



FACULDADE EVANGÉLICA DE GOIANÉSIA
CURSO DE GRADUAÇÃO EM DIREITO

**A PROTEÇÃO DE DADOS NA ERA DIGITAL: ANÁLISE DO CRIME
DE ESTELIONATO À LUZ DAS VULNERABILIDADES ESTRUTURAIS
DA LEI GERAL DE PROTEÇÃO DE DADOS**

GUSTAVO CUNHA ALENCAR
TALIANA NOVAIS SOARES

GOIANÉSIA-GO
2025

GUSTAVO CUNHA ALENCAR
TALIANA NOVAIS SOARES

**A PROTEÇÃO DE DADOS NA ERA DIGITAL: ANÁLISE DO CRIME DE
ESTELIONATO À LUZ DAS VULNERABILIDADES ESTRUTURAIS DA
LEI GERAL DE PROTEÇÃO DE DADOS**

Artigo Científico apresentado junto ao Curso de Direito da Faculdade Evangélica de Goianésia – FACEG, como exigência parcial para a obtenção do grau de Bacharel em Direito.

Orientação: Prof. Esp. Túlio Vinícios Nunes
Morais.

GOIANÉSIA-GO
2025

TERMO DE RESPONSABILIDADE AUTORAL

Nós, autores deste trabalho, declaramos para os devidos fins que este artigo científico é original e inédito. Foi devidamente produzido conforme Regulamento para elaboração, apresentação e avaliação do trabalho de conclusão de curso em Direito da Faculdade Evangélica de Goianésia-Goiás – FACEG.

Declaramos, também, na qualidade de autores do manuscrito, que participamos da construção e formação deste estudo, e assumimos a responsabilidade pública pelo conteúdo deste.

Assim, temos pleno conhecimento de que possamos ser responsabilizados legalmente caso infrinja tais disposições.

FOLHA DE APROVAÇÃO

A PROTEÇÃO DE DADOS NA ERA DIGITAL: ANÁLISE DO CRIME DE ESTELIONATO À LUZ DAS VULNERABILIDADES ESTRUTURAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

Este artigo foi julgado adequado para a obtenção do título de Bacharel em Direito e aprovado em sua forma final pela banca examinadora da Faculdade Evangélica de Goianésia/GO – FACEG.

Aprovado em, 27 de junho de 2025.

Nota Final _____

Banca Examinadora:

Prof. Esp. Túlio Vinícios Nunes Moraes
Professor Orientador

Profa. Ma. Marlana Carla Peixoto Ribeiro
Professora convidada

Prof. Esp. Thiago José da Silva
Professor convidado

A PROTEÇÃO DE DADOS NA ERA DIGITAL: ANÁLISE DO CRIME DE ESTELIONATO À LUZ DAS VULNERABILIDADES ESTRUTURAIS DA LGPD

THE GENERAL DATA PROTECTION LAW AND CASES OF DIGITAL FRAUD

Taliana Novais Soares¹
Gustavo Cunha Alencar²
Túlio Vinícius Nunes Moraes³

¹Discente do curso de Direito da Faculdade Evangélica de Goianésia- *e-mail*:
talianasoes@hotmai.com

²Discente do curso de Direito da Faculdade Evangélica de Goianésia- *e-mail*:
gustavocunha11@yahoo.com.br

³Docente do curso de Direito da Faculdade Evangélica de Goianésia - *e-mail*:
proftulimoraes@gmail.com

RESUMO: A presente pesquisa, intitulada “A proteção de dados na era digital: análise do crime de estelionato à luz das vulnerabilidades estruturais da lei geral de proteção de dados”, discorre sobre análise qualitativa da eficácia da lei 13.709/2018 no combate aos estelionatos digitais e as brechas que a lei possui. O tema se justifica na novidade e atualidade da lei e sua ineficácia retratada no dia a dia dos brasileiros. A problemática que se buscou responder foi: A lei Geral de proteção de dados possui lacunas que podem comprometer a segurança de dados no Brasil fomentando a prática de crimes? Qual é a análise crítica majoritária que pesa sobre a eficácia da LGPD em detrimento dos desafios, garantias e segurança dos dados de usuários? O objetivo geral é analisar os efeitos da LGPD e a sua vulnerabilidade em relação ao estelionato digital. O objetivo específico, por sua vez, trará o entendimento jurisprudencial e doutrinário sobre o tema, abordando pontos fortes e falhas na lei. Busca-se ainda, estabelecer a vínculo da engenharia do crime de estelionato com uso de dados vazados no Brasil. A metodologia utilizada foi de pesquisa bibliográfica sob o método monográfico, por meio da análise da lei e em conjunto com doutrinas e outras obras científicas. A pesquisa constatou que a LGPD apresenta falhas no que se refere à conformidade e padrões de segurança, por estabelecer uma abordagem individualizada a própria análise de risco e responsabilidade do controlador de dados.

Palavras-chave: Proteção de Dados. Estelionatos Digitais. Vazamento de Dados. Governança de dados. LGPD.

ABSTRACT: This research, entitled “Data protection in the digital age: analysis of fraud in light of the structural vulnerabilities of the general data protection law”, discusses a qualitative analysis of the effectiveness of law 13.709/2018 in combating digital fraud and the loopholes that the law has. The theme is justified by the novelty and current nature of the law and its ineffectiveness portrayed in the daily lives of Brazilians. The problem that we sought to answer was: Does the general data protection law have gaps that can compromise data security in Brazil, encouraging the practice of crimes? What is the majority critical analysis that weighs on the effectiveness of the LGPD to the detriment of the challenges, guarantees and security of user data? The general objective is to analyze the effects of the LGPD and its vulnerability in relation to digital fraud. The specific objective, in turn, will bring the jurisprudential and doctrinal understanding on the subject, addressing strengths and flaws in the law. The aim is also to establish the link between the engineering of the crime of fraud and the use of leaked data in Brazil. The methodology used was bibliographic research using the monographic method, through the analysis of the law and in conjunction with doctrines and other scientific works. The research found that the LGPD has flaws in terms of compliance and security standards, as it establishes an individualized approach to the risk analysis and responsibility of the data controller.

Keywords: Data protection. Digital fraud. Data Leak. Data governance. LGPD.

INTRODUÇÃO

O presente estudo justifica-se pela pretensão de realizar a investigação das brechas da lei geral de proteção de dados em razão dos crimes correlatos a vazamento de dados no Brasil. De fato, uma lei nova, que ainda possui lacunas que dificultam a segurança de dados no país, a ponto de causar danos irreparáveis, atrasos e retrocessos, promovendo a vulnerabilidade no tratamento, manutenção e proteção de dados dos brasileiros e estrangeiros naturalizados.

A Lei Geral de Proteção de dados trouxe à tona uma preocupação advinda do avanço da tecnologia e da era digital. Essa inovação trouxe consigo uma mudança de olhar sobre segurança de dados no Brasil e no mundo. Em 2018, foi promulgada na Europa a GRPR – *General Data Protection Regulation*, regras de ouro para a proteção de dados no continente e foi o norte e a mola propulsora para a elaboração da Lei 13.709/2018, publicada em 15 de agosto do referido ano.

A entrega de uma realidade velada e centrada que, ambas as leis, tanto europeia quanto a brasileira foi uma alternativa legal, resultado de um interesse afim de assegurar uma maior e completa privacidade, no controle e adequação do tratamento de dados pessoais, fortalecendo o aparato estatal afim de garantir a regulamentação de empresas e órgãos públicos ou privados.

Portanto, a publicação da lei configura no resultado de uma gestão eficiente sobre os rumos da ação governamental dos dados de pessoas físicas, jurídicas e governamentais em posse de empresas públicas, privadas, repartições públicas, ONGs e entre milhares e milhares de meios e caminhos onde dados de terceiros possam estar armazenados e sendo usados para uma determinada finalidade.

