

PARTE II · DIREITO PENAL E POLÍTICA CRIMINAL · CAPÍTULO 8

A efetividade da tutela penal dos crimes cibernéticos e das deepfakes na Região Norte: uma análise crítica da aplicação da Lei nº 14.155/2021

The effectiveness of criminal law protection against cybercrimes and deepfakes in the Northern Region: a critical analysis of the application of Law No. 14.155/2021

Regina Tomé de Almeida¹

Leonardo Silva de Oliveira Bandeira²

COMO CITAR

ALMEIDA, Regina Tomé de; BANDEIRA, Leonardo Silva de Oliveira. A efetividade da tutela penal dos crimes cibernéticos e das deepfakes na Região Norte: uma análise crítica da aplicação da Lei nº 14.155/2021. In: OLIVEIRA, Emanuelle Góes (org.). **Desafios do Direito Contemporâneo**: volume 15. Rio Branco: Momento Jurídico, 2026. p. 223-257.

RESUMO

Introdução. O presente estudo trata da análise da efetividade da Lei nº 14.155/2021 no enfrentamento das condutas envolvendo *deepfakes* e estelionato eletrônico na Região Norte do Brasil, no período de 2021 a 2025. **Objetivo.** O objetivo geral é analisar a aplicação concreta da lei, cotejando as inovações normativas com a realidade empírica regional. **Método.** A metodologia adotada é qualitativa, de natureza bibliográfica e documental. Foram analisados dados do 18º Anuário Brasileiro de Segurança Pública (2024), legislação, doutrina especializada e jurisprudência do Tribunal de Justiça do Estado do Acre. **Resultados.** Os resultados revelam crescimento significativo dos estelionatos por meio eletrônico na Região Norte, com 31.095 ocorrências registradas apenas em 2023, acompanhados de elevada heterogeneidade entre os estados e expressiva subnotificação.

¹ Discente do 8º período do curso de Bacharelado em Direito pelo Centro Universitário Uninorte.

² Docente do curso de bacharelado em Direito do Centro Universitário Uninorte. Especialista em Direito Civil, Docência do Ensino Superior e Legal Operations: Dados, IA e Performance Jurídica (PUC/PR). Coordenador do NEAD/Uninorte. Advogado (Casas, Ricardo, Bandeira & Soares Advocacia). E-mail: leonardo.bandeira@uninorteac.com.br.

As *deepfakes* permanecem estatisticamente invisibilizadas, diluídas nas estatísticas gerais de fraudes eletrônicas. A análise comparativa entre casos de alta e baixa visibilidade evidenciou assimetria na resposta institucional: condutas envolvendo figuras públicas recebem maior atenção, enquanto os crimes patrimoniais digitais cotidianos apresentam baixos índices de elucidação. Os desafios técnico-investigativos regionais, a ausência de delegacias especializadas em grande parte dos estados, a concentração de recursos nas capitais e a insuficiência de capacitação técnica comprometem a efetividade da lei. **Conclusão.** Conclui-se que a Lei nº 14.155/2021, embora represente avanço normativo relevante, apresenta eficácia limitada na Região Norte, revelando traços de Direito Penal simbólico. A efetividade da tutela penal no ambiente digital depende de políticas públicas integradas, com aprimoramento normativo, fortalecimento institucional e redução das desigualdades regionais no acesso à justiça e à tecnologia.

Palavras-chave: Crimes cibernéticos. Deepfake. Lei 14.155/2021. Perseguição penal. Região Norte.

ABSTRACT

Introduction. This study addresses the effectiveness of Law No. 14,155/2021 in combating conduct involving deepfakes and electronic fraud in Northern Brazil from 2021 to 2025. **Objective.** Within this context, the general objective is to analyze the practical application of the law, comparing normative innovations with regional empirical reality. **Method.** The methodology adopted is qualitative, bibliographical, and documentary in nature. Data from the 18th Brazilian Public Safety Yearbook (2024), legislation, specialized literature, and case law from the Court of Justice of the State of Acre were analyzed. **Results.** The findings reveal a significant increase in electronic fraud in Northern Brazil, with 31,095 reported occurrences in 2023 alone, accompanied by high heterogeneity among states and substantial underreporting. Deepfakes remain statistically invisible, diluted within general electronic fraud statistics. A comparative analysis between high- and low-visibility cases highlighted institutional response asymmetry: offenses involving public figures receive greater attention, whereas routine digital property crimes show low clearance rates. Regional technical-investigative challenges, the lack of specialized police stations in most states, resource concentration in state capitals, and insufficient technical training compromise the law's effectiveness. **Conclusion.** Thus, it is concluded that while Law No. 14,155/2021 represents a relevant normative advancement, it demonstrates limited efficacy in Northern Brazil, exhibiting traits of symbolic criminal law. The effectiveness of

legal protection in the digital environment does not rely solely on isolated legislative reforms, but rather on the implementation of integrated public policies encompassing regulatory improvements, institutional strengthening, and the reduction of regional disparities in access to justice and technology.

Keywords: Cybercrimes. Deepfake. Law 14.155/2021. Criminal prosecution. Northern Brazil.

INTRODUÇÃO

A expansão das tecnologias da informação transformou as interações sociais e consolidou o ambiente digital como espaço indispensável à vida contemporânea. Contudo, esse avanço viabilizou novas modalidades delitivas, destacando-se as *deepfakes*, conteúdos audiovisuais manipulados por inteligência artificial com elevado grau de realismo. O potencial lesivo dessas condutas atinge tanto bens individuais, como a honra e o patrimônio, quanto transindividuais, como a confiança nas instituições. Nesse contexto, a Lei nº 14.155/2021 atualizou o tratamento penal dos crimes patrimoniais digitais ao agravar penas e qualificar a fraude eletrônica (art. 171, § 2º-A, do Código Penal). Todavia, a efetiva repressão exige mais que atualização normativa: demanda estrutura investigativa e capacitação técnica, especialmente em regiões marcadas por limitações logísticas, como a Região Norte.

Diante disso, o problema de pesquisa consiste em analisar em que medida a Lei nº 14.155/2021 se mostra efetiva na investigação e repressão do estelionato eletrônico e das *deepfakes* na Região Norte, frente às suas dificuldades estruturais. O objetivo geral é analisar a aplicação concreta da lei no âmbito regional, cotejando as inovações normativas com a realidade empírica. Especificamente, busca-se: (i) mapear os registros de fraudes digitais nos estados da Região Norte entre 2021 e 2025; (ii) comparar a resposta institucional entre casos de alta e baixa visibilidade; (iii) identificar os desafios técnico-investigativos; e (iv) propor aprimoramentos normativos e institucionais.

A relevância do estudo reside na escassez de pesquisas sobre a efetividade da legislação penal em contextos regionais periféricos. A Região Norte apresenta singularidades geográficas e estruturais que desafiam o sistema de justiça criminal, justificando o recorte empírico. O trabalho divide-se em três capítulos: o primeiro examina a evolução legislativa e o enquadramento das *deepfakes*; o segundo analisa empiricamente a aplicação da lei na região; e o terceiro dedica-se à análise crítica e à proposição de melhorias. A metodologia adota abordagem qualitativa, bibliográfica e documental, com recorte temporal de 2021 a 2025, amparada em dados do 18º Anuário Brasileiro de Segurança Pública, legislação, doutrina e jurisprudência do TJAC.

