



ARGUS MAPURUNGA DE ARAÚJO

ISABEL MARIA ESTRELLA DE SAMPAIO SOARES

FRAUDES ELETRÔNICAS: o papel da LGPD na prevenção contra os crimes virtuais

TERESINA-PI

2025

ARGUS MAPURUNGA DE ARAÚJO

ISABEL MARIA ESTRELLA DE SAMPAIO SOARES

FRAUDES ELETRÔNICAS: o papel da LGPD na prevenção contra os crimes virtuais

Trabalho de Conclusão de Curso
apresentado à Afya Centro Universitário –
Uninovafapi, para obtenção do título de
Bacharel em Direito.

Orientador(a): Prof.(a) Ma. Sara Morgana
Silva Carvalho Lopes

TERESINA – PI

2025

FICHA CATALOGRÁFICA

A663f Araújo, Argus Mapurunga de

Fraudes eletrônicas: o papel da LGPD na prevenção contra os crimes virtuais. / Argus Mapurunga de Araújo; Isabel Maria Estrella de Sampaio Soares. – Teresina: UNINOVAFAPI, 2025.

Orientador (a): Profº. Ms. Sara Morgana Silva Carvalho Lopes – UNINOVAFAPI, 2025.

28.p.; 23cm.

Trabalho de conclusão (Graduação em Direito) – UNINOVAFAPI, Teresina, 2025.

1. Crimes. 2. Virtuais. 3. LGPD. 4. Eficácia. 5. Prevenção. I. Título. II. Araújo, Argus Mapurunga de. III. Soares, Isabel Maria Estrella de Sampaio.

CDD 342.1141

Catálogo na publicação

Francisco Renato Sampaio da Silva – CRB/1028

FOLHA DE APROVAÇÃO

ARGUS MAPURUNGA DE ARAÚJO
ISABEL MARIA ESTRELLA DE SAMPAIO SOARES

FRAUDES ELETRÔNICAS: o papel da LGPD na prevenção contra os crimes
virtuais.

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do
Afya Centro Universitário Uninovafapi,
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Data de Aprovação: 10 / 11 / 2025

BANCA EXAMINADORA

Sara M S C Lopes

Professora Mestre Sara Morgana Silva Carvalho Lopes
Afya Centro Universitário Uninovafapi
(Orientadora)

Francisco de Sousa Vieira Filho

Professor Mestre Francisco de Sousa Vieira Filho
Afya Centro Universitário Uninovafapi
(1º Examinador)

Maria do Socorro Carvalho de Sales Sousa

Professora Mestre Maria do Socorro Carvalho de Sales Sousa
Afya Centro Universitário Uninovafapi
(2º Examinador)

RESUMO

O presente trabalho de conclusão de curso aborda os impactos da Lei Geral de Proteção de Dados e se a presença no ordenamento jurídico dessa lei é suficiente para a prevenção contra crimes virtuais, a exemplo das fraudes eletrônicas. Objetiva-se com essa pesquisa analisar a eficiência da referida lei e seu o papel preventivo contra as fraudes eletrônicas. Para tanto, utilizamos a metodologia de Revisão Bibliográfica Narrativa de abordagem qualitativa, natureza básica de objetivos exploratórios. Os resultados apontam que apesar dos impactos positivos na vida social, ainda existem percalços para a plena efetividade, sobretudo em relação ao sistema de proteção contra fraudes eletrônicas. Logo, conclui-se que para que a LGPD cumpra de forma plenamente eficaz os seus objetivos, deve-se legislar quanto ao detalhamento dos padrões técnicos mínimos obrigatórios que as empresas portadoras de dados devem exercer, assim como, diminuir a burocracia para aderir a LGPD e retificar a gramática utilizada, a fim de tornar fácil a compreensão para todos os públicos.

Palavras-chave: Crimes 1; Virtuais 2; LGPD 3; Eficácia 4; Prevenção 5.

ABSTRACT

This final course project addresses the impacts of the General Data Protection Law and whether the presence of this law in the legal system is sufficient to prevent cybercrimes, such as electronic fraud. The objective of this research is to analyze the efficiency of this law and its preventive role against electronic fraud. To this end, we used the Narrative Literature Review methodology with a qualitative approach and basic exploratory objectives. The results indicate that despite the positive impacts on social life, there are still obstacles to full effectiveness, especially in relation to the system of protection against electronic fraud. Therefore, it is concluded that for the LGPD to fully and effectively fulfill its objectives, legislation must be enacted regarding the details of the minimum mandatory technical standards that data-holding companies must exercise, as well as reducing the bureaucracy involved in complying with the LGPD and rectifying the grammar used, in order to make it easy for all audiences to understand.

Keywords: Crimes 1; Virtual 2; LGPD3; Effectiveness 4; Prevention 5.

SUMÁRIO

1 INTRODUÇÃO	11
2 A LEI GERAL DE PROTEÇÃO DE DADOS E SEU IMPACTO	13
2.1 A NECESSIDADE DE PROTEÇÃO DE DADOS	14
2.2 IMPACTOS NO RAMO EMPRESARIAL.....	16
3 O AVANÇO DOS CRIMES CIBERNÉTICOS	17
3.1 FRAUDES ELETRÔNICAS EM CONTRATOS DE EMPRÉSTIMOS BANCÁRIOS	19
3.2 A NECESSIDADE DE NOVAS FORMAS DE PROTEÇÃO JURÍDICA NOS CONTRATOS VIRTUAIS	21
4. O PAPEL DA LGPD COMO MEIO DE INFORMAÇÃO.....	22
4.1. QUAIS OS “BURACOS” NÃO PREENCHIDOS PELA LGPD? O QUE FICOU FALTANDO PARA SUA EFICÁCIA PLENA?	23
5. CONSIDERAÇÕES FINAIS.	25
REFERÊNCIAS.....	27

1. INTRODUÇÃO.

Devido ao advento da globalização e o desenvolvimento de novas tecnologias, pode-se dizer que a sociedade atual enfrenta a chamada Revolução Informática: A Era da Informação. Com o surgimento da tecnologia da informação, formada por computadores e principalmente pelo advento da internet, as fronteiras físicas se tornaram obsoletas. Desse modo, surge um novo cenário sem regras: o mundo digital. Sendo necessária uma nova legislação para fazer frente aos novos crimes surgidos com a evolução da sociedade moderna (Crespo, 2011).