A Lei brasileira possui o seu objetivo explícito na redação legal que denota sobre a disposição sobre o tratamento de dados pessoais, tanto em meios físicos, tanto digitais, por pessoa natural ou por pessoa jurídica, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural frente a utilização de dados.

A Lei 13.709/2018 é coerente em tratar sobre as qualidades e os direitos fundamentais da proteção de dados. De igual forma, é claro e eficaz o mesmo diploma legal sobre os procedimentos adotados a qualquer instituição, sendo pública ou privada, dando valor sobre as hipóteses do uso de dados e seu tratamento.

Desta forma, a LGPD evidencia que a regulamentação brasileira proporcionou uma inovação sobre a gestão de dados no Brasil, estabelecendo parâmetros a fim de dificultar a comercialização, compartilhamento e entre outros caminhos de transferência de dados e informações de detentores sem o consentimento do titular, visto que na era digital existe uma maior facilidade na transferência de informações.

Todavia, é reportado em jornais de televisão, rádio, internet, testemunhos de vizinhos, parentes e entre outras formas, a notícia da recorrência de crimes realizados via telefone, entre outros caminhos virtuais, por infratores se passando por filho, por neto, por parente, por atendente do banco onde é correntista, enfim, usando de dados que são específicos e pessoais a fim de subtrair para si coisa alheia de forma ilícita, mesmo com uma lei restringindo tais práticas.

Portanto, fica claro que a lei possui um texto eficaz e com nitidez na imperatividade da norma. Diante disso, a problemática abordada nesta pesquisa visa em entender sobre a eficácia e as garantias da lei. Por isso no decorrer deste trabalho responderemos as seguintes perguntas: A lei Geral de proteção de dados possui lacunas que podem comprometer a segurança de dados no Brasil fomentando a prática de crimes? Qual é a análise crítica majoritária que pesa sobre a eficácia da LGPD em detrimento dos desafios, garantias e segurança de usuários?

O objetivo geral é analisar os efeitos da LGPD e a sua vulnerabilidade em relação ao estelionato digital. Também será versado nos objetivos específicos, tratando sobre o entendimento jurisprudencial e doutrinário sobre o tema de proteção de dados, abordando pontos fortes e falhas na lei. Outro ponto tratado será o contato da engenharia do crime de estelionato com os dados vazados a fim de trazer prejuízo para vítima, além de estabelecer a sua aplicabilidade no cotidiano das pessoas capazes e em estado de vulnerabilidade.

A metodologia aplicada foi pesquisa de pesquisa bibliográfica, com foco qualitativo, salientado na abordagem explorativa e discricionária na letra da lei, entendimentos jurisprudenciais, artigos científicos e na doutrina.

O trabalho está dividido em três partes do assunto correlato, além da introdução e das considerações finais. O primeiro tópico trata-se da proteção de dados no Brasil, com considerações à evolução histórica, pontos fortes e fundamentos legais e legislativos, considerando a análise de crescimento tecnológico em conjunto com o surgimento das leis e regras no ordenamento jurídico internacional e nacional.

O segundo tópico, por sua vez, discorre sobre o crime de estelionato e suas aplicações no âmbito digital, demonstrando seu conceito global, natureza jurídica e como é o *modus operandi* do crime de estelionato, em confronto com o estelionato digital, que é objeto da presente pesquisa, ressaltando as concordâncias da lei em virtude as técnicas e métodos criminosos. Já o terceiro tópico tem por título o crime de estelionato e as vulnerabilidades estruturais da LGDP, cuja função é estabelecer um paralelo entre o caso de estelionato e as brechas na proteção de dados no Brasil, trazendo as inovações de cada lei, pontos fortes e fracos por análises doutrinárias e jurisprudência de abrangência nacional.

Como resultado final, a presente pesquisa identificou que a referida lei apresenta uma brecha em sua norma que impossibilita a uma padronização na conformidade de segurança das empresas e detentoras de dados tanto brasileiras quanto estrangeiras com atividades no território nacional. Além disso, sugeriu que seja implantando um normativo padronizador de segurança, bem como uma implementação de educação digital com propagandas em rede nacional e maior atuação da Agência Nacional de Proteção de Dados como forma de contribuir para a efetiva resolução do problema proposto.

Portanto, diante do tema exposto e respaldado em novidade, espera-se que o estudo acrescente em uma visão aprofundada para o discurso acadêmico e atual sobre a proteção de dados no Brasil e os casos de golpes digitais.

1. A PROTEÇÃO DE DADOS NO BRASIL

Na esfera do direito à privacidade, o brasileiro tem como garantia pela constituição de 1988, o direito ativo em manter sobre o seu controle as informações que pode ser disponibilizada para um grupo restrito. De fato, a Constituição Federal de 1988 evidencia que o poder constituinte não apenas objetivou promover a segurança, mas promover o direito que pode vir a existir em relação a reparação ao eventual atingido. Visto que, caso haja danos efetivamente irreparáveis o Poder Judiciário deve intervir, pois tem por prerrogativa o poder de garantir a proteção contra à lesão ou ameaça a esse direito (Bentivegna, 2019).

Consequentemente, o direito absoluto da liberdade de expressão é suscetível de restrição, ou seja, existem limitações a esse direito através do Poder Judiciário e ou do Poder Legislativo. Dessa forma, o direito absoluto é orientado e imposto através

das a normativas da Constituição Federal. Essa flexibilidade garante que a liberdade de expressão não viole outros direitos fundamentais, como privacidade e a honra (Machado, 2019).

Quando ocorre o conflito entre a liberdade de expressão e da comunicação e os direitos da personalidade, ambos protegidos pela Constituição Federal de 1988, a conciliação é essencial. Em uma situação concreta, um desses direitos deverá ser relativizado. Para a efetivação desses direitos, surgem normativas ao longo da história que corroboram para o melhor entendimento da relação ao acesso de dados pessoais e sua proteção, bem como a imposição de limites para quem detém essas informações (Grundrechtskollision *apud*, Bentivegna, 2019, p. XV).

Diante do desvendar histórico sob a égide da criação de uma lei que regulamenta o tema de proteção de dados, aconteceu nos meados dos anos 70 e 80 um movimento estadunidense voltado para o uso controlado de dados de terceiros em posse das empresas. No entanto, essa inauguração legal não aconteceu nas américas, mas sim na Europa, em específico em terras Alemãs em virtude do crescente desenvolvimento das tecnologias computacionais e que foi amplamente difundido por países mais desenvolvidos como França, Noruega, entre outros no que influenciou a União Europeia a firmar o seu regulamento (Santos, Araújo e Rego, 2021).

No território brasileiro, o tema foi inaugurado e tomando assento irrevogável na carta magna do Brasil, com a promulgação da Constituição Federal do Brasil, de 5 de outubro de 1988 (Assis e Mendes 2021). A propósito, a referida Carta Magna, em seu artigo 5, inciso X, dispõe que:

X - 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; (Brasil, 1988).

Com o passar dos anos, em conjunto com as tecnologias implementadas no território nacional e as condutas pessoais dos brasileiros, foi promulgada a Lei nº 9.296/1996 que regulamentou o inciso XII, parte final, do art. 5º da Constituição Federal, ao tornar inviolável o sigilo das ligações telefônicas, das correspondências, das comunicações telegráficas, a não ser por ordem judicial com base legal e fundado em objetivos de investigação criminal e penal, deixando claro que o legislador

brasileiro restringiu ainda mais os parâmetros de direito tornando a privacidade de dados no Brasil mais empoderada (Grinover, 2020).

