**

A Torpeza bilateral ou também conhecida por torpeza liberal ocorre na situação em que o autor e a vítima agem com dolo em situação simultânea e proporcionalmente opostas<sup>86</sup>. É possível que ocorra a situação de torpeza bilateral, pois o tipo penal não faz referência a intenção moral ou boa-fé da vítima.

O autor do estelionato também é enganado pela vítima, ou seja, ele pratica e sofre a ação do engano, mesmo que tenha agido por cobiça, não afasta a sua conduta delituosa de estelionato<sup>87</sup>.

### **2.2.2 Estelionato judicial**

O Estelionato judicial caracteriza-se pela utilização abusiva do sistema judiciário, tendo em vista alguma vantagem pessoal, utilizando de manobras, fundamentos ou teses não apropriadas, com intenção de direcionar o poder judiciário ao erro. O STJ não aceita essa prática, pois não a previsão legal, sendo, portanto, conduta atípica, pois:<sup>88</sup>

3. O estelionato judicial consiste no uso do processo judicial para auferir lucros ou vantagens indevidas, mediante fraude, ardil ou engodo, ludibriando a Justiça, com ciência da inidoneidade da demanda. Percebe-se que a leitura das elementares do art. 171, caput, do Código Penal deve estar em consonância com a garantia constitucional da inafastabilidade jurisdicional (CF, art. 5º, XXXV), do que decorre o entendimento segundo o qual o direito de ação é subjetivo público e abstrato, em relação ao direito material.

Desse modo, verifica-se atipicidade penal da conduta de invocar causa de pedir remota inexistente para alcançar consequências jurídicas pretendidas, mesmo que a parte ou seu procurador tenham ciência da ilegitimidade da demanda.

4. A conduta constitui infração civil aos deveres processuais das partes, nos termos do art. 77, II, do Código de Processo Civil, e pode sujeitar a parte ao pagamento de multa e indenizar a parte contrária pelos danos processuais, consoante arts. 79, 80 e 81 do Código de Processo Civil ilícito processual. Outrossim, conforme art. 34, XIV, da Lei n. 8.906/1994, verifica-se infração profissional do advogado deturpar a situação fática

<sup>86</sup> JALIL, Mauricio S.; FILHO, Vicente G. **Código Penal comentado: doutrina e jurisprudência**. Editora Manole, 2022. E-book. ISBN 9786555767360. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555767360/>. Acesso em: 14 out. 2022, p.587.

<sup>87</sup> **Ibidem. CUNHA, (2021, p. 667).**

<sup>88</sup> **Ibidem. GRECO, (2021, p.1.260).**

com o objetivo de iludir o juízo. Conclui-se, pois, que a conduta descrita não configura infração penal, mas meramente civil e administrativa, sujeita à punição correlata.

5. Habeas corpus não conhecido. Ordem concedida, de ofício, para absolver a paciente quanto ao delito de estelionato tentado (Ação Penal n. 023634-39.2011.8.26.0196).<sup>89</sup>

### **2.2.3 Estelionato contratual**

O estelionato contratual ocorre quando um contrato é firmado e um dos agentes age com intenção de enganar, induzir ao erro e fraudar o patrimônio alheio, ou seja, uma das partes desde o início age com intenção de fraude, não existe a boa-fé, o contrato é um meio usado para se cometer a fraude, pois:

O estelionato contratual difere da modalidade mais usual do estelionato pela inovação quanto ao meio: no estelionato contratual, o instrumento do embuste materializa-se em contrato celebrado entre agente e vítima. Sua principal característica é que o dolo da prática delitativa já estava presente antes mesmo da celebração do negócio jurídico. Em outras palavras, o agente realiza o contrato sabendo, de antemão, que não irá cumpri-lo em sua integralidade. (LOUREIRO, 2020).<sup>90</sup>

Nota-se que a simples inadimplência ou atraso no pagamento não caracteriza o crime de estelionato, o agente não age com dolo de fraudar, apenas não pode no momento cumprir com sua obrigação.

### **2.2.4 Estelionato sentimental**

No estelionato sentimental a vítima é induzida a erro referente à intenção pretendida, o sujeito ativo desde o início do relacionamento age com intuito de obter vantagem, de enganar a vítima e utiliza-se do abuso de confiança obtida pelo relacionamento, além disso, a vítima sofre não só a perda patrimonial, mas também possui a perda sentimental e em alguns casos a violência psicológica, crime do art.147-B do CP.

Embora o crime de estelionato sentimental ocorra no mundo físico, suas vítimas não encontram tipificação legal no Código Penal atualmente, contudo na Câmara Legislativa possui um projeto de Lei nº 6.444 de 2019, em tramitação, de autoria do deputado Júlio Cesar Ribeiro, que busca preencher essa lacuna legal, pois:

Este Projeto de Lei busca tipificar o chamado “estelionato sentimental”. Cumpre ressaltar que cresce a cada dia o número de estelionatos praticados por pessoas que se aproximam do outro com a finalidade de se apropriar de seus bens, aproveitando-se de uma possível vulnerabilidade emocional e amorosa. Entende-se que o estelionato tem por característica induzir alguém a uma falsa concepção de algo com o objetivo

<sup>89</sup> BRASIL, Superior Tribunal de Justiça – STJ. Quinta turma. (HC 435.818/SP, Rel. Ministro RIBEIRO DANTAS, QUINTA TURMA, julgado em 03/05/2018, DJe 11/05/2018). Acesso em 14/10/2022.

<sup>90</sup>*Ibidem*. *Idem*. LOUREIRO, (2015, p. 17).

de adquirir benefício ilícito para si ou para outrem. Deste modo, partindo para a definição da palavra sentimental, observamos que a mesma está intimamente ligada a sentimento ou sensibilidade, bem como a capacidade de sentimentos positivos em relação a outrem, na denominação da psiquiatria forense. A relação interpessoal está fortemente vinculada a fatores de confiança, honestidade e fidelidade de um para o outro. Assim, quando ocorre o rompimento desses elementos essenciais, há o estelionato emocional. É preciso reconhecer que, nessa espécie de estelionato, o prejuízo não é apenas material, mas moral e psicológico também. Outrossim, é certo que tais condutas são repulsivas quando praticadas contra qualquer pessoa, mas tornam-se ainda mais repugnantes quando a vítima é um idoso ou pessoa que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato. Isso porque são alvos mais fáceis deste tipo de crime, pois são mais vulneráveis e costumam agir de boa-fé. Por essa razão, os autores desses delitos devem ser apenados com maior rigor. Desse modo, é indubitável que o presente projeto de lei traz importante modificação em nosso ordenamento jurídico, motivo pelo qual contamos com o apoio de nossos ilustres Pares para a sua aprovação. (BRASIL, 2019).<sup>91</sup>

Por não haver a previsão legal do tipo estelionato sentimental, a conduta punida a depender do caso concreto poderá ser tipificada como extorsão art.158 do CP, a depender do caso se envolver conotação sexual poderá caracterizar o crime de violação mediante fraude, nos termos do art. 215 do CP, ou ainda, se a fraude ocorre pelos meios informáticos, pode caracterizar o crime de fraude eletrônica, nos termos do art.171, parágrafo 2-A do CP.

### ***2.2.5 Estelionato e furto mediante fraude***

O crime de estelionato em sua modalidade comum refere-se ao êxito na obtenção de qualquer vantagem econômica em decorrência de comportamentos fraudulentos que possa acarretar em prejuízo alheio, nos termos do art. 171, caput, do Código Penal de 1940, já o crime de furto mediante fraude consuma-se na situação em que o indivíduo altera o sistema de medição para alterar o resultado deste, por exemplo.

Corroborando as afirmações acerca da distinção entre os crimes em tela, o STJ entende que:

3. O caso dos autos revela não se tratar da figura do "gato" de energia elétrica, em que há subtração e inversão da posse do bem. Trata-se de prestação de serviço lícito, regular, com contraprestação pecuniária, em que a medição da energia elétrica é alterada, como forma de burla ao sistema de controle de consumo, - fraude -, por induzimento ao erro da companhia de eletricidade, que mais se adequa à figura descrita no art. 171, do Código Penal – CP (estelionato). 4. Recurso especial

---

<sup>91</sup>BRASIL, Câmara dos Deputados. **Projeto de Lei nº 6444 de 2019**. [https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra;jsessionid=B1CAB48BBA21A23952DBC0DAEB04A26D.proposicoesWebExterno2?codteor=1854385&filename=Avulso+-PL+6444/2019](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=B1CAB48BBA21A23952DBC0DAEB04A26D.proposicoesWebExterno2?codteor=1854385&filename=Avulso+-PL+6444/2019). Acesso em 26/10/2022.

desprovido. (BRASIL, STJ – AREsp 1418119/DF, Rel. Ministro JOEL ILAN PACIORNIK, QUINTATURMA, julgado em 07/05/2019, DJe 13/05/2019)<sup>92</sup>

Destarte, o crime de furto mediante fraude está elencado no art. 155, § 4<sup>a</sup>, inciso, II do Código Penal e define a conduta em que o furto consuma-se a concordância ou participação da vítima, reconhecido popularmente como a prática de fazer “gato”, tendo em vista que a fraude é empregada para diminuir a vigilância da vítima com o objetivo e a inversão da posse.

Entretanto, no crime de estelionato o sujeito obtém a transferência da coisa que é entregue pela própria vítima induzida, previamente a erro em razão do artifício usado pelo criminoso na fraude empregada.

### **2.2.6 Estelionato privilegiado**

A prática do crime de estelionato também alcança a modalidade privilegiada para atenuar a responsabilização penal do autor, pois nem sempre a investida na obtenção da vantagem atinge um bem jurídico de valor expressivo, e por tanto, o Direito Penal busca a responsabilização por meio do instituto do crime privilegiado, conforme consta no teor do art. 171, § 1<sup>o</sup>, do Código Penal<sup>93</sup>.

Para tanto, a forma privilegiada do estelionato é semelhante à forma privilegiada do crime de furto, pois alcança os mesmos requisitos quanto à primariedade do autor, assim como ser o objeto do crime de pequeno valor. Ocorre que, no crime de estelionato, o valor sobre a coisa tem por parâmetro o salário mínimo vigente.

Cuida-se de uma minorante obrigatória, além da possibilidade de a pena de reclusão poder ser substituída pela de detenção, ou ainda, ocorrer à diminuição destas de um a dois terços ou aplicar apenas a multa. Caso o crime seja apenas tentado leva-se em consideração o valor pretendido<sup>94</sup>.

As figuras equiparadas do crime de Estelionato estão elencadas no § 2<sup>o</sup> do art. 171, - Nas mesmas penas incorre quem:

#### **a) Disposição de coisa alheia como própria**

---

<sup>92</sup> CAVALCANTE, Márcio André Lopes. **Adulterar o sistema de medição da energia elétrica para pagar menos que o devido: estelionato (não é furto mediante fraude)**. Buscador Dizer o Direito, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/11704817e347269b7254e744b5e22dac>. Acesso em: 31/10/2022

<sup>93</sup> **Ibidem. Decreto-Lei 2.848/40.**

<sup>94</sup> **Ibidem. BITENCOURT, (2019, p.849).**

“I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria [...]”;

O agente age ou se dispõe de coisa alheia através de negociação de má fé sobre coisa alheia como se sua, podendo ser coisa móvel ou imóvel em face de um terceiro que age em de boa fé.<sup>95</sup> Além disso, as condutas relacionadas ao crime em tela equivalem a: vender, permutar, dá em pagamento ou em garantia,

Essa espécie se consuma com a realização de qualquer dos verbos, o a ação e negociar coisa alheia como própria. O sujeito ativo age com má fé, o sujeito passivo precisa está com a fé. Aqui se refere ao adquirente, o terceiro envolvido e também configura vítima o dono<sup>96</sup>.