Por sua vez, Augusto Rossini, define crime digital como:

[...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade. (Rossini, 2004, p.110)

Assim, é possível perceber que um *cyber crime* é, de forma simples, qualquer ação errada e ilegal feita usando a tecnologia, seja um computador, um sistema ou a internet. Não importa se a pessoa que cometeu o ato agiu de propósito (com dolo), por descuido (com culpa), se ela fez algo que não devia (ação) ou se deixou de fazer algo que era obrigatório (omissão); o que define o delito é o fato de ter sido praticado por alguém (pessoa física) ou por uma empresa (pessoa jurídica) e que essa ação tenha atacado a Segurança da Informação.

Diante do exposto, como em qualquer crime, existem direitos sendo lesados e, por isso, existe a necessidade da presença da segurança jurídica, fundamentada no art 5º, XXXVI, CF, para combater tais novos delitos (Brasil, 1988). E da presença da Lei da Geral de Proteção de Dados, a fim de intervir, prevenir, o vazamento de dados e cometimento de crimes, a partir destes.

Hodiernamente, novos desafios quanto à segurança jurídica surgiram, a exemplo de fraudes eletrônicas, fazendo-se necessário a adaptação do Direito para com essas novas modalidades.

Por fim, faz-se mister evolver, a fim de alcançar os avanços e garantir os direitos e a segurança de ambas as partes, a exemplo da instauração da boa-fé objetiva no Código Civil (Brasil, 2002), objetivando impor padrões de comportamento a serem seguidos, deixando de lado o animus pré-conduta das partes e a subjetividade das ações e focando no ato concreto e suas consequências (Guersoni, 2019).

Diante do exposto, segue o seguinte questionamento, a LGPD é eficaz contra as fraudes eletrônicas? Tem-se por objeto do trabalho acerca do papel preventivo da LGPD contra as fraudes eletrônicas.

Os objetivos específicos são, avaliar o impacto obtido através da criação e implementação da Lei Geral de Proteção de Dados (LGPD), demonstrar a necessidade de criação de novos meios de proteção jurídica para combater os crimes cibernéticos, e discutir sobre a eficácia preventiva da LGPD contra os crimes virtuais.

Tal pesquisa se encontra justificada pelas problemáticas hodiernas, sobre a dificuldade de prevenir a materialização de crimes virtuais, a exemplo das fraudes eletrônicas, e como a segurança jurídica pode alcançar e proteger o contratante e o contratado, através da LGPD. Após analisar e experienciar os contratos digitais e suas modalidades de assinatura, observa-se a facilidade existente para fraudá-los, seja através de assinaturas eletrônicas e validadores poucos eficazes que permitem a troca ou até mesmo a sobreposição das mesmas dentre outros impasses.

Diante disso, é evidente a necessidade de estudar e elucidar sobre tal tema, tendo em vista a velocidade dos avanços tecnológicos no âmbito jurídico, e que efeitos/consequências os acompanham, e como o Direito pode acompanhar e combater os possíveis males que surgirem provenientes desses avanços, possibilitando um cenário em que a segurança jurídica possa perpetuar, garantindo os direitos e deveres, tornando ínfima as fraudes eletrônicas e a LGPD cumprindo com o seu objetivo de prevenção contra o uso de dados.

Por intermédio de Revisão Bibliográfica Narrativa de abordagem qualitativa, natureza básica de objetivos exploratórios, tendo como base livros virtuais, sites e artigos que abordem sobre a Lei Geral de Proteção de Dados (LGPD) e

como ela pode atuar preventivamente contra fraudes eletrônicas.

2. A LEI GERAL DE PROTEÇÃO DE DADOS E SEU IMPACTO.

A digitalização das relações sociais tornou a celebração de contratos eletrônicos uma prática comum para empresas e indivíduos. A princípio, previsibilidade e a estabilidade das relações contratuais virtuais dependiam, em grande parte, da validação técnica de documentos, como o uso de assinaturas eletrônicas e digitais, com validade jurídica reconhecida (Brasil, 2020).

Contudo, a mera validade formal não garantia a proteção dos direitos fundamentais do indivíduo, que se via em uma posição de vulnerabilidade. A desproporção entre a velocidade da inovação tecnológica e a evolução legislativa criava um vácuo regulatório que, em vez de fomentar a confiança, gerava insegurança.

A fim de tornar ínfima a incontroversa, a Lei Geral de Proteção de Dados (LGPD) reconfigurou a validade e a eficácia desses contratos ao introduzir o consentimento qualificado como uma das principais bases legais para o tratamento de dados. O mero "clique de aceite" em um contrato de adesão online ganha um novo contorno.

Ainda sobre o consentimento, encontra-se fundamentado no art. 5º, XII, da Lei Nº 13.709, de 14 agosto de 2018: "Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Brasil, 2018).

A LGPD não é um mero diploma regulatório; sua natureza jurídica reside na proteção de direitos fundamentais de liberdade, privacidade e livre formação da personalidade do indivíduo. O art. 2º da LGPD aponta que os seus fundamentos são:

- I - O respeito à privacidade;
- II - A autodeterminação informativa;
- III - A liberdade de expressão, de informação, de comunicação e de opinião;
- IV - A inviolabilidade da intimidade, da honra e da imagem (Brasil, 2018).

Tendo em vista o artigo supramencionado e a emenda constitucional nº 115, de 10 de fevereiro de 2022 que afirma: “Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais” (Brasil, 2022). Por fim, cabe-se ressaltar que as relações contratuais virtuais passaram a ter maior previsibilidade e a estabilidade das relações após a implantação jurídica.

2.1. A necessidade da proteção de dados.

Atualmente, os dados são vistos como o novo petróleo Ana Frazão (2020), tornando-se insumos essenciais para diversas atividades econômicas e, por si próprios, um mercado próspero e em constante expansão. Não à toa, surgiu a expressão “economia movida a dados” (*data-driven economy*) para ilustrar o fato de que, conforme aponta Nick Srnicek (2018), o capitalismo do século XXI se concentra na extração e no uso de dados pessoais.