A evolução tecnológica transformou significativamente a forma como os dados são coletados, armazenados e utilizados. Inicialmente, os registros eram feitos manualmente em arquivos físicos, passando posteriormente pela digitalização e armazenamento eletrônico em bancos de dados. Com o avanço da *internet* e da computação em nuvem, o volume de dados compartilhados cresceu exponencialmente, evidenciando a necessidade de regulamentação para garantir a segurança das informações pessoais (Silva, 2024).

Desde o século XIX, a comunicação tem sido um dos pilares da troca de informações. Alexander Graham Bell, em 1876, patenteou o telefone, permitindo a transmissão instantânea de voz (Sousa, 2022). No entanto, foi no final do século XX e início do século XXI que a revolução digital ampliou significativamente a coleta e o processamento de dados pessoais. A invenção do telefone celular por Martin Cooper em 1973 e o lançamento do primeiro smartphone pela IBM em 1994 impulsionaram o compartilhamento de dados em escala global (Anhesini, 2024).

O primeiro marco significativo na legislação de proteção de dados ocorreu na Alemanha Ocidental, em 1970, com a criação de normas para a proteção de informações pessoais. Posteriormente, a União Europeia consolidou suas regras através do *General Data Protection Regulation* – GDPR (Brasil, 2018).

Com a popularização da *internet* e dos dispositivos eletrônicos conectados, tornou-se essencial estabelecer mecanismos para proteger os dados pessoais contra usos indevidos (Almeida e Soares, 2022). O Presidente da Autoridade Nacional de Proteção de Dados (ANPD), Waldemar Gonçalves (2024), destaca que é basal normatizar o tratamento de dados e assegurar o respeito aos direitos do titular. Esse posicionamento reflete a necessidade de regulamentação em um cenário onde a digitalização das informações cresce exponencialmente.

Em 2014, surge a lei que estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, conhecida como *Marco Civil da Internet* (Lei nº 12.965, de abril de 2014), sancionada após um processo de debate político, no qual abarcou diversos setores da sociedade, é a principal legislação que regula o uso da *internet* no Brasil (Leite, 2014).

Embora tenha por objetivo regulamentar a privacidade dos dados e suas gestões, a Lei Geral de Proteção de Dados (LGPD), inspirada no GDPR, surge após

verificar o aumento dos casos de vazamentos de dados e o impacto da tecnologia na vida privada. Sancionada em 2018, entrou em vigor de maneira escalonada. Inicialmente, em 28 de dezembro de 2018, foram instituídos os artigos referentes à criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD). Posteriormente, em 18 de setembro de 2020, os demais artigos passaram a vigorar, com exceção das sanções administrativas, que entraram em vigor somente em 1º de agosto de 2021 (Santos e Freitas, 2024).

Dessa forma, a evolução da coleta e do uso de dados pessoais evidencia a necessidade de regulamentação para garantir a segurança das informações e proteger os direitos fundamentais dos cidadãos diante dos desafios da era digital (Mendes e Branco, 2020).

Em paralelo ao histórico da proteção de dados no mundo, no Brasil foram criados dispositivos legais de natureza protecionista, tais como o Código de Defesa do Consumidor (CDC), que possui manifesto intuito de proteger o consumidor, reconhecendo a sua vulnerabilidade. A propósito, a nova Constituição foi promulgada, trazendo em seu artigo 5º, inciso XXXII, a proteção do consumidor como uma das garantias fundamentais. Observa-se, ainda, no artigo 170, inciso V, a defesa do consumidor como um dos princípios gerais da ordem econômica e financeira (Ribeiro, 2023).

Embora seja possível identificar, no próprio Código de Defesa do Consumidor, aspectos relacionados à proteção de dados pessoais, a necessidade de uma legislação específica tornou-se evidente com o aumento das interações digitais e dos casos de vazamento de informações. De modo geral, o Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados (LGPD) são distintos em suas origens e objetivos, mas se complementam na missão de garantir maior segurança e respeito aos direitos do consumidor (Mendes, 2021).

Nota-se, portanto, uma trajetória histórica comum entre os direitos do consumidor e a proteção de dados pessoais no Brasil. Essa trajetória exige uma constante adaptação às transformações tecnológicas. A implementação do CDC e da LGPD busca assegurar, de forma mais ampla, os direitos fundamentais do consumidor, como o direito à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural (Lugati e Almeida, 2020).

Com a evolução tecnológica e do mercado, surgiu também a valorização financeira dos dados pessoais. Isso acontece porque as informações passaram a ter grande impacto na economia, permitindo que empresas adaptem seus serviços e aumentem seus lucros a partir da coleta e análise desses dados. Diante disso, tornou-se essencial proteger juridicamente esse bem, regulamentando o tratamento de dados pessoais, para que sejam utilizados de forma legítima e sem causar qualquer prejuízo ao consumidor (Feiler, Gazaniga e Vieira, 2024).

A Agência Brasil, publicada no site do Senado Federal em 2020, expõe em seu texto que a Lei 13.709 de 2018 é o marco legal que traz as atribuições sobre o uso, a transferência e a proteção de dados pessoais no território brasileiro garantindo aos cidadãos um maior controle sobre suas informações pessoais, tornando a exigir uma aceitação clara para a obtenção e a utilização dos dados e impera alternativas de edição, visualização e exclusão desses dados, dentre os demais dispositivos criados com o passar dos anos afim de jurisdicionar o tema (Casal Jr., 2020).

O Projeto de Lei da Câmara 53/2018, que origina a LGPD, foi aprovado com unanimidade pelo Senado Federal e em caráter de urgência, tornando matéria de relevante importância para o país. Ao analisar o texto da lei, a eficácia estende até mesmo em empresas estrangeiras, porém com operações em território nacional. Sendo imprescindível para a vedação do cruzamento de informações e dados de uma única pessoa ou de um determinado grupo afim de influenciar decisões políticos partidários e comerciais, ou seja, veda o tratamento de dados pessoais para as atividades que produzem discriminação ilegal ao abusiva (Maldonado e Opice Blum, 2019).

Inspirada no regulamento europeu, a LGPD possui 65 artigos divididos em 10 capítulos. Possui a abrangência de quaisquer dados pessoais, obtidos de qualquer fonte, seja física ou digital. A lei diferencia sobre a prestação de serviços com base em dados pessoais, onde no contrato deve ser evidente tal necessidade, de dados sensíveis. Estes são aqueles que demandam um tratamento diferenciado, ou seja, as informações étnicas e raciais, religiosas, assuntos políticos, filiações sindicais, opiniões filosóficas e políticas; dados relacionados a saúde e vida sexual; dados genéticos ou biomédicos quando vinculados a pessoa natural (Fleming, 2021).

Em segunda análise, a lei impera as sanções administrativas divididas em multas simples, diárias, suspensões onde podem ser parciais ou totais de funcionamento, entre outras, que podem ser uma simples advertência até o

pagamento de R\$ 50.000.000,00 (cinquenta milhões de reais). Torna o responsável cível, todo aquele que em exercício de sua atividade trazer danos patrimoniais, morais, individuais ou coletivos sendo obrigatória a reparação (Casal Jr., 2020).

A revolução da Lei Geral de Proteção de Dados foi a criação de um órgão regulamentador que além de orientar, fiscaliza as empresas e entes públicos e estatais a fim de zelar pela aplicabilidade da Lei. Tem como o papel de comunicar os desvios aos controladores e detentores de dados sob má gestão e vulnerabilidade, além de acionar órgãos federais para a interposição de sanções, multas e penalidades (Santos e Freitas, 2024).

