PONTÍFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
COORDENAÇÃO DO CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA

ARTIGO CIENTÍFICO

ESTELIONATO E VAZAMENTO DE DADOS

A INTERSEÇÃO ENTRE CRIME DIGITAL E PROTEÇÃO DA PRIVACIDADE

ORIENTANDA: NATÁLIA ROCHA ARAÚJO

ORIENTADOR: PROF. MS. ERNESTO MARTIM S. DUNCK

GOIÂNIA-GO

2025

NATÁLIA ROCHA ARAÚJO

ESTELIONATO E VAZAMENTO DE DADOS

A INTERSEÇÃO ENTRE CRIME DIGITAL E PROTEÇÃO DA PRIVACIDADE

Artigo Científico apresentado à disciplina Trabalho de Curso I, da Escola de Direito, Negócios e Comunicação do Curso de Direito da Pontifícia Universidade Católica de Goiás (PUC-GOIÁS).

Prof. Orientador: Ernesto Martim S. Dunck.

GOIÂNIA

2025

NATÁLIA ROCHA ARAÚJO

ESTELIONATO E VAZAMENTO DE DADOS

A INTERSEÇÃO ENTRE CRIME DIGITAL E PROTEÇÃO DA PRIVACIDADE

Data da Defesa: _____ de _____ de 2025

BANCA EXAMINADORA

_____ _____

Orientador: Prof. Ernesto Martim S. Dunck Nota

_____ _____

Examinadora Convidada: Profª. Eufrosina Saraiva Silva Nota

Dedico este trabalho aos meus pais, Alexandry Araújo Cordeiro e Patrícia Augusta Rocha Araújo, e à minha irmã, Gabriela Rocha Araújo, que me incentivaram e foram meus alicerces durante toda a construção deste trabalho.

Agradeço primeiramente aos meus pais, Alexandry Araújo Cordeiro e Patrícia Augusta Rocha Araújo, que sempre me apoiaram e incentivaram durante todos os anos em que estive na faculdade e ao longo de toda a minha vida. Agradeço à minha irmã Gabriela Rocha Araújo, que, mesmo de longe, sempre esteve comigo, auxiliando e guiando-me ao longo deste trabalho. Agradeço ao meu namorado, Victor Fernando Ribeiro, por toda paciência e companheirismo durante todo esse tempo. Ao orientador Ernesto Martim, que me acompanhou neste último ano, oferecendo o auxílio necessário para a elaboração deste trabalho, deixo minha gratidão. Agradeço também à professora convidada, Eufrosina Saraiva, por ter aceitado o convite e por todo o aprendizado proporcionado ao longo do curso.

SUMÁRIO

INTRODUÇÃO.....8

1. O ESTELIONATO DIGITAL E O VAZAMENTO DE DADOS.....11

1.1 CONCEITO.....11

1.2 MÉTODOS MAIS COMUNS DE FRAUDES DIGITAIS.....12

1.3 IMPACTOS DO ESTELIONATO DIGILTAL E O VAZAMENTO DE DADOS.....13

2. PROTEÇÃO DE DADOS E CRIMES DIGITAIS NO CONTEXTO LEGAL.....14

2.1 A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL.....14

2.2 RESPONSABILIDADES DAS EMPRESAS NA PROTEÇÃO DE DADOS PESSOAIS.....15

2.3 MEDIDAS PUNITIVAS E PREVENÇÃO DE CRIMES DIGITAIS.....16

3. DESAFIOS E PERSPECTIVAS NA PROTEÇÃO DA PRIVACIDADE E COMBATE AO CRIME DIGITAL.....17

3.1 NOVAS AMEAÇAS NO AMBIENTE DIGITAL.....17

3.2 O PAPEL DAS TECNOLOGIAS EMERGENTES NA PROTEÇÃO DE DADOS....18

3.3 O PAPEL DAS EMPRESAS E ESTADO NA PREVENÇÃO DE FRAUDES DIGITAIS.....19

3.4 PERSPECTIVAS FUTURAS PARA A PRIVACIDADE E SEGURANÇA DIGITAL.....21

CONCLUSÃO.....22

REFERÊNCIAS.....25

ESTELIONATO E VAZAMENTO DE DADOS:

A INTERSEÇÃO ENTRE CRIME DIGITAL E PROTEÇÃO DA PRIVACIDADE

Natália Rocha Araújo[1]

RESUMO

O artigo aborda o estelionato digital e o vazamento de dados como desafios crescentes na era tecnológica. O estelionato digital refere-se à obtenção de vantagens ilícitas por meio de fraudes virtuais, sendo regulamentado pelo artigo 171 do Código Penal, com penas agravadas pela Lei nº 14.155/2021. Já o vazamento de dados ocorre quando informações pessoais são acessadas ou divulgadas sem autorização, o que pode viabilizar crimes cibernéticos. A relação entre ambos é estreita, pois dados obtidos ilegalmente alimentam golpes financeiros e fraudes online. Dentre os principais métodos de fraude digital destacam-se o *phishing, spoofing, ransomware* e engenharia social, todos explorando falhas tecnológicas e comportamentais. O impacto desses crimes é significativo tanto para indivíduos, que sofrem prejuízos financeiros e psicológicos, quanto para empresas, que podem enfrentar sanções legais e danos à reputação. A Lei Geral de Proteção de Dados (LGPD) estabelece normas para garantir a privacidade dos usuários e impõe responsabilidades às empresas no tratamento de dados pessoais. O artigo também discute os desafios na segurança digital, destacando a necessidade de medidas preventivas como o uso de blockchain, autenticação multifatorial e inteligência artificial. Além disso, enfatiza o papel do Estado e das empresas na mitigação dos riscos, através da regulação eficiente, fiscalização e adoção de boas práticas. Por fim, o estudo aponta perspectivas futuras, considerando a evolução tecnológica e a necessidade de adaptação constante das leis e estratégias de proteção. A colaboração entre governos, setor privado e sociedade é essencial para garantir um ambiente digital mais seguro e confiável.