#### **b) Alienação ou oneração fraudulenta de coisa própria**

“II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias [...]”;

O sujeito vende coisa (móvel ou imóvel) sua, porem essa coisa é impenhorável, age omitindo a existência de gravame, uma restrição, é, portanto, um crime próprio, objeto material também muda, não mais se fala da figura coisa alheia, agora a figura e coisa sua.

O sujeito ativo e o dono da coisa, que é impedido por lei de alienar ou onerar o bem, o sujeito passivo e quem recebe a coisa, sem saber dos impedimentos. Ou seja, sem a ciência do ônus impeditivo da alienação.<sup>97</sup>

#### **c) Defraudação de penhor**

“III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado [...]”;

A ação realizada é defraudar – lesar – ou tirar algo alheio, o tipo penal existe um contrato com garantia pignoratícia; o sujeito ativo é o devedor que possui a posse de coisa penhorada, e o sujeito passivo será o credor do penhor.

---

<sup>95</sup> GONÇALVES, Victor Eduardo R.; LENZA, Pedro. **Esquematizado - Direito Penal - Parte Especial**. [Digite o Local da Editora]: Editora Saraiva, 2022. E-book. ISBN 9786555597738. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555597738/>. Acesso em: 14 out. 2022, p.532.

<sup>96</sup> **Ibidem. BITENCOURT, (2022, p.159).**

<sup>97</sup> **Ibidem. BITENCOURT, (2022, p.159).**

Atente-se para a diferença de defraudação de coisa penhorada, que não configura o crime elencado no inciso III, pois penhora significa servir de garantia na execução, e não pode confundir com penhor que significa garantia de débito.

A defraudação de penhora fraude, ao devedor utilizam-se os bens para garantir a quitação do débito, caracterizando um ilícito civil, ademais a defraudação de penhora pode levar o devedor a insolvência, cometesse-se o crime de Fraude a Execução Art. 179 do CP – “Fraudar execução, alienando, desviando, destruindo ou danificando bens, ou simulando dívidas”<sup>98</sup>.

**d) Fraude na entrega de coisa**

“IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém [...]”;

A ação do delito equivale-se a defraudar, adulterar, modificar por meio de fraude a substância, a essência da coisa, alteração pode ser na qualidade, quantidade que será entregue a alguém, a entrega de coisa gratuita na configura o delito, pois não trará consequência o dano ao patrimônio.

Nota-se que, caso a defraudação que ocorra envolva alimentos, alterados na sua essência, o crime será o elencado no artigo 272 do CP<sup>99</sup>, “Falsificação, corrupção, adulteração ou alteração de substância ou produtos alimentícios”

Ademais, se a fraude recair sobre medicamentos ou produtos medicinais ou terapêuticos,<sup>100</sup> o crime cometido será o de artigo 273 do CP, “falsificação, corrupção, adulteração ou alteração de produto destinado a fins terapêuticos ou medicinais”, e por sua gravidade é um crime Hediondo previsto na Lei 8.072/90 art.1º, inciso, VII-B.<sup>101</sup>

**e) Fraude para recebimento de indenização ou valor de seguro**

“V - destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro [...]”;

O sujeito ativo neste crime é a segurado e o sujeito passivo será a seguradora, é um crime formal, crime de ação múltipla, o elemento objetivo é o dolo e a finalidade específica de obter, conseguir a receber a indenização do seguro.

---

<sup>98</sup> **Ibidem. CUNHA, (2021, p. 670).**

<sup>99</sup> **Idem. (Decreto-Lei 2.848/40).**

<sup>100</sup> **Ibidem. CUNHA, (2021, p.670).**

<sup>101</sup>BRASIL, Lei 8.072/90- **Crimes Hediondos**. Disponível em [http://www.planalto.gov.br/ccivil\\_03/leis/18072.htm](http://www.planalto.gov.br/ccivil_03/leis/18072.htm). Acesso em 16/10/2022.

Nota-se que o Direito Penal brasileiro não se pune e não se incrimina a autolesão, segundo o princípio da Alteridade, salvo quando a autolesão for realizada agindo fraudulentamente, ou seja, e o meio para obtenção de vantagem indevida econômica está será penalizada<sup>102</sup>.

f) **Fraude no pagamento por meio de cheque**

“VI - emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento [...]”;

A conduta do agente é emitir cheque sem saldo suficiente em poder do sacado, ou frustrar o pagamento, o crime é doloso, não há previsão da modalidade culposa. O sujeito ativo é o emitente, são duas as condutas praticadas, a emissão de cheque sem fundo, e a frustração de seu pagamento mediante ordem do banco sacado.

O cheque que for dado pôs datado não configura a modalidade de estelionato, por ser prática costumeira colocar data na cártula, o pôs datar o cheque já subentende que no momento o dono do cheque não possui dinheiro, esse comportamento tira a natureza do cheque que é uma ordem de pagamento a vista<sup>103</sup>, portanto, não configurando a fraude, exigida para configurar o crime de estelionato.

Nesse sentido, a Súmula 246 STF, “Comprovado não ter havido fraude, não se configura o crime de emissão de cheque sem fundos”.<sup>104</sup> Ademais a vigência da Lei nº 14.155/21, cancelou as Súmulas nº521 do STF, e a Sumula nº 244 do STJ, referentes à competência, atribuindo a competência do estelionato mediante cheque fraudulento, ocorra no lugar da agência bancária da vítima.

Além disso, o Informativo nº728 do STJ: “[...] Estelionato. Tentativa de saque com apresentação de cheque fraudulento. Hipótese não prevista na Lei n. 14.155/2021. Consumação do crime no local onde a vítima possui conta bancária.”<sup>105</sup> Algumas modalidades de fraude obtidas por meio de cheque, ao estão tipificadas no art. 171, caput.

Por exemplo, o cheque de conta encerrada, cheque de terceiro falsificado ou furtado. Nestas situações a competência será do local da obtenção da vantagem ilícita, não incide a alteração da lei nº 14.155/21. Nesse sentido temos a Súmula nº 48 do STJ: “[...] Compete ao

---

<sup>102</sup> CAPEZ, Fernando; Prado, Stela. **Código penal comentado**. 6. ed. São Paulo: Saraiva, 2015, p.418-419.

<sup>103</sup> **Ibidem. CUNHA, (2021, p.671).**

<sup>104</sup> BRASIL, Supremo Tribunal Federal – STF. **Sumula nº 246**.

<sup>105</sup> BRASIL, Superior Tribunal de Justiça – STJ. **Informativo nº728**. CC 182.977-PR, Rel. Min. Laurita Vaz, Terceira Seção, por unanimidade, julgado em 09/03/2022, DJe 14/03/2022.

juízo do local da obtenção da vantagem ilícita processar e julgar crime de estelionato cometido mediante falsificação de cheque.”<sup>106</sup>

Além do mais, a utilização de papel moeda grosseira configura o crime de estelionato, conforme a Súmula nº 73 do STJ: “[...] A utilização de papel moeda grosseiramente falsificado configura, em tese, o crime de estelionato, da competência da justiça estadual.”<sup>107</sup>

### 2.2.7 Estelionato qualificado

No ano de 2021, o crime de estelionato sofreu a alteração após o advento da Lei n.º 14.155 na sociedade, com isso houve a inclusão do parágrafo segundo e das letras A e B, no art. 171, do Código Penal, passando a constar em seu teor a seguinte modalidade de fraude:

#### **Fraude eletrônica**

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

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)

§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência. (BRASIL, 2021).

O § 2º-A do art. 171 do Código Penal elenca a nova modalidade de estelionato virtual; essa qualificadora decorre do meio pelo qual é cometido o estelionato, utilizando as tecnologias das informações. A vítima é induzido a erro e o criminoso, após se apossar das informações pessoais adquiridas, seja por redes sociais, aplicativos ou e-mails obtidos por meio de fraude<sup>108</sup>.

As Causas de aumento de pena do crime de estelionato se encontram no parágrafo 3º, do art. 171, a saber: “[...] A pena aumenta-se de um terço, se o crime for cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência”. Sendo assim, o aumento se justifica por ser cometido contra instituições, pois estas prestam serviços essenciais a população<sup>109</sup>, a causa de aumento é referente à natureza da vítima.

Infere-se ser inaplicável o princípio da insignificância no crime de estelionato quando este é cometido contra a administração pública, por ofender aos princípios da administração da

<sup>106</sup> BRASIL, Superior Tribunal de Justiça – STJ. **Sumula nº 48.**

<sup>107</sup> BRASIL, Superior Tribunal de Justiça – STJ. **Sumula nº 73.**

<sup>109</sup> **Ibidem. GRECO, (2021, p.545).**

moralidade, e ofende diretamente o patrimônio público. Nesse sentido, o STJ pacificou o seu entendimento sobre o tema em tela a partir da sua jurisprudência em teses nº 84 da seguinte forma: “[...] O princípio da insignificância é inaplicável ao crime de estelionato quando cometido contra a administração pública, uma vez que a conduta ofende o patrimônio público, a moral administrativa e a fé pública, possuindo elevado grau de reprovabilidade”<sup>110</sup>.

Nesse contexto, o agente que falsifica documentos e os utiliza para enganar a vítima obtendo a vantagem ilícita, com a finalidade de causar prejuízo alheio, o estelionato absolve a falsificação, e esse é o posicionamento que prevalece.

Dessa forma, merece destaque a Súmula 17 do STJ que diz: “[...] Quando o falso se exaure no estelionato, sem potencialidade lesiva, e por este absorvido”<sup>111</sup>. O crime de falsidade é o crime meio para a consumação do estelionato que é o crime fim, sendo assim o crime de falsidade é absolvido, pelo princípio da absorção ou consumação.

### 2.3 Fraude aplicada no sistema previdenciário

O estelionato previdenciário outra modalidade de crimes fraudulentos de destaque na elaboração do presente estudo, pois ocorre quando o criminoso se utiliza de meios ardiloso, falsificação para receber benefício previdenciário; a conduta é vista como causa de aumento de pena, haja vista que a vítima se trata de entidade autárquica de previdência social<sup>112</sup>.

Segundo o entendimento disposto na súmula 24 do STJ, compreende-se que: “[...] aplica-se ao crime de estelionato, em que figure como vítima entidade autárquica da Previdência Social, a qualificadora do § 3. Q do art. 171 do Código Penal”<sup>113</sup>.

Destarte, questiona-se quando fraude do crime de estelionato previdenciário, o crime é permanente, instantâneo ou continuado, o tema é relevante, pois dependendo do entendimento gera reflexos no cálculo da prescrição<sup>114</sup>.

Quando o próprio beneficiário, utiliza de fraude para receber benefício indevido, trata-se de crime permanente, pois o valor do benefício é mensal, a prescrição assim começa a contar da data do último benefício recebido.

---

<sup>110</sup> BRASIL, Superior Tribunal de Justiça, **jurisprudência em teses nº 84**. <https://www.stj.jus.br/publicacaoainstitucional/index.php/JuriTeses/article/view/11332/11461>. Acesso em 28 de outubro de 2022.

<sup>111</sup> BRASIL, Superior Tribunal de Justiça, **Sumula nº 17**.

<sup>112</sup> CUNHA, ROGERIO SANCHES, **Código Penal para concursos: CP.14º** ed. rev. atual e ampl. Salvador: juspodivm 2021.p.672-673.

<sup>113</sup> BRASIL, Superior Tribunal de Justiça, **Sumula nº 24**.