2. O CRIME DE ESTELIONATO E SUAS APLICAÇÕES NO AMBITO DIGITAL

Estelionato é um termo amplamente conhecido em nossa sociedade e sempre associado à ideia de crime, conforme aponta Mirabete (2005). No entanto, sua essência reside na fraude. A própria palavra tem origem em "*stellio*", que se refere a um lagarto capaz de mudar de cor para iludir os insetos dos quais se alimenta. Essa analogia ilustra perfeitamente o jogo de sentido e força implícito no estelionato, que envolve camuflagem, dissimulação, fraude e simulação com o objetivo de obter vantagem em negociações.

A definição legal do estelionato, descrita no artigo 171 do Código Penal Brasileiro, consubstancia os elementos basilares para a tipificação da referida conduta:

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

Desse modo, o estelionato configura-se pela dupla ofensa ao patrimônio e à boa-fé da vítima. Com o dolo específico de obter vantagem patrimonial (*animus lucrandi*) o agente emprega meios fraudulentos para manipular a realidade, induzindo a vítima a um ato que resulta um prejuízo ao seu patrimônio e, ao mesmo tempo, proporciona um proveito indevido ao agente ou a terceiros. A vítima, nesse contexto, pode tanto perder o que já possuía, como uma quantia entregue ao estelionatário, quanto deixar de ganhar o que lhe era devido (Greco, 2025).

Dessa forma, a diversidade de formas que a fraude pode assumir é um dos aspectos que tornam o estelionato um crime complexo. Essa adaptabilidade do estelionatário, que se manifesta tanto em golpes tradicionais quanto em sofisticadas investidas no ambiente virtual, explorando vulnerabilidades e novas tecnologias, reflete a natureza astuta e inteligente do crime, que se aproveita da credulidade ou desatenção da vítima (Nucci, 2020).

Essa análise evidencia a natureza insidiosa do crime, que com frequência se aproveita da boa-fé, da ingenuidade ou até mesmo da ambição da vítima para efetuar o golpe. A linha tênue entre a conduta lícita e a ilícita pode, em certos casos, complicar a identificação e a comprovação do dolo específico do agente (Silva, 2022).

A análise do público-alvo revela, ainda, que certas parcelas da população se mostram mais vulneráveis às investidas dos estelionatários. Idosos, pessoas com menor grau de instrução e indivíduos em momentos de fragilidade emocional ou financeira frequentemente se tornam alvos preferenciais, expondo a dimensão social do crime e a necessidade de estratégias de prevenção e conscientização direcionadas a esses grupos. Sendo assim, o legislador previu pena mais severa quando a vítima é idosa ou vulnerável, conforme o disposto no artigo 171, § 4º do Código Penal: “A pena aumenta-se de um terço ao dobre, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.” (Brasil, 1940).

Em sua essência, o estelionato, configura-se pelo emprego ardil ou outro meio fraudulento que pode levar a vítima ao erro. Essa conduta se trata de uma conduta ardilosa e intencional, utilizada para distorcer a realidade e, assim, obter uma vantagem indevida. Nesse sentido, é importante ressaltar que a fraude no estelionato é o meio para que o autor do crime atinja seu objetivo, e não o próprio fim da conduta, distinguindo-se, por exemplo, da fraude civil. Enfatiza-se que o ardil consiste na encenação de uma situação fictícia ou na dissimulação da verdade, elementos cruciais para a configuração do delito (Bitencourt, 2023).

Para que o crime de estelionato seja caracterizado, a simples existência de um ardil é insuficiente; é primordial que esse meio resulte no induzimento ou na manutenção da vítima em erro. Em outras palavras, a conduta do agente deve ser a causa direta do estado de engano da vítima, levando-a a agir de uma forma que ela não agiria se estivesse ciente da verdade. Nesse contexto, o erro consiste na falsa compreensão da realidade por parte da vítima, o que induz a dispor de seu patrimônio. Portanto, aponta que a ação do agente deve ser eficaz para provocar ou consolidar o

erro da vítima. Esse erro é o ponto de conexão entre a fraude e a disposição prejudicial do patrimônio (Greco, 2024)

No crime de estelionato, um dos aspectos fundamentais é a obtenção de vantagem ilícita para si ou para outrem. Isso significa que o agente, ao usar de fraude para enganar a vítima, procura um ganho financeiro indevido. Essa vantagem pode ser para si próprio ou a um terceiro, o que mostra a abrangência desse crime. A consumação do crime segundo a doutrina e a jurisprudência majoritária, ocorre quando o agente consegue de fato obter vantagem. Portanto a vantagem no estelionato precisa ser econômica, dito de outro modo, e que sua efetiva obtenção é o marco para a consumação do estelionato, independentemente de a vítima ter sofrido prejuízo imediato (Masson, 2022).

No entanto, é possível comparar o crime de estelionato com os demais crimes patrimoniais. A principal diferença entre o estelionato e o furto, por exemplo, está na maneira de como a vítima perde a posse do bem. No estelionato, a vítima, induzida a erro por um ardil ou fraude, entrega voluntariamente o bem ao agente, mesmo que essa decisão seja resultado do engano (Greco, 2024).

Em contrapartida, no furto, a subtração do bem ocorre sem qualquer consentimento da vítima, ou seja, de forma clandestina, mediante arrebatamento ou destreza, sem que haja uma colaboração, ainda que equivocada, da parte lesada, que, conforme ensina Mirabete (2010, p. 189) “o assenhoreamento da coisa com fim de apoderar-se dela com ânimo definitivo”.

A diferenciação entre estelionato e roubo segue a mesma lógica do furto quanto à disposição do bem, mas com um elemento adicional e crucial: a violência ou grave ameaça. Enquanto no roubo o agente emprega violência ou grave ameaça para forçar a vítima a entregar o bem ou a permitir sua subtração, no estelionato, a entrega do patrimônio ocorre em virtude do engano a que a vítima é submetida, sem o uso desses meios coativos. A ausência de coação física ou moral é um elemento essencial para a configuração do estelionato. Assim, a vítima de estelionato age por um erro de percepção da realidade, criado ou mantido pelo fraudador, ao passo que a vítima de roubo tem sua vontade viciada pela intimidação ou pela agressão física (Bitencourt, 2023).

Portanto a adaptabilidade do estelionatário se traduz na multiplicidade de formas que o crime de estelionato pode assumir. Essa diversidade não se limita apenas aos métodos empregados, mas também aos contextos nos quais a fraude se

manifesta, explorando desde a ingenuidade humana até as complexas relações digitais e financeiras. A constante evolução tecnológica, por exemplo, oferece novas ferramentas e cenários para a atuação desses criminosos, tornando a prevenção um desafio contínuo (Silva, 2024).

Mesmo com o avanço tecnológico, os golpes clássicos continuam a fazer inúmeras vítimas, operando sob a premissa de induzir a vítima ao erro por meio de artifícios bem elaborados. O "bilhete premiado", por exemplo, tipifica a manipulação da esperança de um ganho fácil, onde o estelionatário simula a posse de um bilhete de loteria premiado, mas que não pode ser sacado, oferecendo-o à vítima por um valor muito inferior ao prêmio, em troca de dinheiro ou bens. Outra modalidade é o "falso depósito", onde o agente simula um pagamento com envelopes vazios ou cheques sem fundos, induzindo a vítima a liberar um produto ou serviços antes da compensação (Capez, 2024).

O advento da *internet* e a popularização do ambiente digital impulsionaram o surgimento e a sofisticação do estelionato online, também conhecido como cibercrimes de natureza patrimonial. O *phishing*, por exemplo, simula comunicações legítimas com propósito de capturar dados pessoais e sensíveis. Os golpes em redes sociais, como perfis falsos ou ofertas fraudulentas, e fraudes em *e-commerce* e aplicativos, que envolvem a venda de produtos inexistentes ou de baixa qualidade, são táticas que se valem da engenharia social para manipular o comportamento da vítima no ambiente virtual (Nucci, 2023).