É fácil de perceber que basicamente todas as relações de consumo, principalmente as virtuais, baseiam-se na coleta de dados, seja para criar um cadastro em uma rede social até mesmo uma conta bancária em um aplicativo de banco online.

Esse fenômeno, evidentemente, transcende a esfera econômica, gerando inúmeras consequências para a vida dos cidadãos, além de reestruturar por completo as relações sociais e políticas. Dessa forma, os dados adquiriram uma importância transversal, tornando-se pilares para a vida, a liberdade individual, a sociedade e até mesmo a democracia.

No contexto contemporâneo, encaixa-se o conceito de *Big Data* que surgiu no meio da década de 1990, utilizado pela primeira vez pelo cientista John Mashey para se referir à manipulação e análise de um grande volume de dados (Kitchin, 2014). Diante disso, somado ao advento da evolução tecnológica, o aludido fenômeno se refere ao enorme crescimento na quantidade de dados produzidos no mundo.

Com uma enorme quantidade de dados, estes sendo “matéria-prima” valiosa para qualquer relação de consumo ou não, surge uma necessidade de organizar e proteger. Tendo em vista que todo dado significa informações pessoais de um indivíduo. Os dados se tornam importante recurso organizacional na medida em que podem ser analisados e transformados em informação.

Embora a informação contenha mais valor agregado, o dado também possui certo valor. Esta é a razão pela qual há necessidade de proteção de dados (Hintzbergen *et. al.*, 2018).

Dessa forma, um dado ao ser organizado vira informação, esta por sua vez tem um valor maior subentendido. Qualquer informação pessoal não devidamente protegida pode cair em mãos erradas prejudicando o indivíduo por traz dela. Em uma reportagem do Senado Federal (Brasil, 2025), foi destacado o prejuízo monetário advindo dos crimes cibernéticos, em 2024, em que aproximadamente 40 milhões de brasileiros foram vítimas golpes e fraudes, resultando em déficit financeiro.

Nesse sentido, a LGPD no Brasil, baseada no Regulamento Geral de Proteção de Dados da União Europeia, a lei Regulamento (UE) 2016/679) ou RGPD, ou a sigla em inglês, GDPR (*General Data Protection Regulation*), seguiu a mesma linha de que, existe a necessidade a proteção dessa enorme quantidade de dados, deixando evidente a intenção do legislador em considerar a proteção de dados pessoais como um direito fundamental (Serpro, 2025). Portanto, tanto a manipulação de dados quanto as informações geradas a partir deles são protegidas pela LGPD.

Conforme Botelho (2020), a lei exige que os controladores, operadores e encarregados adotem medidas para promover uma maior segurança da informação. Em conclusão, a LGPD estabelece um novo paradigma, garantindo que o tratamento de dados pessoais seja feito com respeito aos direitos dos titulares, o que fortalece a confiança e a segurança na era digital.

2.2. Impactos da LGPD no ramo empresarial.

Com o decorrer dos séculos o acesso à informação veio se tornando cada vez mais célere, novos meios foram produzidos, tecnologias sendo criadas e melhoradas, até chegar aos tempos atuais em que beira ao imediato, haja vista que não há mais barreiras entre nações, o que acontece no interior da China é informado no Brasil em questão de segundos. Corroborando com a ideia, Milton Santos afirma:

A técnica da informação assegura esse comércio, que antes não era possível. Por outro lado, ela tem um papel determinante sobre o uso do tempo, permitindo, em todos os lugares, a convergência dos momentos, assegurando a simultaneidade das ações e, por conseguinte, acelerando o processo histórico (Santos, 2001, p.12).

Dessa forma, os avanços tecnológicos garantiram o compartilhamento sincronizado em alta escala de informação e nas bases de dados. Porém, a segurança jurídica também evoluiu, e a partir deste aprimoramento, o ramo empresarial foi diretamente impactado pela LGPD.

Antes da implementação, os dados fornecidos não eram devidamente resguardados, a exemplo da inadimplência em proteger, faz-se comentar sobre a indenização paga pela empresa construtora Cyrela, em 2018, pela divulgação dos dados de um cliente para empresas concorrentes e estas o passaram a assediar fortemente, segundo (G1, 2020). Comprovando-se a fragilidade protetiva.

Hodiernamente, foi atribuído ao rol de responsabilidades das empresas um controle de dados mais refinado e robusto, a fim de assegurar os direitos previstos e atuação preventiva contra crimes cibernéticos.

Com base no art. 6º, LGPD, para que as empresas possam realizar o gerenciamento de informações, devem cumprir requisitos como, transparência, garantia de proteção ao consumidor, responsabilização pelos dados e consentimento quanto ao uso (Brasil, 2018). E caso descumpram?

Na hipótese de deveres descumpridos ou realizados sem moderação, objetivando o combate ao imbróglio, a legislação supramencionada, em seu art.

52, impõe sanções e medidas práticas a quem viola os institutos, os quais serão aplicados pela Agência Nacional de Proteção de Dados (ANPD):

I - Advertência, com indicação de prazo para adoção de medidas corretivas;

II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - Multa diária, observado o limite total a que se refere o inciso II;

IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - Eliminação dos dados pessoais a que se refere a infração. (Brasil, 2018)

Desse modo, além de impactar positivamente na segurança entre as partes contratantes e tornar as relações transparentes, o âmbito empresarial também é assegurado, pois a não violação da legislação evita a aplicação de multas e mantém a boa reputação da empresa.

Ademais, a aplicação da LGPD nas empresas é um diferencial. Baseado no estudo *IT Trends Snapshot*, realizado pela empresa Logicalis, em 2023, apenas 36% das empresas declararam estar em conformidade total com a lei (Lisboa; Takano, 2023). Logo, somente uma pequena parcela das empresas segue à risca a legislação, fazendo-se com que essas se destaquem quanto à confiabilidade que transmite aos clientes.

Por fim, em tese, a adesão à LGPD carrega consigo uma boa reputação para a empresa, pois é uma garantia que os dados dos clientes serão resguardados, e quanto mais consumidores, maior a receita financeira.

