CURSO DE DIREITO

THAYNÁ JORGE DA CUNHA ARAUJO

CRIMES CIBERNÉTICOS E O GOLPE DO FALSO ADVOGADO: EFETIVIDADE DO DIREITO PENAL BRASILEIRO COM ENFOQUE NO ESTADO DE MATO GROSSO

Rondonópolis-MT
2026

CURSO DE DIREITO

THAYNÁ JORGE DA CUNHA ARAUJO

CRIMES CIBERNÉTICOS E O GOLPE DO FALSO ADVOGADO: EFETIVIDADE DO DIREITO PENAL BRASILEIRO COM ENFOQUE NO ESTADO DE MATO GROSSO

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito, da Faculdade Fasipe Rondonópolis, como requisito para a obtenção do título de Bacharel em Direito. Orientadora: Prof. Luisa Oliveira Vacaro.

Rondonópolis-MT
2026

THAYNÁ JORGE DA CUNHA ARAUJO

CRIMES CIBERNÉTICOS E O GOLPE DO FALSO ADVOGADO: EFETIVIDADE DO DIREITO PENAL BRASILEIRO COM ENFOQUE NO ESTADO DE MATO GROSSO

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito da Faculdade Fasipe Rondonópolis, como requisito para a obtenção do título de Bacharel em Direito.

Aprovado em:

Professora Orientadora: Luisa Oliveira Vacaro:
Docente Faculdade Fasipe Rondonópolis

Professor(a) Avaliador(a):

Professor(a) Avaliador(a):

Neuzimar Ferrari da Cruz Magalhães
Coordenadora do Curso de Direito Faculdade Fasipe Rondonópolis

Rondonópolis-MT
2026

DEDICATÓRIA

Dedico este trabalho, primeiramente, a Deus, que me deu forças e sabedoria ao longo desta caminhada. Dedico ainda, a todos aqueles que acreditaram no meu potencial e contribuíram direta ou indiretamente, para concretização desta conquista.

AGRADECIMENTOS

Agradeço a Deus por ter me concedido saúde, força e sabedoria para superar todas as dificuldades encontradas ao longo desta caminhada.

À minha mãe e aos meus irmãos, expresso minha eterna gratidão pelo amor, incentivo e apoio.

Aos meus amigos, companheiros de jornada acadêmica e irmãos de coração, que fizeram parte da minha formação e continuarão presentes em minha vida, agradeço pelo companheirismo, pelas palavras de incentivo, pelas risadas compartilhadas e pelo carinho que tornaram esta trajetória mais leve, feliz e significativa.

A todos que, direta ou indiretamente, contribuíram para minha formação pessoal e profissional, deixo o meu mais sincero agradecimento.

Por fim, agradeço a mim mesma, pela perseverança, dedicação e coragem para seguir em frente diante dos desafios, sem desistir dos meus objetivos. Cada obstáculo superado tornou esta conquista ainda mais valiosa e especial.

O ignorante afirma, o sábio dúvida, o sensato reflete. (Aristóteles)

ARAUJO, Thayná Jorge da Cunha. Crimes Cibernéticos e o golpe go falso advogado: efetividade do Direito Penal brasileiro com enfoque no Estado de Mato Grosso.2026. 43 páginas. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade Fasipe Rondonópolis, Rondonópolis, Mato Grosso, 2026.

RESUMO

Este trabalho teve como objetivo analisar a efetividade do Direito Penal brasileiro no enfrentamento das fraudes cibernéticas, com foco no golpe do falso advogado, com o intuito de identificar os dispositivos do Direito Penal brasileiro aplicáveis aos crimes cibernéticos previstos no código penal (estelionato, estelionato digital, falsidade ideológica e uso de documento falso, como também, examinar as principais dificuldades de investigação criminal (rastreamento de IP, anonimato, provas digitais), bem como discutir a responsabilidade das plataformas digitais na prevenção do golpe do falso advogado. Este trabalho apresenta uma análise crítica da efetividade do Direito Penal, tanto em âmbito nacional como no Estado de Mato Grosso, pois com a rapidez das interações virtuais, o anonimato e a transnacionalidade da internet colocam em xeque os mecanismos tradicionais de investigação e repressão penal, tornando imprescindível a reflexão sobre a adequação das normas jurídicas e das estratégias de combate a tais delitos, como a conscientização, capacitação e cooperação entre as partes envolvidas na prevenção e combate aos crimes digitais, incluindo órgão governamentais, setor privado e sociedade civil.

Palavras-chave: Fraudes cibernéticas, golpe do falso advogado e estelionato.

ARAUJO, Thayná Jorge da Cunha. Crimes Cibernéticos e o golpe go falso advogado: efetividade do Direito Penal brasileiro com enfoque no Estado de Mato Grosso.2026. 43 páginas. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade Fasipe Rondonópolis, Rondonópolis, Mato Grosso, 2026.

ABSTRACT

This study aimed to analyze the effectiveness of Brazilian Criminal Law in combating cyber fraud, focusing on the fake lawyer scam, in order to identify the provisions of Brazilian Criminal Law applicable to cybercrimes foreseen in the penal code (fraud, digital fraud, ideological falsehood, and use of false documents), as well as to examine the main difficulties of criminal investigation (IP tracking, anonymity, digital evidence), and to discuss the responsibility of digital platforms in preventing the fake lawyer scam. This work presents a critical analysis of the effectiveness of Criminal Law, both nationally and in the State of Mato Grosso, because the speed of virtual interactions and the anonymity that has provided a transnationality of the internet puts traditional mechanisms of criminal investigation and repression to the test, making it essential to reflect on the adequacy of legal norms and strategies to combat such crimes, such as awareness, training, and cooperation between the parties involved in the prevention and combating of digital crimes, including government agencies, the private sector, and civil society.

Keywords: Cyber fraud, fake lawyer scam, and fraud

LISTA DE SIGLAS

VPN – Rede Privada Virtual

IP – Protocolo de Internet

CP – Código Penal

CPP – Código de Processo Penal

MPSC – Ministério Público de Santa Catarina

CNJ – Conselho Nacional de Justiça

STJ – Superior Tribunal de Justiça

TJMT – Tribunal de Justiça do Estado de Mato Grosso

PIX – Pagamento instantâneo

DOC – Documento de ordem de crédito

TED – Transferência eletrônica disponível

SUMÁRIO

1. INTRODUÇÃO

Com a grande evolução e expansão da tecnologia, surgiu a necessidade de adequação do ordenamento jurídico, com o intuito de garantir uma maior segurança no ambiente virtual e impedir que ele se torne uma verdadeira “terra sem lei”. Nessa perspectiva, a legislação brasileira busca acompanhar os avanços tecnológicos por meio da criação e atualização de normas específicas, como a Lei Geral de Proteção de Dados (LGPD), nº 13.709/2018, bem como a tipificação do crime de fraude eletrônica, prevista no artigo 171, §2º-A, do Código Penal incluído pela Lei nº 14.155/2021. Em conjunto, as regulamentações têm o objetivo de causar reconhecimento e mostrar a urgência de proteger a privacidade dos indivíduos e apresentar o esforço contínuo que o ordenamento jurídico tem apresentado para a prevenção das fraudes cibernéticas.

Nesse contexto de progresso tecnológico contínuo, emergem novas formas de criminalidade que desafiam a eficácia das leis penais, como o golpe do falso advogado em plataformas digitais. Essa atividade, que envolve a usurpação de identidade profissional, coleta de dados pessoais na rede e a manipulação psicológica das vítimas, o que demostra a fragilidade das interações virtuais e a ineficácia de métodos de repressão penal. A complexidade dessa fraude demanda não só a modernização das leis, mas também uma abordagem integrada que envolva o Direito Penal, investigação digital e principalmente a conscientização social, visando aumentar a segurança nas interações online.

Apesar da criação de marcos legais significativos, a dinâmica acelerada do desenvolvimento tecnológico impõe impedimentos complexos quanto à aplicação das medidas, as variadas atividades ilícitas que surgem diariamente no ambiente virtual desafiam o sistema jurídico a acompanhar essas mudanças. Ademais, as dificuldades de rastreamento dos perfis ou da localização desses criminosos que atuam no âmbito virtual, evidenciam as limitações e os grandes desafios impostos para punir essas condutas e até de desenvolver mecanismos eficazes de prevenção as novas modalidades de crimes virtuais que surgem todos os dias.

O Capítulo II Discute as principais barreiras que as autoridades enfrentam ao investigar crimes online. Mostra como o anonimato na internet, o uso de VPNs e a ocultação de endereços IP que dificulta a identificação dos culpados. Detalha as

restrições técnicas que afetam a coleta e a manutenção de evidências digitais, além dos desafios trazidos pelo Marco Civil da Internet. O texto também aborda a identificação de quem comete os crimes e a relevância dos logs e das gravações eletrônicas nas investigações.

O Capítulo III Discute a atuação das plataformas digitais no combate às fraudes cibernéticas apresentando métodos que a legislação criou para tentar combater as práticas ilícitas como a LGPD e o Marco Civil da Internet, apontando os limites entre a colaboração entre autoridades e órgãos. Examina ainda uma utilização de meios mais rigorosos para a proteção dos dados, bem como avalia a efetividade da atuação das plataformas digitais no combate e repressão das fraudes cibernéticas.