Os golpes financeiros representam uma faceta do estelionato que atinge diretamente a esfera econômica da vítima, muitas vezes explorando o desejo de lucros rápidos ou a necessidade de segurança financeira. Os esquemas de "pirâmide financeira" ilustram essa modalidade, prometendo retornos exorbitantes por meio de um sistema insustentável, onde o lucro dos investidores antigos depende do ingresso de novos participantes, culminando no colapso do esquema e no prejuízo da maioria (Greco, 2023).

Observa-se que não é restrito apenas às diversas formas de sua execução, mas também se manifesta na análise do público-alvo. A compreensão do perfil das vítimas e dos fatores que as tornam suscetíveis é crucial para o desenvolvimento de estratégias eficazes de prevenção e combate a esse tipo de crime. A partir desse pressuposto, a análise do público-alvo mostra que algumas parcelas da população são mais vulneráveis ao estelionato, tornando-se alvos preferenciais (Silva, 2024).

Os fatores de vulnerabilidade não se limitam a características inerentes à vítima, mas se ampliam para circunstâncias que potencializam a ação do estelionatário, como a falta de informação e o isolamento social. A ganância pode levar a crer em lucros rápidos. A ingenuidade impede a percepção das inconsistências. O isolamento social reduz a rede de apoio, e a pressão financeira pode gerar decisões precipitadas. Esses elementos, combinados, criam um ambiente propício ao estelionato (Greco, 2023).

Observa-se que o perfil das vítimas tem se reconfigurado com a ascensão das novas tecnologias e a proliferação dos golpes online, abrangendo agora indivíduos mais jovens e com maior letramento digital. Isso mostra que a familiaridade com a tecnologia não garante imunidade. Golpes sofisticados alcançam um espectro mais amplo da população, incluindo pessoas com alto grau de instrução. Essa mudança reflete a constante adaptação dos estelionatários e a necessidade de expandir a conscientização e a prevenção para todos os estratos sociais (Nucci, 2023).

Diante disso, a crescente facilidade no manuseio de dados e a ampla propagação de dados pessoais sensíveis na era digital, intensificam o crime de estelionato. Essa vulnerabilidade na proteção de dados, que deveria ser resguardada por lei, permite que criminosos orchestrem golpes mais eficazes. A fragilidade na obtenção e tratamento dessas informações é a porta para a ação criminosa. A própria estrutura da internet se tornou um mecanismo de exploração de dados, onde a vulnerabilidade individual alimenta a engenharia social e as fraudes. Assim, a análise de como a gestão insegura de dados fomenta o estelionato é crucial para entender a dinâmica desse crime (Leite e Lemos, 2014).

3. ESTELIONATO E A PROTEÇÃO DE DADOS.

Diante do advento da criação das tecnologias, capazes de facilitar as atividades humanas em um mundo globalizado e moderno, podemos destacar a criação da *internet* como a principal ferramenta e troféu deste momento da história da humanidade. Quando observado as etapas da evolução tecnológica humana, observa-se que o seu tempo vão traduzindo a necessidade de tais equipamentos, descobertas e afins. Contudo com a *internet* não é diferente, criada no período da Guerra Fria (1947 – 1991) onde 2 blocos polarizados via regras e atividades diversas,

sendo econômicas, militares e aeroespaciais se desenvolverem sob o comando e o olhar da União Soviética socialista contra o capitalismo americano (Silva, 2024).

Além disso, assim como outras tecnologias criadas para uma determinada finalidade foi colocada à disposição da humanidade de forma em geral, como por exemplo, a criação do micro-ondas, *wi-fi*, entre outras, a *internet* foi criada para facilitar a comunicação entre os departamentos de defesa dos Estados Unidos. Com o passar do tempo, ao finalizar a guerra fria, passa-se então a difundir a rede para outros países muito impulsionada por empresas provedoras de acesso. Outro fato importante, foram os estudos acadêmicos que permitiram a criação de hipermídias capazes de comportar texto, mídias, som e imagens de maneira instantânea e segura como o WWW (Silva, 2024).

De fato, com um mundo extremamente digitalizado e com grandes vantagens tecnológicas, as empresas de tecnologias compreendem a 12% do PIB mundial, muitas delas presentes nos EUA e na China. Estas empresas se empenharam para que o computador deixasse de ser uma máquina para ser uma ferramenta capaz de oferecer recursos e alternativas que possibilita a uma facilitação da vida das pessoas e seus usuários, favorecendo para a grande disseminação da tecnologia pelo mundo (Silva, 2024).

Contudo, é de se notar que a *internet* não trouxe somente benefícios e nem facilidades no mundo o qual é considerado como moderno devido tais adventos. De fato, existem pessoas que utiliza das redes e meios de transmissão de dados a fim de adquirir para si ou para outrem de maneira ilícita vantagens para si e essas práticas são consideradas como cyber crimes ou crimes virtuais (Silva, 2024).

Portanto, os crimes praticados do âmbito da *internet* são conhecidos dentro do ordenamento jurídico como estelionato digital ou virtual, em alguns casos são chamados de fraudes digitais, mas a sua regulamentação e a sua norma está no artigo 171, no parágrafo 2-A do Código Penal, incluída no código pela lei 14.155 de 2021, Brasil (1940):

§ 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)

A Lei 14.155 de 2021 inseriu ao Código Penal uma maior abrangência para os crimes de estelionato e violação de dispositivos eletrônicos, incluindo o artigo 154-A a criminalização de dispositivos informáticos de uso alheio, conectados ou não na *internet* afim de adulterar as informações sem autorização do usuário. Ainda regula em seu corpo sobre a fraude eletrônica e sua criminalização, estelionato contra idoso e vulnerável sob o artigo 171 do referido código. Verifica-se, assim, uma preocupação do legislador em criminalizar e trazer pena sob a engenharia social e ótica da teoria do crime (Silva, 2024).

Ademais, Crespo (2011), orienta o fato da 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.

Portanto, neste fundamento que a referida lei 14.155 de 2021 que é nominada de Lei Contra o Estelionato e o furto virtual validam a intenção do legislador em estancar uma inofensiva ingenuidade de vulneráveis e usuários em comum para a obtenção de forma ilícita de bens móveis, com penas indo de 4 a 8 anos de prisão com agravantes de acordo com o desenrolar das ilicitudes e seus praticantes inserindo no ordenamento jurídico o texto da lei tornando-a pública e atuante (Silva, 2024).

Os autores Aguiar e Amaral (2024) na obra Estelionato por meio de fraude eletrônica: um não remédio para um atual fato antigo, publicado em 4 de dezembro de 2024 expõem o seu olhar sob o tema relacionando o caput do artigo 171 do Código Penal – Decreto-Lei 2.848/1940 já criminalizando a sequencia criminosa, conforme a leitura do texto da lei por Brasil (1940):

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.

Os autores, salientam que o acréscimo do parágrafo 2-A, não traz novidade ou inovação, sendo somente uma repetição da parte do caput onde diz “erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”, não trazendo a supressão das omissões, mas sim dizendo do mesmo com outras palavras (Aguiar e Amaral, 2024).

Verifica-se, assim, que os dispositivos não se sustentam em demonstrar somente a essência da ilicitude de estelionato digital, mas sim, minar os motivos que os originam. A justificativa do Plenário da Câmara dos Deputados na oportunidade de

incluir em pauta o assunto, mostra a preocupação dos crescentes casos dos crimes e em especial aos vulneráveis sob a necessidade de criar caminhos e punições rígidas para o fenômeno, porém não foi concluída, na realidade possui suas lacunas (Aguiar e Amaral, 2024).