3. O AVANÇO DOS CRIMES CIBERNÉTICOS.

Os crimes cibernéticos, ou seja, ações criminosas cometidas através de dispositivos informáticos, estão presentes nas sociedades desde o século XX (Cazaroti; Pinheiro, 2021). Combinado com os avanços tecnológicos, a prática tornou-se cada vez mais corriqueira.

No Brasil, o delito criminoso cibernético que gerou a maior repercussão e impacto social, foi o Caso da Carolina Dieckmann, ocorrido em 2011, no entanto, como se pode explicar a presença de crimes no ambiente virtual?

Em primazia, Émile Durkheim diz:

Não há, portanto, um fenômeno que apresente de maneira tão irrefutável como a criminalidade todos os sintomas da normalidade, dado que surge como estreitamente ligada às condições da vida coletiva. Transformar o crime numa doença social seria o mesmo que admitir que a doença não é uma coisa accidental, mas que, pelo contrário, deriva em certos casos da constituição fundamental do ser vivo; consistiria em eliminar qualquer distinção entre o fisiológico e o patológico. (Durkheim, 2007, p. 67)

Seguindo a linha de raciocínio, o crime é um fato decorrente da vida em sociedade, do aglomerado de pessoas e das relações interpessoais, logo, é inerente ao ser humano, não se restringindo ao fator presencial. Consequentemente, com o advento da internet, relações virtuais se formaram e corroborado com o vácuo sancionatório, não à toa que a rede é conhecida como “terra sem lei”, o crime passou a se propagar também nos meios virtuais.

De início, a conduta não era tão lesiva para as partes, haja vista que não havia divulgação de dados e os meios não eram tão favoráveis para tamanho delito, no entanto, ao decorrer da globalização os meios tecnológicos foram evoluindo, consequentemente, também os crimes. Segundo a Associação de Defesa dos Dados do consumidor: “Foram cerca de 5 milhões de golpes praticados em 2024, o que representa um crescimento entre 35% e 45% em relação ao ano anterior)” (ADDP, 2024). Destaca-se o avanço meteórico dos golpes eletrônicos num curto espaço de tempo.

Baseado em Ferreira (2005, 2005. p. 209-211 apud Sarak, 2018) os avanços dos meios virtuais propiciaram o acréscimo e heterogeneidade das ações criminosas, ou seja, diferentes delitos surgiram a partir dos anos 80. Culminando no reconhecimento da fragilidade, mas também da necessidade de novas formas de controle e sanções dos delitos. Hodiernamente, fraudes eletrônicas, *fake news*, *bullying*, pornografia infantil, os mais diversos delitos se estenderam para o campo virtual, pois isso é a internet, uma expansão da realidade.

Por fim, o Código Penal, acerca do princípio da legalidade, impõe que: “Não há crime sem lei anterior que o defina, nem pena sem prévia a cominação legal” (Brasil, 1940). Dessa forma, a implantação de obstáculos com o objetivo de frear os crimes eletrônicos ficam enfraquecidos, pois a evolução jurídica não acompanha a criminosa, uma vez que além da necessidade do conhecimento do crime, o processo legislativo não é célere, fazendo-se necessário novos meios que atuem de forma a otimizar o trâmite legislativo e preventivo de crimes.

3.1 Fraudes eletrônicas em contratos de empréstimo bancário.

Em primazia, resulta-se da tecnologia da informação o aumento exponencial do número de contratações eletrônicas, objetivando a aquisição de bens e serviços, por intermédio da utilização de eletrônicos, a exemplo de celular, tablet, computadores etc. Os quais dispensam o deslocamento dos consumidores aos estabelecimentos físicos dos fornecedores e o uso de papel.

A rapidez e a comodidade contidas nesta nova forma de realizar negócios jurídicos, trazem consigo riscos de prejuízos aos contratantes, em sua maioria, crimes financeiros. Dentre as possíveis infrações, as fraudes bancárias eletrônicas têm seu lugar consolidado.

Como consequência, os supramencionados têm sido alvos constantes de perdas financeiras, resultantes da ação de infratores que praticam fraudes nos sistemas de informática usados pelos fornecedores para a efetivação dos contratos digitais (Soares; Carvalho, 2023).

O Código Penal vigente, em seu artigo 171, conceitua fraude como: “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” (Brasil, 1940).

Dessa forma, fraude é toda ação ilícita e desonesta, que tem por objetivo enganar terceiro para obter vantagem ilícita para si ou outrem. (Michaelis, 2020). Trazendo para o cenário dos contratos eletrônicos, estes que segundo Belanda e Cavalcanti (2021) são contratos celebrados total ou parcialmente no

meio digital (eletrônico ou telemático), sem o uso de papel, com o auxílio de um sistema de informática computacional e/ou da internet.

O resultado é que vários problemas surgiram nas contratações digitais, potencializando riscos para ambos os contratantes, sendo um deles as fraudes em operações bancárias, assunto que tem figurado em número significativo de processos judiciais no Brasil.

De acordo com o Migalhas (2023), um caso comum são as fraudes em contratos de empréstimos bancários. Antigamente, para contratar empréstimo consignado, o tomador devia comparecer no representante bancário e assinar o contrato. Hoje, com o acesso facilitado a aparelhos eletrônicos com internet, esse tipo de empréstimo passou a ser celebrado a distância, sem necessidade de deslocamento para assinatura do contrato. Isso pode ser feito do próprio domicílio ou de qualquer outro lugar, bastando acessar o site ou aplicativo da instituição financeira, seguir o passo a passo indicado, principalmente as dicas de segurança informando que não solicita transferência de valores para terceiros, e assinar o documento com uma *selfie*.

Exemplificando, destaca-se a Apelação Cível: 1007767-95.2021.8.26.0597 “Sertãozinho”, do tribunal de justiça de São Paulo. O caso trata de uma ação declaratória de inexistência de débito e reparação por danos materiais e morais, onde a autora alega não ter contratado um empréstimo consignado. O banco, por sua vez, não apresentou provas que demonstrassem a efetiva manifestação de vontade da mutuária, como gravações e documentos de aceitação. A autora questiona a validade do contrato, apontando inconsistências na captação de dados e na geolocalização, e busca a devolução em dobro dos valores descontados, além de indenização por danos morais.