1 CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Os crimes cibernéticos representam manifestação contemporânea da criminalidade cuja expansão decorre diretamente da intensificação da digitalização das relações sociais e econômicas, impondo ao Direito Penal e ao Direito Processual Penal desafios estruturais relacionados à adequação típica, à produção probatória e à efetividade da tutela jurisdicional. O avanço das tecnologias da informação e comunicação ampliou significativamente as formas de interação no ambiente virtual, ao mesmo tempo em que viabilizou o surgimento de novas modalidades delitivas praticadas por meio de sistemas informáticos e redes digitais.

Nesse contexto, o cibercrime pode ser compreendido como a prática de infrações penais em que computadores, sistemas informáticos ou redes digitais são utilizados como instrumento, meio ou ambiente de execução. Essas condutas abrangem desde invasões de dispositivos e subtração de dados pessoais até fraudes financeiras e demais práticas que se valem indevidamente da infraestrutura tecnológica para a realização de ilícitos penais.

No ordenamento jurídico brasileiro, o enfrentamento dessas condutas demanda constante atualização normativa no âmbito do Direito Penal e Processual Penal, em razão da velocidade com que se transformam as dinâmicas tecnológicas e se sofisticam as práticas criminosas. Tal cenário impõe ao legislador o desafio permanente de adequação dos tipos penais e dos instrumentos investigativos, com vistas à proteção eficaz dos bens jurídicos atingidos.

Nesse cenário, a Lei nº 12.737/2012 representou marco inicial relevante ao tipificar a invasão de dispositivo informático no Código Penal, fortalecendo a tutela da privacidade e da segurança no ambiente digital. Posteriormente, a Lei nº 14.155/2021 promoveu alterações significativas ao agravar as penas dos crimes de furto e estelionato praticados por meio eletrônico, em resposta à expressiva expansão das fraudes digitais.

Apesar dos avanços legislativos, observa-se o surgimento de formas cada vez mais sofisticadas de criminalidade digital, impulsionadas pelo desenvolvimento de tecnologias emergentes. Entre essas inovações, destacam-se as *deepfakes*, consistentes na criação de conteúdos audiovisuais manipulados por inteligência artificial com elevado grau de realismo, capazes de simular pessoas e situações com aparência de veracidade.

Diante desse cenário, impõe-se a necessidade de análise não apenas da evolução normativa do combate aos crimes cibernéticos, mas também do enquadramento jurídico das *deepfakes* e dos desafios inerentes à sua persecução penal. Entre tais desafios, destacam-se a produção e valoração da prova digital, o anonimato dos agentes, a volatilidade das evidências no ambiente virtual e a transnacionalidade dessas condutas, fatores que, em conjunto, tensionam a capacidade de resposta do sistema de justiça criminal sob uma perspectiva de efetividade jurisdicional.

1.1 EVOLUÇÃO LEGISLATIVA

O enfrentamento legislativo dos crimes cibernéticos no Brasil passou por processo gradual de consolidação normativa, especialmente dian-

te da histórica insuficiência de tipos penais específicos voltados às condutas praticadas em ambiente digital. Essa lacuna normativa, sob a ótica da tipicidade penal, produziu déficits de subsunção típica e ampliou espaços de atipicidade material diante de condutas emergentes da criminalidade tecnológica.

Nesse contexto, a doutrina contemporânea enfatiza a necessidade de constante reconfiguração do Direito Penal diante da dinâmica tecnológica. Conforme Bastos (2016), a neutralidade normativa frente à inovação tecnológica revela-se incompatível com a função de tutela de bens jurídicos em um cenário de mutação contínua das formas de agressão penalmente relevantes.

O marco inicial relevante nesse processo foi a Lei nº 12.737/2012, que introduziu o art. 154-A, o qual passou a tipificar a invasão de dispositivo informático alheio mediante violação indevida de mecanismo de segurança, com finalidade de obtenção, adulteração ou destruição de dados sem autorização do titular, enquanto o art. 154-B disciplinou a ação penal, estabelecendo regra de procedibilidade condicionada à representação.

Segundo Delmanto (2016, p.548):

Em boa hora o Legislador acrescentou este art. 154-A ao Código Penal. O avanço tecnológico, que tantas maravilhas e facilidades proporciona, traz também um grande risco de as pessoas terem a sua privacidade violada. São inúmeras as formas com as quais os chamados hackers conseguem acessar a memória de computadores alheios, geralmente por meio da internet.

Não obstante o avanço legislativo, a doutrina identifica déficits de completude normativa, especialmente na interface entre crimes informáticos e delitos patrimoniais tradicionais. Bastos (2016) aponta a assimetria dogmática entre bens jurídicos tutelados, o que compromete a coerência sistêmica na repressão às fraudes digitais.

Posteriormente, a Lei nº 14.155/2021 promoveu reestruturação relevante da tutela penal dos crimes patrimoniais praticados em ambiente digital, com majoração de penas e criação de figuras qualificadas. Segundo Cunha (2021), trata-se de resposta legislativa à intensificação da criminalidade econômica digital, marcada por elevada sofisticação executiva e redução de rastreabilidade.

Sob a ótica da política criminal, a reforma introduz maior densidade normativa ao sistema repressivo, especialmente ao tipificar o furto mediante fraude eletrônica (art. 155, §4º-B) e a fraude eletrônica no estelionato (art. 171, §2º-A), cuja distinção dogmática reside no elemento volitivo da vítima. No primeiro, há subtração sem manifestação de vontade válida; no segundo, há disposição patrimonial viciada por erro induzido. Já no plano processual, a modificação do art. 70 do Código de Processo Penal revela racionalidade de desconcentração jurisdicional, voltada à mitigação dos efeitos da dispersão espacial típica dos delitos informáticos.

Nesse contexto, a lógica fraudulenta não constitui fenômeno recente, mas estrutural às relações sociais, como observa Greco (2014, p. 236), ao afirmar que desde a formação das relações sociais o indivíduo se vale de artifícios para ocultar a verdade e obter vantagens indevidas.

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas.

Em perspectiva sistêmica, a evolução legislativa evidencia processo incremental de adaptação do Direito Penal à criminalidade tecnológica. Todavia, sob a ótica da efetividade da tutela penal, a expansão tipológica isolada não se mostra suficiente, exigindo integração entre capacidade investigativa, tecnologia forense e cooperação jurídica internacional estruturada.

1.2 CONCEITO JURÍDICO DE DEEPFAKE E ENQUADRAMENTO TÍPICO

A *deepfake*, sob uma perspectiva técnico-jurídica, constitui produto da manipulação sintética de conteúdos audiovisuais por inteligência artificial generativa, com aptidão para simular identidade visual e sonora de terceiros com elevado grau de verossimilhança. Trata-se de tecnologia de potencial ofensivo multidimensional, apta a atingir simultaneamente bens jurídicos individuais e transindividuais.