Portanto, é possível discorrer em 3 erros evidentes no dispositivo. O primeiro deles é de legalidade. Ou seja, é claro o entendimento que o estelionato é um crime contra o patrimônio, mas o que torna sem nexos é a diferenciação do uso de dispositivo telefônico para a sua consumação, sendo, o caput do artigo 171 capaz de englobar todo e qualquer meio ou veículo a fim de obter de maneira ilícita para si ou para outrem bem material e móvel, não fazendo sentido a necessidade de diferenciação dependendo do meio usado pelo criminoso (Aguiar e Amaral, 2024).

Um segundo problema é o da proporcionalidade. A pena prevista no *caput* do 171 do Código Penal é de reclusão de 1 a 5 anos, e multa. Contudo, a penalização permite o benefício descrito no artigo 89 da lei do Juizado Especial – 9.099/95 da suspensão condicional do processo. Já no parágrafo 2-A do mesmo artigo penaliza a ilicitude com reclusão de 04 a 08 anos, afastando a suspensão condicional do processo e ainda nega a oportunidade de Acordo de Não Persecução Penal devido a pena mínima ser exatamente 4 anos, ferindo as condições descritas no artigo 28-A do Código de Processo Penal (Aguiar e Amaral, 2024).

O último e terceiro problema, é de tipificação ou de escrita. A abrangência do texto da lei atrapalha a sua aplicação e omite eventos importantes que validam as alternativas do crime (Aguiar e Amaral, 2024).

Diante das evidências e preocupações sobre o artifício da lei, pode-se notar no enaltecimento sobre o tratamento jurídico em sua totalidade. Outros contudo, enaltece a importância das leis criadas a fim de garantir o máximo de justiça para os usuários de redes digitais e os tratamentos de dados no ordenamento jurídico brasileiro. A autora traz lições que a primeira lei de suma importância relacionado aos crimes virtuais foi a 12.737/2012 com o advento do vazamento de fotos íntimas após o computador da vítima ser levado para a manutenção. A referida lei é conhecida como Lei Carolina Dieckmann (Silva, 2024).

Verifica-se o destaque que a referida lei ocasiona é a inauguração de 3 novos crimes, sendo estes no artigo 154-A, o artigo 266 sofreu uma manutenção e o crime descrito no artigo 298 do Código Penal. Por sua vez, o crime de invasão de dispositivo foi inserido no Código Penal agregando como crime de informática, que formaliza no

ato de afetar o sistema computacional. Esse dispositivo, orienta a autora, que é a representação constitucional tutelar do inciso X no artigo 5 da Constituição Federal de 1988 onde impetra a o direito da inviolabilidade da intimidade das pessoas (Silva, 2024).

Porém, a principal lei que regulamenta o uso da *internet* no Brasil é a 12.965/2014, conhecida com Marco Civil da *Internet*, possui a sua estrutura baseada em 5 capítulos onde possui a sua função principal a garantia da liberdade de expressão, a proteção a privacidade, proteção de dados pessoais entre outros, de acordo com Aguiar e Amaral (2024), e mediante o artigo 3 da lei (Brasil, 2014):

Art. 3º 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;
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.

Diante de tal marco é criado a lei de forma específica para o tratamento da matéria em específico ao tratamento de Dados no Brasil sob o número de 13.709/2018 conhecido como a Lei Geral de Proteção de Dados, Silva (2024). A autora sustenta que a referida lei trás a máxima da abrangência do artigo 3 da lei do Marco Civil da *Internet*, Lei 12.965/2014 e supre as brechas e padroniza o tratamento de dados em empresas, órgãos públicos, imputando penalidades as violabilidades da regra e criando a Agência Nacional de Proteção de Dado (ANPD) cuja função é fiscalizar o cumprimento da lei.

Por outro lado, outros entendimentos traz o foco na dependência central dos meios digitais na concretizado do fato ilícito. No esparramar da *internet* em um mundo contemporâneo, afetando o dia a dia das pessoas mundo a fora, carrega consigo, uma onda de acontecimentos de vazamento de dados nominado como “Epidemia de Vazamento de Dados”, tornando claro que a rede mundial de computadores possui seus pontos fortes, mas também seus pontos fracos. Portanto, pesquisas em órgãos públicos e organismos internacionais de pesquisa comprova com dados a expressão.

No Brasil, o autor revela que no ano de 2022, das empresas pesquisadas 69% delas sofreram algum tipo de vazamento de dados e destas, 65% acredita que o investimento e segurança digital não são o suficiente para assegurar a segurança de dados no país (Marcolini, 2024).

Ainda que não seja indicado afirmar que uma empresa de fato se encontra em total conformidade com a LGPD, o número alto de incidentes é melhor compreendido quando observamos que, em 2023, 64% das empresas não possuíam um nível satisfatório em seu programa de privacidade, portanto justifica-se os números elevados na esfera nacional (Prado, 2022).

O Supremo Tribunal Federal, por ocasião do julgamento da ADI 6649, de relatoria do eminente Ministro Gilmar Mendes, traz considerações significativas sob a temática. Isso porque, é evidente o dever estatal em assegurar a segurança das informações pessoais dos cidadãos e em especial na qualidade segura da transferência de dados entre órgãos do próprio governo (Brasil, 2023).

A propósito:

Ementa: DIREITO CONSTITUCIONAL. DIREITOS FUNDAMENTAIS À PRIVACIDADE E AO LIVRE DESENVOLVIMENTO DA PERSONALIDADE. TRATAMENTO DE DADOS PESSOAIS PELO ESTADO BRASILEIRO. COMPARTILHAMENTO DE DADOS PESSOAIS ENTRE ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL. ADI E ADPF CONHECIDAS E, NO MÉRITO, JULGADAS PARCIALMENTE PROCEDENTES. INTERPRETAÇÃO CONFORME À CONSTITUIÇÃO. DECLARAÇÃO DE INCONSTITUCIONALIDADE COM EFEITOS FUTUROS 1.(...) 3. O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. 4. Interpretação conforme à Constituição para subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público. (ADI 6649, Relator(a): GILMAR MENDES, Tribunal Pleno, julgado em 15-09-2022, PROCESSO ELETRÔNICO DJe-s/n DIVULG 16-06-2023 PUBLIC 19-06-2023). (original sem destaques).

No mesmo sentido, o artigo 6, IV, da Lei Geral de Proteção de Dados, dispõe

sobre o Princípio da Segurança, a qual aborda que medidas tecnológicas e administrativas precisam ser tomadas, veja-se:

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativa aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (Brasil, 2018).

Outro princípio a ser tomado em vista é o Princípio da Prevenção, onde o agente deve promover a qualidade de seus suportes a fim de prevenir as ocorrências praticáveis (Marcolini, 2024). E outro princípio defendido é o da Responsabilização e prestação de contas que estabelece o principal meio de acesso ao responsável por incidentes de vazamentos de dados, reafirmando a necessidade das medidas:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (Brasil, 2018).

A lei promove a verificação de formalidade e conformidade legal, além das implementações de acordo com as suas próprias ponderações, com base em todas as linhas e ciclos de atividade na gestão, uso e tratamento de dados de seus usuários (Marcolini, 2024). Ademais, conforme ensina o autor:

Nesse sentido, a realização das avaliações de conformidade não possui determinações específicas pela LGPD. Contudo, práticas de mercado recomendam que o controlador avalie o tratamento com base nos princípios da LGPD, com destaque para os princípios da finalidade, da adequação e da necessidade, analisando se os direitos dos titulares não são sobrestados pelo tratamento de dados e se a hipótese legal alocada é válida.