<sup>114</sup> **Ibidem. p. 672.**

Corroborando esse pensamento, o Supremo Tribunal Federal pacificou o seu entendimento da seguinte forma<sup>115</sup>:

Ementa: PENAL. HABEAS CORPUS. **ESTELIONATO PREVIDENCIÁRIO**. ART. 171, § 3º, DO CÓDIGO PENAL. CRIME PERMANENTE. BENEFICIÁRIO. **PRAZO PRESCRICIONAL**. INÍCIO DA CONTAGEM. CESSAÇÃO DA PERMANÊNCIA. ORDEM DENEGADA. 1. O agente que perpetra a fraude contra a Previdência Social recebe tratamento jurídico-penal diverso daquele que, ciente da fraude, figura como beneficiário das parcelas. O primeiro pratica crime instantâneo de efeitos permanentes; já o segundo pratica crime de natureza permanente, cuja execução se prolonga no tempo, renovando-se a cada parcela recebida da Previdência. 2. Consectariamente, em se tratando de crime praticado pelo beneficiário, o prazo prescricional começa a fluir da cessação da permanência. Precedentes: HC nº 99.112, rel. Min. Marco Aurélio, j. 20/4/2010, 1ª Turma; HC 101.481, rel. min. Dias Toffoli, j. 26/4/2011, 1ª Turma; HC 102.774/RS, rel. Min. Ellen Gracie, j. 14/12/2010, 2ª Turma, DJ de 7/2/2011. 3. In casu, narra a denúncia que o paciente participou não apenas da fraude à entidade de Previdência Social, por meio de conluio com servidor do INSS, mas figurou como destinatário dos benefícios previdenciários, que recebeu até 30/10/2006. 4. Dessa forma, forçoso reconhecer que o prazo prescricional teve início apenas na referida data, em que cessada a permanência. 5. Ordem denegada. (HC 102049, Relator(a): Min. LUIZ FUX, Primeira Turma, julgado em 22/11/2011, ACÓRDÃO ELETRÔNICO DJe-234 DIVULG 09-12-2011 PUBLIC 12-12-2011 RT v. 101, n. 918, 2012, p. 680-684)<sup>116</sup>.

Além disso, o STJ, em seu entendimento publicado na jurisprudência em teses nº 84-4, afirma que:

O delito de estelionato previdenciário (art. 171, § 3º do CP), praticado pelo próprio beneficiário, tem natureza de crime permanente uma vez que a ofensa ao bem jurídico tutelado é reiterada, iniciando-se a contagem do prazo prescricional com o último recebimento indevido da remuneração. (BRASIL, 2021)<sup>117</sup>.

Além do mais, quando um crime de estelionato é cometido por terceiro, refere-se à prática crime instantâneo, bem como no que se refere a sua prescrição, está se inicia na data do recebimento do primeiro benefício indevido, conforme entendimento do STJ em mais uma de suas publicações de julgados na jurisprudência em teses nº 84-5, a saber:

O delito de estelionato previdenciário, praticado para que terceira pessoa se beneficie indevidamente, é crime instantâneo com efeitos permanentes, iniciando-se a contagem do prazo prescricional a partir da primeira parcela do pagamento relativo ao benefício indevido. (BRASIL, 2021)<sup>118</sup>.

<sup>115</sup> CAVALCANTE, Márcio André Lopes. **Estelionato previdenciário (art. 171, § 3º do CP): crime permanente ou instantâneo?** Buscador Dizer o Direito, Manaus. Disponível em: <<https://buscador.dizerodireito.com.br/jurisprudencia/detalhes/9cb67ffb59554ab1dabb65bcb370ddd9>>. Acesso em: 29/10/2022.

<sup>116</sup> BRASIL, Supremo Tribunal Federal – STF. **HC 102049**, Relator (a): Min. LUIZ FUX, Primeira Turma, julgado em 22/11/2011, ACÓRDÃO ELETRÔNICO DJe-234 DIVULG 09-12-2011 PUBLIC 12-12-2011 RT v. 101, n. 918, 2012, p. 680-684.

<sup>117</sup> BRASIL, Superior Tribunal de Justiça, - STJ. **jurisprudência em teses nº 84-4**. <https://www.stj.jus.br/publicacao-institucional/index.php/JuriTeses/article/view/11332/11461>. Acesso em 28 de outubro de 2022.

<sup>118</sup> **Idem. STJ, jurisprudência em teses nº 84-5**.

Ademais, a figura do sujeito que tem direito ao benefício legitimamente, por um período de tempo, deveria ter cessado, porém, continuou a receber em silêncio, ou o beneficiário faleceu e alguém continua a receber o benefício indevidamente, a prescrição se inicia com o último benefício recebido, por ser continuidade delitiva.

Nessa linha de raciocínio, a jurisprudência em tese nº 84-6, do STJ é no sentido de que:

Aplica-se a regra da continuidade delitiva (art. 71 do CP) ao crime de estelionato previdenciário praticado por terceiro, que após a morte do beneficiário segue recebendo o benefício regularmente concedido ao segurado, como se este fosse, sacando a prestação previdenciária por meio de cartão magnético todos os meses. (BRASIL, 2021)<sup>119</sup>.

### **2.3.1 Fraude contra pessoa idosa e vulnerável: Reflexos civis e penais**

É possível que no estelionato previdenciário a reparação do dano, assim como os valores recebidos de forma indevida – antes do recebimento da denúncia – enquadre na figura do arrependimento posterior, nos termos do art. 16 do Código Penal, não se extinguindo a punibilidade do crime, de acordo com art. 171 § 3 do mesmo diploma legal.

De acordo com jurisprudência em teses nº 84-7 do STJ, compreende-se ainda que:

A devolução à Previdência Social da vantagem percebida ilicitamente, antes do recebimento da denúncia, não extingue a punibilidade do crime de estelionato previdenciário, podendo, eventualmente, caracterizar arrependimento posterior, previsto no art. 16 do CP. (BRASIL, 2021)<sup>120</sup>.

O dispositivo foi alterado pela Lei n.º 14.155/21 que incluiu também a vulnerabilidade da vítima, bem como modificando a pena que antes era de 1/3; agora, com a nova redação, a pena é aplicada em dobro. Contudo, por se tratar de novidade legislativa – *novatio legis in melius* –, a modificação poderá retroagir e alcançar quem já cometeu o delito.

Ademais, a vítima do crime em comento deverá ser pessoa idosa com idade de 60 anos ou pessoa considerada como vulnerável para alcançar o aumento de pena, conforme dispõe o art. 171, caput, do Código Penal, e as figuras equiparadas no § 2 do mesmo diploma legal.

Nota-se que, a idade da vítima precisa ser conhecida do agente para se incidir o aumento de pena, caso não saiba este ser alcançado pela figura penal do erro de tipo<sup>121</sup>. Quanto à ação penal, infere-se que também houve modificação com publicação da Lei n.º 13.964/19, conhecida por Pacote Anticrime, esta incluiu o § 5 no art. 171 do CP.

<sup>119</sup>**Ibidem. STJ, jurisprudência em teses nº 84-6.**

<sup>120</sup>**Ibidem. STJ, jurisprudência em teses nº 84-7.**

<sup>121</sup>**Ibidem. GRECO, (2021, p.545).**

Nesse contexto, os crimes de estelionato são de ação penal pública condicionada a representação, aplicando-se também, a exceção constante no §5º do artigo citado – crimes contra a Administração pública, criança ou adolescente, idoso e vulnerável e pessoa com deficiência. A Lei 14.155/21 trouxe modificações no Código de Processo Penal em seu art. 70§4, referente à competência, a saber:

§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. (BRASIL, 2019)<sup>122</sup>.

Nesse mesmo sentido, o STJ entende que: “[...] O crime de estelionato praticado por meio saque de cheque fraudado compete ao Juízo do local da agência bancária da vítima”<sup>123</sup>. Ademais, para fins de competência, a regra do art.70, §4º do Código de Processo Penal, deve-se prevalece o domicilio da vítima, não importando o local aonde a vítima possua conta bancaria.

Observa-se que, existe a exceção quanto o crime de estelionato praticado na modalidade de saque de cheque onde a competência refere-se a do local da agência bancária da vítima lesada, de acordo com o entendimento do STJ publicado no informativo nº 728, que diz: “[...] Estelionato. Tentativa de saque com apresentação de cheque fraudulento. Hipótese não prevista na Lei n.º 14.155/2021. Consumação do crime no local onde a vítima possui conta bancária”<sup>124</sup>.

Não obstante, as hipóteses em que não for alcançada pelo disposto no art. 70, § 4º, do Código de Processo Penal, a fixação da competência para o julgamento da matéria deverá ser a do local da consumação do fato, conforme dispõe o informativo n.º 736 do STJ, a saber: “[...] No crime de estelionato, não identificadas às hipóteses descritas no § 4º do art. 70 do CPP, a competência deve ser fixada no local onde o agente delituoso obteve, mediante fraude, em benefício próprio e de terceiros, os serviços custeados pela vítima”<sup>125</sup>.

Registra-se, que a pena nos crime de estelionato *caput* e nas modalidades do § 2º do art.171 do Código Penal será de reclusão dom pena de 1 a 5 anos ou multa. Além disso, a pena

<sup>122</sup> BRASIL, decreto lei nº 3689, **Codigo de processo penal**, [http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del3689compilado.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm). Acesso em 01/11/2022.

<sup>123</sup> **Ibidem. STJ, Informativo em Jurisprudência nº 728.**

<sup>124</sup> **Idem.**

<sup>125</sup> **Ibidem. STJ, Informativo nº736.**

é amentada de 1/3 se o crime for cometido contra idoso ou pessoa vulnerável, ou poderá ser diminuída caso o criminoso for primário e o prejuízo for de pequeno valor<sup>126</sup>.

Por fim, caso o crime for praticado no meio informático, de acordo com o elencado no § 2º-A do art. 171 – fraude eletrônica –, também conhecido por estelionato virtual, a pena poderá ser elevada de 04 (quatro) e chegar até 08 (oito) anos de reclusão após o advento da Lei n.º 14.155/21 para inibir tal comportamento<sup>127</sup>.

---

<sup>126</sup> **Ibidem. GRECO, (2022, p.545).**

<sup>127</sup> **Ibidem. JALIL, (2022, p.591).**

### 3. O REFLEXO DOS CRIMES VIRTUAIS EM FACE DO OLHAR JURÍDICO E DA SOCIDADE NO CONTEXTO ATUAL

O estelionato praticado pela internet é uma das modalidades recorrentes no contexto atual, dada facilidade que muitos autores empregam na maneira para chegarem até as vítimas; muitos enganam, criam perfis falsos nas redes sociais, além de invadirem contas e dados alheios com o único objetivo, chantagear e obter vantagem ilícita.

Portanto, estelionato virtual é uma conduta praticada através dos meios eletrônicos, que busca obter vantagem econômica para si ou para outro, a vantagem é obtida de forma ilícita, fraudulenta, usa-se de meios e artifícios ardilosos virtualmente, levando a vítima a agir sob engano e fornecer ou entregar informações aos criminosos, gerando o prejuízo econômico e patrimonial da vítima.

Observa-se que os reflexos da prática de crimes virtuais são destrutivos, ao reforçarem a cultura da dominação e exploração do próprio ser, como, por exemplo, na prática de assédio sexual no ambiente de trabalho remoto, além de outros resultados, como o prejuízo patrimonial para a vítima adquirida por meio fraudulento e erro.

Segundo as lições de Capez, (2022) ao analisar os reflexos da violação da dignidade da pessoa humana em face da prática de qualquer modalidade de crime virtual, afirma que:

Consiste em induzir ou manter alguém em erro, mediante o emprego de artifício, artil, ou qualquer meio fraudulento, a fim de obter, para si ou para outrem, vantagem ilícita em prejuízo alheio. Trata-se de crime em que, em vez da violência ou grave ameaça, o agente emprega um estratagema para induzir em erro a vítima, levando-a a ter uma errônea percepção dos fatos, ou para mantê-la em erro, utilizando-se de manobras para impedir que ela perceba o equívoco em que labora. (CAPEZ, 2022)<sup>128</sup>.

Nessa senda, a difusão da internet e maior quantidade de usuários on-line, principalmente durante a pandemia da Covid -19 levou o crime de estelionato a se aperfeiçoar, tendo em vista que a realização do trabalho, assim como compras pela internet quase que dobrou nesse período, o que acarretou na facilitação quanto ao *modus operandi* dos criminosos no ambiente virtual.

Conforme com o Anuário Brasileiro de Segurança Pública – ABSP – houve um crescimento significativo no número de denúncias em 2022 quanto à prática de estelionatos cometidos por meios eletrônicos em comparação com os anos entre 2018 e 2021, totalizando um aumento de 495%<sup>129</sup> em todo o Brasil na prática dessa modalidade de crime virtual.