O Capítulo IV se trata especificamente sobre a efetividade do direito penal no Estado do Mato Grosso, apontando um panorama dos crimes cibernéticos nesse Estado, cujas fraudes cibernéticas tem o segundo maior índice de golpes do país, diante desse alarmante crescimento o TJMT passou a desenvolver campanhas, cartilhas preventivas relacionadas ao denominado golpe do falso advogado, com o intuito de não só alertar a população sobre as práticas fraudulentas, como também analisar os casos concretos.

O Capítulo V apresenta uma análise crítica da efetividade do Direito Penal apresentando a eficiência da legislação vigente no enfrentamento dos crimes digitais, destacando os avanços normativos trazidos por leis recentes, como exemplo a Lei 15.397/2026, além de evidenciar as lacunas existentes no combate às fraudes eletrônicas, principalmente diante da rapidez da tecnologia e da dificuldade da produção probatória.

Apresenta casos concretos, tanto no âmbito nacional, quanto no Estadual que exemplificam a gravidade do fenômeno e as respostas jurídicas e sociais que têm sido implementadas. São discutidas tendências jurisprudenciais e os principais desafios enfrentados na aplicação da lei, especialmente no que concerne à identificação dos autores dos golpes e à efetividade das decisões judiciais.

Portanto, este estudo buscou contribuir para o debate acadêmico e jurídico sobre a proteção das vítimas no ambiente digital e a necessária evolução do marco normativo brasileiro, buscando garantir um espaço virtual mais seguro e respeitoso.

1.1 Problematização

Diante do aumento das fraudes cibernéticas, especialmente o golpe do falso advogado em plataformas digitais, até que ponto o Direito Penal brasileiro se mostra efetivo na prevenção e repressão dessas práticas criminosas?

1.2 Justificativa

A escolha do tema “O Golpe do Falso Advogado nas Plataformas Digitais: Análise da Efetividade do Direito Penal Brasileiro Frente às Fraudes Cibernéticas” justifica-se pela crescente incidência de crimes praticados em ambientes virtuais, especialmente aqueles que exploram a confiança e a vulnerabilidade das vítimas. O golpe do falso advogado representa uma dessas práticas, em que os criminosos, utilizando-se de ferramentas digitais, se passam por profissionais da advocacia para obter vantagens ilícitas. Trata-se de um problema relevante não apenas por seus impactos financeiros, mas também pelos danos emocionais e sociais causados às vítimas, que frequentemente se encontram em situações de fragilidade.

1.3 Hipóteses

Apesar das recentes atualizações para combater e ampliar as medidas contra as fraudes cibernéticas, como a lei 14.155/2021, o direito penal brasileiro ainda se mostra parcialmente ineficaz no combate do golpe do falso advogado em plataformas digitais, em razão da dificuldade de investigação, da exposição dos dados pessoais em processo que são públicos, da produção de provas eletrônicas e da limitada cooperação das plataformas digitais, sendo necessária a adoção de medidas legislativas, investigativas e preventivas complementares para garantir maior proteção ás vítimas.

1.4 Objetivos

1.4.1 Geral

Analisar a efetividade do Direito Penal brasileiro no enfrentamento das fraudes cibernéticas, com foco no golpe do falso advogado.

1.4.2 Específicos

Os objetivos específicos desta pesquisa consistem em identificar os dispositivos do Direito Penal brasileiro aplicáveis aos crimes cibernéticos previstos no Código Penal, tais como estelionato, estelionato digital, falsidade ideológica, uso de documento falso e associação criminosa, entre outros. Busca-se, ainda, examinar as principais dificuldades enfrentadas nas investigações criminais envolvendo delitos praticados no ambiente digital, especialmente aquelas relacionadas ao rastreamento de endereços IP, ao anonimato dos agentes e à obtenção e preservação de provas digitais. Além disso, pretende-se discutir a responsabilidade das plataformas, na prevenção do golpe do falso advogado, analisando sua atuação na adoção de mecanismos de segurança, na colaboração com as autoridades competentes e na mitigação dos riscos decorrentes dessas práticas criminosas.

CAPÍTULO 1: O GOLPE DO FALSO ADVOGADO E SUA INSERÇÃO NOS CRIMES CIBERNÉTICOS

1.1 Evolução dos crimes cibernéticos

A evolução dos crimes cibernéticos está diretamente ligada ao crescimento do avanço tecnológico. Ao final dos anos 1950, a Internet não passava de um projeto embrionário, o termo “globalização” não havia sido cunhado e a transmissão de dados por fibra óptica não existia. (PINHEIRO, 2026). Informação, nesse contexto, era um item valioso e com pouco acesso. Nessa época o mundo jurídico se desenvolvia por meios tradicionais como papel e caneta.

Os primeiros crimes cibernéticos surgiram na década de 1960, nos Estados Unidos, inicialmente relacionados a práticas como sabotagem e espionagem por meio de computadores. Na década de 1970, passaram a ser objeto de estudos científicos, e, a partir dos anos 1980, houve significativa intensificação dessas condutas, especialmente com fraudes bancárias, pirataria de software e outras práticas ilícitas no ambiente digital (Câmara dos Deputados do Brasil, 2006).

Conforme leciona Tarcísio Teixeira, o avanço tecnológico e a digitalização das relações sociais ampliaram o alcance das condutas humanas, possibilitando também o surgimento de novas práticas criminosas no ambiente virtual. Nesse cenário, o Direito Digital assume papel fundamental na adaptação do ordenamento jurídico, especialmente quanto à necessidade de instrumentos eficazes para lidar com os crimes cibernéticos e a produção de provas digitais (TEIXEIRA, 2025, p. 6).

Diante deste cenário, observa-se que a evolução dos crimes cibernéticos acompanha diretamente o desenvolvimento da era tecnológica, tornando cada vez mais aperfeiçoados, além de classificar os métodos deixando assim mais difícil de serem reconhecidos e defrontados pelo Estado.

1.2 Estelionato digital no Direito Penal brasileiro

O crime de estelionato está previsto no artigo 171 do Código Penal Brasileiro (Decreto-Lei nº 2.848/1940), consiste em obter vantagem ilícita para si ou para outrem, causando prejuízo alheio, induzindo ou mantendo alguém em erro.

Deste modo, o artigo não comportava as fraudes eletrônicas, com isso, passou por relevantes transformações legislativas, especialmente com a promulgação da Lei nº 14.155/2021. Além disso, passou a classificar particularmente o estelionato praticado em ambiente cibernético, nos § 2º-A e 2º-B, do artigo 171 do Código Penal.

É válido ressaltar que, em 16 de novembro de 2020, foi lançado oficialmente pelo Banco Central do Brasil o PIX, uma ferramenta de transferências bancárias que tinha como intuito tornar as operações mais rápidas e menos burocráticas, diferentemente do DOC e TED, ferramentas disponíveis até o momento, as quais possuíam limite máximo de transferência e horário específico para que o dinheiro fosse depositado na conta, sendo processadas no mesmo dia apenas se realizadas até às 17 horas.

Contudo, a implementação dessa ideia trouxe à tona consequências imprevistas, além de contribuir para a facilitação das transações financeiras, também colaborou para o aumento expressivo de fraudes no ambiente digital.

Nesse sentido, verifica-se uma crescente evolução nas tentativas de golpes em comparação com o ano de 2021, demonstrando uma enorme vulnerabilidade dos usuários frente às novas modalidades de crimes cibernéticos (PSafe, 2022).

Dados publicados em agosto de 2025, pelo Anuário Brasileiro de Segurança Pública, apontaram um aumento de 17% nos casos de estelionato por meio eletrônico. Para endurecer as regras o anuário apontou que o Senado está analisando um projeto de lei (PL 4161/2020), que muda o código para aumentar em dois terços a pena para quem comete crimes de estelionato e de fraude no comércio por meio da internet (Anuário Brasileiro de Segurança Pública, 2024).

Conforme alterações promovidas pela Lei nº 14.155/2021, a referida lei tinha como objetivo tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet, com o intuito de definir a competência em modalidades de estelionato figurado no ciberespaço, denominado “fraude eletrônica”, sob a seguinte disposição:

Fraude eletrônica

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

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

Cumpre mencionar que, o Congresso Nacional sancionou recentemente a Lei 15.397/2026, publicada em 30 de abril de 2026, a qual passou a prever a chamada "cessão de conta laranja", incluindo no art. 171, § 2º, inciso VII, do Código Penal a conduta de quem "cede, gratuita ou onerosamente, conta bancária para que nela transitem recursos destinados ao financiamento de atividade criminosa ou que dela sejam fruto".

Essas inovações demonstram que, a legislação vem tentando se atualizar conforme a evolução dos crimes cibernéticos acontece.

1.3 Tipificação penal aplicável ao golpe do falso advogado

O intitulado "Golpe do Falso Advogado", não possui tipificação penal própria no sistema jurídico, sendo enquadrado em tipos penais já previstos no código, sendo adaptado conforme as características da atitude dos criminosos.