Segundo um guia ilustrado do STF (2024):

A expressão “*deepfake*” surge da união dos termos “*deep*” – extraída da tecnologia deep learning, “aprendizado profundo” – e “*fake*”, que significa “falso”, em inglês. Não existe uma palavra em português para descrever esse fenômeno. Contudo, em tradução livre as *deep-fakes* nada mais são do que “falsidades profundas”, ou seja, conteúdos falsos produzidos com um alto grau de elaboração.

Botelho e Nöth (2021) descrevem as Redes Adversárias Generativas (GANs) como arquitetura algorítmica estruturada em competição entre rede geradora e discriminadora, mecanismo que intensifica progressivamente o realismo das simulações e reduz a detectabilidade humana.

No plano dogmático, (Chesney; Citron, 2019 apud Ferreira; Leme, 2023) situam as *deepfakes* como tecnologia de aprendizado profundo de uso dual (dual use technology), apta a finalidades lícitas ou ilícitas, o que impõe dificuldades de delimitação do desvalor da conduta, especialmente na fronteira entre usos socialmente tolerados e práticas penalmente relevantes.

Sob a perspectiva dos direitos fundamentais, Oliveira e Ávila (2024) vinculam o fenômeno à tutela penal dos direitos da personalidade, especialmente imagem, honra e privacidade, evidenciando ampliação do risco jurídico-penal em ambientes de hiper-realismo digital. Já no âmbito da segurança da informação, Oliveira e Ávila (2024) apontam a utilização de *deepfakes* em ataques de engenharia social e fraudes biométricas, inserin-

do o fenômeno na esfera da criminalidade tecnológica de alta sofisticação.

Do ponto de vista estritamente penal, a ausência de tipificação específica impõe subsunção por adequação típica indireta. Assim, a calúnia (art. 138 do CP) exige imputação falsa de fato criminoso; a difamação (art. 139 do CP) tutela a reputação objetiva; o estelionato (art. 171 do CP), inclusive em sua forma eletrônica, exige induzimento a erro com vantagem ilícita; e a falsidade ideológica (art. 299 do CP) incide quando há inserção de declaração falsa com relevância jurídica.

Sob a ótica da tipicidade conglobante, a análise das *deepfakes* demanda avaliação não apenas formal, mas material da conduta, considerando sua inserção no sistema jurídico como unidade de valoração normativa. A multiplicidade de enquadramentos revela simultaneamente a plasticidade do Direito Penal e suas limitações estruturais diante de tecnologias disruptivas.

(Chesney; Citron, 2019 apud Ferreira; Leme, 2023) distinguem *disinformation* e *misinformation*, sendo a primeira caracterizada pelo dolo específico de enganar, elemento central na imputação subjetiva em contextos de manipulação audiovisual sintética.

Em perspectiva funcional do Direito Penal, o fenômeno se relaciona à tutela do Estado Democrático de Direito (Jhonatan Ferreira, 2024), especialmente quando utilizado para manipulação de processos eleitorais e erosão da confiança institucional, podendo atrair a incidência dos crimes previstos na Lei nº 14.197/2021.

A ausência de tipificação penal específica das *deepfakes* no ordenamento jurídico brasileiro deve ser analisada à luz do debate legislativo contemporâneo, especialmente diante da tramitação do Projeto de Lei nº 2.338/2023. A proposta estabelece um marco regulatório abrangente para a inteligência artificial no país, adotando uma abordagem baseada em risco e prevendo mecanismos de governança, transparência e responsabilização, com destaque para os sistemas de alto risco e para a mitigação de

danos decorrentes de conteúdos sintéticos. Embora o projeto não institua, até o momento, um tipo penal autônomo para as *deepfakes*, ele introduz instrumentos normativos relevantes, como o dever de transparência, o direito à explicação e a responsabilização objetiva em determinados casos, que podem incidir diretamente sobre a produção e circulação desses conteúdos.

Nesse contexto, evidencia-se que o legislador brasileiro tem priorizado, ao menos inicialmente, uma regulação de natureza preventiva e civil-administrativa, em detrimento da intervenção penal imediata. Tal opção reforça a atual dependência da subsunção das *deepfakes* aos tipos penais tradicionais, ao mesmo tempo em que sinaliza uma possível evolução futura para modelos mais específicos de tutela penal, conforme a maturação do debate regulatório e a intensificação dos riscos associados ao uso dessa tecnologia. Tal diretriz mostra-se especialmente relevante no contexto brasileiro, em que o Projeto de Lei nº 2.338/2023 já incorpora princípios de transparência e governança de sistemas de IA podendo servir como base normativa para a futura internalização de mecanismos específicos de rotulagem de conteúdos sintéticos, à semelhança do modelo europeu.

Em síntese, as *deepfakes* constituem categoria de risco penal emergente, cuja disciplina jurídica depende de construção interpretativa sistemática, em razão da insuficiência de tipificação específica e da necessidade de reconstrução dogmática da imputação penal em ambientes de inteligência artificial generativa.

1.3 DESAFIOS DA PERSECUÇÃO PENAL EM AMBIENTE DIGITAL

A persecução penal dos crimes cibernéticos enfrenta obstáculos estruturais inerentes às próprias características do ambiente digital. A transnacionalidade das condutas, o anonimato dos agentes, a volatilidade das provas e a elevada complexidade técnica das investigações comprometem a efetividade das fases de prevenção, apuração e repressão desses

delitos. Nesse sentido, Dias (2012) destaca que tais fatores impactam diretamente a capacidade de resposta do sistema de justiça criminal.

Um dos principais desafios reside na transnacionalidade das condutas. A ausência de fronteiras no ambiente digital permite a atuação simultânea em múltiplas jurisdições, dificultando a fixação de competência e a aplicação da lei penal. Dias (2012) observa, ainda, a existência dos chamados “paraísos cibernéticos”, caracterizados por legislações permissivas ou pela ausência de cooperação internacional, o que favorece a impunidade e fragmenta a persecução penal.

A heterogeneidade normativa entre Estados agrava esse cenário, na medida em que determinadas condutas podem ser lícitas em algumas jurisdições e ilícitas em outras, incentivando a deslocação da atividade criminosa. Embora o ordenamento jurídico brasileiro tenha avançado com a Lei nº 14.155/2021, a cooperação internacional ainda depende de mecanismos formais que não acompanham a velocidade da criminalidade digital.

Sob a ótica da tipicidade funcional, observa-se a ausência de harmonização normativa entre os ordenamentos jurídicos, o que compromete a repressão eficaz das condutas praticadas em ambiente digital. Soma-se a isso o anonimato dos agentes, potencializado por tecnologias como criptografia, redes privadas virtuais (VPNs) e mecanismos de ocultação de identidade, os quais dificultam a identificação do autor e, por consequência, a atribuição de responsabilidade penal.