[1] Acadêmico do curso de Direito da Pontifícia Universidade Católica de Goiás, e-mail: nataliaaraujo3535@gmail.com

ABSTRACT

This article addresses digital fraud and data leaks as growing challenges in the technological era. Digital fraud refers to obtaining illicit advantages through virtual fraud, and is regulated by article 171 of the Penal Code, with penalties increased by Law No. 14,155/2021. Data leaks occur when personal information is accessed or disclosed without authorization, which can enable cybercrimes. The relationship between the two is close, as illegally obtained data fuels financial scams and online fraud. Among the main methods of digital fraud are phishing, spoofing, ransomware, and social engineering, all of which exploit technological and behavioral flaws. The impact of these crimes is significant both for individuals, who suffer financial and psychological losses, and for companies, which may face legal assessments and damage to trust. The General Data Protection Law (LGPD) establishes rules to guarantee user privacy and imposes responsibilities on companies in the processing of personal data. The article also discusses the challenges in digital security, highlighting the need for preventive measures such as the use of blockchain, multifactor authentication and artificial intelligence. In addition, we emphasize the role of the State and companies in mitigating risks, through efficient regulation, monitoring and adoption of good practices. Finally, the study points out future perspectives, considering technological evolution and the need for constant adaptation of laws and protection strategies. Collaboration between governments, the private sector and society is essential to ensure a safer and more reliable digital environment.

INTRODUÇÃO

O desenvolvimento tecnológico das últimas décadas remodelou profundamente as formas de interação social, econômica e profissional, consolidando o ambiente digital como espaço essencial da vida contemporânea. No entanto, essa crescente digitalização também intensificou as ameaças cibernéticas, entre as quais se destaca o estelionato digital, crime caracterizado pelo uso fraudulento de tecnologias para obtenção de vantagem ilícita.

Conforme dito acima, esse fenômeno se soma o vazamento de dados pessoais, evento cada vez mais recorrente que amplia os riscos à privacidade e à integridade dos indivíduos no ciberespaço.

Ambos os problemas, embora distintos em natureza, se entrelaçam em uma lógica comum: o uso indevido de informações sensíveis como instrumento para a prática de fraudes. A divulgação ou apropriação indevida de dados pessoais, muitas vezes oriunda de falhas nos sistemas de segurança de empresas ou da negligência dos próprios usuários, abre caminho para práticas criminosas sofisticadas que geram impactos devastadores.

As consequências não se limitam ao campo financeiro, onde prejuízos materiais podem comprometer a estabilidade das vítimas, mas também alcançam a dimensão psicológica, afetando o bem-estar emocional, a confiança nas relações digitais e o exercício da cidadania.

Diante desse cenário, surgem novos desafios não apenas para os cidadãos e as empresas, mas também para o Estado e os operadores do Direito. As dificuldades enfrentadas pelas autoridades na identificação e responsabilização dos infratores revelam-se especialmente complexas diante da natureza transnacional dos crimes digitais, da utilização de técnicas avançadas de anonimização e da limitada cooperação internacional.

Ao mesmo tempo, persistem entraves internos como a morosidade processual, a escassez de recursos técnicos e a baixa capacitação especializada nas instituições responsáveis pela investigação e repressão dessas condutas.

A esse quadro se somam fragilidades significativas no setor privado. Embora legislações como a Lei Geral de Proteção de Dados (LGPD) imponham

deveres explícitos de governança e segurança da informação, muitas empresas ainda falham em implementar práticas eficazes de proteção.

Ausência de auditorias, sistemas obsoletos, treinamento insuficiente de colaboradores e a falta de políticas de segurança estruturadas são apenas algumas das deficiências que expõem dados pessoais a vazamentos, cenário que compromete não apenas os direitos dos titulares, mas também a reputação e a sustentabilidade das organizações.

Para investigar essas questões, este trabalho adota o método dedutivo, ancorando-se em pesquisa bibliográfica e documental.

A análise parte do ordenamento jurídico vigente, especialmente da LGPD, do Código Penal Brasileiro e de normativas internacionais como o Regulamento Geral sobre a Proteção de Dados (RGPD), explorando a aplicação dessas normas a partir de casos concretos, artigos acadêmicos, jurisprudências e relatórios técnicos. A escolha metodológica permite compreender, a partir das normas gerais, os efeitos práticos e os desafios específicos que envolvem o enfrentamento do estelionato digital e a proteção de dados pessoais no Brasil.