---

<sup>128</sup> **Ibidem.** CAPEZ, (2022, p.245).

<sup>129</sup> **Ibidem.** Fórum brasileiro de segurança pública, (2022, p.110-111).

Além disso, o Ministério da Justiça e Segurança Pública – MJSP – ao fazer um levantamento sobre a prática dos crimes virtuais chegou ao resultado quanto à posição ocupada pelo Brasil no ranking de crimes virtuais, sendo o 5º país que sofreu golpes da internet em 2021; os golpes virtuais empregados por qualquer meio ardil e fraudulento a partir da invasão a dispositivos eletrônicos e que visa apenas na obtenção de vantagem econômica, conforme já salientado<sup>130</sup>.

Registra-se que a Polícia Federal em cooperação público privada com a FEBRABAN, propõe troca de informações entre as instituições com intuito de inibir e punir tais fraudes eletrônicas. Ressalta-se, que só em 2021, segundo a FEBRABAN, o prejuízo milionário causado aos clientes chegou a R\$ dois bilhões de reais<sup>131</sup>.

Ademais, de acordo com a Polícia Civil do Estado de São Paulo, as fraudes eletrônicas mais comuns são: a clonagem de WhatsApp, o boleto falso, aonde o estelionatário altera o código de barra passando a ser o beneficiário, falso atendente bancário o integrante da quadrinha que possuem dados da vítima e pedem dados da conta para terem acesso.

Outro exemplo que pode ser elencado cuida-se do golpe do falso motoboy em que ocorre quando um estelionatário liga para a vítima e informa problemas com o cartão, e informa ao usuário que um motoboy irá recolhê-lo, além do *phishing* com envio de e-mails ou links maliciosos, sites de comércio falso ou clonado, aonde a vítima pensando ser um site confiável realiza suas compras, porém o dinheiro vai para uma conta do criminoso e o produto nunca chegará<sup>132</sup>.

Ante a isso, o poder dever do Estado de punir atua para suprir as lacunas legislativas e coibir os ilícitos que surgem, sendo o direito Penal a última *ratio*, com caráter subsidiário, ou seja, só atua quando os outros ramos do direito não são eficazes, em proteger os bens tutelados. O Código Penal Português contempla duas figuras de burla (fraude), a burla informática e a burla das telecomunicações, ambas tipificadas no artigo 221<sup>133</sup> do Código Penal Português.

---

<sup>130</sup> BRASIL. **Ministério da Justiça e Segurança Pública. Notícias.** <https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos>.

<sup>131</sup> **Idem.**

<sup>132</sup>BRASIL, Polícia civil de São Paulo. **Delitos Praticados na internet, perguntas e respostas.** <https://www.policiacivil.sp.gov.br/portal/>

<sup>133</sup> Artigo 221.º **CÓDIGO PENAL PORTUGUÊS**

Burla informática e nas comunicações:

1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, mediante interferência no resultado de tratamento de dados, estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.

2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente

Com sua legislação precursora, o Governo Português, no ano de 1995, propôs uma reforma por meio do Dec. Lei n.º 48/95 de 15 de março que de forma inovadora, foi criada uma lei que combatia a conduta de burla, e os crimes da internet com pena de prisão<sup>134</sup>. Em que pese o cenário legislativo brasileiro na atualidade, precisamente em face da repressão aos crimes virtuais, ainda há muito trabalho a ser enfrentado.

A legislação penal precisa se atualizar constantemente de acordo com a realidade criminal da sociedade, tendo em vista a necessidade de as leis estarem em harmonia com a necessidade punitiva em face das situações que surgem. Percebe-se um esforço e preocupação das autoridades no tratamento a segurança, prevenção e inibição dos crimes da internet.

Não obstante, as políticas públicas de combate e enfrentamento ao crime cibernético são atuantes, tivemos uma CPI – Comissão Parlamentar de Inquérito – dos crimes cibernéticos, conhecida como CPICIBER<sup>135</sup>.

Na Câmara dos Deputados, abordando os temas sobre crimes da internet, após a CPI, elaborou-se um relatório que apontava o crescente aumento dos crimes de internet, o que levou a criação de projetos de lei:

A CPI dos Crimes Cibernéticos, instaurada em agosto de 2015, reuniu em mais de 35 (trinta e cinco) encontros diversos segmentos da sociedade, de instituições voltadas à área de Tecnologia e Segurança da Informação a órgãos investigativos, incluindo representantes de movimentos sociais e organizações não governamentais, a sociedade civil, dentre outras entidades. Os debates são acolhidos em reuniões deliberativas e em audiências públicas, realizadas em Brasília, capital do Brasil, na tentativa de equiparar o Direito Digital à realidade virtual (BRASIL, 2015)<sup>136</sup>.

Ademais, o Direito Penal é baseado segundo o princípio da fragmentariedade, protege-se apenas os bens jurídicos de maior relevância, que sofram ataques e violações sobre estes,

---

ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.

3 - A tentativa é punível.

4 - O procedimento criminal depende de queixa.

5 - Se o prejuízo for:

a) De valor elevado, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias;

b) De valor consideravelmente elevado, o agente é punido com pena de prisão de 2 a 8 anos.

6 - É correspondentemente aplicável o disposto no artigo 206.º

<sup>134</sup> COSTA, António Manuel de A. **A Burla no Código Penal Português**. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2020. E-book. ISBN 9789724084428. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9789724084428/>. Acesso em: 25 fev. 2023.

<sup>135</sup> BRASIL, CAMARA. <https://www.camara.leg.br/noticias/487063-comissao-parlamentar-de-inquerito-dos-crimes-ciberneticos-aprova-relatorio-final/>.

<sup>136</sup> PATURY, Fabrício Rabelo, Fernanda Veloso Salgado. **A Política Criminal do Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia no enfrentamento aos ilícitos cometidos no âmbito digital**. MPBA. Disponível em [https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/a\\_politica\\_criminal\\_do\\_nucleo\\_d\\_e\\_combate\\_aos\\_crimes\\_ciberneticos\\_do\\_ministerio\\_publico\\_do\\_estado\\_da\\_bahia.\\_-\\_fabricio\\_rabelo\\_patury\\_e\\_fernanda\\_veloso\\_salgado.pdf?download=1](https://www.mpba.mp.br/sites/default/files/biblioteca/criminal/artigos/diversos/a_politica_criminal_do_nucleo_d_e_combate_aos_crimes_ciberneticos_do_ministerio_publico_do_estado_da_bahia._-_fabricio_rabelo_patury_e_fernanda_veloso_salgado.pdf?download=1). Acesso em 13/02/2023.

conforme as lições de Reale, (2020)<sup>137</sup> compreende-se que: “[...] o direito Penal por ser obrigatoriamente seletivo, incriminando apenas, algumas condutas lesivas a determinado valor, as de grau elevado de ofensividade.”

O legislador deve observar na construção de um tipo penal, os limites constitucionais sobre a tutela dos Direitos Fundamentais, assim como âmbito do Direito Penal brasileiro em que legislador está vinculado ao princípio constitucional da Proporcionalidade e razoabilidade para que nenhum limite seja ultrapassado em face do *jus puniendi* do Estado.

Canotilho, (2020)<sup>138</sup> desdobra o princípio da proporcionalidade em seus estudos e afirma que:

Pelo princípio da necessidade, tem o cidadão direito à menor desvantagem possível, devendo ser evitada a limitação desnecessária de direitos fundamentais, ou seja, o legislador deve adotar a medida eficaz menos restritiva de direitos. Já pelo princípio da proporcionalidade em sentido estrito, examina-se se “o resultado obtido com a intervenção é proporcional à carga coativa da mesma” ou, em outras palavras, se o meio utilizado é ou não desproporcionado em relação ao fim. Trata-se, pois, de uma questão de medida ou desmedida para se alcançar um fim. (CANOTILHO, 2020).

Registra-se, que o Princípio da legalidade é a base do Estado Democrático de Direito, pois as normas incriminadoras e punitivas só podem existir no sistema jurídico brasileiro se forem elaboradas por meio de leis, tendo em vista que nenhum fato pode ser considerado crime e nenhuma pena pode ser aplicada se não houver lei anterior ao fato que o defina como crime.

Além do mais, o princípio da Legalidade está prevista na Constituição de 1988, em seu art.º 5 XXXIX: “[...] não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, nesse mesmo sentido, se inicia o Código Penal, em seu art. 1º, prevê que: “[...] Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”.

De acordo com Mendes, (2020), o Princípio da legalidade é a base de todo o direito público, assim sendo, para o Direito penal, a sua base, surge no princípio da legalidade, “*nullum crimen nulla poena sine lege*”<sup>139</sup> pois:

Todo o Direito está construído sobre o princípio da legalidade, que constitui o fundamento do Direito Público moderno. O Direito Penal funda-se no princípio de

<sup>137</sup> JR., Miguel R. Fundamentos de Direito Penal. [Digite o Local da Editora]: Grupo GEN, 2020. E-book. ISBN 9788530991609. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530991609/>. Acesso em: 11 fev. 2023.p.9.

<sup>138</sup> CANOTILHO, José Joaquim Gomes, apud, REALE, Miguel Junior. **Fundamentos de Direito Penal**. Grupo GEN, 2020. E-book. ISBN 9788530991609. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788530991609/>. Acesso em: 11 fev. 2023, p.21.

<sup>139</sup> “**nullum crimen nulla poena sine lege**”- Expressão em Latim que significa: não há crime nem pena sem lei prévia.

que não há crime sem lei anterior, nem pena sem prévia cominação legal (art. 5º, XXXIX). (MENDES, 2020)<sup>140</sup>.

### 3.1 O estelionato virtual sob a égide penal

Com a transformação constante da sociedade, novos desafios surgem no mundo jurídico, por exemplo, com a interação do mundo físico com o mundo virtual, alguns crimes migraram e se aperfeiçoaram para também ocorrerem no ambiente virtual, é o caso do estelionato virtual, pois:

No Brasil o crime que ganha destaque no mundo dos delitos virtuais é o estelionato, crime pelo qual o autor do fato obtém, para si ou para outrem, vantagem ilícita, em prejuízo alheio, mediante artifício, ardil ou qualquer meio fraudulento, previsto no artigo 171 do Código Penal brasileiro. Este tipo de crime ampliou sobretudo pela crescente demanda do e-commerce, uma característica dos tempos modernos fez com que emergissem novas formas de execução. (PATURY, 2023)<sup>141</sup>.

Com o intuito de inibir e punir com mais rigor esses ilícitos, alguns parlamentares foram inquiridos a legislar e tipificar a conduta de fraude eletrônica, surgindo assim, o Projeto de Lei n.º 4554/20, de autoria do Senador Izalci Lucas no Distrito Federal, que a princípio modificaria apenas o art. 155 do CP, seria criado o nome do delito de “combate à fraude eletrônica”, seriam acrescentados os parágrafos 8º e 9º, no artigo referido<sup>142</sup>.

A justificativa do projeto de lei é o aumento do número de casos de fraude, o projeto de lei buscava intensificar a pena do delito, furto praticado mediante fraude, contudo após o projeto ir para apreciação dos deputados federais, passou a ter um novo relator, o Deputado Federal Vinicius Carvalho, que propôs ao projeto ampliar não apenas o delito de furto, mas também o delito de estelionato<sup>143</sup>.

Com a aprovação dos projetos de lei, foi promulgada a Lei n.º 14.155/21, que criou aos artigos 154-A, invasão de dispositivo, artigo 155 e seus parágrafos 4-B e C, crime de furto mediante fraude cometido por meio eletrônico, com aumento de pena para servidor localizado no exterior, e o modificou o artigo 171 do CP, criando as qualificadoras do parágrafo 2º - A e B, quais sejam: fraude eletrônica e utilizar servidor no estrangeiro para cometer a fraude<sup>144</sup>.