A volatilidade da prova digital constitui outro ponto crítico. Os dados eletrônicos apresentam elevada suscetibilidade à alteração, exclusão ou dispersão, o que compromete sua preservação e confiabilidade. Nesse sentido, Dias (2012) enfatiza a necessidade de procedimentos técnicos rigorosos na coleta e preservação dessas provas, a fim de assegurar sua integridade e validade no processo penal. A fragilidade da cadeia de custódia digital impõe rigor metodológico e atuação pericial especializada para garantir autenticidade e admissibilidade probatória.

No plano normativo, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu parâmetros relevantes para a guarda e acesso a registros digitais. Todavia, os prazos legais de armazenamento podem ser insuficientes diante da complexidade das investigações, especialmente em contextos transnacionais ou de elevada complexidade probatória. Ademais, a exigência de ordem judicial para acesso a dados, embora compatível com garantias constitucionais, pode impactar a celeridade investigativa diante da rapidez de apagamento ou migração de informações.

Sob uma perspectiva funcional do Direito Penal, observa-se que a estrutura normativa e procedimental vigente ainda não acompanha plenamente a dinâmica de produção e desaparecimento das evidências digitais. A elevada tecnicidade dos crimes cibernéticos impõe a necessidade de conhecimentos especializados em tecnologia da informação, perícia digital e análise de dados, além de constante capacitação dos agentes estatais.

Outro fator relevante é a cifra negra, caracterizada pela subnotificação dos crimes cibernéticos. Muitas vítimas deixam de comunicar as ocorrências por receio de danos reputacionais ou por descrença na efetividade da resposta estatal, o que contribui para a subestimação estatística do fenômeno. Soma-se a isso a sobrecarga do Poder Judiciário e a insuficiência de especialização técnica em determinados órgãos jurisdicionais, o que compromete a tramitação célere e adequada dos processos envolvendo crimes digitais.

Diante desse panorama, constata-se que os desafios da persecução penal em ambiente digital são múltiplos e interdependentes, exigindo respostas integradas do sistema de justiça criminal. Essas dificuldades tendem a se intensificar em contextos marcados por limitações estruturais e logísticas, especialmente em regiões com menor densidade de infraestrutura tecnológica e pericial, como na Região Norte do país, evidenciando a necessidade de fortalecimento institucional e descentralização da capacidade investigativa no enfrentamento da criminalidade cibernética.

2 APLICAÇÃO DA LEI 14.155/2021 NA REGIÃO NORTE

A Lei nº 14.155/2021 representou um avanço relevante na repressão aos crimes patrimoniais praticados em ambiente digital, ao promover a qualificação típica e o recrudesimento sancionatório das condutas de furto e estelionato cometidas por meio eletrônico. A reforma legislativa buscou adequar o sistema penal à crescente sofisticação das fraudes digitais, especialmente aquelas executadas mediante engenharia social, invasão de dispositivos e manipulação de dados, fenômenos que se intensificaram com a ampliação do uso de tecnologias da informação.

Todavia, a efetividade da norma penal não se esgota na sua previsão abstrata, dependendo, em grande medida, das condições concretas de aplicação pelos órgãos de persecução penal. Nesse sentido, a análise da incidência da Lei nº 14.155/2021 na Região Norte revela um campo particularmente relevante de investigação, considerando as especificidades estruturais, geográficas e institucionais que influenciam a atuação estatal nessa localidade.

A Região Norte apresenta desafios singulares relacionados à extensão territorial, à dispersão populacional, às limitações de infraestrutura tecnológica e à desigual distribuição de recursos humanos especializados, fatores que impactam diretamente a capacidade investigativa e a produção probatória em crimes cibernéticos. Tais elementos podem comprometer a efetividade da persecução penal, sobretudo em delitos que exigem atuação técnica especializada, rapidez na coleta de evidências digitais e articulação com provedores de serviços, frequentemente situados fora da jurisdição local.

Além disso, a aplicação da Lei nº 14.155/2021 nesse contexto demanda análise sob a perspectiva da eficiência administrativa e da isonomia na tutela penal, na medida em que eventuais limitações estruturais podem gerar assimetrias na resposta estatal em comparação a outras regiões do país. A investigação empírica e doutrinária dessa realidade permite

compreender em que medida a inovação legislativa tem sido capaz de produzir efeitos concretos no enfrentamento da criminalidade digital.

Diante desse cenário, o presente capítulo tem por objetivo examinar a aplicação prática da Lei nº 14.155/2021 na Região Norte, considerando os desafios operacionais enfrentados pelos órgãos de segurança pública e pelo Poder Judiciário, bem como avaliar a efetividade das medidas adotadas no combate aos crimes cibernéticos nessa realidade regional.

2.1 MAPEAMENTO DE CASOS DE DEEPFAKE NA REGIÃO NORTE (2021-2025)

A análise da aplicação da Lei nº 14.155/2021 na Região Norte do Brasil demanda, como pressuposto metodológico, o mapeamento dos casos de fraudes digitais e *deepfakes* registrados nos estados que compõem a região (Acre, Amapá, Amazonas, Pará, Rondônia, Roraima e Tocantins) no período de 2021 a 2025. Este levantamento, contudo, enfrenta como primeiro e significativo obstáculo a escassez de dados estatísticos sistematizados e a dispersão das informações entre as diversas unidades federativas.

Ressalte-se, desde logo, que os dados oficiais disponíveis não individualizam, de forma específica, ocorrências envolvendo *deepfakes*, as quais permanecem estatisticamente invisibilizadas. Nesse contexto, tais práticas devem ser compreendidas como inseridas no fenômeno mais amplo das fraudes digitais e dos estelionatos eletrônicos, especialmente aqueles tipificados pelo §2º-A do art. 171 do Código Penal, introduzido pela Lei nº 14.155/2021.

O Fórum Brasileiro de Segurança Pública (2024), por meio do 18º Anuário Brasileiro de Segurança Pública, apresenta dados relevantes sobre os crimes patrimoniais na Região Norte. No que se refere aos estelionatos por meio eletrônico, os registros revelam crescimento expressivo e heterogêneo entre os estados.

O Pará contabilizou 16.884 ocorrências em 2023, com taxa de 207,9 por 100 mil habitantes e aumento de 28,9% em relação ao ano anterior. Rondônia registrou 6.532 ocorrências, com taxa de 413,1 e crescimento de 10,1%. O Tocantins apresentou 4.043 casos, com taxa de 267,5 por 100 mil habitantes, com aumento de 31,4%. O Amazonas, embora com números absolutos inferiores (877 ocorrências), destacou-se pelo crescimento de 109,3%. Já o Amapá registrou 618 ocorrências, com taxa de 84,2 por 100 mil habitantes, com incremento de 62,6% (FBSP, 2024).

Esses dados evidenciam não apenas o crescimento das fraudes digitais na região, mas também significativa heterogeneidade entre os estados, indicando assimetrias estruturais na capacidade de registro, investigação e repressão desses delitos. Por outro lado, Acre e Roraima apresentaram números absolutos reduzidos, 248 e 1.893 ocorrências, respectivamente, o que não necessariamente indica menor incidência criminosa, mas possivelmente reflete limitações nos sistemas de notificação e sub-registro de ocorrências.