O caso evidencia que não é possível o consumidor receber um *link* de determinado aparelho, ler os termos do contrato em outro, realizar o aceite em terceiro e capturar o reconhecimento facial em um quarto aparelho. Ressalta-se que a geolocalização registrada na assinatura era divergente da sua, evidenciando uma relação de fraude.

Diante do exposto, após apreciado o caso, é evidente a vulnerabilidade do consumidor em tais contratações. Também se sobressai a insuficiência tecnolagnormativa do Direito: como proteger o contratante diante desse novo cenário tecnológico?

3.2 A necessidade de novas formas de proteção jurídica nos contratos virtuais.

A reflexão acerca da falta de normas no ordenamento jurídico brasileiro para lidar com a criminalidade digital é de urgente e extrema importância, e vem sendo foco de discussões e debates há anos por estudiosos e doutrinadores de diversas áreas, principalmente a jurídica.

A necessidade de novas formas de proteção jurídica contra crimes cibernéticos, especialmente no contexto dos contratos virtuais, decorre de diversos fatores que evidenciam a fragilidade do ordenamento jurídico atual. Embora o direito digital seja, em essência, a aplicação dos princípios legais já existentes no ambiente virtual (Tashiro, 2015), o sistema jurídico enfrenta a incompletude e a inconsistência do direito penal para lidar com a criminalidade digital (Haikal; Pinheiro, 2016), o que resulta em impunidade e incentiva a prática de crimes no meio cibernético.

Adicionalmente, o crescente número de crimes digitais no Brasil está diretamente relacionado à falta de providências para punir os infratores e à carência de normas específicas para o ambiente cibernético, as quais são poucas no ordenamento jurídico brasileiro (Brasil, 2012).

Os crimes cibernéticos eram irrisórios até o século XX, porém, com o avanço tecnológico, a vinda das redes sociais, e-books, materiais virtuais, os crimes cibernéticos vieram juntos, a exemplo de: Fraudes bancárias, crimes relacionados a abuso sexual infantil, crimes de ódio no âmbito virtual, estelionato. Destaca-se que, em 2024, a Polícia Federal participou de 107 operações, no Paraná, de janeiro à dezembro, contra crimes virtuais relacionados ao abuso sexual infantil (Brasil, 2025).

As leis de proteção digital existentes no Brasil se concentram em direitos e deveres gerais, mas não contemplam as especificidades do direito penal, como

a definição de territorialidade e a competência para julgar crimes cometidos na internet (Weber, 2016).

Por fim, a demora na resposta e a burocracia do sistema jurídico (Vianna, 2023) fazem com que as vítimas de crimes digitais percam a chance de pleitear seus direitos, o que acaba por encorajar os criminosos a continuarem praticando delitos, sabendo que dificilmente serão responsabilizados. A ausência de regulamentação clara sobre como tratar esses crimes virtuais e a falta de limites para a responsabilização tornam o combate a essas infrações um grande desafio (Zanatta, 2017).

Em suma, a transição para o ambiente digital, marcada pelo aumento da celebração de contratos virtuais, evidencia uma lacuna crítica no ordenamento jurídico brasileiro. Embora os princípios do direito tradicional ainda sejam aplicáveis, a inércia estatal, a incompletude do direito penal e a burocracia do sistema se mostram insuficientes para combater a criminalidade cibernética com a agilidade e a especificidade que a era digital exige.

A necessidade de novas formas de proteção jurídica não se restringe apenas à tipificação de novos delitos, mas abrange, sobretudo, a criação de normas claras sobre competência territorial e a responsabilidade dos agentes, além de um sistema legal mais célere para garantir a efetiva punição dos infratores.

Conclui-se, portanto, que a segurança jurídica nas relações contratuais virtuais depende intrinsecamente de uma atualização legislativa e de uma mudança de postura do sistema jurídico, que precisa se adaptar às complexidades do ambiente cibernético para proteger a confiança e a validade dos negócios jurídicos digitais.

4. O PAPEL DA LGPD COMO MEIO DE INFORMAÇÃO.

Em primazia, cabe informar sobre o lapso temporal de existência da LGPD. A legislação entrou em vigor em 2020, a partir da aprovação pelo Senado da MP 959/2020 (PLV 34/2020) no final de agosto (Brasil, 2020).

Destaca-se que a legislação foi um marco legal no combate à proliferação indevida de dados pessoais, tanto na esfera informativa como preventiva. Haja vista que a sua implementação acarretou num processo de conscientização sobre direitos que os titulares possuem sobre os seus dados.

A exemplo, a ANPD, no ano de 2022, no seu relatório de gestão da Ouvidoria, informou que:

Os tipos mais frequentes de demandas tratadas pela Ouvidoria da ANPD dizem respeito a esclarecimentos quanto a aplicabilidade da Lei Geral de Proteção de Dados Pessoais e a atuação da ANPD, representando 58% das demandas. (Brasil, 2023)

Com base no relatório, entende-se que juntamente com a Constituição Federal, por meio da Emenda Constitucional 115/2022, a LGPD sana o vácuo de fontes informativas, acerca da proteção de dados, no âmbito normativo. Consequentemente, pode-se afirmar que a carta magna é a fonte para se basear sobre os direitos e a obrigação do controle de dados. Todavia, ainda persistem imbróglios acerca da aplicabilidade da LGPD, tais como a burocracia e a falta de compreensão das empresas.

Segundo a página LGPD Brasil (2023), em 2021, cerca de 74% das empresas não se sentiam aptas para aderir a LGPD. Assim como, de 508 empresas as quais foram entrevistadas, 72% iriam contratar empresas terceirizadas para implementar a LGPD, haja vista a falta de conhecimento para tal ação.

Logo, fica claro que a transição do espaço teórico para a prático é o “calcanhar de Aquiles” da supramencionada lei. Portanto, haja vista a problemática exposta, torna-se necessário analisar se há outras deficiências na lei anteriormente citada.