Considerando que o crime de estelionato de forma eletrônica, já foi tratado no tópico anterior, neste, vamos tratar de outros tipos penais que também se encaixam na conduta aplicada pelos criminosos nestes casos.

Dentre os variados tipos penais que se pode encaixar neste tema, temos o crime de falsa identidade que está tipificado no artigo 307 do Código Penal:

Falsa identidade

Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. (Código Penal)

Para a configuração do delito, é essencial o dolo, que tenha a finalidade específica de obter vantagem ou causar dano, neste caso não será admitida a modalidade culposa, pois o delito se consuma no instante que o agente atribui para si ou para outrem identidade falsa com o fim de obter vantagem ou causar dano, mesmo que esses objetivos não sejam alcançados (REIS; ELTZ, 2022). O referido procedimento é vital para a concretização do golpe, pois o agente utiliza da confiança da vítima na atuação do capacitado profissional para obter a vantagem.

Ademais, podemos encaixar em algumas condutas o crime de invasão de dispositivo informático, que está previsto no artigo 154-A do CP[1], que foi incluído pela Lei nº 12.737/2012, tal conduta consiste em "invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismos de segurança com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita (CABETTE, 2021).

Constata-se também, a prática do delito de associação criminosa que está previsto no artigo 288 do Código Penal, uma vez que esses golpes são frequentemente executados por grupos organizados, com divisão de tarefas e uma estrutura minimamente articulada, evidenciando a profissionalização da atividade criminosa no ambiente digital.

Em determinados casos, a depender do grau de organização e da complexidade da atuação dos agentes, pode haver ainda a configuração do crime de organização criminosa, previsto na Lei nº 12.850/2013, tendo em vista que o §1º do artigo 1º da referida lei conceitua organização criminosa como a associação de quatro ou mais pessoas estruturalmente ordenadas, caracterizado pela divisão de tarefas, com o objetivo de obter vantagem de qualquer natureza.

Sob essa perspectiva, observa-se que muitos desses golpes ultrapassam a atuação individual, sendo praticados por grupos organizados que utilizam estratégias estruturadas para a obtenção de vantagens ilícitas no ambiente digital.

[1] "Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita." (Art. 154-A do Código Penal).

Diante disso, nota-se que o golpe do falso advogado, apesar de ter como base o estelionato eletrônico, abrange um conjunto de ações penalmente relevantes que, quando combinadas, aumentam a reprovabilidade da conduta.

1.4 *Modus operandi* nas plataformas digitais.

O golpe do falso advogado demonstra um *modus operandi* estruturado e sofisticado, pois utiliza meios eletrônicos para facilitar e ampliar o alcance dos criminosos a informações privilegiadas.

Conforme o Tribunal Regional Federal da 3ª Região (TRF3, 2025), a fraude ocorre em etapas da seguinte maneira, em primeiro lugar os criminosos acessam bancos de dados públicos, plataformas processuais ou redes ilícitas para reunir informações detalhadas das vítimas – como nome completo, CPF, número de processos, valores, tipo de ação e principalmente o nome do advogado constituído, essas informações darão maior credibilidade aos agentes no momento de aplicar o golpe.

Na sequência, ocorre o contato com a vítima (TRF3, 2025), geralmente por meio de aplicativo de mensagens, como o WhatsApp, neste momento os criminosos se passam pelo advogado constituído nos autos da vítima, utilizando os dados captados, neste momento são aplicadas técnicas como a engenharia social[2], senso de urgência e a utilização de linguagem técnico-jurídica, com o intuito de induzir a vítima ao erro (TRF3, 2025).

Por fim, há a solicitação de pagamento indevidos, sendo comum a exigência de valores “antecipados” para a liberação dos supostos créditos judiciais. Entre as justificativas apresentadas, destacam-se: taxa de desbloqueio, despesas cartorárias, taxa de transferências, imposto de renda, novo imposto e etc. A urgência nesses casos é um fator predominante para a aplicação do golpe, pois os criminosos alegam que, caso não haja o pagamento, os valores que as vítimas teriam a receber desses processos serão bloqueados ou retornarão aos cofres públicos (TRF3, 2025), esses pagamentos são solicitados para conta de terceiros, geralmente com nomes de pessoas ou empresas de fachada e, após, a realização da transação, os criminosos bloqueiam a vítima e encerram o contato (TRF3, 2025).

[2] Engenharia social: técnica utilizada por criminosos para manipular psicologicamente a vítima, explorando confiança, medo ou urgência, com o objetivo de obter informações ou induzir a prática de determinadas ações.

É válido ressaltar, que conforme apontado pelo Tribunal Regional Federal da 3ª Região (TRF3, 2025), há cenários que os criminosos chegam a usar vídeos gravados, áudios com linguagem jurídica, com o objetivo de simular a presença legítima do profissional ou do escritório, dando uma maior credibilidade à fraude.

1.4 Vulnerabilidade das vítimas no ambiente virtual

A violência digital vem sendo reconhecida como uma grave violação de direitos fundamentais. Nesse sentido, destaca-se que “a violência digital constitui uma violação direta dos direitos humanos fundamentais, incluindo o direito à privacidade e à dignidade da pessoa humana” (RIVELLI, 2025, p. 14).

A vulnerabilidade das vítimas assume papel central na compreensão da dinâmica delitiva, especialmente em fraudes como o chamado “golpe do falso advogado”. Conforme leciona Patrícia Peck a disseminação de desinformação ou discursos de ódio, de certa maneira causa danos irreparáveis às vítimas, não só financeiramente, pois traz consigo uma variável astronômica e incontrolável (PINHEIRO, 2026).

O golpe do falso advogado, utiliza vínculos familiares, necessidade de urgência, para ludibriar as vítimas e usar da vulnerabilidade social, para obter vantagem imprópria, e enganar as vítimas, os agentes utilizam de roteiros estruturados e dados verídicos, aplicando métodos como o *phishing* e o *spear phishing*. (MPSC, 2026).

De acordo com a *Fortinet*, o *phishing* e o *spear phishing* são definidos como:

> Spear phishing é um método de ataque cibernético que os hackers usam para roubar informações confidenciais ou instalar malware nos dispositivos de vítimas específicas. Os ataques de spear phishing são altamente direcionados, extremamente eficazes e difíceis de prevenir. Já o Phishing é um termo amplo para ataques enviados a várias pessoas na tentativa de enganar o maior número possível de vítimas. Ataques de phishing envolvem um e-mail falsificado que pretende ser de um remetente ou organização genuína. A mensagem contém um link que, quando os destinatários clicam nele, solicita que eles insiram suas informações pessoais e, em seguida, baixam malware em seu dispositivo. (Fortinet, 2026)

No contexto jurídico, essa vulnerabilidade apresenta desafios consideráveis à repressão penal, pois a consumação do crime frequentemente depende da cooperação não intencional da própria vítima. Isso não isenta o criminoso de sua responsabilidade, mas destaca a urgência de políticas públicas focadas na

conscientização digital, além de exigir que as plataformas digitais implementem mecanismos de proteção mais eficientes.

CAPÍTULO 2 – DIFICULDADES INVESTIGATIVAS NOS CRIMES CIBERNÉTICOS

2.1 Anonimato e rastreamento de IP

O anonimato no ambiente virtual constrói um dos grandes desafios na investigação e cumprimento da lei nos crimes cibernéticos. Embora a Constituição Federal assegure a livre manifestação do pensamento, o artigo 5º, inciso IV, estabelece que essa liberdade é garantida, sendo vedado o anonimato. Assim, o dispositivo constitucional busca impedir que indivíduos se escondam por trás do anonimato para praticar atos ilícitos sem responsabilização.

No ambiente digital, nota-se um anonimato relativo, pois os criminosos utilizam mecanismos tecnológicos capazes de dificultar sua identificação, como os VPNs pois com essas redes virtuais privadas é possível criar um "túnel" criptografado que mascara o IP e a geolocalização, dificultando o rastreamento da origem da conexão, além dos VPNs, podemos citar os servidores proxy, redes públicas de acesso à internet, todas essas são técnicas de mascaramento de dados. Esses sistemas permitem que os agentes ocultem ou dificultem sua localização real o que compromete a eficácia das investigações.

O autor Guilherme de Souza Nucci destaca que, no processo penal, a identificação do autor do delito deve estar amparada por um conjunto probatório sólido, não sendo suficiente a existência de indícios isolados para fundamentar a responsabilização penal[3].

No caso do “golpe do falso advogado”, as dificuldades decorrentes do anonimato digital também impactam diretamente a atuação das instituições financeiras. Os criminosos, ao utilizarem mecanismos de ocultação de identidade, como VPNs e contas abertas com dados fraudulentos, dificultam a vinculação entre o autor do delito e as transações realizadas. Embora os bancos disponham de sistemas de monitoramento e prevenção a fraudes, a identificação do responsável pelas movimentações

[3] NUCCI, Guilherme de Souza. *Código de Processo Penal Comentado*. 17. ed. Rio de Janeiro: Forense, 2023.

financeiras nem sempre é imediata, especialmente quando os acessos são realizados por meio de endereços IP mascarados ou dispositivos não rastreáveis.