Essa hipótese é reforçada pela análise dos estelionatos totais, que incluem tanto modalidades presenciais quanto eletrônicas, os quais apresentaram crescimento em todos os estados da Região Norte, com destaque para Rondônia (19,6%), Amazonas (13,2%) e Tocantins (4,5%) (FBSP, 2024). Tal cenário sugere expansão consistente da criminalidade patrimonial, com progressiva migração para o ambiente digital.

Lima e Bueno (2023, p. 93) observam que os estelionatos atingiram patamar recorde no Brasil, com mais de 1,8 milhão de ocorrências anuais, impulsionados sobretudo pela ampliação do uso de redes sociais e aplicativos de mensagens. Segundo os autores, diferentemente dos crimes patrimoniais tradicionais, que sofreram retração durante a pandemia, os golpes virtuais apresentaram crescimento exponencial, evidenciando uma reconfiguração estrutural da criminalidade econômica.

Na Região Norte, esse fenômeno assume contornos ainda mais complexos. A extensão territorial, a dispersão populacional e as limita-

ções de infraestrutura tecnológica e institucional dificultam tanto o registro quanto a investigação dos crimes digitais. Como destacam Lima e Bueno (2023, p. 96), a sobrecarga das polícias civis e a insuficiência de recursos humanos e tecnológicos comprometem a capacidade estatal de resposta, problema que se intensifica em regiões com menor densidade institucional.

A ausência de delegacias especializadas em crimes cibernéticos em grande parte dos estados nortistas contribui para a subnotificação e para a classificação inadequada das ocorrências. Muitos casos são registrados como estelionato comum, sem a devida identificação da qualificadora eletrônica, o que invisibiliza estatisticamente fenômenos mais sofisticados, como as *deepfakes* utilizadas em fraudes e manipulações de identidade digital.

No âmbito processual, a Lei nº 14.155/2021 introduziu o §4º ao art. 70 do Código de Processo Penal, estabelecendo que:

Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção (Brasil, 1941).

Todavia, embora represente avanço sob a ótica normativa, sua efetividade prática na Região Norte encontra limitações estruturais significativas. Em localidades remotas, a ausência de unidades policiais estruturadas e a dificuldade de acesso a serviços públicos ainda constituem barreiras concretas ao registro de ocorrências e à instauração de investigações, o que compromete a eficácia da persecução penal.

A jurisprudência do Tribunal de Justiça do Estado do Acre ilustra esse cenário. No Agravo de Instrumento nº 1001508-23.2024.8.01.0000, a Segunda Câmara Cível reconheceu a ocorrência de estelionato cibernético e determinou a suspensão imediata das cobranças indevidas, com funda-

mento na falha na prestação do serviço bancário e no dever de cautela das instituições financeiras (Acre, 2024). Em sentido semelhante, no Agravo de Instrumento nº 1001933-50.2024.8.01.0000, o Tribunal reafirmou esse entendimento, destacando a responsabilidade objetiva das instituições financeiras em casos de fraudes digitais (Acre, 2024).

Registre-se, por oportuno, que os acórdãos analisados tramitaram na esfera cível, e não na penal. Tal circunstância, longe de enfraquecer o argumento aqui desenvolvido, constitui evidência da hipótese central deste trabalho: a de que a resposta penal às *deepfakes* e às fraudes digitais na Região Norte permanece, em larga medida, invisível. A existência de pronunciamentos judiciais exclusivamente na esfera cível, versando sobre fatos que, em tese, poderiam ensejar responsabilização penal, indica que as vítimas têm buscado, preferencialmente, a tutela ressarcitória, em razão das limitações estruturais da persecução penal.

Nesse contexto, a utilização desses julgados como fonte documental configura escolha metodológica consciente, voltada a evidenciar o deslocamento da tutela jurídica para o âmbito civil e, por conseguinte, a insuficiência da resposta penal diante da complexidade dessas condutas. A atuação do Poder Judiciário, nesses casos, revela sensibilidade à proteção do consumidor e à contenção dos danos, mas também expõe as fragilidades do sistema penal frente às novas formas de lesão mediadas por tecnologias digitais.

Em síntese, o mapeamento dos casos de *deepfake* e fraudes digitais na Região Norte revela um cenário marcado por crescimento expressivo dos estelionatos eletrônicos, subnotificação de ocorrências, ausência de especialização institucional e fragilidade nos sistemas de coleta de dados. Tais fatores comprometem a efetividade da Lei nº 14.155/2021 e evidenciam a necessidade de fortalecimento da estrutura estatal, com investimentos em tecnologia, capacitação profissional e aprimoramento dos mecanismos de investigação e cooperação, especialmente em regiões periféricas do sistema de justiça criminal, nas quais a invisibilidade estatística

das *deepfakes* compromete não apenas a formulação de políticas públicas, mas também a própria compreensão da dimensão real do fenômeno.

2.2 ANÁLISE COMPARATIVA: CASOS DE ALTA E BAIXA VISIBILIDADE

A compreensão da real dimensão dos estelionatos, especialmente aqueles praticados por meio eletrônico, exige abordagem que ultrapasse a análise de dados quantitativos. Mostra-se essencial distinguir os níveis de visibilidade dos diferentes fenômenos delitivos, contrapondo-se os casos que alcançam ampla repercussão pública àqueles que permanecem invisibilizados no cotidiano, seja pela dificuldade de apuração, seja pela baixa capacidade institucional de resposta estatal. Tal distinção permite evidenciar não apenas a extensão do problema, mas também os entraves estruturais à efetividade da repressão penal.

De um lado, situam-se os casos de alta visibilidade, geralmente associados ao emprego de tecnologias sofisticadas, como as *deepfakes*, especialmente quando vinculadas ao contexto político-eleitoral ou à exposição de figuras públicas. Conforme apontam (Chesney; Citron, 2019 apud Ferreira; Leme, 2023), essas tecnologias possuem elevado potencial de manipulação informacional, sendo capazes de distorcer o debate público, comprometer a formação da vontade política e fragilizar a confiança nas instituições democráticas.

A utilização de inteligência artificial para simular falas, imagens ou comportamentos de agentes públicos produz impacto imediato, mobilizando não apenas a opinião pública, mas também órgãos de controle e regulação, a exemplo da Justiça Eleitoral. Trata-se, portanto, de fenômeno qualitativamente relevante, cuja gravidade transcende o prejuízo individual e alcança dimensões institucionais. Nesse sentido, Chesney e Citron (2019 apud Ferreira; Leme, 2023) apontam que tais tecnologias podem corroer a confiança em instituições públicas e privadas.

Em contraposição, observa-se a predominância dos casos de baixa visibilidade, que compõem a maior parcela dos crimes patrimoniais no

ambiente digital e que revelam uma profunda reconfiguração na dinâmica criminal brasileira. Segundo dados do Fórum Brasileiro de Segurança Pública (2024), o Brasil registrou 1.965.353 ocorrências de estelionato em 2023, um crescimento de 8,2% em relação ao ano anterior. O referido Anuário destaca que este número já supera o total de roubos no país, evidenciando uma inversão relevante no padrão da criminalidade patrimonial.