Portanto, a vinculação entre as prerrogativas apresentadas das falhas na lei aos casos de vazamento de dados se converge na estrutura vista nos crimes que diariamente são acometidos no Brasil. A brecha da lei, não permite a responsabilização civil e criminalmente de forma rápida e verídica, tornando o erro de conformidade de segurança sem a capacidade de rastreabilidade, com isso, a inoperância da Agência Nacional de Proteção de Dados no quesito de responsabilização civil e criminal nos casos de vazamento de dados é comprovada, fato que os casos ilícitos não são barrados e nem estancados no Brasil.

CONSIDERAÇÕES FINAIS

A Lei nº 13.709/2018 estabelece um marco no ordenamento jurídico Brasileiro no quesito de evolução nas garantias da proteção de dados. Precedidas das demais outras, como a Lei Caroline Dieckmannn – Lei 12.737/2012, a Lei do Marco Civil da *Internet* – Lei 12.965/2014, Constituição Federal do Brasil, Código de Defesa do Consumidor, a LGPD possui uma estrutura capaz de orientar e fiscalizar as ações decorrentes do tratamento e segurança de dados no país e em empresas estrangeiras com atuação dentro do território nacional.

Mas, apesar de toda a estrutura, a lei possui lacunas que permitem a não padronização da segurança de dados dentro das empresas detentoras, comprometendo a segurança de dados e colaborando com a pratica de crimes no Brasil. Foi constatado que são as próprias empresas que possuem a função de estabelecer os parâmetros e critérios de conformidade, muito bem estruturados pelo Órgão Nacional de Proteção de Dados – ANPD, mas com parâmetros próprios e com base no artigo 6 da própria lei. Nisso, favorece para um enfraquecimento dos princípios de segurança tornando factível o vazamento de dados pessoais.

Em todas as pesquisas bibliográficas, foi demonstrado a preocupação jurisprudencial do estado em se autorregular e nas medidas de segurança a serem tomadas pelas empresas e entidades públicas ou privadas. Portanto, a doutrina e a jurisprudência denotam a ineficiência da lei frente aos desafios, garantias e segurança de dados de usuário, apesar de uma lei nova, com fundamentos, enraizados no artigo 5 da Constituição Federal de 1988, artigo 3 da lei do marco civil, falha em sua essência: proteção.

De fato, os criminosos em posse dos dados de pessoas, conseguem através da ardis atividade ilícita corromper o direito a propriedade, instigando por meios sensíveis, usando os dados a fim de cometer o estelionato, ou seja, falando em nome da filha, do banco, do parente, entre outros meios.

Diante da problemática, a pesquisa consultou a doutrina e foi encontrada a resposta clara que a engenharia do crime de estelionato consiste na vulnerabilidade legal em tratar o assunto. A atividade possui o princípio em usar de artifícios, dados, fatos ou a vulnerabilidade para tomar de outrem patrimônio ou riqueza de forma ilícita e imprópria, tornado, claro que o caso de vazamento de dados nutre a máquina criminosa.

O ordenamento jurídico promove uma penalização para quem atua de forma desonesta na obtenção de vantagem ou apropriação indébita de outro, por meio de artifícios digitais, telefônicos ou virtuais. O chamado estelionato virtual ou digital inaugurado no Código Penal Brasileiro no artigo 171 paragrafo 2-A infere sobre uma tentativa de conter os crescentes números de ocorrências no país. Apesar das tentativas do legislador em consolidar uma resposta rápida sobre este tema, fica claro que os números tendem a aumentar a cada dia.

A análise realizada ao longo deste trabalho demonstra que a Lei possui um aparato legal e administrativo a fim de promover uma melhor gestão sobre o tema. Porém, a mesma lei abre brechas para a conformidade da segurança abordada dentro das empresas e repartições públicas, não estabelecendo uma padronização do processo de segurança ou rito de tratamento de dados, simplesmente, existe o caminho da análise de risco a operação comercial de cada controlador e o mesmo estabelece os seus parâmetros, tornando o sistema vulnerável, não preservando a garantia dos direitos do cidadão brasileiro, impossibilitando a validação da responsabilidade civil e criminal em casos de golpes virtuais com uso de dados, pois como não exposto, não há caminho para a rastreabilidade de culpa em vazamentos de dados em sua totalidade ou de forma parcial.

De fato, em um mundo globalizado e voltado para o acesso a informações, o processo de compra e venda não está mais alicerçado no possuir e nem na necessidade, mas sim na experiência vivida. Ser atendido no conforto do seu lar, realizar as transações bancárias com facilidade e rapidez, ter acesso a filmes, música e tv com facilidade e agilidade, o acesso a informação é o princípio da riqueza em um mundo conectado e moderno.

Diante disso, munidos de dados sensíveis, os estelionatários se passam por atendentes de empresas, de bancos, de prestadoras de serviços entre outras formas para atentar contra o patrimônio das pessoas, realizando ligações telefônicas, enviando mensagens, entre outras e que possuem ter propriedade nas confirmações de informações pessoais causando danos ao cidadão.

Portanto, apesar da imperatividade da lei, força de cobrança e condição legal, o desafio que ela possui para a sua eficácia ser notada é a elaboração de parâmetros técnicos e legais ou estabelecer regras e princípios a fim de padronizar e rastrear o vazamento e incoerências de dados, proporcionando sanções legais para o operador irregular, dando assim condições de rastreabilidade da ocorrência.

Conclui-se, ainda, que a necessidade da criação de meios tecnológicos com mecanismos capazes de notificação rápida e necessária às vítimas nos casos de vazamento de seus dados. Além de exigir uma ação imperativa e robusta da Agência Nacional de Proteção de Dados resultando na identificação e na responsabilização das empresas irregulares e fora de conformidade. Outrossim, faz-se necessário uma ação educacional do governo federal em promover uma educação voltada para o controle, uso e armazenamento de dados da população brasileira, com implementação da semana de conscientização da proteção de dados, assim como é do meio ambiente, do trânsito, entre outras, além da difusão de propagandas educativas na rede de rádio e televisão.

Acredita-se, portanto, que as atitudes apresentadas em comum a alteração do texto da LGPD em específico no artigo 6 por um Projeto de Lei – PL, contribuirá para a redução dos casos de golpes virtuais em decorrência de dados vazados.

REFERÊNCIAS BIBLIOGRÁFICAS

- AGUIAR, Daniel; AMARAL, Rodrigo. **Estelionato por meio da fraude eletrônica: um não remédio para um atual fato antigo**. 2024. Disponível em <https://www.conjur.com.br/2024-dez-04/estelionato-por-meio-de-fraude-eletronica-um-nao-remedio-para-um-atual-fato-antigo/>. Acesso em 28 maio 2025.
- ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. **Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital**. Scielo Brasil, 2022. Disponível em: <https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/>. Acesso em: 20 mar. 2025.
- ANHESINI, Victória. **Quando foi inventado o celular?** 2024. Disponível em: <https://www.terra.com.br/byte/quando-foi-inventado-o-celular-descubra,b645c4bdd9bae591626631b318ccf9426c6pwys9.html#>. Acesso em: 29 de março de 2025.
- BENTIVEGNA, Carlos Frederico B. **Liberdade de expressão, honra, imagem e privacidade: os limites entre o lícito e o ilícito**. Barueri: Manole, 2019. *E-book*. p.Capa. ISBN 9788520463321. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788520463321/>. Acesso em: 12 mai. 2025.
- BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte especial 2**. 18. ed. São Paulo: Saraiva Educação, 2023.
- BRASIL. **Associação nacional de proteção de dados (anpd): 4 anos da Lei Geral de Proteção de Dados Pessoais**. 2022. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/4-anos-da-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 8 abr. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 02 junho 2025.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Institui sobre o Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 02 junho 2025.

BRASIL. **Lei nº 12.737/2012, de 30 de novembro de 2012**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 10 jun 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Institui sobre a Marco civil da internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 junho 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Institui sobre a proteção de dados pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 maio 2025.