Nesse cenário, o rastreamento do IP, embora relevante, mostra-se insuficiente de forma isolada, exigindo a integração de dados bancários, registros de conexão e outros meios de prova para a efetiva identificação dos agentes envolvidos.

No ordenamento jurídico brasileiro, o Marco Civil da Internet estabelece proteções à privacidade e dos dados dos usuários no uso da internet. O artigo 10º, §1º, do Marco Civil da Internet, estabelece que o provedor responsável pela guarda dos registros somente será obrigado a disponibilizar informações que possam contribuir para a identificação do agente mediante ordem judicial. Nos termos do dispositivo:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º [...]. (Planalto, 2014).

Deste modo, evidencia-se que a identificação dos criminosos está condicionada à prévia autorização judicial, demonstrando que o ordenamento jurídico busca o equilíbrio entre a proteção de dados e a necessidade de investigação das referidas práticas criminosas.

2.2 Limitações técnicas da investigação criminal

As investigações de crimes cibernéticos enfrentam diversas dificuldades técnicas que comprometem a persecução penal do delito, especialmente em razão do crescimento das tecnologias utilizadas pelos agentes, pois os crimes cometidos em ambientes virtuais podem deixar rastros imateriais, o que compromete a investigação.

Neste sentido, o autor Hoffmann-Riem Wolfgang, diz que:

> Há muitas possibilidades de coleta de dados e posterior processamento pelas autoridades privadas e públicas.1 Aqui, gostaríamos de destacar alguns tipos importantes de coleta e processamento de dados – um exemplo é o chamado rastreamento on-line. Isso se refere à observação eletrônica

> (registro e avaliação) do comportamento digital de uma pessoa. Fontes para rastreamento são conteúdo de comunicação, mas também metadados (como o Hypertext Transfer Protocol [HTTP], endereços IP). O rastreamento é utilizado em particular como preparação para a criação de perfis2, mas também para a segmentação. (Hoffmann-Riem Wolfgang, 2022).

As limitações técnicas da investigação criminal também devem observar os direitos e garantias fundamentais previstos no ordenamento jurídico brasileiro.

Nesse contexto, a atuação policial encontra limites relacionados à legalidade, proporcionalidade e proteção da privacidade dos investigados, especialmente no que se refere à obtenção de provas digitais e realização de medidas invasivas no ambiente virtual. Conforme destaca Galvão & Silva Advocacia, a investigação criminal deve ocorrer “dentro dos procedimentos e limites estabelecidos pela legislação brasileira”, respeitando as garantias constitucionais dos indivíduos envolvidos.

2.3 Identificação da autoria delitiva

A identificação de autoria delitiva nos crimes digitais constitui um dos maiores impasses do Direito Penal, especialmente pelas peculiaridades existentes no âmbito digital, marcado pelas dificuldades investigativas, rastros imateriais o que compromete a investigação e consequentemente a identificação da autoria delitiva.

Diferentemente dos “crimes tradicionais”, em que a materialidade e autoria devem ser demonstrados por prova testemunhal, oral ou por meios físicos, os crimes digitais devem ser demonstrados através de rastreamento de IP, informações armazenadas por aplicativos ou instituições financeiras.

É válido ressaltar que, os *logs* são importantes meios de prova computacional, pois de acordo com o Marco Civil da Internet comentado em seu artigo 13º eles: “permitem a identificação de quem praticou certo ato em ambiente eletrônico, incluindo ilícitos de cunho civil e penal. O *log* também é conhecido como *log* de dados.” Esse sistema é capaz de visualizar o histórico ou os rastros deixados pelos agentes.

Ocorre, que as entidades públicas tem prazo de 1 (um) ano para solicitar esses dados sigilosos das conexões, dificultando a coleta de informações dado a lentidão do andamento processual no Brasil.

Somado aos elementos técnicos e informáticos, a investigação criminal pode demandar outros meios de prova aptos à identificação do autor do delito, dentre eles o reconhecimento de pessoas.

Quando se fizer necessário realizar o reconhecimento de pessoa, proceder-se-á da maneira entabulada no artigo 226 do Código de Processo Penal que diz:

> Art. 226. Quando houver necessidade de fazer-se o reconhecimento de pessoa, proceder-se-á pela seguinte forma: I - a pessoa que tiver de fazer o reconhecimento será convidada a descrever a pessoa que deva ser reconhecida; II - a pessoa, cujo reconhecimento se pretender, será colocada, se possível, ao lado de outras que com ela tiverem qualquer semelhança, convidando-se quem tiver de fazer o reconhecimento a apontá-la; III - se houver razão para recear que a pessoa chamada para o reconhecimento, por efeito de intimidação ou outra influência, não diga a verdade em face da pessoa que deve ser reconhecida, a autoridade providenciará para que esta não veja aquela; IV - do ato de reconhecimento lavrar-se-á auto pormenorizado, subscrito pela autoridade, pela pessoa chamada para proceder ao reconhecimento e por duas testemunhas presenciais. Parágrafo único. O disposto no no III deste artigo não terá aplicação na fase da instrução criminal ou em plenário de julgamento. (Código de Processo Penal).

Destarte, conforme leciona Rogério Greco, a prova no processo penal deve ser analisada com cautela, especialmente quando baseada em elementos indiretos, sob pena de se atribuir responsabilidade penal sem a devida certeza quanto à autoria. Ainda de acordo com Rogério Greco, as provas devem ser analisadas com cautela, especialmente quando só há provas imateriais ou elementos que se mostrem indiretos, pois para o Direito Penal punir o agente é necessário provas materiais que comprovem sua conduta.

Neste contexto, o ordenamento jurídico brasileiro, como o Marco Civil da Internet estabelece diretrizes importantes para obtenção e os tratamentos de dados como a guarda de registros de acesso e a responsabilidade de danos decorrentes de conteúdo gerado por terceiros.

CAPÍTULO 3 – A ATUAÇÃO DAS PLATAFORMAS DIGITAIS NO COMBATE ÀS FRAUDES

3.1 Marco Civil da Internet e a LGPD.

A partir da chegada da internet para sua utilização em sociedade, uma das principais preocupações jurídicas no Brasil era como ela se encaixaria no âmbito do direito penal. Os crimes praticados através da internet têm muita repercussão social, principalmente quando a vítima é uma pessoa ou ente público. Então, a criminalidade virtual sempre foi um receio para a sociedade, e, consequentemente, um objeto de atenção aos profissionais do direito penal e dos legisladores. A partir disso começou a se discutir quais os direitos e deveres de uma pessoa que usa a internet, para definir o que se pode ou não fazer na web, como exemplos de métodos para combater os crimes oriundos da chegada da internet temos o Marco Civil da Internet e a LGPD.

O Marco Civil da Internet, também ficou conhecido como, “Constituição da internet”, tendo em vista que foi criado um site para que pessoas de vários setores contribuíssem na elaboração da Lei, para se chegar a um consenso que abrangeria a maior parte das pessoas possíveis, visto que a finalidade era criar uma Lei que determinaria os rumos a serem seguidos no que concerne ao uso da internet no Brasil, conforme aduz George Leite e Ronaldo Lemos:

> Outro aspecto importante do processo do Marco Civil foi a transparência. No processo de consulta pública, os participantes poderiam ver em tempo real a contri- buição de todos os outros participantes. Desse modo, criou-se um modelo propício ao embate racional de ideias. Considerando-se que os participantes do processo de consulta do Marco Civil envolviam indivíduos, usuários, bibliotecários, tradutores, empresas de tecnologia, provedores de serviços de internet, empresas de telecomu- nicações, radiodifusores, associações de classe e assim por diante, construiu-se um verdadeiro fórum híbrido, onde todos tinham igualdade de vozes. Empresas de tele- comunicações contribuíam de forma aberta e lado a lado com usuários individuais da rede. Os argumentos de um e de outro competiam por sua fundamentação, não por sua origem ou autoridade. Além disso, a possibilidade de se enxergarem as posições públicas de cada participante serviu para ampliar e qualificar o debate. (Leite e Lemos, 2014, p. 6).

Assim, é importante ressaltar que o Marco Civil da Internet não dispõe de tipos penais. A lei, tem o condão de regular a utilização da internet no Brasil através de princípios, direcionando também, instruções para que o Estado possa atuar.

E seus pilares estão elencados no art. 3º, vejamos:

> 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. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (Lei 12.965, de 23 de abril de 2014)

Assim, temos a Lei Geral da Proteção de Dados – LGPD, sendo a Lei nº 13.709, de 14 de agosto de 2018, foi sancionada com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Com isso a lei provocou diversas mudanças em empresas e nos segmentos do mercado, dispondo a respeito do tratamento de dados pessoais. A LGPD é uma regulamentação do tratamento de dados pessoais, para atingir qualquer atividade feita com dados pessoais, desde o momento que os dados entram no banco de dados de uma empresa, até o instante que os dados saem desse “banco de dados” (PALHARES; PRADO; VIDIGAL, 2021).