---

<sup>140</sup> MENDES, Gilmar F.; BRANCO, Paulo G. Série IDP - Linha Doutrina - Curso de direito constitucional. Editora Saraiva, 2020. E-book. ISBN 9788553618088. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553618088/>. Acesso em: 11 fev. 2023, p.945.

<sup>141</sup> **Ibidem. PATURY, (2020, p.27).**

<sup>142</sup> **Ibidem. Projeto de Lei n.º 4554/20.**

<sup>143</sup> **Ibidem. SYDOW, (2022, p.624).**

<sup>144</sup> **Idem.**

Ademais, a referida lei também modificou o artigo 70, caput, do Código de Processo Penal, relativos à competência nos crimes de estelionato, na modalidade de cheque sem fundo ou frustrado o pagamento, agora a competência é o domicílio da vítima.

### 3.2 Elementos do tipo penal

O *Scamming*, deriva do verbo Scam, que em inglês significa fraudar ou enganar,<sup>145</sup> é o nome dado para caracterizar o processo fraudulento, ou seja, o modo de agir no estelionato virtual, quais seja, a fraude empregada através dos dispositivos eletrônicos, possuindo a intenção enganar, para obter vantagem ilícita e causar dano ao patrimônio da vítima pretendida<sup>146</sup>.

O tipo penal se classifica, por crime doloso, visto que todas as condutas tipificadas são dolosas, pois não há previsão para modalidade culposa do delito, quanto ao bem jurídico, todas as formas praticas são Impuras, pois o bem jurídico atingido é o patrimônio, a internet é o meio utilizado para se praticar os crimes na figura do modo arдил e meio fraudulento, logo quanto ao resultado o crime é de dano, já quanto ao agente, o crime não necessita de nenhuma qualidade especial, sendo por tanto um crime comum, o crime é unissubjetivo pois não previsão de concurso necessário, os crimes quanto ao resultado se classificam como matérias pois a conduta exige vantagem ilícita<sup>147</sup>.

Além disso, na parte processual, os crimes praticados através dos meios eletrônicos, são não transeuntes; isso significa que são aqueles que deixam vestígios<sup>148</sup>. O *scam*, (fraude) também conhecido por *phishing-scam*, são as técnicas utilizadas, de pesca na internet para selecionar suas vítimas, mais vulneráveis e propensas a cair nos golpes<sup>149</sup>.

O *Scammer* é a pessoa que pratica o delito, sendo que esse agente delituoso não age aleatoriamente, pois usa seu conhecimento lógico, e usa suas iscas eficientes, para induzir a vítima ao erro; o objetivo é roubar dados, dinheiro, enganar, tomar as redes sociais, para através destas informações, se passarem pelo usuário para cometer crimes como se fosse a própria pessoa, se passam por ela, para enganar mais vítimas, seus contatos, familiares ou amigos.

A qualificadora do Estelionato, nos termos do art. ° 171§ 2° – A, estelionato mediante fraude eletrônica – conhecida também como estelionato virtual, e a qualificadora do § 2°- B,

---

<sup>145</sup> <https://dictionary.cambridge.org/pt/dicionario/ingles/scam>.

<sup>146</sup> **Idem. SYDOW, (2022, p. 612).**

<sup>147</sup> **Idem. SYDOW, (2022, p. 624).**

<sup>148</sup> **Idem.**

<sup>149</sup> **Idem.**

utilização de servidor mantido fora do território nacional, foram acrescidos pela Lei n.º 14.155, a pena passou a ser mais grave, pois:

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

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021). (BRASIL, 2021).

Destaca-se, que o Decreto Legislativo nº 37 de 21, traz o conceito de fraude informática, em seu artigo 8º, onde cada Governo adotará medidas, além de cooperação e criara por meio de lei medidas que tipifiquem e punam a conduta de fraude informática<sup>150</sup>.

Nesse sentido, compreende-se que a nova lei corresponde à – *novatio legis in pejus* –, pois a qualificadora trouxe um tratamento mais rígido aos crimes de estelionato praticado no meio virtual; a nova lei não pode, portanto, retroagir a fatos ocorridos anteriormente a sua publicação.

Assim, como ocorreu com o crime de furto, que atualmente possui uma qualificadora por ser praticado no meio digital e com uso de servidor localizado no exterior, assim quando a vítima ou terceiro é induzido em erro por meio: meio de rede sócias, contatos telefônicos, e-mail, ou qualquer outro meio fraudulento, pois:

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. Um exemplo recorrente envolve os cartões de crédito. O fraudador telefona para alguém e afirma, por exemplo, que a instituição financeira detectou indícios de fraude com o cartão dessa pessoa. Pede a ela que confirme dados e digite a senha do cartão. Com a senha à disposição, o agente faz compras, efetua saques, toma empréstimos etc.;

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, o estelionatário pode obter os dados pessoais e bancários inseridos em formulários eletrônicos;

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.)<sup>151</sup>. (SANCHES, 2021).

<sup>150</sup> **Ibidem. Decreto Legislativo nº37 de 2021.**

<sup>151</sup> SANCHES, Rogério Cunha, apud. GRECO, Rogério. **Código Penal Comentado**: Grupo GEN, 2021. E-book. ISBN 9786559770700. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559770700/>. Acesso em: 26 jan. 2023.

A qualificadora incide quando terceiro ou a vítima for conduzida por meio fraudulento por meio de redes sociais, que são estruturas sócias de comunicação, onde pessoa ou organizações estão conectadas, são exemplos: Facebook, Tiktok, You tube, tendo em vista que:

A transmutação do conceito de "comunidade" em "redes sociais". Esta mudança se deve em grande parte à explosão das comunidades virtuais no ciberespaço, fato que acabou gerando uma série de estudos não apenas sobre essa nova maneira de se fazer sociedade, mas igualmente sobre a estrutura dinâmica das redes de comunicação. No centro dessa transformação, conceitos como capital social, confiança e simpatia parcial são invocados para que possamos pensar as novas formas de associação que regulam a atividade humana em nossa época. (COSTA, 2005)<sup>152</sup>.

Nota-se, que para incidir nessa qualificadora do art. 171, § 2º - A, captura ou obtenção dos dados ou informação sigilosos, mediante fraude eletrônica, precisa ser usada pelo criminoso para alcançar vantagem ilícita e causar prejuízo patrimonial<sup>153</sup>. Contudo, se ação praticada pelos criminosos, for apenas coletar dados de forma não autorizada, sem haver a fraude para a obtenção das informações o crime cometido será o de invasão de dispositivos informático, tipificado no art.º 154-A, do Código Penal:

Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. (BRASIL, 1940).

Outro tipo penal, que precisa ser diferenciado é Furto mediante fraude por dispositivo eletrônico ou informático, tipificado no art.º 155§ 4-B, o dispositivo foi alterado devido a seu resultado ser mais gravoso ao utilizar meios eletrônicos, foi introduzido ao CP, pela Lei nº 14.155/21, o furto recebe a qualificadora por ser cometido por meio eletrônicos ou informáticos, conectados ou não a internet:

155 § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (BRASIL, 1940).

Entretanto, na fraude eletrônica, a fraude é cometida com o uso de informações ou dados que são fornecidos pela própria vítima ou por terceiro, através do engano, do agente delinquente; os meios eletrônicos são os meios utilizados, para a obtenção da fraude que pode ser por redes sócias, e-mails fraudulentos ou falsos, contatos telefônicos, ou qualquer meio fraudulento análogo, o legislador optou por deixar a interpretação ampla:

<sup>152</sup> COSTA, R. **Por um novo conceito de comunidade: redes sociais, comunidades pessoais, inteligência coletiva**. Interface - Comunic., Saúde, Educ., v.9, n.17, p.235-48, mar/ago 2005. Acesso em 22/02/2023.

<sup>153</sup> **Ibidem. JALIL, (2022, p. 58).**

171§ 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, 2021).

Ademais, o informativo nº 135 do STJ merece destaque ao reconhecer os elementos constitutivos do furto mediante fraude e do Estelionato, a saber:

O furto mediante fraude não pode ser confundido com o estelionato. No furto, a fraude é utilizada para burlar a vigilância da vítima, para lhe tirar a atenção. No estelionato, a fraude objetiva obter consentimento da vítima, iludi-la para que entregue voluntariamente o bem. (BRASIL, 2021)<sup>154</sup>.

A pena prevista no art.º 171§ 2 – A, considera de suma importância o resultado gravoso, aumentando assim de 1/3(um terço) a 2/3 (dois terços), caso o a fraude eletrônica tenha utilizado para o seu cometimento, servidor localizado no exterior. Ademais, a pena da fraude eletrônica, é de reclusão, de 04 (quatro) anos a 08 (oito) anos, e multa, se a fraude é cometida com a utilização, de informações fornecidas pela vítima ou por terceiro induzido ao erro, por meio de redes sociais, contatos telefônicos, ou envio de e-mail (correio eletrônico), fraudulento, ou por qualquer outro meio análogo<sup>155</sup>.

A pena cominada em abstrato, do delito da fraude eletrônica, impossibilita a concessão do benefício despenalizado do Sursis (suspensão condicionada do processual), prevista no art. 89 da lei n.º 9.099/95, o benéfico pode ser aplicado nos delitos em que a pena mínima cominada for igual ou inferior a um ano<sup>156</sup>. Além do mais, não é possível por força de lei, ao benefício do Acordo de não persecução penal, art. 28-A do CPP, acrescido pela Lei n.º 13.964 de 2019 que prevê a concessão do benefício para crimes com pena inferior a 04 (quatro) anos<sup>157</sup>.

Ressalta-se, ainda que a prática de “Cola eletrônica” não configura o delito de estelionato virtual, também não se enquadra em nenhuma espécie de estelionato, pois antes da Lei n.º 12.550/11 entrar em vigor a conduta era considerada atípica. Nesse contexto, cita-se que o STF, no Julgado n.º 1.145 decidindo que a conduta de fraude, por não se encontrar previsão legal, não deveria ser empregada, para não haver analogia em malam parte, nesse entendimento,

---

<sup>154</sup> **Ibidem. STJ, Informativo nº315.**

<sup>155</sup> BRASIL, **Código Penal de 1940** - Art.171§ 2-A.

<sup>156</sup> BRASIL, **Lei nº 9.099/95**. Art. 89: Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena.”

<sup>157</sup> BRASIL, **Código de Processo Penal** - Art. 28-A do CPP. “Não sendo caso de arquivamento e tendo o investigado confessado formal e circunstancialmente a prática de infração penal sem violência ou grave ameaça e com pena mínima inferior a 4 (quatro) anos...”

o STJ, em seu Informativo n.º 506: “[...] A "cola eletrônica", antes do advento da Lei n. 12.550/2011, era uma conduta atípica, não configurando o crime de estelionato”<sup>158</sup>.

Após a promulgação da Lei n.º 12.550/11 foi criada a figura do crime de fraudes em certames de interesse público, introduzido no Código Penal o art. 311-A, que pune as condutas de utilizar ou divulgar, conteúdo indevidamente, com o fim de beneficiar a si ou a outrem, que comprometer a credibilidade do certame.

Nesse sentido, não é considerado fraude eletrônica a conduta de crime fraude com a utilização de ativos virtuais, valores mobiliários e ativos financeiros. A conduta foi tipificada como crime com a Lei n.º 14.478 de 21 de dezembro de 2022, passando a ser uma espécie de Estelionato, específica para transações de ativos eletrônicos, a nova lei encontrasse no *vacatio legis* (180) dias para iniciar sua vigência.

Ademais, a referida lei regulamenta as prestadoras de ativos virtuais<sup>159</sup>, inserindo no Código Penal um novo artigo, qual seja: art. 171-A, com a seguinte redação:

Art. 171-A. Organizar, gerir, ofertar ou distribuir carteiras ou intermediar operações que envolvam ativos virtuais, valores mobiliários ou quaisquer ativos financeiros com o fim de obter vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento.  
Pena - reclusão, de 04 (quatro) a 08 (oito) anos, e multa. (BRASIL, 2022).