Diferentemente dos casos de grande repercussão, esses delitos atingem, em regra, vítimas anônimas e envolvem fraudes cotidianas. A modalidade de estelionato por meio eletrônico respondeu por 235.393 registros, com crescimento de 13,6% em relação ao ano anterior, o que equivale a um golpe a cada 16 segundos (FBSP, 2024). O Fórum Brasileiro de Segurança Pública (2024) indica que tais fraudes vêm se consolidando como relevante vetor de atuação do crime organizado no ambiente digital. A pulverização das condutas, aliada à dificuldade de rastreamento dos agentes e à frequente utilização de infraestrutura tecnológica transnacional, contribui para elevados índices de subnotificação e baixíssimas taxas de elucidação.

Essa assimetria entre visibilidade e incidência revela um problema estrutural: enquanto os casos de grande repercussão recebem resposta institucional mais célere e articulada, a massa de delitos cotidianos permanece em uma zona de baixa visibilidade no sistema de persecução penal, contribuindo para o aumento da cifra oculta da criminalidade. Tal cenário compromete a função preventiva e repressiva do Direito Penal, especialmente diante da migração progressiva da criminalidade para o ambiente digital.

No plano normativo, a Lei nº 14.155/2021 promoveu relevante incremento punitivo ao introduzir qualificadoras e causas de aumento de pena no âmbito do estelionato eletrônico. Destacam-se, nesse contexto, o §4º do art. 171 do Código Penal, que prevê aumento de pena quando o crime é cometido contra idoso ou vulnerável, e o §2º-B, que majora a sanção quando há utilização de servidor localizado no exterior.

Todavia, a incidência prática destes dispositivos encontra limitação significativa na necessidade de identificação da autoria delitiva, o que raramente ocorre nos crimes digitais massificados. Conforme aponta o Fórum Brasileiro de Segurança Pública (2024), as instituições policiais não dispõem de capacidade de resposta proporcional ao crescimento dessa modalidade criminosa.

Dessa forma, verifica-se que a efetividade das inovações legislativas permanece condicionada à superação de obstáculos investigativos estruturais. Em cenários de baixa resolutividade, tais previsões legais assumem, em certa medida, caráter simbólico, na medida em que sua aplicação concreta depende de condições raramente verificadas na prática investigativa. Assim, a discrepância entre a sofisticação normativa e a capacidade operacional do Estado evidencia um descompasso que compromete a eficácia da política criminal voltada ao enfrentamento das fraudes digitais.

Portanto, a análise comparativa entre casos de alta e baixa visibilidade revela um duplo desafio: de um lado, a necessidade de resposta institucional a ameaças como as *deepfakes*, que impactam diretamente o processo democrático; de outro, a urgência de aprimoramento dos mecanismos de investigação e repressão dos delitos patrimoniais cotidianos, que, por sua magnitude, atingem massivamente a população. Sem o fortalecimento estrutural das instituições responsáveis pela persecução penal, a tendência é a manutenção de um cenário em que a legislação penal, embora formalmente rigorosa, apresenta eficácia limitada no plano concreto.

2.3 DESAFIOS TÉCNICO-INVESTIGATIVOS REGIONAIS

A persecução penal dos delitos de estelionato digital não encontra obstáculos apenas na legislação ou na definição da competência jurisdicional. Ela esbarra, de forma significativa, em desafios de natureza técnica e estrutural que comprometem a efetividade da resposta estatal, especialmente quando considerada a realidade da Região Norte do Brasil. A com-

plexidade inerente aos cibercrimes exige aparato investigativo altamente especializado, dotado de recursos tecnológicos adequados e de profissionais devidamente capacitados, realidade ainda distante em grande parte das polícias judiciárias nortistas.

A doutrina especializada converge para a identificação de três eixos centrais de deficiência na investigação de crimes digitais: a insuficiência de equipamentos tecnológicos, a ausência de softwares forenses especializados e a capacitação inadequada dos agentes públicos.

Conforme aponta Dias (2012), o elevado grau de tecnicidade do cibercrime, frequentemente associado ao uso de criptografia, credenciais de acesso e servidores operando em redes transnacionais, como a *deep web* e a *dark web*, exige do investigador conhecimentos e ferramentas compatíveis para o rastreamento das operações, a identificação da autoria e a adequada coleta de provas digitais aptas à utilização em juízo. Nesse sentido, a autora destaca que a carência desses recursos “impõe elevada exigência técnica ao investigador, dificultando tanto a investigação quanto a produção probatória, o que eleva a probabilidade de impunidade” (Dias, 2012, p. 73).

Esse quadro se intensifica diante do avanço de tecnologias de falsificação digital, cuja detecção apresenta elevado grau de complexidade técnica. No caso das *deepfakes*, Oliveira e Ávila (2024) ressaltam que a identificação dessas manipulações demanda conhecimento especializado e multidisciplinar, envolvendo áreas como inteligência artificial, análise audiovisual e ciência de dados, competências que, em regra, extrapolam a formação tradicional dos órgãos de investigação.

Os autores também evidenciam uma dinâmica de constante evolução tecnológica, na qual os mecanismos de detecção buscam identificar padrões como inconsistências faciais ou anomalias visuais, ao passo que as ferramentas de criação se aperfeiçoam continuamente, tornando os conteúdos cada vez mais realistas e de difícil distinção.

Ao transpor essa problemática para a realidade da Região Norte, verifica-se que tais limitações assumem contornos ainda mais acentuados. Os dados apresentados por Souza (2025) evidenciam significativa disparidade na estrutura de enfrentamento aos crimes cibernéticos entre os estados da região.

Enquanto o Amapá dispõe de Delegacia Especializada de Repressão à Fraude Eletrônica (DRFE) e o Pará conta com Diretoria Estadual de Combate a Crimes Cibernéticos (DECCC) estruturada em divisões específicas, outras unidades federativas apresentam capacidade institucional reduzida. O Estado do Acre, por exemplo, conta apenas com o Núcleo Especializado de Apoio a Investigações de Crimes Cibernéticos (NECIBER), cuja atuação se limita ao suporte técnico às demais unidades policiais, sem constituir unidade investigativa autônoma (Gadelha, 2021 apud Souza, 2025).

Em cenário ainda mais crítico, Souza (2025) aponta que, nos estados de Rondônia e Roraima, não se identificam estruturas formalmente especializadas no enfrentamento de crimes digitais. Tal realidade impõe às delegacias comuns, já sobrecarregadas com a criminalidade tradicional, a condução de investigações que demandam elevado grau de especialização técnica e recursos tecnológicos específicos, para os quais, em regra, não estão adequadamente preparadas.

Além da escassez de unidades especializadas, há um fator estrutural adicional: a concentração desses recursos nas capitais. Conforme evidenciado pelo referido estudo, mesmo nos estados que possuem estruturas voltadas ao combate ao cibercrime, estas permanecem centralizadas nos grandes centros urbanos.