É válido ressaltar que, a LGPD trouxe mais segurança com suas medidas de proteção, como podemos ver no artigo 46 da lei, vejamos:

> 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. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (Lei 13.709, de 14 de agosto de 2018)

Desta maneira, em se tratando de proteção de dados, privacidade de usuários, podemos dizer que o Direito Penal está tentando acompanhar o rápido crescimento dos crimes digitais, colocando em aplicação leis que têm o objetivo de proteger os

indivíduos tornando as informações ou rompimentos destas um ambiente mais seguro e com medidas de proteção.

3.2 Limites da colaboração com autoridades

A colaboração entre autoridades e órgãos de persecução penal deve observar limites impostos pelo Estado Democrático de Direito, especialmente quanto à preservação das garantias fundamentais do investigado. Fábio da Silva Bozza sustenta que a expansão do direito penal contemporâneo tem provocado a flexibilização de institutos processuais e a mitigação de direitos defensivos, transformando o processo penal em instrumento de gestão de riscos sociais e controle estatal. Nesse contexto, a atuação cooperativa entre instituições não pode justificar restrições desproporcionais ao contraditório, à ampla defesa e à legalidade, sob pena de comprometer a própria função garantista do direito penal (BOZZA, 2015).

Observa-se que, o Direito impõe limites na colaboração com autoridades, pois a atividade excessiva do poder estatal pode resultar em grandes infrações das garantias fundamentais que são de direitos do investigado. Desta maneira, a atuação conjunta dos órgãos obtém dificuldades dentro do contexto, pois como já dito não se pode exceder ou quebrar a preservação do devido processo legal,

Conforme destaca Heribert Prantl, citado por Fábio da Silva Bozza, “O direito penal do inimigo é a retirada de todas as garantias jurídicas que foram dadas ao homem desde o ato-habeas-corpus de 1679, desde a famosa lei inglesa para a proteção da liberdade pessoal. Quando o estado não trata mais de acordo com o direito as pessoas que se desviaram do direito, ele não é mais um estado de direito” (PRANTL apud BOZZA, 2015).

Mesmo diante da necessidade de repressão à criminalidade, o poder punitivo estatal não é absoluto, encontrando limites nos princípios constitucionais e nas garantias fundamentais do indivíduo. Dessa forma, a colaboração entre autoridades deve respeitar o devido processo legal, a proporcionalidade e a dignidade da pessoa humana, evitando abusos no exercício da atividade investigativa e punitiva (MOTA, 2021).

A atuação do Estado na investigação criminal deve observar os limites constitucionais que impeçam os excessos no exercício do poder que punitivo, pois assim, a colaboração entre as autoridades não possa ultrapassar os parâmetros legais e nem justificar medidas rigorosas durante a investigação criminal.

3.3 Medidas de prevenção e segurança

As medidas de prevenção e segurança, possuem relevantes funções na defesa e amparo na vulnerabilidade dos dados digitais. Uma utilização de meios mais rigorosos para a proteção dos dados, como criptografia, identificação de chamadas de Spam, *Phishing*, *Malware*[4] e etc.

Conforme destaca Ana Frazão, os programas de *compliance*[5] e segurança da informação possuem importante função preventiva, uma vez que "se encaixam precisamente nessa ideia de contenção de riscos, de criar uma organização compatível com os riscos assumidos, a fim de evitá-los". Nesse sentido, as medidas de prevenção e segurança contribuem para a proteção de dados e para a redução de vulnerabilidades no ambiente digital (FRAZÃO, 2023, p. 10).

No contexto do golpe do falso advogado, as medidas de prevenção e segurança torna-se indispensáveis para reduzir as ocorrências de fraudes que vem sendo praticadas mediante a utilização indevida dos perfis profissionais dos advogados, assim podemos destacar meios para verificar a veracidade dos fatos, destacam-se a verificação da autenticidade do profissional por meio dos canais oficiais da OAB, a confirmação de informações processuais diretamente dos tribunais.

Os golpistas usam nomes e registros verdadeiro dos advogados para dar veracidade ao golpe, por isso a vítima não deve fornecer dados bancários, senhas, enviar pix, fazer depósito, em troca de "liberação de valores", pois Tribunal de Justiça não cobra valores antecipados para "liberar" valores de indenizações ou qualquer

[4] Definição de Malware: é um software mal-intencionado feito para interromper, prejudicar ou obter acesso não autorizado a sistemas de computador. Criminosos cibernéticos usam malware para infectar dispositivos, roubar dados, obter credenciais bancárias, vender acesso a recursos computacionais ou informações pessoais ou extorquir vítimas.

[5] Compliance refere-se ao conjunto de práticas, regras, políticas e controles internos adotados por uma organização para garantir que ela opere em total conformidade com as leis vigentes, regulamentações do setor e seus próprios padrões

outro movimento processual antecipado. Além disso, escritórios de advocacia devem passar a alertar os clientes dos possíveis golpes e utilizar de telefones fixos, e-mails institucionais para contatar os clientes, visando dificultar a atuação de criminosos que se utilizam de engenharia social para obtenção de vantagens ilícitas.

3.4 Efetividade da atuação das plataformas

A função das plataformas digitais é essencial na luta contra delitos cibernéticos, especialmente no que diz respeito à prevenção de fraudes, à manutenção de dados eletrônicos e à colaboração com as instituições encarregadas da ação penal. Com a expansão das interações online e o uso de aplicativos de mensagens e mídias sociais, essas plataformas tornaram-se cruciais na troca de informações e nas operações que ocorrem no espaço virtual.

A colaboração entre plataformas digitais e autoridades investigativas nem sempre ocorre de maneira célere e eficiente, especialmente em situações que envolvem empresas estrangeiras ou servidores localizados fora do território nacional. Tal circunstância pode dificultar a obtenção de registros eletrônicos e dados necessários para identificação dos autores das fraudes virtuais. Conforme destaca Patrícia Peck Pinheiro, “a velocidade da tecnologia supera a capacidade de reação do Direito” (PINHEIRO, 2021).

Dentre todos esses impasses encontrados, é válido ressaltar que culpa o estelionatário por má-fé e a vítima por desatenção é mais fácil do que cobrar das plataformas digitais um aumento da segurança digital. Neste caso, podemos citar a plataforma WhatsApp, da qual tem meios suficientes para investir em segurança para seus usuários, fazendo uma verificação rigorosa de perfis, para que possa tentar diminuir as fraudes digitais.

Neste aspecto, conforme destacado por Guerra, “o golpe acontece em segundos, já a investigação leva dias, semanas ou meses”, cenário que evidencia o descompasso entre a rapidez das fraudes digitais e a capacidade estatal de investigação e responsabilização penal dos agentes envolvidos (MIGALHAS, 2026).

CAPÍTULO 4 – EFETIVIDADE DO DIREITO PENAL NO ESTADO DE MATO GROSSO

4.1 Panorama dos crimes cibernéticos no Estado do Mato Grosso

Os crimes cibernéticos vêm apresentando crescimento significativo no Estado de Mato Grosso, segundo pesquisa divulgada pelo Instituto DataSenado em parceria com a Nexus Pesquisa e Inteligência de Dados, Mato Grosso ocupa a segunda posição entre os Estados brasileiros com a maior incidência de golpes digitais, sendo que aproximadamente 28% da população mato-grossense relatou já ter sido vítima de algum tipo de fraude praticada no ambiente virtual. O Estado ficou atrás apenas de São Paulo, no qual cerca de 30% da população afirmou já ter sofrido golpe pela internet. (TOMASELLI, 2024).

A expressiva inserção de Mato Grosso no topo do ranking nacional de fraudes virtuais, está relacionada com o perfil socioeconômico do Estado, marcado pela forte atuação do Agronegócio e pela intensa circulação de expressivos ativos financeiros, fatores que transformam o Estado em um ambiente atrativo para criminosos.

Além dos grandes centros urbanos, é evidente que os crimes virtuais têm se espalhado também para cidades menores do interior do Estado, revelando a extensa disseminação das fraudes online em Mato Grosso. A ampliação do acesso à internet e das transações financeiras digitais permitiu que esses golpes virtuais impactassem diversas camadas sociais, abrangendo pequenos empresários, agricultores e consumidores que utilizam plataformas digitais nas suas atividades diárias.

Entre as atividades criminosas mais frequentes na esfera digital, destacam-se fraudes em contas bancárias, clonagem de aplicativos de mensagens, anúncios de venda fraudulentos, invasão de contas e golpes que visam a obtenção ilícita de informações pessoais e financeiras. Nesse contexto, os criminosos empregam métodos cada vez mais avançados para coletar dados das vítimas.

Em decisões recentes, o TJMT reconheceu a prática de estelionato eletrônico em fraudes realizadas por meio de aplicativos de mensagens e transferências bancárias digitais, destacando a utilização de mecanismos tecnológicos para induzir as vítimas ao erro. Além disso, o Tribunal vem analisando demandas relacionadas ao denominado “golpe do falso advogado”, evidenciando o aumento das fraudes praticadas mediante utilização indevida da imagem e dos dados profissionais de advogados no ambiente virtual (TJMT, 2026).