### 3.3 A causa de aumento do art.º 171, §2º - “b”

A causa de aumento de pena no parágrafo segundo, alínea “b”, do artigo 171, é uma causa de aumento exclusiva, do artigo 171, § 2º-A, embora outros tipos estelionato possam ser praticados usando dispositivos eletrônicos, ao se criar a nova lei 14.155/21, que alterou o artigo 171, criando o tipo penal do estelionato virtual.

O legislador escolheu utilizar essa causa de aumento somente na fraude, onde o criminoso induz a erro o terceiro ou a vítima a fornecem dados ou informações, por meio de

<sup>158</sup> **Ibidem, STJ, Informativo STJ, nº 506. HC 245.039-CE.**

<sup>159</sup> **Art. 3º da Lei nº 14.478/22.**

“Para os efeitos desta Lei, considera-se ativo virtual a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento, não incluídos:

I - moeda nacional e moedas estrangeiras;

II - moeda eletrônica, nos termos da Lei nº 12.865, de 9 de outubro de 2013;

III- instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e

IV- representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento, a exemplo de valores mobiliários e de ativos financeiros.”

redes sociais, bem como através de contatos telefônicos ou pelo recebimento de correio eletrônico fraudulento, ou por qualquer meio fraudulento análogo<sup>160</sup>.

Por provedor de internet, segundo as lições Sydow, (2022) define-se por: “[...] ser um programa de computador ou dispositivo que provem um serviço a outro programa de computador e seus usuários ,são os cliente, o Data Center, o servidor é um dispositivo físico em que o programa é executado”<sup>161</sup>.

Nesse sentido, o Decreto Legislativo n.º 37 de 2021, conhecido por Convenção sobre os crimes cibernéticos, em seu artigo primeiro, classifica servidor por:

Provedor de serviços: (i) qualquer entidade pública ou privada que permite aos seus usuários se comunicarem por meio de sistema de computadores, (ii) qualquer outra entidade que realiza o processamento ou armazenamento de dados de computador em nome desses servidores, de comunicação ou de seus usuários. (BRASIL, 2021).

Destaca-se que, a causa de aumento de pena é aplicada sempre a quem comete o ilícito de estelionato virtual, pois os servidores das redes sociais e os gerenciadores dos e-mails se encontram no exterior, mesmo que grandes empresas possuam representação no Brasil, sua sede e seus servidores encontram-se hospedados no exterior<sup>162</sup>, pois:

Eleva-se a pena se o servidor, de onde partem os ataques a dispositivos alheios são hospedados em território fora do Brasil, porque dificulta muito a investigação e a descoberta da autoria. O aumento deve basear-se no grau de dificuldade da apuração do caso. (SYDOW, 2022)<sup>163</sup>.

Outro ponto encontrado versa sobre a dificuldade no fornecimento de dados e seus rastreios como prova na identificação de crimes cometidos na internet, como os servidores, em sua grande maioria se localizam no exterior, sua privacidade é protegida de forma mais restrita, bem como por se tratar de empresas privadas, protegem além disso a privacidade de seus clientes que não estão sujeitos as leis Brasileiras.

Registra-se, que mesmo o Brasil fazendo parte da Convenção de Budapeste na cooperação entre os países na prevenção e punição dos crimes virtuais, assim como na pratica obter informações que comprovem a autoria e materialidade nos crimes em tela, não é tão simples, seja pela burocracia, ou pela demora, o que dificulta na punição e leva muitas vezes a prescrição dos crimes.

Na oportunidade, a Lei n.º 14.155/21 acrescentou ao art.º 171 o § 4º, que prevê o aumento de pena para estelionato cometido contra idoso ou pessoa vulnerável, a saber: “[...] §

---

<sup>160</sup> **Ibidem.** SYDOW, (2022, p. 635).

<sup>161</sup> **Ibidem.** SYDOW, (2022, p. 636).

<sup>162</sup> **Idem.**

<sup>163</sup> **Ibidem.** NUCCI, (2022, p.456).

4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime for cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso”.

O grau de aumento da pena está relacionada ao resultado gravoso gerado a vítima, tendo em vista que, quanto maior o dano gerado a vítima, maior será a fração aplicada a pena, a causa de aumento de pena é aplicada, com vítima idosa, ou vulnerável, nos moldes da Lei n.º 10.741/03, art. 1º, caput - Estatuto da Pessoa Idosa.

Ademais, o legislador não conceitua a figura da pessoa considerada vulnerável de forma objetiva, mas equiparou-a situação de dificuldade ou impossibilidade de defesa em decorrência de indução ao erro, a fraude ou qualquer situação que reduza a sua capacidade de oferecer resistência, de acordo com a tipificação penal esculpida na conduta do crime de estupro de vulnerável, nos termos do art. 217 – A, do Código Penal de 1940.

No citado artigo, são considerados veneráveis, menores de 14 anos; alguém que se encontre em enfermidade ou doença mental, e não possua o discernimento na pratica do ato, ou qualquer pessoa que de alguma maneira não possa oferecer resistência. Nessa senda, por analogia, são utilizadas as mesmas características das vítimas vulneráveis do artigo 217-A, na aplicação da causa de aumento de pena do art.º 171, §4º e do art.º 155, §4º, inciso II <sup>164</sup>.

Para tanto, compreende-se que o ambiente virtual tem sido o *modus operandi* de inúmeros criminosos no Brasil e no mundo, dada sua amplitude de facilitação quanto ao acesso aos dados sensíveis ou informações financeiras de milhares de usuários que se quer tem a dimensão de como a ausência de segurança e proteção de seu uso de forma adequada pode trazer grandes prejuízos.

É preciso que não só a legislação seja atualizada com o objetivo ao enfrentamento dos crimes virtuais, tão pouco no que se refere ao aumento de pena como a única solução para uma possível responsabilização penal, compreende-se, que o enfrentamento à persistência nessa modalidade de crime seja fomentado através do reforço aos usuários por meio do uso da tecnologia de forma adequada.

---

<sup>164</sup> **Ibidem. SYDOW, (2022, p. 640).**

## CONCLUSÃO

A internet, ao longo dos anos, passou a transformar a vida das pessoas, inicialmente possuiu seu surgimento para fins militares, no entanto com o fim da Guerra Fria, tivemos a comercialização da rede.

A digitalização da sociedade, ou a Modernidade Líquida, do Filósofo Zygmunt Bauman, (2001) que compara à sociedade a água que muda e transforma muito rápido, na sociedade contemporânea nada é feito para durar, segundo o autor o mundo é sólido e firme.

Bauman, (2001), afirma ainda que, as relações eram duradouras, as mudanças eram difíceis de acontecer, hoje com o nosso mundo é líquido, o mundo se transforma, a cada minuto, com grande rapidez, atualmente isso acontece com frequência através da tecnologia, que nos aproximou, possuímos muitas amizades, ou seguidores, desses quais são realmente sólidos?

A democratização do acesso à internet e o investimento de grandes empresas de tecnologia, voltadas tanto para *Hardware*, quanto para desenvolvimento de *software*, como por exemplo, das gigantes Microsoft e Apple, tornou popular a internet, não apenas entre os jovens, com a gama de funções que proporcionam passou a transformar a tecnologia da informações, o comércio, transações bancárias, a moeda, o ensino, a medicina.

Para Pierre Lévy, (2012)<sup>165</sup>, as novas práticas e novos costumes, vocabulário que se desenvolve no ciberespaço, isto é, na internet, são conhecidos por cybercultura, a cultura contemporânea que é caracterizada pelo uso das tecnologias, possibilita a interação das culturas geograficamente remotas.

Contudo, a internet não trouxe apenas benefícios, surgiram os crimes cometidos na internet, algumas figuras criminosas são tipificadas no CP, os delitos migraram ou se aperfeiçoaram, para ser cometidos na internet, a internet é assim um meio pelo qual se comete o crime gerando um resultado mais gravoso pelo seu poder de alcance.

O tipo penal do estelionato virtual, embora esse tipo específico de estelionato não estivesse escrito no Código Penal, sua prática ocorria, é intensificava, principalmente durante a Pandemia Covid -19, porém, sua pratica não era punida por não haver tipificação do tipo,

---

<sup>165</sup> LÉVY, Pierre apud. CUNHA, Úrsula Nascimento de Sousa, **cibercultura e as identidades líquidas: reflexão sobre a cultura na era das novas tecnologias**, Revista: Pontos de Interrogação: Linguagens, identidades e letramentos - Vol. 2, n. 2, jul./dez. 2012, p.163. Disponível <https://www.revistas.uneb.br/index.php/pontosdeint/article/view/1558>. Acesso em 11 de janeiro de 2023.

durante o isolamento social, houve um aumento de usuários online e por consequência houve mais crimes.

Constatou-se, ao longo da pesquisa um aumento demasiado no número de crimes de Estelionato praticados por meios eletrônicos, segundo o Anuário Brasileiro de Segurança Pública (ABSP), publicado no ano de 2022, houve o crescimento do número dos estelionatos cometidos por meio eletrônico, foram estudados o período dos anos de 2018-2021.

Verificou-se, ainda que ocorreu um aumento elevadíssimo no cometimento desse delito, a análise e realizado com estatísticas a nível nacional e estadual, em ambos os cenários, o crescimento ocorreu duplicado, por exemplo, a nível nacional o período estudado, o crescimento foi de 495%, o Anuário Brasileiro é realizado, segundo informações, em relatórios e estatísticas, coletados das Polícias civis, Polícias militares, e Polícia federal, Secretarias de Segurança Públicas de todos os estados brasileiros <sup>166</sup>.

Durante a realização da pesquisa, observou-se que o Estado Brasileiro, está combatendo e criando mecanismos legislativos para inibir e punir os crimes da internet, ao longo da última década verificou-se que foi criada a Lei Carolina Dickemann n.º 12.737, que pune invasões de eletrônicos. Foram criada a Lei Marcos cível da Internet Lei n.º 12.965 que regulamenta o uso e os princípios da internet no Brasil, foi publicado a LGPD, lei n.º 13.709.

A citada lei visa proteger o tratamento de dados, a constituição federal colocou os dados com status de Direitos Fundamentais, com a emenda n.º 115, garantindo assim maior proteção. Ademais, com a ratificação do Brasil a Convenção de Budapeste, fortalece o combate aos crimes da internet, e propicia a cooperação internacional, no combate e punição desses delitos.

Compreende-se que, ao longo dos anos a figura delituosa do estelionato se modernizou e passou a ser praticado no meio virtual, notamos um elevado número de crescimento dessa prática, o que trouxe prejuízo ao comércio, isso fomentou o Congresso a criar uma lei que tipificasse tal conduta, o que resultou publicação na Lei n.º 14.155/21.

O Estelionato um dos crimes que mais sofreu alterações nos últimos 5 anos (2019-2023), foram elas: a lei n.º 13.964/19, que alterou a ação penal, que passou a proceder mediante queixa da vítima, a mudança da competência, aonde é fixada no local de domicílio da vítima, com exceção das vítimas do §5, quais sejam, administração direta e indireta, criança ou adolescente, pessoa com deficiência mental ou maior de 70 anos.

---

<sup>166</sup> **Ibidem. Fórum brasileiro de segurança pública, (2022, p.112-113).**

Além disso, ocorreram outras mudanças após o advento da Lei n.º 14.155/21, que incluiu ao artigo 171 do Código Penal, estelionato, o §2º-A e B, e o §4º. A fraude eletrônica acrescentada no crime de estelionato, §2º - A, tem pena de reclusão, de 04 (quatro) a 08(oito) anos e multa, se a fraude for cometida com a utilização de informação fornecidas pela vítima ou terceiro, que foram induzidas a erro, utilizando as redes sócias, meios telefônicos, falsos e-mails, ou qualquer outro meio eletrônico, o legislador deixou em aberto, a interpretação extensiva, podendo alcançar novas formas, ou outros meios fraudulentos.