O trabalho está estruturado em três seções. A primeira seção dedica-se à compreensão conceitual do estelionato digital e do vazamento de dados, apresentando os métodos mais recorrentes de fraudes digitais, como phishing, spoofing, ransomware e engenharia social e os impactos concretos dessas práticas na vida das vítimas e das organizações. A abordagem considera os efeitos financeiros, legais e psicológicos gerados pela violação da privacidade, destacando a vulnerabilidade crescente diante da exposição digital.

A segunda seção enfoca o contexto jurídico da proteção de dados, com atenção especial à LGPD. São discutidas as obrigações legais impostas às empresas, as medidas punitivas previstas em caso de descumprimento e a importância da conformidade como mecanismo de prevenção. A seção também destaca o papel das empresas na construção de uma cultura de segurança da informação, abordando a figura do encarregado de dados (DPO) e as estratégias corporativas de governança de dados.

Por fim, a terceira seção analisa os desafios e as perspectivas no combate ao crime digital, observando a evolução das ameaças, a importância das tecnologias

emergentes, como blockchain, inteligência artificial e autenticação multifatorial, e o papel colaborativo do Estado e do setor privado na proteção da privacidade digital.

A seção propõe ainda uma reflexão sobre os rumos futuros da segurança da informação, enfatizando a necessidade de políticas públicas eficazes, investimentos em tecnologia e educação digital como pilares de um ecossistema cibernético mais seguro e confiável.

Assim, este estudo busca não apenas descrever o fenômeno do estelionato digital vinculado ao vazamento de dados, mas também problematizar suas implicações jurídicas e sociais, refletindo sobre os limites e possibilidades do ordenamento jurídico brasileiro frente à complexidade das relações digitais contemporâneas.

1. O ESTELIONATO DIGITAL E O VAZAMENTO DE DADOS

1.1 Conceito

O estelionato digital pode ser definido como a obtenção de vantagem ilícita por meio de fraude em ambientes virtuais, aproveitando da vulnerabilidade das vítimas e das tecnologias utilizadas. Essa prática é regulada no Brasil pelo artigo 171 do Código Penal, que recebeu alterações significativas por meio da Lei nº 14.155/2021.

Esta legislação aumentou as penas para crimes de fraude cometidos utilizando dispositivos eletrônicos ou meios digitais, mostrando a seriedade crescente do problema no cenário tecnológico atual hegemonia da prática crescente na era digital. De acordo com o Código Penal, as punições podem oscilar entre quatro a oito anos de prisão, acompanhadas de multas, conforme a seriedade da transgressão cometida assim como seus reflexos econômicos e sociais.

Por outro lado, o vazamento de dados ocorre quando informações pessoais são divulgadas, acessadas ou utilizadas sem autorização, geralmente devido a falhas em sistemas de segurança, negligência ou ataques cibernéticos planejados. Esses dados englobam informações sensíveis como números de documentos, endereços, registros financeiros e históricos médicos que podem ser explorados para atividades fraudulentas, incluindo o crime cibernético.

De acordo com a Lei Geral de Proteção de Dados (LGPD), as empresas tem o dever de garantir a segurança dessas informações e podem sofrer penalidades administrativas e legais se não cumprirem com essa exigência.

A relação entre o estelionato digital e o vazamento de dados é indissociável. Conforme o artigo “Golpes e venda ilegal de dados no mundo virtual: desafios da segurança cibernética no Brasil” de Danilo e Priscilla, os dados adquiridos de forma ilegal ou por descuido se tornam um recurso essencial na realização de golpes virtuais.

Essas informações podem ser comercializadas em plataformas clandestinas como a Deep web ou usadas diretamente por criminosos para atividades como criar falsas contas bancárias e obter empréstimos fraudulentos e efetuar compras ilegais. A crescente adoção de plataformas digitais para transações

financeiras e interações diárias aumentou consideravelmente essas ameaças, colocando tanto pessoas quanto organizações em risco de sofrer perdas significativas.

Além disso, o problema do golpe virtual é exacerbado pela falta de conscientização sobre segurança cibernética não apenas entre usuários comuns, mas também nas empresas em geral.

Muitos indivíduos ainda utilizam senhas fracas, não verificam se mensagens suspeitas são legítimas, além de compartilharem informações pessoais sem considerarem as possíveis consequências. Da mesma forma, as empresas frequentemente deixam de adotar medidas essenciais de proteção, como a criptografia de dados e autenticação multifatorial. Isso cria um cenário propício para que criminosos explorem vulnerabilidades tanto tecnológicas quanto comportamentais.

1.2 Métodos mais comuns de fraudes digitais

A prática do golpe digital envolve vários métodos diferentes que exploram diversas vulnerabilidades tecnológicas e humanas. Dentre os mais usuais estão os seguintes:

a) *Phishing*. Consiste no envio de mensagens falsas, principalmente por e-mail ou aplicativos de mensagens que imitam comunicações legítimas de instituições financeiras ou empresas governamentais e levam as vítimas a fornecer informações confidenciais, como senhas bancárias ou números de cartão de crédito.

b) *Spoofing*. é quando alguém falsifica identidades online para enganar as pessoas, como criar páginas falsas que parecem ser legítimas. Isso também pode envolver mexer com números de telefone ou endereços de e-mail para esconder de onde vêm as mensagens enganosas.