4.2 Atuação do Tribunal de Justiça de Mato Grosso e demais órgãos

Diante do crescimento dos crimes cibernéticos no Estado, o Tribunal de Justiça de Mato Grosso e os demais órgãos responsáveis pela persecução penal vêm intensificando medidas voltadas ao enfrentamento das fraudes praticadas no ambiente digital.

A atuação institucional ocorre por meio de decisões judiciais, campanhas de conscientização e fortalecimento das investigações relacionadas aos delitos eletrônicos, especialmente aqueles envolvendo estelionato digital e utilização indevida de dados pessoais (TJMT, 2025).

O Tribunal de Justiça de Mato Grosso exerce papel relevante na garantia da prestação jurisdicional e no enfrentamento das demandas relacionadas aos crimes virtuais. Conforme esclarece o próprio TJMT, a Justiça Estadual constitui a principal “porta de entrada” do Poder Judiciário, sendo estruturada em primeira e segunda instâncias, responsáveis pela análise e julgamento das demandas cíveis e criminais no âmbito estadual (TJMT, 2017).

Nesse sentido, o TJMT passou a desenvolver campanhas preventivas direcionadas à população, alertando acerca dos riscos relacionados ao denominado golpe do falso advogado. As ações possuem o objetivo de conscientizar os cidadãos sobre práticas fraudulentas realizadas por criminosos que utilizam indevidamente nomes, imagens e informações profissionais de advogados para induzir vítimas ao erro.

O Tribunal também orienta a população quanto à necessidade de confirmação das informações diretamente com os profissionais responsáveis pelos processos judiciais. (TJMT, 2025).

A Polícia Civil do Estado de Mato Grosso desempenha uma função importante no enfrentamento dos delitos cibernéticos, sobretudo através de apurações ligadas a fraudes online, acesso não autorizado a sistemas e golpes financeiros realizados em ambientes digitais.

A atuação das delegacias especializadas demonstra a necessidade de adaptação das instituições de segurança pública frente à crescente sofisticação das práticas criminosas realizadas no ambiente virtual (POLÍCIA CIVIL DE MATO GROSSO, 2025).

Neste contexto, podemos citar a Delegacia de Repressão a Crimes Informáticos (DRCI), que no Estado do Mato Grosso fica localizada na capital, na cidade de Cuiabá. Essa unidade é especializada em investigar delitos cometidos em ambiente virtual ou por meio de dispositivo eletrônico.

Apesar dos avanços institucionais e legislativos, ainda persistem dificuldades relacionadas à rapidez das transferências bancárias, ao anonimato digital e à complexidade na obtenção de provas eletrônicas, fatores que impactam diretamente a efetividade das investigações e da responsabilização penal dos agentes envolvidos (TJMT, 2026).

É válido ressaltar que, conforme cartilha elaborada pela Ordem dos Advogados do Brasil - Seccional Mato Grosso (OAB-MT)[6], a instituição lançou um material informativo apresentando como acontecem os denominados golpes do falso advogado, mostrando como evitar ser uma vítima e o que fazer caso seja enganado.

Além das medidas legislativas, o Poder Judiciário também tem adotado mecanismos tecnológicos para reforçar a segurança no acesso de dados processuais. Neste sentido, destaca-se a implementação do novo sistema de autenticação para

[6] ORDEM DOS ADVOGADOS DO BRASIL – SECCIONAL MATO GROSSO (OAB-MT). OAB-MT lança cartilha orientando população a não cair em golpes. Disponível em: https://www.oabmt.org.br/noticia/22369/oab-mt-lanca-cartilha-orientando-populacao-a-nao-cair-em-golpes.

acesso ao Processo Judicial Eletrônico (PJe)[7], que passou a exigir a validação por código gerado em aplicativo de celular. Segundo o CNJ (2025), “a medida de segurança desenvolvida pelo Conselho Nacional de Justiça (CNJ) contribui para evitar o golpe do falso advogado”.

4.3 Análise de casos concretos (golpe do falso advogado)

Uma aposentada de 66 anos, em tratamento contra o câncer, foi vítima do golpe do falso advogado, segundo o TJMT (2026), a mulher foi procurada via WhatsApp por criminosos que se passavam por sua advogada. Eles a informaram que ela teria valores a receber de uma suposta “ação judicial” e que, para receber a quantia, seria necessário participar de uma suposta audiência online para a liberação do valor. Durante a chamada de vídeo, os golpistas capturaram sua imagem para validar a biometria facial junto ao banco. Após isso, conseguiram acessar o aplicativo bancário e realizar um empréstimo bancário em nome da vítima.

Em julgamento realizado pela Primeira Câmara de Direito Privado do TJMT do Processo nº 1039453-05.2025.8.11.0041, foi reconhecida a nulidade de empréstimos consignados de forma fraudulenta, após criminosos se passarem pela advogada da vítima, a decisão se baseou na Súmula 479 do Superior Tribunal de Justiça, que estabelece a responsabilidade objetiva dos bancos nesses casos, “As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.”.

Com a decisão, o contrato foi declarado nulo pois, para o relator a validação por biometria facial não afasta irregularidades, além disso, o banco deverá pagar R$ 5.000,00 (cinco mil reais) por danos morais (TJMT, 2026).

[7] O PJe é uma plataforma digital desenvolvida pelo CNJ em parceria com diversos Tribunais e conta com a participação consultiva do Conselho Nacional do Ministério Público, Ordem dos Advogados do Brasil, Advocacia Pública e Defensorias Públicas. O PJe caracteriza-se pela proposição da prática de atos jurídicos e acompanhamento do trâmite processual de forma padronizada, mas considerando características inerentes a cada ramo da Justiça.

Além disso, em outro julgamento realizado também pela Primeira Câmara de Direito Privado do TJMT (Processo nº 1016790-88.2025.8.11.0000), a decisão envolvendo indícios do denominado “golpe do falso advogado”, o Tribunal de Justiça de Mato Grosso determinou a suspensão imediata dos descontos referentes a empréstimo consignado supostamente contratado mediante fraude eletrônica.

No caso, a vítima alegou ter sido induzida a fornecer informações pessoais após contato realizado por criminosos que se passaram por profissionais da advocacia, circunstância que levantou dúvidas acerca da regularidade da contratação bancária. Ao analisar o caso, o TJMT entendeu estarem presentes elementos suficientes para demonstrar a probabilidade do direito da vítima e o risco de dano decorrente da continuidade dos descontos em benefício previdenciário, razão pela qual foi deferida medida liminar para suspensão da cobrança até o julgamento definitivo da demanda (MIGALHAS, 2025).

Os dois casos examinados correspondem apenas a uma fração das fraudes que realmente chegam ao sistema judiciário, visto que muitas vítimas não informam as autoridades sobre os golpes sofridos devido ao constrangimento, à vergonha ou ao medo de serem expostas. Essa situação resulta na subnotificação dos delitos cibernéticos e torna mais desafiador compreender a verdadeira extensão estatística dessas ações criminosas no espaço digital.

CAPÍTULO 5 – ANÁLISE CRÍTICA DA EFETIVIDADE DO DIREITO PENAL

5.1 Eficiência da legislação vigente

A eficiência da legislação vigente no enfrentamento dos crimes digitais deve ser analisada a partir de uma perspectiva crítica, que considere tanto os avanços normativos já incorporados ao ordenamento jurídico quanto os obstáculos práticos que ainda limitam a investigação, a persecução penal e a responsabilização dos agentes.

Sob essa perspectiva, o art. 70, § 4º, do Código de Processo Penal, o art. 171, § 2º-A, do Código Penal, a Lei nº 12.737/2012, a Lei nº 12.965/2014, a Lei nº 14.155/2021, a Lei nº 15.397/2026 e a Súmula nº 479 do Superior Tribunal de Justiça representam instrumentos relevantes para a compreensão da resposta jurídica brasileira diante das fraudes eletrônicas, dos delitos informáticos e das práticas criminosas realizadas em ambiente virtual.

Inicialmente, é possível afirmar que a legislação vigente se mostra eficaz em certa medida, sobretudo por reconhecer juridicamente a gravidade das condutas praticadas por meios eletrônicos. O art. 171, § 2º-A, do Código Penal, ao tratar do estelionato praticado mediante fraude eletrônica, representa importante avanço repressivo, pois diferencia a fraude tradicional daquela realizada com o emprego de redes sociais, contatos telefônicos, envio de mensagens, sistemas digitais, conforme art.171, §2º-A, do Código Penal, incluído pela Lei nº 14.155/2021.

A recente Lei nº 15.397/2026 reforçou o combate às fraudes digitais ao ampliar mecanismos de repressão penal relacionados aos crimes patrimoniais praticados por meio eletrônico, evidenciando a constante necessidade de atualização legislativa diante da evolução das tecnologias e das novas modalidades de golpes virtuais.

Além disso, a jurisprudência também demonstra preocupação com a proteção das vítimas de fraudes eletrônicas. O Tribunal de Justiça de Minas Gerais reconheceu a responsabilidade da instituição financeira diante da invasão do sistema bancário por hackers, entendendo que a falha na prestação do serviço autoriza a indenização por

danos morais decorrentes das movimentações eletrônicas fraudulentas (TJMG, Apelação Cível nº 1.0105.09.324823-2/001, Rel. Des. Pereira da Silva, 10ª Câmara Cível, j. 28 fev. 2012, apud PINHEIRO, 2021, p. 712).