Ao decorrer do estudo observou-se ainda que o aumento de pena do §2º-B, que incide ao crime quando for praticado com o uso de servidor mantido fora do território nacional, porém esse aumento será sempre calculado, ou seja, todo criminoso que cometer Fraude Eletrônica recebera o aumento de pena instantâneo, pois todos os servidores se encontram no Exterior, mesmo que possuam representação da empresa no Brasil, o processamento e armazenamento se encontram fora do território brasileiro<sup>167</sup>.

À luz de todas as análises tecidas na elaboração do presente estudo, conclui-se que, a nova modalidade de estelionato virtual, é um crime que está em movimento constante, a cada instante surgem novas forma de golpes ou meios ardis, é necessário que o poder público punitivo do Estado, continue atuando na prevenção destes ilícitos, a participação popular em denunciar os crimes e encaminhar as autoridades, faz com que haja uma investigação e punição adequada.

---

<sup>167</sup> **Ibidem. SYDOW, (2022, p.638).**

## REFERÊNCIAS

BALDAN, Édson Luís. **Estelionato. Enciclopédia jurídica da PUC-SP.** Celso Fernandes Campilongo, Álvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Penal. Christiano Jorge Santos (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/> Acesso em 26. out. 2022.

BAUMAN, Zygmunt. **Modernidade Líquida.** Tradução: Plínio Dentzien. Rio de Janeiro: Jorge Zahar Ed., 2001.

BIOLCATI, Fernando Henrique De O. **Internet, Fake News e Responsabilidade Civil das Redes Sociais.** (Coleção Direito Civil Avançado). [Digite o Local da Editora]: Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276410. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786556276410/>. Acesso em: 08 out. 2022.

BITENCOURT, Cezar R. **Código penal comentado.** Editora Saraiva, 2019. E-book. ISBN 9788553615704. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books>. Acesso em: 12 out. 2022.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial: crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos - arts. 155 a 212. v.3:** Editora Saraiva, 2022. E-book. ISBN 9786553622074. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books> Acesso em: 15 out. 2022.

BITTENCOURT, Rodolfo Pacheco Paula. **O anonimato, a liberdade, a publicidade e o direito eletrônico, 2016.** Disponível em: <https://rodolfoppb.jusbrasil.com.br/artigos/>. Acesso em: 18 de mai. 2021.

BRASIL, Decreto nº 7.962 de, 15 de março de 2013. **Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/) Acesso em: 11. ago. 2022.

BRASIL, Lei nº 14.478 de, 21 de dezembro de 2022. **Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para prever o crime de fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros; e altera a Lei nº 7.492, de 16 de junho de 1986, que define crimes contra o sistema financeiro nacional, e a Lei nº 9.613, de 3 de março de 1998, que dispõe sobre lavagem de dinheiro, para incluir as prestadoras de serviços de ativos virtuais no rol de suas disposições.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Acesso em: 11. jan. 2023.

BRASIL, Câmara dos Deputados. Projeto de Lei nº 6444 de 2019. **Altera o art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal, para dispor sobre o estelionato sentimental.** Disponível em: <https://www.camara.leg.br/>. Acesso em: 26. out. 2022.

BRASIL, Câmara dos Deputados. Projeto de Lei nº 4554/20. **Combate a prática de fraude eletrônica, modifica o art. 155 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e apresenta hipóteses agravantes.** Disponível em: <https://www25.senado.leg.br/>. Acesso em: 21. jan. 2023.

BRASIL, Lei nº 8.078 de, 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/). Acesso em: 11. ago. 2022.

BRASIL, **Constituição da República Federativa do Brasil de 1988.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 19. mai. 2021.

BRASIL, Senado Federal. Decreto Legislativo nº 37 de, 16 de dezembro de 2021. **Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001.** Disponível em: <https://legis.senado.leg.br/>. Acesso em: 08. jan. 2023.

BRASIL, Dec. Lei nº 3.689 de, 03 de outubro de 1941. **Código de Processo Penal.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/). Acesso em: 01. nov. 2022.

BRASIL, INPUTEC. **Marco civil da internet: o que você precisa saber e qual a sua relação com a IgpD?** Bahia – BA, 2020. Disponível em: <https://www.inputec.com.br/marco-civil>. Acesso em: 12. mai. 2021.

BRASIL, Lei nº 8.072 de, 25 de julho de 1990. **Dispõe sobre os crimes hediondos, nos termos do art. 5º, inciso XLIII, da Constituição Federal, e determina outras providências.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03](https://www.planalto.gov.br/ccivil_03). Acesso em: 16. out. 2022.

BRASIL, Lei nº 12.550/11 de, 15 de dezembro de 2011. **Autoriza o Poder Executivo a criar a empresa pública denominada Empresa Brasileira de Serviços Hospitalares - EBSEH; acrescenta dispositivos ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/). Acesso em: 16. out. 2022.

BRASIL, Lei nº 12.737 de, 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Acesso em: 19. mai. 2021.

BRASIL, Lei nº 12.965 de, 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Acesso em: 19. mai. 2021.

BRASIL, Lei nº 13.853 de, 8 de julho de 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Acesso em: 19. mai. 2021.

BRASIL, 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: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Acesso em: 28. mai. 2021.

BRASIL, Portal G1. **Denúncias de crimes cometidos pela internet mais que dobram em 2020.** Disponível em: <https://g1.globo.com/economia/tecnologia/> Acesso em: 12. mai. 2021.

BRASIL, Superior Tribunal de Justiça – STJ. **Informativo nº 728. Empréstimo comum em conta-corrente. Limitação dos descontos das parcelas. Não cabimento. Lei n. 10.820/2003. Aplicação analógica. Impossibilidade.** Tema 1085. Disponível em: <https://www.stj.jus.br/publicacaoinstitucional/>. Acesso em: 28. out. 2022.

BRASIL, Superior Tribunal de Justiça – STJ. **Informativo nº 736. Execução penal. Condenação por pena privativa de liberdade no curso da execução de pena restritiva de direitos. Reconversão. Possibilidade. Condenação substituída por pena alternativa superveniente. Unificação automática. Impossibilidade.** Tema 1106. Disponível em: <https://processo.stj.jus.br/jurisprudencia/>. Acesso em: 28. out. 2022.

BRASIL, Superior Tribunal de Justiça – STJ. **Jurisprudência em teses nº 84. O delito de estelionato previdenciário (art. 171, § 3º do CP), praticado pelo próprio beneficiário, tem natureza de crime permanente uma vez que a ofensa ao bem jurídico tutelado é reiterada, iniciando-se a contagem do prazo prescricional com o último recebimento indevido da remuneração.** Disponível em: <https://scon.stj.jus.br/SCON/>. Acesso em: 28. out. 2022.

BRASIL, Superior Tribunal de Justiça – STJ. **Enunciado de Sumula nº 24. Aplica-se ao crime de estelionato, em que figure como vítima entidade autárquica da previdência social, a qualificadora do § 3º, do art. 171 do Código Penal.** Disponível em: <https://scon.stj.jus.br/SCON/>. Acesso em: 28. out. 2022.

BRASIL, Superior Tribunal de Justiça – STJ. **Enunciado de Sumula nº 17. Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido.** Disponível em: <https://scon.stj.jus.br/SCON/>. Acesso em: 28. out. 2022.

BRASIL, Superior Tribunal de Justiça – STJ. **Enunciado de Sumula nº 73. A utilização de papel moeda grosseiramente falsificado configura, em tese, o crime de estelionato, da competência da Justiça Estadual.** Disponível em: <https://scon.stj.jus.br/SCON/>. Acesso em: 28. out. 2022.

BRASIL, Superior Tribunal Federal – STF. **Enunciado de Súmula. nº 246. Comprovado não ter havido fraude, não se configura o crime de emissão de cheque sem fundos.** Disponível em: <https://jurisprudencia.stf.jus.br/>. Acesso em: 27. out. 2022.

BRASIL, Superior tribunal de justiça – STJ. HC 435.818/SP, Rel. Ministro Ribeiro Dantas. 5ª Turma. Julgado em 03/05/2018. Publicado no DJe em 11/05/2018. Disponível em: <https://scon.stj.jus.br/SCON/>. Acesso em 14. out. 2022.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal.** Disponível em: [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Acesso em 05. out. 2022.

BRASIL, Lei nº 10.406 de, 10 de janeiro de 2002. **Institui o Código Civil.** Disponível em: [https://www.planalto.gov.br/ccivil\\_03/](https://www.planalto.gov.br/ccivil_03/). Edição atualizada de acordo com a Lei n. 14.030/2020. 7. ed. rev., atual São Paulo: Manole, 2021. E-book. (1 recurso online). ISBN 9786555763591. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 20 out. 2021.

BRASIL. EC nº 115/22. **Emenda Constitucional nº115 de 10 de fevereiro de 2022. Alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.** [http://www.planalto.gov.br/ccivil\\_03/](http://www.planalto.gov.br/ccivil_03/). Acesso em: 04. out. 2022.

BRASIL, Conselho Nacional de Justiça – CNJ. **Resolução nº 332 de, 21 de agosto de 2020. Dispõe sobre a ética, a transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências.** Disponíveis em: <https://atos.cnj.jus.br/atos/detalhar/3429>. Acesso em: 10. out. 2022.

BRASIL, Federação Brasileira de Bancos – FEBRABAN. **Lei endurece penas para crimes eletrônicos, como clonagem do WhatsApp e outros golpes via internet.** FEBRABAN News. 28/05/2021 <https://portal.febraban.org.br/noticia/3631/pt-br/>. Acesso em: 22. set. 22.

BRASIL, FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública: 2022.** São Paulo: FBSP, 2022.

BRASIL, ISTO É. – Big Techs. **História e internet: conexões possíveis.** *Revista Tempo e Argumento*, vol. 6, nº. 12. 2014. Universidade do Estado de Santa Catarina. ISTO É- BigTechs: 2021, o ano em que as gigantes de tecnologia se tornaram insuperáveis Isto é Dinheiro <https://www.istoedinheiro.com.br/>. Reportagem 20/12/21.

BRASIL, Policia civil de São Paulo. **Delitos Praticados na internet, perguntas e respostas.** <https://www.policiacivil.sp.gov.br/portal/image.ns/CRIMES%20CIBERN%C3%89TICOS%20-%20PERGUNTAS%20E%20RESPOSTAS%20V2.pdf>. Acesso em 03. març. 2023.

BRASIL, Superior Tribunal de Justiça – STJ. **Informativo nº 663, 14 de Fevereiro de 2020. Recuperação judicial. Tutela de urgência. Stay Period. Suspensão de atos expropriatórios. Execução fiscal. Competência do juízo da recuperação judicial.** Disponível em: <https://processo.stj.jus.br/jurisprudencia/>. Acesso em: 12. dez. 2019.

CAPEZ, Fernando. **Curso de direito penal: parte especial – Arts. 121 a 212. v. 2.** Editora Saraiva, 2022. E-book. ISBN 9786555596045. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555596045/>. Acesso em: 23 jan. 2023.

CAPEZ, Fernando; Prado, Stela. **Código penal comentado.** 6. ed. São Paulo. Saraiva, 2015.

CARVALHO, MARCELO SÁVIO REVOREDO MENEZES DE **A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança** [Rio de Janeiro] 2006 XX, 239 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Sistemas e Computação, 2006) Dissertação – Universidade Federal do Rio de Janeiro, COPPE.

CAVALCANTE, Márcio André Lopes. **Adulterar o sistema de medição da energia elétrica para pagar menos que o devido: estelionato (não é furto mediante fraude).** Buscador Dizer o Direito, Manaus. Disponível em: <https://www.buscadordizerodireito.com.br/> Acesso em: 31. out. 2022.

CAMBRIDGE. <https://dictionary.cambridge.org/pt/dicionario/ingles/scam>

CAVALCANTE, Márcio André Lopes. **Estelionato previdenciário (art. 171, § 3º do CP): crime permanente ou instantâneo?** Disponível em: <https://buscadordizerodireito.com.br/>- Acesso em: 15. out. 2022.