4.1. Quais os “buracos” não preenchidos pela LGPD? O que ficou faltando para sua eficácia plena?

Como fora abordado anteriormente, a legislação possui da eficácia informativa. Contudo, destacam-se brechas na em seus modos operandi e preventivo. Salienta-se que as lacunas da LGPD não são necessariamente falhas no texto da lei, mas sim pontos onde a lei foi insuficiente ou onde a sua regulamentação

e aplicação ainda não atingiram a profundidade necessária para combater os crimes cibernéticos.

Em seu artigo 46 a LGPD traz a seguinte redação:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas 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).

Nesse sentido, em seu próprio texto, é possível perceber a ausência de detalhamento técnico e obrigatório. Quais são os padrões mínimos de segurança que todos os agentes de tratamento (especialmente grandes detentores de dados) devem seguir para garantir a confidencialidade, integridade e disponibilidade? Conceitos estes que são vistos como pilares e indispensáveis para garantir a segurança das informações (Brasil, 2012).

Segundo o Ministério Público do estado do Mato Grosso, os pesquisadores apontaram que de janeiro a julho de 2024, o governo federal registrou 3.253 vazamentos de dados, mais do que o dobro dos casos somados entre 2020 e 2023. Já os crimes de estelionato virtuais, ou fraudes, alcançaram 2,17 milhões de ocorrências em 2024, o equivalente a 4 fraudes por minuto, segundo o Anuário do Fórum Brasileiro de Segurança Pública (Ministério Público, 2025).

De acordo com Alexandre Arns Gonzales, integrante do DiraCom, entidade integrante CDR:

O aumento expressivo de vazamentos e golpes digitais mostra que a LGPD ainda não tem aplicação efetiva no dia a dia das pessoas. Falta estrutura e independência para a ANPD, fiscalização ativa e políticas públicas de prevenção (Security Leaders, 2025).

Em suma, a principal limitação da LGPD em sua função preventiva reside no seu caráter excessivamente principiológico. Embora exija dos controladores a adoção de "medidas de segurança, técnicas e administrativas" para proteger a tríade de confidencialidade, integridade e disponibilidade dos dados, a lei é omissa quanto ao detalhamento dos padrões técnicos mínimos obrigatórios.

Essa lacuna regulatória impede a uniformização das práticas de segurança, permitindo que diversos agentes de tratamento apliquem medidas insuficientes ou desiguais. Consequentemente, a falta de um "padrão de segurança" claro, compromete o Princípio da Prevenção, facilitando os vazamentos em massa que servem de combustível para o crescente mercado de *phishing* e fraudes virtuais, demonstrando a urgência de uma regulamentação técnica mais incisiva por parte da ANPD.

5. CONSIDERAÇÕES FINAIS.

Ao longo do presente trabalho foi analisado sobre os impactos do advento da Lei Geral de Proteção de Dados, a evolução dos crimes cibernéticos e acerca da eficácia da LGPD, quanto meio de informação e prevenção a crimes virtuais.

Em primazia, ao término da avaliação dos impactos da LGPD, chegou-se à conclusão que os impactos foram protuberantes na vida social, pois preencheram o vácuo sancionatório anteriormente existente, atuaram de forma a conscientizar a sociedade quantos os seus direitos de terem seus dados guardados. Como também, coagiu as empresas de forma direta, através de multas e sanções, a protegerem os dados de seus consumidores.

Ademais, após o estudo acerca da evolução dos crimes cibernéticos, em prol de demonstrar a necessidade de novos meios de proteção jurídica, as pesquisas corroboraram com a informação. Haja vista a fragilidade do sistema jurídico digital hodierno em acompanhar os avanços dos crimes cibernéticos.

Cabe salientar também sobre a seara informativa da LGPD. Por mais que o campo teórico teve sua lacuna preenchida, tanto os usuários a serem protegidos, quanto as organizações que devem proteger, encontram dificuldades de interpretar a legislação, seja pela sua linguagem técnica ou pela sua generalidade em certos por tópicos. O mesmo ocorre no âmbito preventivo, a LGPD é omissa quanto ao detalhamento dos padrões técnicos mínimos obrigatórios, acarretando numa dificuldade na uniformização das práticas de segurança, que a torna uma ínfima fonte preventiva contra crimes digitais.

Considerando os objetivos específicos que foram investigados e a metodologia aplicada, conclui-se que a LGPD ainda não é plenamente eficaz, conforme os fatos apresentados no trabalho que comprovam a existência de percalços para sua completa efetividade, sobretudo em relação ao sistema de proteção contra fraudes eletrônicas.

Contudo, não quer dizer que a referida lei seja "descartável" e sem utilidade, tendo em vista que ela representa um grande avanço na tentativa de legislar sobre a proteção de dados. Muito embora exista o decreto federal nº 10.474/2020, o decreto municipal 21.838/2023 e o decreto municipal 23.197/2022, estes não conseguem transmitir de maneira eficaz quais medidas devem ser adotadas pelas empresas, o que configura uma lacuna e resulta em insegurança jurídica.

Por fim, para que ela se torne plenamente eficaz, existe uma necessidade de incluir medidas como, legislar quanto ao detalhamento dos padrões técnicos mínimos obrigatórios, diminuir a burocracia para adesão à lei e retificar a gramática utilizada, a fim de tornar fácil sua compreensão por todos os públicos. Dessa forma, é possível que ela se torne uma norma eficaz e que sirva para combater e diminuir a incidência de crimes digitais.

REFERÊNCIAS

ADDP. **Golpes on-line tiveram alta significativa em 2024**. ADDP, [S. l.], 2024. Disponível em: <https://addp.com.br/addp/golpes-on-line-tiveram-alta-significativa-em-2024/>. Acesso em: 29 set. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Relatório anual da Ouvidoria da ANPD revela alta procura por esclarecimentos quanto a aplicabilidade da LGPD**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/relatorio-anual-da-ouvidoria-da-anpd-revela-alta-procura-por-esclarecimentos-quanto-a-aplicabilidade-da-lgpd>. Acesso em 21 out. 2025.

BELANDA, Douglas; CAVALCANTI, Ana Elizabeth Lapa Wanderley. **A incompetência do Juizado Especial Cível em caso de necessidade de prova pericial em contratos eletrônicos**. Revista dos Tribunais. São Paulo: RT, vol. 1024, 2021, p. 3.