Sob o mesmo entendimento, o Superior Tribunal de Justiça tem reafirmado a necessidade de proteção das vítimas diante das fraudes praticadas em ambiente digital. Conforme entendimento no julgamento do REsp 2.222.059/SP, de relatoria do Ministro Ricardo Villas Bôas Cueva, a Terceira Turma do STJ reconheceu que as instituições têm o dever de criar mecanismos inteligentes capazes de identificar movimentações suspeitas, horários atípicos e transações fora do padrão do consumidor.

No âmbito do Tribunal de Justiça de Mato Grosso, o Tribunal de Justiça tem identificado a importância de resguardar aqueles que são vítimas de fraudes digitais, principalmente em casos que envolvem idosos em situação de vulnerabilidade. Seguindo esta linha, ao analisar o Agravo de Instrumento nº 1016790-88.2025.8.11.0000, a Primeira Câmara de Direito Privado do TJMT, constatou a existência de evidências sólidas relacionadas ao chamado “golpe do falso advogado” e determinou a suspensão mediante concessão de tutela provisória de urgência. A decisão leva em conta a vulnerabilidade da vítima.

Verifica-se que as normas ajudam efetivamente nas investigações criminais, mas não eliminam os principais entraves da persecução penal em ambiente virtual. A legislação fornece instrumentos para enquadramento jurídico das condutas, definição de competência, proteção de dados e responsabilização, mas a efetividade investigativa depende da capacidade de identificar os autores, rastrear movimentações, obter registros e vincular determinada conduta a uma pessoa concreta.

Entretanto, sua existência formal não garante, isoladamente, efetividade prática. A eficiência dessas normas depende da adequada aplicação pelos órgãos de persecução penal, da atuação célere e técnica na coleta de elementos informativos, da colaboração efetiva das plataformas digitais e instituições financeiras, do equilíbrio entre proteção de dados e investigação criminal e da capacidade do sistema jurídico de acompanhar a constante evolução dos crimes praticados em ambiente digital

5.2 Lacunas no combate às fraudes digitais

Apesar dos avanços institucionais, ainda persistem dificuldades relacionadas à rapidez das transferências bancárias, ao anonimato digital e à complexidade na obtenção de provas eletrônicas, fatores que impactam diretamente a efetividade das investigações e da responsabilização penal dos agentes envolvidos (TJMT, 2026).

Nesse aspecto, o Delegado da Polícia Civil do Estado do Paraná e titular da Delegacia de Estelionatos de Curitiba, Emmanoel David, ao abordar as dificuldades relacionadas à investigação dos crimes cibernéticos, destacou que:

> Esses crimes se tornaram mais frequentes porque a tecnologia democratizou tanto o acesso à informação quanto aos meios de fraude. Qualquer pessoa com conhecimento básico de internet pode adquirir ferramentas ilícitas na dark web e aplicá-las em escala. Além disso, o ambiente digital acelerou a comunicação e reduziu o senso de desconfiança — fatores que os criminosos exploram com maestria (DAVID, 2025).

A declaração do delegado evidencia que a expansão tecnológica, embora tenha proporcionado avanços nas relações digitais e ampliado o acesso à informação, também contribuiu para o aperfeiçoamento dos mecanismos utilizados na prática de fraudes eletrônicas. Nesse cenário, a facilidade de acesso a ferramentas ilícitas e a velocidade da comunicação digital tornam mais complexa a atuação dos órgãos responsáveis pela persecução penal dos crimes cibernéticos.

5.3 Influência das dificuldades investigativas e probatórias.

Conforme destacado por Migalhas, “arquivos eletrônicos podem ser facilmente alterados, apagados ou manipulados”, circunstância que dificulta a produção probatória nos crimes praticados no ambiente digital (MIGALHAS, 2025).

A produção de provas em delitos praticados por meios tecnológicos exige cuidados específicos relacionados à preservação da autenticidade, integridade e cadeia

de custódia dos elementos digitais, considerando que arquivos eletrônicos podem ser facilmente alterados, apagados ou manipulados.

Conforme o entendimento do Superior Tribunal de Justiça, são inadmissíveis as provas digitais sem registro documental acerca dos procedimentos adotados, para resguardar a integridade, autenticidade e da confiabilidade dos elementos informáticos. (STJ, 2023).

Os desafios envolvidos na coleta e manutenção de evidências digitais revelam que a eficácia do Direito Penal no combate aos delitos cibernéticos não se baseia apenas na existência de leis específicas, mas também na implementação de técnicas apropriadas para a investigação e obtenção de provas. Assim, a formação dos órgãos encarregados da persecução penal e a atualização dos métodos investigativos são fundamentais para assegurar uma resposta mais efetiva contra as fraudes realizadas no espaço virtual.

6. CONCLUSÃO

O presente trabalho analisou a efetividade do Direito Penal brasileiro no combate ao golpe do falso advogado, com enfoque nas dificuldades investigativas, na produção de provas digitais e na atuação das plataformas digitais no Estado de Mato Grosso, tendo como problema de pesquisa a identificação das dificuldades enfrentadas pelo Direito Penal para prevenir e reprimir essas práticas criminosas, bem como verificar até que ponto ele se mostra efetivo diante dos crimes digitais.

A hipótese inicialmente levantada, de que a legislação brasileira ainda apresenta limitações para enfrentar adequadamente os crimes cibernéticos, especialmente quanto à responsabilização dos agentes, à identificação dos autores e à obtenção de provas digitais, foi confirmada pela pesquisa realizada.

A análise da doutrina, da legislação e das decisões jurisprudenciais demonstrou que, embora existam importantes instrumentos normativos, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD), o Código Penal e alterações legislativas recentes voltadas ao combate às fraudes eletrônicas, ainda persistem obstáculos relevantes na investigação e repressão do golpe do falso advogado, sobretudo em razão do anonimato digital, da rápida disseminação das fraudes e da dificuldade de cooperação entre plataformas, instituições financeiras e órgãos de persecução penal.

Os estudos de caso e a jurisprudência analisada evidenciaram que o Poder Judiciário vem reconhecendo a gravidade dos crimes cibernéticos e ampliando a proteção às vítimas, porém ainda há desafios relacionados à uniformização das decisões, à celeridade na quebra de sigilo de dados e à efetiva responsabilização dos envolvidos nas fraudes eletrônicas.

O problema de pesquisa que norteou este trabalho foi respondido de maneira satisfatória ao longo da investigação, demonstrando que, apesar dos avanços legislativos e jurisprudenciais, ainda existem lacunas que comprometem a efetividade do enfrentamento penal dos crimes digitais. Verificou-se a necessidade de aprimoramento legislativo, fortalecimento das técnicas investigativas especializadas e maior integração entre os órgãos de segurança pública, o Poder Judiciário, as plataformas digitais e as instituições financeiras.

Conclui-se que o combate ao golpe do falso advogado demanda não apenas a aplicação rigorosa das normas já existentes, mas também constante atualização legislativa, investimento em capacitação tecnológica e desenvolvimento de políticas públicas preventivas voltadas à educação digital da população, a fim de reduzir a incidência das fraudes eletrônicas e promover maior segurança no ambiente virtual. Declaração de uso de ferramenta de Inteligência Artificial.[8]

[8] Declaração de uso de ferramenta de Inteligência Artificial: A ferramenta ChatGPT, desenvolvida pela OpenAI, foi utilizada exclusivamente como apoio instrumental para correção ortográfica e gramatical, organização da revisão bibliográfica e direcionamento preliminar da pesquisa, sem substituir a análise crítica, a seleção das fontes, a redação final e a responsabilidade acadêmica do autor. Essa formulação é segura porque não apresenta a IA como autora, não a transforma em fonte científica e preserva sua autoria intelectual.

REFERÊNCIAS

AGÊNCIA NAC AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Delegado fala sobre os golpes mais comuns, desafios no combate e a importância da conscientização digital.** Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/delegado-fala-sobre-os-golpes-mais-comuns-desafios-no-combate-e-a-importancia-da-conscientizacao-digital. Acesso em: 21 maio 2026.

BRASIL. Câmara dos Deputados. **Conheça a evolução dos crimes cibernéticos**. Brasília, 23 ago. 2006. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos/. Acesso em: 23 mar. 2026.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. **Institui o Marco Civil da Internet e estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil**. Brasília, DF: Presidência da República, 2014. Disponível em: Planalto – Lei nº 12.965/2014. Acesso em: 7 maio 2026.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, 2018. Disponível em: Planalto – Lei nº 13.709/2018. Acesso em: 7 maio 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), **para dispor sobre crimes eletrônicos**. Brasília, DF: Presidência da República, 2021. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2021/lei-14155-27-maio-2021-791396-norma-pl.html. Acesso em: 23 mar. 2026.

BRASIL, Superior Tribunal de Justiça. **Súmula n. 479.** 01/08/2012. Disponível em: https://processo.stj.jus.br/SCON/sumstj/toc.jsp?sumula=479.num. Acesso em: 23 mar. 2026.