BRASIL. **Lei nº 13.964/2019, de 24 de dezembro de 2019**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em 10 jun 2025.

BRASIL. **Lei nº 14.155/2021, de 27 de maio de 2021**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em 10 jun 2025.

BRASIL. **Lei nº 9.099/1995, de 26 de setembro de 1995**. 1995. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9099.htm. Acesso em 10 jun 2025.

BRASIL. **Projeto de Lei 53/2018: Senado Federal**. 2018. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acesso em: 08 jun. 2025.

BRASIL. **Quando a LGPD entrou em Vigor?** Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/perguntas-frequentes/perguntas-frequentes/1-lei-geral-de-protecao-de-dados-pessoais-lgpd/1-3-quando-a-lgpd>. Acesso em 20 abril 2025.

BRASIL. Supremo Tribunal Federal. **Direito constitucional. Direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade. Tratamento de dados pessoais pelo estado brasileiro. Compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal. Adi e adpf conhecidas e, no mérito, julgadas parcialmente procedentes. Interpretação conforme à constituição. Declaração de inconstitucionalidade com efeitos futuros**. Julgamento em: 15 set. 2022. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&queryString=lgpd&sort=_score&sortBy=desc. Acesso

em: 03 maio 2025.

CAPEZ, Fernando. **Curso de Direito Penal: parte especial**. Arts.121 a2012-vol 2 – 25ª. ed. São Paulo: Saraiva Educação, 2024.

CASAL JR. Marcello. **Entenda o que muda com a Lei Geral de Proteção de Dados**. 2020.Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-09/entenda-o-que-muda-com-a-lei-geral-de-protecao-de-dados>. Acesso em 04 abril 2025.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva Jur, 2011. E-book. (1 recurso online). ISBN 9788502136663 p.12-16. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788502136663>. Acesso em: 3 abril. 2025.

FEILER, Anneliese Regina; GAZANIGA, Felipe; VIEIRA, Thiago André Marques. **O valor fundamental dos dados pessoais: uma análise comparativa entre a LGPD e GDPR sob a ótica da análise econômica do direito**. *Revista de Direito*, Viçosa, v. 16, n. 02, 2024. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/17158>. Acesso em: 11 jun. 2025.

FLEMING, Maria Cristina. **LGPD: diferenças no tratamento de dados pessoais e sensíveis**. Consultor Jurídico, 06 de março de 2021. Disponível em: <https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis/>. Acesso em: 11 jun. 2025.

GRECO, Rogério. **Código Penal Comentado** - 18ª Edição 2025. 18. ed. Rio de Janeiro: Atlas, 2025. E-book. p.542. ISBN 9786559776887. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786559776887/>. Acesso em: 03 jun. 2025.

GRECO, Rogério. **Curso de Direito Penal: Parte Especial - Vol. III: Dos Crimes Contra o Patrimônio e Contra a Dignidade Sexual**. 21. ed. Niterói, RJ: Impetus, 2024.

GRECO, Rogério. **Curso de Direito Penal: parte especial**. 20. ed. Niterói: Impetus, 2023.

GRINOVER, Ada Pellegrini. **Liberdades públicas e processo penal - as intercetações telefônicas**. São Paulo: Revista dos Tribunais, 2020.

LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet**. São Paulo: Atlas, 2014.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. **Da Evolução das Legislações sobre Proteção de Dados: A Necessidade de Reavaliação do Papel do Consentimento como Garantia**. *Revista de Direito*, v. 1, n. 38, p. 1-19, 2020.

MACHADO, Jónatas E. M. **Liberdade de Expressão e Restrições Legais**. Coimbra: Coimbra Editora, 2002.

MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2019.

MARCOLINI, Bruno Junqueira Meirelles. **Entre riscos e obrigações: a atuação do controlador em incidentes de segurança, 2024**, Revista 2 Prêmio Danilo Doneda De Artigos Científicos Da Anpd. Acessado em <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/concurso-de-monografias-da-anpd-premio-danilo-doneda/premio-danilo-doneda-2a-edicao.pdf>. Acesso em 02 de Junho 2025.

MASSON, Cleber. **Direito Penal Esquematizado: Parte Especial - Arts. 121 a 234 do CP**. 17. ed. Rio de Janeiro: Forense; São Paulo: Método, 2022.

MENDES, Eduardo Souza. **A relação entre a Lei Geral de Proteção de Dados e o Código de Defesa do Consumidor**. 2021. Disponível em: <https://www.jusbrasil.com.br/artigos/a-relacao-entre-a-lei-geral-de-protecao-de-dados-e-o-codigo-de-defesa-do-consumidor/1188236339>. Acesso em: 8 abr. 2025.

MENDES, Eduardo Lopes. **LGPD: o impacto do normativo SARB-025/2021**. São Paulo: Assis & Mendes Sociedade de Advogados, 22 fev. 2022. 3 p. Disponível em: minutodaseguranca.blog.br/wp-content/uploads/2022/03/ASSIS-E-MENDES-LGPD-O-IMPACTO-DO-NORMATIVO-SARB-025-2021-2022.02.22.pdf. Acesso em: 08 jun. 2025.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 15. ed. São Paulo: Saraiva Educação, 2020.

MIRABETE, Júlio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal: Parte Geral**, v. 1. 27. ed. São Paulo: Atlas, 2010.

MIRABETE, Julio Fabbrini. **Manual de Direito Penal**. 23. ed. São Paulo: Atlas, 2005. p. 303, 323

NUCCI, Guilherme de Souza. **Curso de direito penal, v. 2: parte especial: arts. 121 a 212 do Código Penal**. 7. ed. Rio de Janeiro: Forense, 2023.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 16. ed. Rio de Janeiro: Forense, 2020.

RIBEIRO, Leonardo Soares Madeira Iorio. **Constituição e Defesa do Consumidor**. Rio de Janeiro: Lumen Juris, 2023.

SANTOS, Italo Kelson Pereira dos; FREITAS, Gisela Carvalho de. **Vazamento De Dados Pessoais Em Tempos De Informação Instantânea**. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 10, n. 6, p. 488–504, 2024. DOI: 10.51891/rease.v10i6.14400. Disponível em: <https://periodicorease.pro.br/rease/article/view/14400>. Acesso em: 20 março de 2025.

SANTOS, Maykon Adler Oliveira; ARAÚJO, Jeferson Sousa de; REGO, Ighor Jean. **A história Brasileira de proteção aos dados: o advento da lei geral de proteção de dados pessoais e a sua influência no acesso aos dados médicos no Brasil.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 06, Ed. 12, Vol. 01, pp. 172-198. Dezembro de 2021. ISSN: 2448-0959. Disponível em: <https://www.nucleodoconhecimento.com.br/lei/advento-da-lei> Acesso em: 12 marco de 2025.

SILVA, Beatriz Mussalem de Sousa. **Estelionato sob a ótica do dolo específico.** 2022. Universidade Anhembi Morumbi, São José/SC. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/29986>. Acesso em: 3 jun. 2025.

SILVA, José Geraldo da. **Teoria Geral do Crime.** 8. ed. Leme, SP: Mizuno, 2024.

SILVA, Natália dos Santos. **O estelionato virtual e a sua estrutura jurídica.** 2024 Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/4809/1/DISSERTA%C3%87%C3%83O_NAT%C3%81LIA%20DOS%20SANTOS%20SILVA_MESTRADO%20PROFISSIONAL%20EM%20DIREITO%20ECON%C3%94MICO_2023.pdf. Acesso em 28 maio 2025.

SOUZA, Thiago. **História do Telefone.** 2022. Disponível em: <https://www.todamateria.com.br/historia-do-telefone/> Acesso em 29 de marco de 2025.