BOTELHO, Marcos. **A proteção de dados pessoais enquanto direito fundamental**: considerações sobre a lei geral de proteção de dados pessoais. Argumenta Journal Law, Jacarezinho – PR, Brasil, n. 32, 2020, p. 191-207. Disponível em: <https://periodicos.uenp.edu.br/index.php/argumenta/article/view/312/pdf>. Acesso em: 23 out.2025

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, [1988]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 out. 2025

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 out. 2025.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. **Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais**. Diário Oficial da União, Brasília, DF, 10 fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso: 23 out.2025

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**. Brasília, DF: Diário Oficial da União, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 23 out.2025

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 23 out.2025

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União: seção 1, Brasília, DF, ano 156, nº 157, p. 59-64, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 out.2025

BRASIL. Lei nº 14.063, de 23 de setembro de 2020. **Dispõe sobre o uso de assinaturas eletrônicas**. Diário Oficial da União, Brasília, DF, 23 setembro de 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm. Acesso: 23 out.2025.

BRASIL. Polícia Federal. **Diretoria de Combate a Crimes Cibernéticos - DCIBER**. Brasília, (2025). Disponível em: <https://www.gov.br/pf/pt-br/aceso-a-informacao/estatisticas/diretoria-de-combate-a-crimes-ciberneticos-dciber>. Acesso em: 15 de agosto 2025.

BRASIL. **Relatório anual da Ouvidoria da ANPD revela alta procura por esclarecimentos quanto a aplicabilidade da LGPD**. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/relatorio-anual-da-ouvidoria-da-anpd-revela-alta-procura-por-esclarecimentos-quanto-a-aplicabilidade-da-lgpd>. Acesso em: 25 out. 2025.

BRASIL. Tribunal de Justiça de São Paulo. **Apelação Cível nº 1002579-20.2021.8.26.0597**. Relator: Desembargador Edgard Rosa. 22ª Câmara de Direito Privado, Sertãozinho, SP, 2 set. 2022. Diário da Justiça Eletrônico, São Paulo, 2 set. 2022. Disponível em: <https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=GL00047X30000&processo.foro=597&processo.numero=1007767-95.2021.8.26.0597>. Acesso em: 24 set. 2025.

BRASIL. **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: 21 out. 2025

CAZAROTI, Tatiane Martins Barros; PINHEIRO, Eduardo Fernandes. **Crimes Cibernéticos. TCC- Faculdade de Direito**, 2021. Disponível em: [file:///C:/Users/SASC/Downloads/admin,+CRIMES+CIBERN%C3%89TICOS%20\(2\).pdf](file:///C:/Users/SASC/Downloads/admin,+CRIMES+CIBERN%C3%89TICOS%20(2).pdf). Acesso em: 29 out.2025.

Constantino, E. da S., Carvalho, O. de S., Constantino, E. da S., & Flores, K. S. (2025). **ENTRE A LEI E A INVASÃO: A LGPD E A PROTEÇÃO REAL AO CIDADÃO**. Revista Ibero-Americana De Humanidades, Ciências E Educação, 11(6), 3521–3533. <https://doi.org/10.51891/rease.v11i6.19919>

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. 1ª Ed. São CYRELA é multada em R\$ 10 mil por infração à Lei Geral de Proteção de Dados. In: **G1**. Rio de Janeiro, 30 set. 2020. Disponível em: <https://g1.globo.com/economia/noticia/2020/09/30/cyrela-e-multada-em-r-10-mil-por-infracao-a-lei-geral-de-protecao-de-dados.ghtml>. Acesso em: 13 out. 2025.

DOS. **Contratação digital e a indústria dos golpes - Migalhas**. Disponível em: <https://www.migalhas.com.br/depeso/385381/contratacao-digital-e-a-industria-dos-golpes>. Acesso em: 28 out. 2025.

DURKHEIM, Emile. **As regras do método sociológico**. Tradução Paulo neves, 3ª ed. São Paulo: Martins Fontes, 2007. Disponível em: <https://pedropeixotoferreira.wordpress.com/wp-content/uploads/2014/03/durkheim-c3a9mile-as-regras-do-mc3a9todo-sociolc3b3gico-3-ed-sc3a3o-paulo-martins-fontes-2006.pdf>. Acesso em: 23 out.2025

GUERSONI, Angelo Junqueira. **SEGURANÇA JURÍDICA NA INTERPRETAÇÃO DOS CONTRATOS DIANTE DA BOA-FÉ OBJETIVA**. Ratio Juris. Revista Eletrônica da Graduação da Faculdade de Direito do Sul de Minas, Pouso Alegre, v. 2, n. 2, p. 56-68, jul./dez. 2019. Disponível em: [file:///C:/Users/SASC/Downloads/adminojs,+2019-2+-+Seguran%C3%83%C2%A7a+jur%C3%83_dica+na+interpreta%C3%83%C2%A7%C3%83%C2%A3o+dos+contratos+diant+da+boa-f%C3%83%C2%A9+objetiva%20\(2\).pdf](file:///C:/Users/SASC/Downloads/adminojs,+2019-2+-+Seguran%C3%83%C2%A7a+jur%C3%83_dica+na+interpreta%C3%83%C2%A7%C3%83%C2%A3o+dos+contratos+diant+da+boa-f%C3%83%C2%A9+objetiva%20(2).pdf). Acesso em: 24/10/2025.

HAIKAL, Victor; PINHEIRO, Patrícia Peck. **Nova lei de crimes digitais**. In: PINHEIRO, Patrícia Peck (coord.). **Direito digital aplicado 2.0**. 2. ed. São Paulo: Thomson Reuters, 2016. p. 19-32.

HINTZBERGEN, Jule et. al. **Fundamentos de segurança da informação: com base na ISSO 27001 e na ISSO 27002**. Rio de Janeiro: Brasport, 2018. Disponível em: [https://www.kufunda.net/publicdocs/Fundamentos%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%20com%20base%20na%20ISO%2027001%20e%20na%20ISO%2027002%20\(%20etc.\)%20\(z-lib.org\).pdf](https://www.kufunda.net/publicdocs/Fundamentos%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%20com%20base%20na%20ISO%2027001%20e%20na%20ISO%2027002%20(%20etc.)%20(z-lib.org).pdf). Acesso em: 28 out. 2025.