Ransomware, embora seja comumente conhecido como um tipo específico de ciberataque, o *ransomware* também pode ser utilizado para enganar digitalmente as pessoas ao sequestrar informações pessoa ou corporativas importantes em troca de dinheiro para liberá-las novamente.

Engenharia Social: Ela se baseia na manipulação psicológica das vítimas para obter acesso a dados confidenciais. Por exemplo, criminosos podem fingir ser

representantes credíveis para convencer as pessoas a compartilhar informações pessoais sensíveis. Essas táticas muitas vezes exploram dados previamente vazados para aumentar sua eficiência. Uma situação ilustrativa é quando dados pessoais vazados são empregados para adaptar golpes de *phishing* de maneira mais persuasiva e convincente.

1.3 Impactos do estelionato digital e o vazamento de dados

Os efeitos do golpe digital e da violação dos dados são vastos e atingem tanto pessoas quanto organizações no geral, impactados profundamente por essas situações adversas econômicas causadas por fraudadores online que agem sem autorização realizando saques financeiros fraudulentos e adquirindo produtos ilegalmente em nome das vítimas resultando em despesas indevidas.

Além do exposto anteriormente, a recuperação da perda monetária pode ser um processo extenso e angustiante, que requer uma série de procedimentos burocráticos junto às instituições financeiras e entidades governamentais para contestar as transações fraudulentas realizadas.

Do ponto de vista psicológico, os efeitos englobam ansiedade, estresse e diminuição da confiança nas interações online. As vítimas descrevem a sensação de violação da sua privacidade e de vulnerabilidade a futuros ataques, o que pode resultar em exclusão digital e dificuldades na adaptação às exigências da sociedade tecnológica.

As empresas, por sua vez, enfrentam consequências negativas em sua reputação e finanças quando ocorrem violações de dados. Para além das penalidades estabelecidas na LGPD, companhias que não protegem adequadamente as informações de seus clientes sofrem com a perda de confiança de seu público-alvo, o que pode levar a uma diminuição nas receitas dificultando sua competitividade no mercado.

Exemplos recentemente divulgados de grandes empresas que experimentaram brechas na segurança de dados, evidenciam como tais incidentes podem ter impactos prejudiciais sobre a imagem os resultados financeiros das entidades organizacionais.

A repercussão conjunta também não pode ser desconsiderada. Vazamentos massivos de dados comprometem a segurança de sistemas financeiros e de infraestruturas críticas, acarretando em aumento dos custos relacionados à cibersegurança e à redução de danos. Além disso, eles sobrecarregam o sistema judiciário, com o aumento das demandas legais envolvendo fraudes digitais e proteção de informações pessoais.

Enfrentando essas dificuldades é fundamental adotar uma abordagem abrangente que una medidas legais, técnicas educativas para reduzir os perigos relacionados à fraude online vazamento de informações. A legislação, inquestionavelmente vital, necessita ser fortalecida por investimentos em tecnologia de segurança, tal como sistemas de inteligência artificial para identificação de golpes juntamente com programas informativos que incentivem uma mentalidade de segurança digital entre usuários organizações.

2. PROTEÇÃO DE DADOS E CRIMES DIGITAIS NO CONTEXTO LEGAL

2.1 A Lei Geral de Proteção de Dados no Brasil

De acordo com a LGPD (Lei Geral de Proteção de Dados), “proteger dados pessoais tem como base o respeito à privacidade e à liberdade de expressão e informação” (BRASIL 2018).

As responsabilidades impostas pela LGPD aos controladores e processadores de dados são severas e incluem sanções para aqueles que violarem suas regras estabelecidas. Garantir a segurança dos dados pessoais é cada vez mais crucial em um contexto de crescente digitalização da sociedade. Com base no artigo “Proteção de Dados: Desafios Jurídicos e Tecnológicos na LGPD”, que teve sua curadoria por Marcelo Tadeu, a legislação sobre proteção de dados precisa evoluir em paralelo com as novas tecnologias para enfrentar os desafios emergentes de forma eficiente.

O respeito à privacidade é um direito essencial garantido pela Constituição Federal de 1988 no artigo 5º X que assegura a inviolabilidade da vida íntima e privada

das pessoas. Esta salvaguarda foi fortalecida com a implementação da LGPD que estabelece normas claras sobre a utilização dos dados pessoais.

Além disso, a Lei Geral de Proteção de Dados (LGPD) garante direitos específicos aos indivíduos em relação aos seus dados pessoais, como por exemplo o direito de acessar corrigir apagar ou transferir as informações. Essas prerrogativas fortalecem a autonomia dos cidadãos em relação às suas informações pessoais demandando das empresas uma atitude mais transparente e responsável.

A Lei Geral de Proteção de Dados (LGPD) marca um progresso notável na legislação do Brasil, no entanto seu sucesso está diretamente relacionado à conscientização dos indivíduos sobre seus dados pessoais e à aderência estrita por parte das organizações envolvidas. A atuação da Autoridade Nacional de Proteção de Dados (ANPD) será fundamental para assegurar a correta implementação e fiscalização das normas estabelecidas.