CORREA, Fabiano Simões. **Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da internet.** 2013. Dissertação (Mestrado em Psicologia) - Faculdade de Filosofia, Ciências e Letras de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2013. Doi:10.11606/D.59.2013.tde-08102013-162610 Acesso em: 28. ago. 2022.

CORREIA, Pedro Miguel Alves Ribeiro; JESUS Inês Oliveira Andrade - **Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas.** REVISTA DIREITO GV | SÃO PAULO | V. 12 N. 2 | 542-563 | MAI-AGO 2016.

COSTA, António Manuel de A. **A Burla no Código Penal Português.** Grupo Almedina (Portugal), 2020. E-book. ISBN 9789724084428. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9789724084428/>. Acesso em: 25 fev. 2023.

COSTA, R. **Por um novo conceito de comunidade: redes sociais, comunidades pessoais, inteligência coletiva.** Interface - Comunic., Saúde, Educ., v.9, n.17, p.235-48, mar/ago 2005. acesso em 22. fev. 2023.

COSTA, Taís Barros Trajano Ribeiro da. **O aumento do crime cibernético durante a pandemia da COVID-19.** Faculdade Damas, Recife-PE, 2020. Disponível em: <https://jus.com.br/>- Acesso em: 18. mai. 2021.

COUNCIL OF EUROPE. **Details of Treaty No. 108.1981.** Disponível em: <https://www.coe.int/en/web/conventions/> Acesso em 03. out. 2022.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva Jur, 2011. E-book. (1 recurso online). ISBN 9788502136663. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788502136663>. Acesso em: 3 ago. 2022.

CUNHA, Úrsula Nascimento de Sousa, **cibercultura e as identidades líquidas: reflexão sobre a cultura na era das novas tecnologias,** Revista: Pontos de Interrogação: Linguagens,

identidades e letramentos - Vol. 2, n. 2, jul./dez. 2012 | 163. Disponível <https://www.revistas.uneb.br/index.php/pontosdeint/article/view/1558>. Acesso em 11 de jan. 2023.

DA SILVA, Patrícia Santos. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015.

DINIZ, F. F.; CARDOSO, J. R.; PUGLIA, E. H. P. O crime de estelionato e suas implicações na era contemporânea: o constante crescimento dos golpes via internet. **LIBERTAS DIREITO**, [S. l.], v. 3, n. 1, 2022. Disponível em: <https://www.periodicos.famig.edu.br/>. Acesso em: 17 set. 2022.

DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel. **Estudos sobre proteção de dados pessoais**. São Paulo: Expressa, 2022. E-book. (1 recurso online). (Direito, tecnologia, inovação e proteção de dados num mundo em transformação). ISBN 9786553620810. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 11 jul. 2022.

FERNADES Claudio. Guerra Fria. Disponível em: <https://www.historiadomundo.com.br/>- Acesso 22. ago. 2022.

FERNANDES, Bernardo Gonçalves. **Curso de direito Constitucional. 12. ed.** rev. atual, e ampl. Salvador. Editora juspodivm, 2020.

FERREIRA, Ivette Senise. **A criminalidade informática. Direito e internet: aspectos jurídicos relevantes**. Tradução. Bauru, São Paulo: EDIPRO, 2001.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2. ed. São Paulo: Saraiva Jur, 2016. E-book. (1 recurso online). ISBN 9788547204198. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 06 out. 2022.

FORBES 2022 promissor: mercado de games ultrapassará US\$ 200 bi até 2023.FORBES. 03 de janeiro de 22

GABRIEL MACHADO, D. R.; GROTT, S. Estelionato virtual. **Revista Científica Multidisciplinar do CEAP**, v. 4, n. 1, p. 10, 9 jun. 2022.

GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. Editora Blucher, 2020. E-book. ISBN 9786555060164. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 08 out. 2022.

GIL, Antônio de Loureiro. **Fraudes Informatizadas**. 2ª ed. 1ª tiragem, 2000.

GONÇALVES, Victor Eduardo R.; LENZA, Pedro. **Esquematizado - Direito Penal - Parte Especial** Editora Saraiva, 2022. E-book. ISBN 9786555597738. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 14 out. 2022.

GRECO, Rogério. **Código Penal Comentado. Grupo GEN, 2021**. E-book. ISBN 9786559770700. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 05 out. 2022.

GRECO, Rogério. **Manual de Direito Penal: Grupo GEN, 2022**. E-book. ISBN 9786559642830. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 27 fev. 2023.

GRECO, Rogério. **Código Penal comentado**. 21. ed. rev., atual., ampl Rio de Janeiro: Forense, 2021. E-book. (1 recurso online). ISBN 9788530993443. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 10 jul. 2022.

HARARI, Yuval Noah. **Homo Deus: uma breve história do amanhã**. Tradução: Paulo Geiger. 1 ed. São Paulo: Companhia das Letras, 2016.

HARARI, Yuval Noah. **Sapiens: uma breve historia da humanidade**; tradução: Jorio Dauster. 1º ed. São Paulo: Companhia das Letras, 2020.

JALIL, Mauricio S.; FILHO, Vicente G. **Código Penal comentado: doutrina e jurisprudência**. Editora Manole, 2022. E-book. ISBN 9786555767360. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 14 out. 2022.

JESUS, Damásio E. de. **Marco civil da internet: comentários à Lei n. 12.965, de 23 de abril de 2014**. São Paulo: Saraiva, 2014. E-book. (1 recurso online). ISBN 9788502203200. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 09 jul. 2022.

LAFLOUFA, Jacqueline. Hackativismo: **Crime cibernético ou legítima manifestação digital?** Com Ciência, Campinas, n. 131, 2011. Disponível em <http://comciencia.scielo.br/scielo>. Acesso em: 12. nov. 2022.

LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. Grupo GEN, 2014. E-book. ISBN 9788522493401. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 06 out. 2022.

LEITE, Luiza; CAMARGO, Matheus. **Open Banking: inovação aberta no sistema financeiro**. Editora Saraiva, 2022. E-book. ISBN 9786553620353. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 12 nov. 2022.

LIMA, Cíntia Rosa Pereira D. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. E-book. ISBN 9788584935796. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 08 out. 2022.

LÓSSIO, Claudio Joel Brito. **Manual Descomplicado de Direito Digital: guia para Profissionais do Direito e da Tecnologia-2**. Ed.rev atual. Ampl- São Paulo: editora JusPodivm, 2021.

LOUREIRO, Antônio Carlos Tovo. **Perfil do estelionato contratual no ordenamento jurídico-penal brasileiro**. 2014. Tese (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015. doi:10.11606/T.2.2015.tde-26082015-113642. Acesso em: 26. out. 2022.

MEDEIROS, Claudio Lucio de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos, 2020**. Disponível em: <http://www.pgi.ce.gov.br/esmp/publicações/edf> Acesso: 18. mai. 2021.

MELLO Danilo: **Fraude contra cliente cresce 65% por e 2021**. Agencia Brasil. Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2021-10/fraudes-contras-clientes-de-bancos-crescem-165-em-2021>. São Paulo, publicação 29/10/2021. Acesso em 28. ago. 2022.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 17. ed. São Paulo: Saraiva Jur, 2022. E-book. (1 recurso online). (IDP. Linha doutrina). ISBN 9786553620506. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 11 jul. 2022.

MENDES, Laura Schertel; MATTIUZZO, Marcela. **Discriminação algorítmica: conceito, fundamento legal e tipologia**. Revista de Direito Público, Brasília, v. 16, n. 90, p. 39-64, 2019. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/>. Acesso em: 10 jul. 2022.

MOROSOV Evgeny. **Big Tech: A ascensão dos dados e a morte da política**: – Edição padrão, editora Ubu, 4 dezembro 2018.

NUCCI, Guilherme de Souza. **Código de Processo Penal comentado**. 20. ed. rev., atual., ampl. Rio de Janeiro: Forense, 2021. E-book. (1 recurso online). ISBN 9788530993474. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 10 jul. 2022.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. 3. ed. São Paulo. Saraiva jur, 2020.

PINHEIRO, Patricia Peck. **#Direito digital**. 7. ed. rev. ampl., atual. São Paulo: Saraiva Jur, 2021. E-book. (1 recurso online). ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 10 jul. 2022.

BRASIL, PORTAL G1. **Denúncias de crimes cometidos pela internet mais que dobram em 2020**. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/09>. Acesso em 21. set. 22.

PORTUGAL. **Código penal português**. Disponível em: <https://www.codigopenal.pt/>. Acesso em 25. fev. 2023.

PROJURIS. **Os golpes mais comuns da internet.** Disponível em: <https://www.projuris.com.br/>. Acesso em 21. set. 22.

REALE, Miguel Junior; WUNDERLICH, Alexandre. “**Justiça negocial e o vazio do Projeto Anticrime**”. In: *Boletim IBCCRIM*, n. 318, maio 2019, pp.06-08. Acesso em 28. out. 2022.

REALE, Miguel Junior. **Fundamentos de Direito Penal.** Grupo GEN, 2020. E-book. ISBN 9788530991609. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 13 jan. 2023.

SIQUEIRA Regina Loureiro Oliveira, S.; GUILHERMINA DE OLIVEIRA, M.. Marco Civil da Internet: Uma Questão Tecnológica e Jurídica. **Revista Eletrônica Direito & TI**, v. 1, n. 13, p. 6, 23 jul. 2020. Disponível em: <https://www.direitoeti.com.br/>. Acesso 08. out. 2022.

RONDON Filho, E. B.; KHALIL, K. P. SCAMMERS: **Estelionato sentimental na internet.** Revista Direito e Justiça: Reflexões Sociojurídicas, v. 21, n. 40, p. 43-57, 24 maio 2021.

SAMPAIO, Inês Vitorino. **Discriminação algorítmica e inclusão em sistemas de inteligência artificial: uma reflexão sob a ótica dos direitos da criança no ambiente digital.** Revista de Direito Público, Brasília, v. 18, n. 100, p. 245-271, Out/Dez. 2021. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/>. Acesso em: 08 out. 2022.

BRASIL, Secretaria de segurança pública do distrito federal – SSP/DF. **Não caia em golpes.** Disponível em: <http://www.ssp.df.gov.br/>. Acesso em: 10. out. 2022.

SANCHES, Rogério Cunha. **Código Penal para concursos: CP.** 14. Ed. rev. atual e ampl. Salvador: juspodivm, 2021.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas.** 2. ed. São Paulo: Saraiva Jur, 2015. E-book. (1 recurso online). (Saberes monográficos). ISBN 9788502229488. Disponível em: <https://integrada.minhabiblioteca.com.br/>. Acesso em: 2 out. 2022.

SYDOW, Spencer Toth. **Curso de Direito Penal Informatico, parte geral e especial.** 3. ed.

rev. e.atual. Salvador: Editora JusPodivm, 2022.

VIANA, Eduardo- **criminologia**, 9. ed. rev. atual. e ampl-Salvador: Juspodivm, 2021.

VINGANÇA digital: **compartilhamento não autorizado de conteúdo íntimo na internet - Procedimentos de exclusão e investigação policial. 1. ed.** ISBN 9788592842082. Rio de Janeiro: Mallet, 2017.

WENDT, E. CIBERGUERRA, INTELIGÊNCIA CIBERNÉTICA E SEGURANÇA VIRTUAL: alguns aspectos. **Revista Brasileira de Inteligência**, n. 6, p. 15-26, 1 abr. 2011.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012.

WOLFGANG, Hoffmann-Riem. **Teoria Geral do Direito Digital.** Grupo GEN, 2021. E-book. ISBN 9786559642267. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559642267>. Acesso em: 11 out. 2022.

WUNDERLICH, A.; Lima, C. E. de; MARTINS Costa, A.; Ramos, M. B. Acordo de não persecução penal. **Revista da Defensoria Pública do Estado do Rio Grande do Sul**, Porto Alegre, n. 26. 2020. Disponível em: <https://revistadpers.emnuvens.com.br/>. Acesso em: 28. out. 2022.