CABETTE, Eduardo Luiz Santos. **Invasão de dispositivo informático, furto eletrônico, estelionato eletrônico e competência** – Lei 14.155/21. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2021/07/30/invasao-de-dispositivo-informatico-furto-eletronico-estelionato-eletronico-e-competencia-lei-14-15521/. Acesso em: 24 mar. 2026.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Processo Judicial Eletrônico** (PJe). Brasília, DF: CNJ, [s.d.]. Disponível em: https://www.cnj.jus.br/programas-e-acoes/processo-judicial-eletronico-pje/. Acesso em: 28 maio 2026.

FOLHA VITÓRIA. **Educação, tecnologia e golpes digitais**. Disponível em: https://www.folhavitoria.com.br/educacao/educacao-tecnologia-golpes-digitais/. Acesso em: 21 maio 2026.

FORTINET. **O que é spear phishing? Definição e prevenção**. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/spear-phishing. Acesso em: 26 mar. 2026.

FRAZÃO, Ana. **Proteção de dados e inteligência artificial: diálogos sobre regulação.** Revista CNJ, Brasília, v. 7, n. 1, p. 9-14, jan./jun. 2023. Disponível em: Revista CNJ. Acesso em: 13 maio 2026.

GALVÃO, Caio de Souza. **Os limites da atuação policial na investigação criminal**. Disponível em: https://www.galvaoesilva.com/blog/direito-criminal/os-limites-da-atuacao-policial-na-investigacao-criminal/. Acesso em: 26 maio 2026.

GRECO, Rogério. **Curso de Direito Penal** Vol.1 - 28ª Edição 2026. 28. ed. Rio de Janeiro: Atlas, 2026. E-book. pág.340. ISBN 9786559778157. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559778157/. Acesso em: 29 abr. 2026.

JOVEM PAN. **Com dois anos de existência, Pix acelera democratização de serviços financeiros e aumenta competitividade do Brasil**. 2022. Disponível em: https://jovempan.com.br/noticias/economia/com-dois-anos-de-existencia-pix-acelera-democratizacao-de-servicos-financeiros-e-aumenta-competitividade-do-brasil.html. Acesso em: 23 mar. 2026.

LEITE, George S.; LEMOS, Ronaldo. **Marco Civil da Internet**. Grupo GEN, 2014. E-book. ISBN9788522493401. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788522493401/. Acesso em: 07 maio. 2026.

MATO GROSSO. Tribunal de Justiça de Mato Grosso (TJMT). **Golpe do falso advogado leva à anulação de empréstimo e indenização a aposentada**. Cuiabá: TJMT, 2026. Disponível em: https://www.tjmt.jus.br/noticias/2026/3/golpe-falso-advogado-leva-a-anulacao-emprestimo-e-indenizacao-a-aposentada. Acesso em: 21 maio 2026.

MIGALHAS. **Crimes de natureza sexual e a dificuldade na produção probatória**. Disponível em: https://www.migalhas.com.br/depeso/448652/crimes-de-natureza-sexual-e-a-dificuldade-na-producao-probatoria. Acesso em: 21 maio 2026.

MIGALHAS. **O crime é rápido, a investigação é lenta e as big techs lucram**. Disponível em: https://www.migalhas.com.br/depeso/451831/o-crime-e-rapido-a-investigacao-e-lenta-e-as-big-techs-lucram. Acesso em: 26 maio 2026.

MINISTÉRIO PÚBLICO DE SANTA CATARINA. **Fraudes cibernéticas e engenharia social: a resposta do Ministério Público à nova criminalidade organizada**. Disponível em: https://www.mpsc.mp.br/w/artigo/fraudes-cibern%C3%A9ticas-e-engenharia-social-a-resposta-do-minist%C3%A9rio-p%C3%BAblico-%C3%A0-nova-criminalidade-organizada. Acesso em: 26 mar. 2026.

MOTA, Maria Clara. **Quais os princípios limitadores do poder punitivo estatal?** Politize!. Publicado em 13 dez. 2021. Disponível em: https://www.politize.com.br/poder-punitivo-estatal/. Acesso em: 13 maio 2026.

OPENAI. **ChatGPT**. Versão GPT-5.5 Thinking. [S.I.]: OpeanAI, 2026. Disponível em: https://chatgpt.com/. Acesso em 7 de maio de 2026.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Compliance digital e LGPD**. São Paulo: Thomson Reuters Brasil, 2021. Acesso em: 7 de maio de 2026.

PINHEIRO, Patrícia P. **Direito Digital** - 7ª Edição 2021. 7. ed. Rio de Janeiro: Saraiva Jur, 2021. E-book. pág.712. ISBN 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555598438/. Acesso em: 27 maio. 2026.

PINHEIRO, Patrícia P. **Direito Digital** - 8ª Edição 2026. 8. ed. Rio de Janeiro: SRV, 2026. E-book. pág.2. ISBN 9786553624979. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786553624979/. Acesso em: 19 mar. 2026.

PINHEIRO, Patrícia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 maio 2026.

POLÍCIA CIVIL DE MATO GROSSO. **Polícia Civil intensifica combate aos crimes cibernéticos no Estado**. Disponível em: https://www.pjc.mt.gov.br. Acesso em: 21 maio 2026.

REIS, Anna C G.; ELTZ, Magnum K F. **Direito penal IV**. Porto Alegre: SAGAH, 2022. E-book. pág.123. ISBN 9786556903163. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556903163. Acesso em: 24 mar. 2026.

RIVELLI, Fabio. **A violência digital e seus efeitos nas vítimas: desafios contemporâneos e perspectiva do ser humano digital**. Disponível em: https://revista.provitima.org/ojs/index.php/rpv/article/view/100/136. Acesso em: 25 mar. 2026.

SILVA, Bozza, Fábio da. **Bem jurídico e autorização de excesso como limites à expansão penal**. São Paulo: Almedina Brasil, 2024. E-book. pág.107. ISBN 9788584931033. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788584931033/. Acesso em: 13 de maio. 2026.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **A cadeia de custódia no processo penal: do Pacote Anticrime à jurisprudência do STJ.** Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/23042023-A-cadeia-de-custodia-no-processo-penal-do-Pacote-Anticrime-a-jurisprudencia-do-STJ.aspx. Acesso em: 26 maio 2026.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico** - 9ª Edição 2025. 9. ed. Rio de Janeiro: SRV, 2025. E-book. pág.6. ISBN 9788553624317. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553624317/. Acesso em: 23 mar. 2026.

TOMASELLI, Giordano. **MT é o 2º estado com mais golpes digitais do País, diz pesquisa.** MidiaNews, Cuiabá, 24 set. 2024. Disponível em: https://www.midianews.com.br/conteudo.php?sid=3&cid=478815. Acesso em: 16 maio 2026.

TRIBUNAL DE JUSTIÇA DE MATO GROSSO (TJMT). **Como funciona o golpe do falso advogado.** Disponível em: https://www.tjmt.jus.br/noticias/2025/7/justica-segura-saiba-como-funciona-o-golpe-falso-advogado-e-reforca-alerta-a-populacao. Acesso em 27 maio 2026.

TRIBUNAL DE JUSTIÇA DE MATO GROSSO (TJMT). **Envio de comprovante falso de Pix caracteriza estelionato eletrônico**. Disponível em: https://www.tjmt.jus.br/noticias/2026/1/envio-comprovante-falso-pix-caracteriza-estelionato-eletronico. Acesso em: 21 maio 2026.

TRIBUNAL DE JUSTIÇA DE MATO GROSSO (TJMT). **Entenda direito: estrutura da Justiça Estadual**. Disponível em: https://www.tjmt.jus.br/noticias/2017/9/entenda-direito-estrutura-justica-estadual. Acesso em: 21 maio 2026.

TRIBUNAL DE JUSTIÇA DE MATO GROSSO (TJMT). **Justiça Segura: saiba como funciona o golpe do falso advogado e reforça alerta à população**. Disponível em: https://www.tjmt.jus.br/noticias/2025/7/justica-segura-saiba-como-funciona-o-golpe-falso-advogado-e-reforca-alerta-a-populacao. Acesso em: 21 maio 2026.

TRIBUNAL DE JUSTIÇA DE MATO GROSSO (TJMT). Justiça Segura: **TJMT reforça campanha de alerta sobre golpe do falso advogado.** Disponível em: https://www.tjmt.jus.br/noticias/2026/1/envio-comprovante-falso-pix-caracteriza-estelionato-eletronico. Acesso em: 21 maio 2026.

TRIBUNAL DE JUSTIÇA DO ESTADO DE MATO GROSSO (TJMT). **Direito do consumidor – indícios de golpe do falso advogado contra pessoa idosa autorizam suspensão liminar de consignado**. Portal Ementário, ed. 25, 2025. Disponível em: https://jurisprudencia.tjmt.jus.br/portal-ementario?edicao=25&ano=2025. Acesso em: 29 maio 2026.

WOLFGANG, Hoffmann-Riem. **Teoria Geral do Direito Digital** - 2ª Edição 2022. 2. ed. Rio de Janeiro: Forense, 2021. E-book. p.103. ISBN 9786559642267. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786559642267/. Acesso em: 27 abr. 2026.