2.2 Responsabilidades das empresas na proteção de dados pessoais

É crucial para as empresas cumprirem com suas responsabilidades de proteger informações pessoais de acordo com a Lei Geral de Proteção de Dados (LGPD). As empresas que coletam dados pessoais devem implementar medidas técnicas e administrativas para assegurar a proteção dessas informações.

Conforme estabelecido no artigo 6º da LGPD, “as práticas de processamento de dados pessoais devem respeitar princípios fundamentais, como transparência na finalidade do tratamento dos dados, adequação às necessidades específicas do processamento, segurança na manipulação das informações, prevenção contra possíveis riscos, discriminação como prática proibida, responsabilidade compartilhada entre os envolvidos e prestação de contas” (BRASIL, 2018).

As empresas precisam seguir essas diretrizes com um planejamento estratégico que priorize a segurança dos dados, o que implica estabelecer políticas de privacidade robustas, conduzir auditorias periódicas e treinar seus colaboradores adequadamente.

As punições previstas na LGPD podem incluir advertências verbais ou escritas, multas financeiras consideráveis ou até mesmo a paralisação temporária ou permanente das atividades de uma organização. Essas medidas punitivas evidenciam a seriedade da legislação vigente, destacando a importância da conformidade. É fundamental encarar a conformidade com a LGPD não apenas como uma obrigação legal, mas também como um diferencial competitivo, uma vez que os consumidores estão cada vez mais preocupados com a segurança de seus dados pessoais.

Preocupar-se com a segurança dos dados também implica em contar com profissionais especializados, como os Encarregados de Proteção de Dados *(Data Protection Officers - DPOs)*. Esses especialistas tem o papel de supervisionar se as empresas estão em conformidade com as leis e oferecer orientações sobre melhores práticas empresariais.

Portanto, é a empresa quem tem uma grande responsabilidade na proteção dos dados que é multifacetada; exige um compromisso constante com a segurança e a transparência. Adotar medidas proativas não só garantirá os direitos dos titulares dos dados, como também solidificará a reputação e a credibilidade das empresas perante o mercado e a sociedade.

2.3 Medidas punitivas e prevenção de crimes digitais

As empresas têm um papel crucial na proteção dos dados pessoais de acordo com a LGPD. Para garantir a segurança das informações que coletam, armazenam e processam, é necessário que adotem medidas técnicas e administrativas adequadas. De acordo com o artigo 6º da LGPD, é fundamental que as atividades relacionadas ao tratamento de dados pessoais sejam realizadas de forma ética, seguindo os princípios da finalidade, adequação, necessidade, segurança, prevenção de discriminação, além da responsabilização e prestação de contas.

As empresas precisam seguir essas diretrizes com um planeamento estratégico que priorize a segurança dos dados empresariais. Isso envolve estabelecer políticas de privacidade claras, realizar auditorias frequentemente e capacitar os colaboradores adequadamente. Sob a perspectiva do artigo “Guia Prático

de Governança Corporativa e Proteção de Dados”, redigido por Lucas Mura do site Negócios Globais, é crucial adotar boas práticas de governança corporativa focadas na proteção de dados para reduzir riscos e evitar penalidades legais.

As consequências previstas pela LGPD englobam avisos prévios, finança e inclusive a suspensão parcial ou total das atividades de uma empresa. Estas punições evidenciam a seriedade da legislação e para saber mais sobre isso Braga mostra, "A conformidade com a LGPD deve ser encarada como um diferencial competitivo e também como uma obrigação legal, já que os consumidores estão cada vez mais preocupados com a segurança de seus dados".

Preocupar-se com a segurança dos dados também envolve ter especialistas qualificados envolvidos no processo, como os Encarregados de Proteção de Dados *(Data Protection Officers - DPOs)*. Esses profissionais tem o papel de supervisionar se as empresas estão em conformidade com as leis e oferecer orientações sobre boas práticas empresariais relacionadas ao assunto.

Tal como expresso por José Eduardo Melo no artigo “Encarregado de Dados (DPO): importância e obrigatoriedade da LGPD”, designar um DPO capacitado é uma das principais formas de assegurar que uma empresa siga corretamente as diretrizes da LGPD e se proteja contra possíveis vulnerabilidades.

Assim sendo a responsabilidade das empresas na salvaguarda dos dados é diversificada e requer um compromisso constante com a segurança e a transparência. A implementação de ações preventivas não apenas resguarda os direitos dos detentores dos dados como também solidifica a reputação e a credibilidade das empresas frente ao mercado e à sociedade.

3. DESAFIOS E PERSPECTIVAS NA PROTEÇÃO DA PRIVACIDADE E COMBATE AO CRIME DIGITAL

3.1 Novas ameaças no ambiente digital

Os avanços nas tecnologias da informação trouxeram novos desafios para a privacidade e a segurança digital na sociedade contemporânea. Com a evolução da

inteligência artificial, a expansão da Internet das Coisas (IoT) e o uso crescente do *big data*, os riscos relacionados à segurança cibernética se tornaram mais complexas e frequentes.