KITCHIN, Rob. **The data Revolution: big data, open data, data infrastructure & their consequences**. Thousand Oaks: Sage Publications, 2014. Disponível em: https://se.moevm.info/lib/exe/fetch.php/courses:smart_data:the_data_revolution_big_data_open_data_data_infrastructures_and_their_consequences_by_rob_kitchin_z-lib.org_.pdf. Acesso em: 28 out. 2025.

LGPD BRASIL. **74% das empresas brasileiras não estão preparadas para a LGPD**. [S.l.]: LGPD Brasil, [20--]. Disponível em: <https://lqpdbrasil.com.br/84-das-empresas-brasileiras-nao-estao-preparadas-para-a-lqpd/>. Acesso em: 27 out. 2025.

LISBOA, Sofia; TAKANO, Yassuki. **IT Trends Snapshot 2023**. Logicalis. 2023. Disponível em: https://imagine.la.logicalis.com/hubfs/IT%20Snapshot%202023/it-trends-snapshot-2023_logicalis.pdf. Acesso em: 13 out. 2025.

MICHAELIS, **Dicionário Brasileiro de Língua Portuguesa**. Editora Melhoramentos Ltda., 2020. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/fraude>. Acesso em 06 de agosto de 2025.

MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO. **7 anos da LGPD: vazamentos disparam e uso de dados seguem sem limites, afirma análise**. Disponível em: <https://www.mpmt.mp.br/portalcão/news/1217/163260/7-anos-da-lgpd-vazamentos-disparam-e-uso-de-dados-seguem-sem-limites-afirma-analise>. Acesso em: 21 out. 2025.

Paulo: Saraiva, 2011. E-book. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/prefix/14602/1/Crimes%20digitais.pdf>. Acesso em: 28 out. 2025.

PÓ, M. N. **7 anos da LGPD: vazamentos disparam e uso de dados seguem sem limites, afirma análise - Security Leaders**. Disponível em: <https://securityleaders.com.br/7-anos-da-lgpd-vazamentos-disparam-e-uso-de-dados-seguem-sem-limites-afirma-analise/>. Acesso em: 21 out. 2025

ROSSINI, A. E. S. et al. (2004). **Informática, telemática e direito penal**. São Paulo: Memória Jurídica. Disponível em https://www.dhnet.org.br/dados/cursos/anp/rossini_cibercrime.pdf . Acesso em: 28 out. 2025.

SANTOS, Milton. **Por uma outra globalização: do pensamento único à consciência universal**. 6. ed. Rio de Janeiro: Record, 2001. Disponível em: https://pedropeixotoferreira.wordpress.com/wp-content/uploads/2010/03/santos_por-uma-outra-globalizacao-e28093-do-pensamento-unico-a-consciencia-universal_livro.doc. Acesso em: 24 out.2025

SARAK, Mayra Matuck. Cibernética: contextualizando vestígios dos delitos informáticos. **Empório do Direito**, [s. l.], 30 jun. 2018. Disponível em: <https://emporiოდodireito.com.br/leitura/cibernetica-contextualizando-vestigios-dos-delitos-informaticos>. Acesso em: 29 out.2025

SENADO FEDERAL. **Golpes virtuais aumentam e não fazem distinção de idade**. Brasília, DF: Senado Federal, 25 abr. 2025. Disponível em: <https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade>. Acesso em: 6 set. 2025.

SENADO FEDERAL. **Lei Geral de Proteção de Dados entra em vigor**. *Senado Notícias*, Brasília, DF, 18 set. 2020. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor#:~:text=A%20entrada%20em%20vigor%20da,passar%20pela%20aprova%C3%A7%C3%A3o%20do%20Senado>. Acesso em: 27 de out. 2025.

SOARES, Dennis Verbicaro; CARVALHO, Emerson Benjamin Pereira de. **Fraudes em contratos eletrônicos de empréstimos bancários: vulnerabilidade do**

consumidor, inteligência artificial e prova pericial em sistemas de biometria.

Revista Pensamento Jurídico, São Paulo, v. 17, n. 2, p. 1-22, maio/set. 2023.

Disponível em:

<https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/813/645>. Acesso em: 23 out. 2025

TASHIRO, William. **Direito ao anonimato na Internet**. Jusbrasil, 2015. Disponível

em: <https://www.jusbrasil.com.br/artigos/direito-ao-anonimato-na-internet/123456789>.

Acesso em: 17 ago. 2025.

TEIXEIRA, Leonardo Augusto Barçante. **Sete anos do GDPR: impactos na LGPD e o uso de dados para prevenção a fraudes**. Disponível em:

<https://www.serpro.gov.br/menu/noticias/noticias-2025/sete-anos-do-gdpr>. Acesso em 29 out. 2025.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 2. ed.

São Paulo: Thomson Reuters Brasil, Revista dos Tribunais, [2020]. Disponível em:

<https://bdjur.stj.jus.br/server/api/core/bitstreams/f8a5ffd5-bbb8-469b-a0e7-b89a8ab1e07e/content>. Acesso em: 24 out. 2025

VIANNA, Rafael. **Fraudes na Internet**. 2023. Disponível em: <https://cra-pr.org.br/fraudes-na-internet/>. Acesso em: 17 nov. 2025.

WEBER, Sandra Paula Tomaz. **A utilização da assinatura eletrônica biométrica na formação dos contratos**. In: PINHEIRO, Patrícia Peck (coord.). Direito digital aplicado 2.0. 2. ed. São Paulo: Thomson Reuters, 2016. Disponível em:

<https://nexyon.com.br/utilizacao-da-assinatura-eletronica-biometrica-na-formacao-dos-contratos/>. Acesso em: 24 out. 2025

ZANATTA, Leonardo. **O Direito Digital e as implicações cíveis decorrentes das relações virtuais**. Trabalho de Conclusão de Curso para obtenção do grau de Bacharel em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul. 2010. Disponível em:

http://35.238.111.86:8080/jspui/bitstream/123456789/241/1/Zanatta_Leonardo_O%20direito%20digital.pdf. Acesso em 20 out. 2025.