Tal configuração revela-se incompatível com a natureza descentralizada e frequentemente transnacional dos delitos digitais. O agente pode atuar a partir de qualquer localidade, inclusive fora do território nacional, enquanto os meios técnicos para sua identificação permanecem geograficamente restritos, gerando entraves logísticos e comprometendo a celeri-

dade necessária à obtenção e preservação de dados telemáticos, os quais são, por sua própria natureza, voláteis.

Dessa forma, os desafios técnico-investigativos regionais configuram um dos principais entraves à efetividade da norma penal no âmbito dos crimes digitais. A conjugação entre deficiência de infraestrutura tecnológica, limitações na capacitação profissional, complexidade intrínseca das novas formas de fraude e concentração dos recursos especializados produz um cenário de baixa capacidade investigativa e reduzida resolutividade.

Tal realidade contribui diretamente para a manutenção de elevados índices de subnotificação e para o fortalecimento da percepção de impunidade, comprometendo, em última análise, a eficácia concreta do tipo penal de fraude eletrônica, cuja aplicação tende a se tornar residual, evidenciando o descompasso entre a sofisticação normativa e a capacidade operacional do Estado na Região Norte.

3 EFETIVIDADE PUNITIVA E PROPOSTAS DE APRIMORAMENTO

A análise empreendida no capítulo anterior revelou as significativas limitações que comprometem a aplicação da Lei nº 14.155/2021 na Região Norte, desde a escassez de dados sistematizados sobre *deepfakes* até a precariedade da infraestrutura investigativa. A constatação desses entraves, contudo, não esgota a investigação sobre a resposta penal estatal às fraudes digitais. Torna-se necessário, neste momento, examinar em que medida a reforma legislativa tem produzido efeitos concretos no enfrentamento da criminalidade cibernética e, sobretudo, identificar caminhos para o aprimoramento do sistema punitivo.

O presente capítulo dedica-se, portanto, a uma análise crítica da eficácia da Lei nº 14.155/2021 na Região Norte, cotejando as expectativas doutrinárias que saudaram a inovação legislativa com a realidade regional documentada empiricamente. A partir desse diagnóstico, são examinadas as limitações estruturais e jurídicas que dificultam a persecução penal e,

ao final, apresentadas propostas de aprimoramento normativo e institucional voltadas a conferir maior efetividade à tutela penal no ambiente digital, especialmente em contextos marcados por assimetrias estruturais como as que caracterizam a Região Norte.

3.1 ANÁLISE CRÍTICA DA EFICÁCIA DA LEI NA REGIÃO NORTE

A Lei nº 14.155/2021 promoveu significativa reformulação no tratamento penal dos crimes patrimoniais praticados em ambiente digital, especialmente ao agravar as penas e introduzir qualificadoras específicas para condutas cometidas por meios eletrônicos. Dentre as principais inovações, destacam-se a alteração do art. 154-A do Código Penal, com supressão da exigência de violação de mecanismo de segurança e aumento da pena para o crime de invasão de dispositivo informático; a criação da qualificadora do furto mediante fraude eletrônica (art. 155, §4º-B); e a introdução da fraude eletrônica como forma qualificada de estelionato (art. 171, §2º-A), com recrudesimento sancionatório e ampliação do âmbito de incidência dos tipos penais, além de causas de aumento vinculadas à transnacionalidade da conduta e à vulnerabilidade da vítima.

Conforme destaca Rogério Sanches Cunha (2021), a reforma legislativa teve como objetivo central superar lacunas normativas e conferir maior rigor punitivo às condutas praticadas no ambiente virtual, sobretudo diante da crescente sofisticação dos meios utilizados pelos agentes criminosos. O doutrinador enfatiza a importância da distinção entre as duas novas figuras qualificadas: no furto mediante fraude eletrônica, a manobra ardilosa visa afastar a vigilância da vítima e possibilitar a subtração sem que ela perceba; já no estelionato digital, a vítima, induzida em erro, fornece voluntariamente informações sob erro induzido, permitindo ao agente a obtenção da vantagem ilícita.

No âmbito processual, a Lei nº 14.155/2021 resolveu antiga controvérsia jurisprudencial ao introduzir o §4º no art. 70 do Código de Processo Penal, fixando o domicílio da vítima como foro competente para julgar-

mento nos crimes de estelionato praticados mediante depósito, transferência de valores ou emissão de cheques sem fundos.

Até então, como observa Cunha (2021), a Terceira Seção do Superior Tribunal de Justiça oscilava entre fixar a competência pelo local da agência bancária da vítima, quando se tratava de saque ou compensação de cheque, e pelo local da conta de destino dos valores, quando a vítima efetuava depósito ou transferência. A nova regra, portanto, pacificou a matéria e conferiu previsibilidade ao processo, alinhando a disciplina legal à lógica de proteção da vítima e à facilitação do acesso à justiça, ainda que sem resolver os entraves investigativos subjacentes.

Contudo, a análise da eficácia da Lei nº 14.155/2021 na Região Norte revela um cenário de descompasso entre a sofisticação normativa e a capacidade operacional do sistema de justiça criminal. Embora o legislador tenha promovido o recrudescimento das penas e ampliado o alcance dos tipos penais, a aplicação concreta dessas disposições encontra limitações estruturais significativas, já evidenciadas no capítulo anterior.

Em primeiro lugar, observa-se que o incremento punitivo, isoladamente considerado, revela-se insuficiente como instrumento de política criminal eficaz. Isso porque a incidência das normas penais depende, necessariamente, da identificação da autoria delitiva, o que constitui um dos principais entraves nos delitos cibernéticos. A natureza transnacional dessas condutas, aliada ao uso de tecnologias de anonimização e à volatilidade das provas digitais, dificulta sobremaneira o rastreamento dos agentes e a produção probatória apta à condenação.

Além disso, a própria estrutura dos tipos penais introduzidos pela Lei nº 14.155/2021 pressupõe um nível de apuração técnica que nem sempre é viável na prática investigativa regional. A caracterização da fraude eletrônica, por exemplo, exige a demonstração do meio empregado (redes sociais, contatos telefônicos, correio eletrônico fraudulento ou outro meio análogo), da indução em erro e da obtenção da vantagem ilícita, elementos que, em muitos casos, dependem de perícias digitais complexas e

de cooperação com provedores de serviços localizados fora do território nacional.

Outro aspecto relevante refere-se às causas de aumento de pena previstas na lei, especialmente aquelas relacionadas à utilização de servidores no exterior (art. 155, §4º-C, I, e art. 171, §2º-B). Conforme aponta Cunha (2021), a referência à “relevância do resultado gravoso” deve servir não para definir a incidência da majorante, mas para graduar a fração de aumento dentro dos limites legais. Não obstante a pertinência dogmática da observação, a aplicação prática desses dispositivos é limitada pela dificuldade de comprovação da transnacionalidade da execução criminosa, o que depende de recursos técnicos e de cooperação internacional nem sempre disponíveis aos órgãos de investigação da Região Norte.