Conforme descrito por Marcos Alves dos Santos Júnior, na obra “Crimes cibernéticos: ameaças virtuais e práticas de prevenção”, o ambiente virtual passou a representar um espaço propício para a prática de crimes digitais, exigindo a implementação de medidas preventivas por parte dos legisladores, autoridades reguladoras e operadores do sistema de justiça para garantir a proteção dos dados e a segurança dos usuários.

Além do aumento no número de ataques cibernéticos, ocorreu um aprimoramento nas estratégias utilizadas pelos criminosos digitais. O phishing, ransomware e os ataques que se aproveitam da engenharia social ainda são ameaças significativas, agora ampliadas com novas técnicas baseadas em inteligência artificial.

Uma questão adicional de preocupação está relacionada à fragilidade dos dados confidenciais armazenados por grandes empresas e órgãos públicos. Possíveis falhas na segurança das informações podem acarretar consequências extremamente sérias, indo desde danos financeiros até ameaças à segurança nacional. Um exemplo notável, foi o vazamento de informações de milhões de cidadãos brasileiros em ataques aos sistemas governamentais, que expõe vulnerabilidades estruturais na proteção cibernética do país.

Neste contexto específico mencionado por especialistas é ressaltada a importância de manter em dia as políticas de segurança digital de forma consistente ao longo do tempo para evitar consequências prejudiciais significativas. A adoção de medidas para identificar precocemente possíveis problemas e agir prontamente pode reduzir os danos causados.

Portanto, é crucial entender as novas ameaças presentas no ambiente digital para fortalecer um sistema legal sólido e eficiente. A segurança de dados precisa acompanhar o ritmo das novidades tecnológicas para assegurar privacidade e proteção das informações em um contexto de mudanças constantemente ocorrendo.

3.2 O papel das tecnologias emergentes na proteção de dados

As novas tecnologias tem um papel crucial na proteção dos dados pessoais contra crimes digitais, métodos como a cripto segurança avançada, a blockchain e a inteligência artificial são comumente empregados para manter as informações em segurança impedindo acessos não autorizados.

A utilização da tecnologia blockchain tem se revelado eficiente na proteção de informações pessoais devido à sua estrutura descentralizada e imutável. Esse sistema evita alterações não autorizadas nos dados armazenados, garantindo assim maior confiança nas informações contidas.

Conforme o pensamento desenvolvido pela revista da PUCRS, “Blockchain: A Revolução na Segurança de Dados para sua Empresa”, o uso do blockchain representa um avanço importante na segurança digital, pois dificulta fraudes e ataques virtuais ao estabelecer um sistema distribuído de registros que podem ser auditados.

Autenticação em duas etapas (2FA), também é amplamente utilizada para diminuir os riscos relacionados ao acesso não autorizado em sistemas e plataformas online. Ao requerer diferentes métodos para verificar identidades dos usuários simultaneamente tornam complexas as tentativas de os criminosos cibernéticos agirem com sucesso.

Por último, mas não menos importante, o campo da segurança na internet baseada em inteligência artificial tem vindo à tona na luta contra as ameaças digitais. Os sistemas automatizados conseguem detectar anomalias em tempo real e prevenir atividades maliciosas antes que provoque danos significativos.

Assim sendo, a utilização de tecnologias em ascensão é fundamental para reforçar a segurança dos dados e reduzir os perigos relacionados aos delitos cibernéticos. No entanto, é imprescindível que a integração dessas soluções seja acompanhada por diretrizes transparentes e normas adequadas para assegurar sua utilização de maneira ética e produtiva.

3.3 O papel das empresas e do Estado na prevenção de fraudes digitais

É crucial que empresas trabalhem em conjunto com o governo para prevenir e combater fraudes digitais com eficiência crescente diante da sofisticação

dos crimes cibernéticos atuais, estratégias integradas são essenciais para a redução das vulnerabilidades e o fortalecimento da proteção dos dados conforme destacado por Menezes tendo como base o artigo “A Transformação Digital do Setor Público no Contexto das Plataformas Digitais”, a troca de informações entre setor privado e público é essencial para superar os obstáculos do ambiente digital e promover inovação na gestão pública.

É crucial para o Estado estabelecer regulamentos que visem proteger os dados pessoais e garantir segurança cibernética efetiva ao monitorar o cumprimento das leis pertinentes nesta área.

Leis como a Lei Geral de Proteção de Dados (LGPD) e o marco civil da Internet tem como objetivo prevenir violações e salvaguardar direitos básicos dos cidadãos brasileiros. Contudo, é essencial que entidades como a Autoridade Nacional de Proteção de Dados (ANPD) atuem de maneira eficiente para garantir a implementação bem-sucedida dessas regulações.

Conforme a tese defendida “Gestão de Riscos e Fraudes em Ambientes Digitais”, publicado pela NoBug, é fundamental estabelecer regulamentações robustas para assegurar confiança no cenário digital e resguardar os cidadãos contra práticas fraudulentas.

Por outro lado, as organizações devem constantemente investir em recursos de segurança da informação, como autenticação multifatorial, criptografia de dados, dados cifrados e verificações regulares. Além disso, medidas relacionadas à governança corporativa e governança empresarial, as empresas devem ocorrer ao lado de treinamentos internos para evitar situações-problema relacionadas com vazamentos de informações sensíveis.

Além de tomar medidas preventivas contra fraudes cibernéticas, é importante estabelecer parcerias entre empresas privadas e o governo, para compartilhar informações sobre ameaças digitais, como uma forma eficiente de combate à fraude online. A colaboração internacional também desempenha um papel crucial já que muitos ataques virtuais tem origem em países estrangeiros, o que tornam difícil sua repressão efetiva.

Portanto, a prevenção de fraudes digitais exige um esforço conjunto e contínuo entre empresas e Estado. O fortalecimento da legislação, a adoção de novas

tecnologias de segurança e a conscientização da população são aspectos essenciais para mitigar riscos e garantir um ambiente digital mais seguro para todos.

3.4 Perspectivas futuras para a privacidade e segurança digital

A maneira como a privacidade e a segurança digital serão influenciadas no futuro, é resultado dos avanços tecnológicos e da adaptação das leis às novas realidades do mundo virtual em constante mudança. Com a sociedade se tornando cada vez mais digitalizada, a quantidade de dados que são armazenados e processados está prevista para aumentar significativamente, portanto é crucial implementar medidas de proteção ainda mais rigorosas.

Nos próximos anos, uma das tendências principais será a ampliação do uso da inteligência artificial na detecção de ameaças virtuais e no reforço da segurança online. Através de algoritmos sofisticados, é possível reconhecer padrões suspeitos antecipadamente para prevenir possíveis ataques, diminuindo a necessidade de intervenção humana.

Além disso, é provável que novas leis sejam criadas para lidar com questões em evolução como a segurança dos dados na nuvem e a proteção dos dispositivos conectados à Internet (IoT). O estabelecimento de diretrizes globais mais rigorosas para a segurança digital pode também impactar as políticas locais no Brasil, resultando em ajustes regulares nos padrões existentes.

Outro ponto importante, é o aumento da preocupação com privacidade digital por parte dos cidadãos, que estão cada vez mais sensíveis em relação à utilização de seus dados pelas empresas, exigindo maior transparência na maneira como suas informações são obtidas e utilizadas. Esse cenário pode resultar em uma maior valorização das empresas, que adotam políticas rigorosas sobre privacidade e práticas éticas no manuseio dos dados.

No final das contas, vai depender da capacidade de adaptação dos governos, a igualdade digital será vital para garantir um ambiente online confiável.

CONCLUSÃO

A pesquisa atual teve como objetivo examinar a estreita ligação entre o crime cibernético de fraude e a divulgação de informações pessoais sensíveis, destacando como isso afeta a privacidade das pessoas e os desafios que enfrentamos nas esferas jurídica e tecnológica da sociedade moderna.

Durante o decorrer da investigação, pode-se notar que o ambiente digital tem permitido o surgimento de novos tipos de atividades criminosas, nos quais as informações pessoais expostas tornam-se um recurso valioso para a execução de golpes elaborados. Portanto o golpe digital não deve ser visto sozinho, é parte de uma série de acontecimentos que começa com o acesso indevido a dados sigilosos culminando em danos financeiros ou emocionais para as vítimas.

Na primeira seção, foram examinadas as ideias fundamentais do golpe digital e da violação de dados e os métodos comuns usados pelos fraudadores como *phishing* e engenharia social foram discutidos em detalhes.

Foi destacado que as consequências financeiras dessas práticas podem ser devastadoras e algumas vezes irreparáveis para as vítimas necessitando delas não somente tempo e recursos para restabelecerem sua estabilidade, mas também enfrentar um turbilhão emocional caracterizado por angústia medos e sensação de impotência.

Violar a privacidade não afeta apenas o bem-estar financeiro das pessoas, também mina a confiança dos indivíduos no uso de tecnologias digitais e pode levá-los a se distanciar de ferramentas que são cada vez mais essenciais para o dia a dia.

Na parte seguinte do texto falamos sobre as regras de proteção de dados no Brasil, destacando especialmente os requisitos da LGPD para as empresas lidarem com informações pessoais com segurança adequada.

Apesar de ser um avanço importante em termos legais, ainda há vários desafios para garantir sua efetiva implementação. Neste momento é evidente a

complexidade enfrentada pelas autoridades para identificar os responsáveis por atividades criminosas online.

Muitas vezes os criminosos utilizam métodos avançados de tecnologia para esconder suas identidades como servidores internacionais e redes cripto-anônimas. A falta de cooperação internacional efetiva e a morosidade nas investigações enfraquecem a resposta das autoridades e contribuem para a impunidade dos infratores.

Além disso foi observado que muitas violações de dados acontecem devido a falhas internas nas políticas de segurança implementadas pelas empresas. A falta de auditorias regulares, a utilização de sistemas desatualizados, a insuficiência de treinamento para os funcionários e a negligência na implementação de medidas de proteção como a autenticação multifatorial contribuem para o aumento da vulnerabilidade no ambiente online.

A mentalidade corporativa frequentemente subestima a importância da segurança da informação como uma prioridade estratégica, tratando-a apenas como um custeio operacional, o que revela uma falha significativa na gestão empresarial.

Na última parte do estudo foram explorados os desafios atuais frente às novas ameaças digitais e a relevância da utilização de tecnologias emergentes como blockchain e inteligência artificial na prevenção de fraudes. Também foi debatido o papel essencial que deve ser desempenhado em conjunto pelo governo, setor privado e sociedade civil. É crucial a colaboração entre esses atores para fortalecer a segurança jurídica, incentivar a alfabetização digital e estabelecer políticas públicas de proteção de dados mais eficientes.

Resumindo de forma simples e direta: os crimes cibernéticos ligados à divulgação de dados pessoais exigem um enfoque amplo e coordenado que inclua melhorias constantes nas leis existentes e investimentos em tecnologia junto com conscientização social.

A proteção da privacidade como um direito básico deve ser assegurada de maneira eficaz e isso só será alcançado com a participação comprometida e unida de todos os envolvidos no assunto. O futuro da segurança digital vai depender

principalmente da capacidade coletiva de equilibrar avanços tecnológicos com responsabilidade ética na utilização de dados pessoais.

REFERÊNCIAS

BRASIL. *Código Penal. Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 28 ago. 2024.

BRASIL. *Lei Geral de Proteção de Dados Pessoais (LGPD). Lei nº 13.709, de 14 de agosto de 2018.* Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1 set. 2024.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Diário Oficial da União: Brasília, DF, 15 ago. 2018.

COMPUWORKS. *Impacto da IA na cibersegurança: oportunidade ou ameaça?* Disponível em: CompuWorks. Acesso em: 12 maio 2025.

CONTÁBEIS. *Encarregado de Dados (DPO): importância e obrigatoriedade da LGPD.* Disponível em: Contábeis. Acesso em: 12 maio 2025.

DALLA VECCHIA, Igor. *A Transformação Digital do Setor Público no Contexto das Plataformas Digitais.* IPPUR-UFRJ, 2023. Disponível em: IPPUR-UFRJ. Acesso em: 12 maio 2025.

ECO, Humberto. *Como se faz uma tese.* 23. ed. Tradução de Gilson Cesar Cardoso de Souza. São Paulo: Perspectiva, 2010.

JUS. *Estelionato virtual: desafios para investigar e punir, 2023.* Disponível em: https://jus.com.br/artigos/108885/estelionato-virtual-os-desafios-enfrentados-pelo-estado-brasileiro-na-investigacao-e-punicao. Acesso em: 27 set. 2024.

JUSBRASIL. *Direitos Humanos na Era Digital: Desafios e Perspectivas para a Proteção dos Indivíduos.* Disponível em: Jusbrasil. Acesso em: 12 maio 2025.

LAKATOS, Eva Maria; *MARCONI, Marina de Andrade. Fundamentos de metodologia científica.* 5. ed. São Paulo: Atlas, 2003.

LEGALE EDUCACIONAL. *Proteção de Dados: Desafios Jurídicos e Tecnológicos na LGPD.* Disponível em: Legale Educacional. Acesso em: 12 maio 2025.

MARTINS, Antônio Eduardo Senna. *O Direito à Privacidade na Era Digital: Desafios e Implicações Jurídicas.* Jusbrasil, 2023. Disponível em: Jusbrasil. Acesso em: 12 maio 2025.

MEZZAROBA, Orides; MONTEIRO, Claudia Servilha. *Manual de metodologia de pesquisa no direito*. 5. ed. São Paulo: Saraiva, 2009.

NEGÓCIOS GLOBAIS. *Guia Prático de Governança Corporativa e Proteção de Dados.* Disponível em: Negócios Globais. Acesso em: 12 maio 2025.

NOBUG. *Gestão de Riscos e Fraudes em Ambientes Digitais*. Disponível em: NoBug. Acesso em: 12 maio 2025.

PUCRS ONLINE. Blockchain: *A Revolução na Segurança de Dados para sua Empresa.* Disponível em: PUCRS Online. Acesso em: 12 maio 2025.

REIS ADVOCACIA*. Estelionato e Fraudes: Entenda as Leis, E Como Funciona!* 2023. Disponível em: https://advocaciareis.adv.br/blog/criminal/como-lei-penal-estelionato-fraudes/. Acesso em: 26 out. 2024.

REY ABOGADO. *Entenda o Conceito de Estelionato na Internet e suas Implicações Legais, 2023.* Disponível em: https://reyabogado.com/brasil/o-que-e-estelionato-na-internet/. Acesso em: 3 nov. 2024.

RIBEIRO, Danilo Francis; ORTLEPP, Priscilla Gomes. *Golpes e venda ilegal de dados no mundo virtual: desafios da segurança cibernética no Brasil.* Revista FT, v. 27, ed. 129, dez. 2023. Disponível em: Revista FT. Acesso em: 12 maio 2025.

SANTOS, A. P. *Impactos da Digitalização na Privacidade dos Dados.* São Paulo: Editora Nova Era, 2022.

UNIÃO EUROPEIA. *Regulamento Geral sobre a Proteção de Dados (RGPD).* Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril

de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 15 nov. 2024.

WIMMER, Miriam. *Tratado de Proteção de Dados Pessoais.* São Paulo: Editora XYZ, 2021. Capítulo 13: O Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público.

4 STRATS. *Arquiteturas de Big Data para Privacidade e Segurança: com IA.* Disponível em: Blog 4 Strats. Acesso em: 12 maio 2025.