No mesmo sentido, a majorante relativa à condição da vítima, idoso ou vulnerável (art. 155, §4º-C, II, e art. 171, §4º), também enfrenta obstáculos probatórios relevantes, sobretudo em crimes praticados em larga escala, nos quais o agente não possui contato direto com a vítima, dificultando a demonstração do dolo quanto a essa circunstância. Cunha (2021) adverte que a majoração da pena pressupõe a ciência dessas condições pelo agente, o que nem sempre ocorre em razão da natureza impessoal dos crimes cibernéticos.

Diante desse panorama, verifica-se que a Lei nº 14.155/2021 possui elevada densidade normativa, mas eficácia prática limitada na Região Norte. O problema central não reside propriamente na inadequação dos tipos penais ou na insuficiência das penas cominadas, mas na incapacidade estrutural do Estado de operacionalizar a persecução penal em face de crimes que exigem elevada especialização técnica.

Assim, confirma-se a hipótese de que o recrudescimento legislativo, desacompanhado de investimentos institucionais e tecnológicos, tende a produzir efeitos predominantemente simbólicos, caracterizando fenômeno que a doutrina denomina de Direito Penal simbólico, conceito formulado por Hassemer (2008, p. 215-216):

Portanto, “simbólico”, em sua compreensão crítica, consiste no atributo que uma norma penal apresenta, segundo o qual as funções latentes da norma suplantam suas funções manifestas, de maneira a gerar a expectativa de que o emprego e o efeito da norma concretizarão uma situação diversa da anunciada pela própria norma.

A lei, nesse contexto, cumpre relevante função de reafirmação dos valores protegidos pelo ordenamento jurídico, mas não se traduz, de forma consistente, em aumento da capacidade de investigação, processamento e punição dos agentes.

Portanto, a análise crítica da eficácia da Lei nº 14.155/2021 na Região Norte evidencia que, embora a reforma tenha representado avanço no plano normativo, sua efetividade permanece condicionada à superação de obstáculos estruturais, especialmente no âmbito da investigação criminal. Sem a reestruturação dos mecanismos investigativos e o fortalecimento institucional dos órgãos de persecução penal, a tendência é a manutenção de um cenário em que a resposta penal permanece formalmente rigorosa, porém materialmente ineficaz.

3.2 PROPOSTAS DE APRIMORAMENTO

O diagnóstico traçado ao longo deste trabalho revela que a efetividade da Lei nº 14.155/2021 na Região Norte é comprometida por limitações que operam em múltiplas dimensões (normativa, estrutural e operacional), exigindo respostas igualmente diversificadas.

Nesse sentido, apresentam-se propostas de aprimoramento que contemplam tanto o aperfeiçoamento do arcabouço jurídico quanto o fortalecimento da capacidade institucional do Estado, com especial atenção às assimetrias regionais que caracterizam o sistema de justiça criminal brasileiro. No plano normativo, impõe-se, em primeiro lugar, o reconhecimento de que a ausência de tipo penal específico para condutas envolvendo *deepfakes* constitui lacuna relevante no ordenamento jurídico.

Oliveira e Ávila (2024) demonstram que essa tecnologia não se amolda com precisão aos tipos penais atualmente existentes, demandando esforço de adequação típica que, por vezes, tensiona o princípio da legalidade estrita. Os autores propõem recomendações e soluções voltadas à proteção dos indivíduos contra os abusos decorrentes do uso dessa tecnologia, destacando a necessidade de adaptação do Direito Penal ao enfrentamento dessa nova forma de criminalidade.

Nesse contexto, a criação de tipo penal autônomo para a conduta de criar, divulgar ou utilizar *deepfakes* com finalidade ilícita conferiria maior segurança jurídica à persecução penal e possibilitaria a produção de dados estatísticos mais precisos sobre o fenômeno, superando a atual invisibilidade estatística evidenciada neste trabalho.

No plano internacional, o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, conhecido como *AI Act*, em vigor desde agosto de 2024, oferece modelo regulatório apto a inspirar o legislador brasileiro. O art. 50, § 4º, do referido diploma estabelece obrigação específica para os implementadores de sistemas de IA que gerem ou manipulem conteúdos que constituam *deepfakes*, determinando que seja divulgada, de forma clara, a natureza artificial do conteúdo, salvo nas hipóteses em que a utilização seja autorizada por lei para fins de detecção, prevenção, investigação ou repressão de infrações penais, ou quando o material integrar obra manifestamente artística, criativa, satírica ou ficcional, caso em que a exigência de transparência se limita a uma divulgação adequada que não prejudique sua fruição.

Complementarmente, o § 2º do mesmo artigo impõe aos fornecedores de sistemas de IA que geram conteúdo sintético, de áudio, imagem, vídeo ou texto, o dever de assegurar que tais conteúdos sejam marcados em formato legível por máquina e detectáveis como artificialmente gerados ou manipulados. Trata-se de uma abordagem regulatória de caráter eminentemente preventivo, centrada na identificação e na rastreabilidade do conteúdo sintético, que contrasta com a resposta predominantemente

repressivo-penal observada no ordenamento jurídico brasileiro, ainda ancorada na subsunção a tipos penais tradicionais.

Nesse contexto, a eventual incorporação de mecanismos análogos no Brasil, especialmente a imposição de deveres de rotulagem e transparência, combinada com a responsabilização penal em hipóteses de utilização dolosa para a prática de ilícitos, poderia ampliar a efetividade da tutela dos bens jurídicos afetados pelas *deepfakes*, reduzindo a assimetria atualmente existente entre a sofisticação tecnológica desses sistemas e a capacidade de resposta estatal.

Em segundo lugar, a obtenção de provas digitais constitui um dos principais gargalos da investigação criminal, especialmente em regiões com infraestrutura limitada, como a Região Norte. O Marco Civil da Internet (Lei nº 12.965/2014) estabelece, em seus arts. 10 e 11, que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet devem observar a preservação da intimidade e da vida privada, sendo condicionadas, em regra, à prévia ordem judicial.

O art. 22, por sua vez, prevê a possibilidade de requisição judicial desses registros, desde que presentes fundados indícios da ocorrência do ilícito, justificativa quanto à utilidade da medida e delimitação temporal adequada. Embora tais dispositivos representem avanço relevante na disciplina da matéria, a efetividade da persecução penal nos crimes digitais demanda regulamentação mais detalhada da prova digital no Código de Processo Penal, com a definição de parâmetros claros quanto à coleta, preservação, cadeia de custódia, admissibilidade e valoração judicial dessas evidências, de modo a conferir maior celeridade, segurança jurídica e padronização procedimental.

Em terceiro lugar, revela-se necessária a implementação de mecanismos mais céleres e eficazes de cooperação jurídica internacional para a obtenção de dados armazenados em servidores localizados no exterior, conferindo efetividade, inclusive, às causas de aumento de pena relacio-

nadas à transnacionalidade da conduta, como previsto no §2º-B do art. 171 do Código Penal.

A celebração e o aprimoramento de acordos bilaterais e multilaterais que simplifiquem o intercâmbio de informações digitais mostram-se essenciais para evitar que a persecução penal seja inviabilizada pela fragmentação jurisdicional característica do ambiente virtual. No plano institucional, as medidas devem priorizar o fortalecimento da estrutura investigativa nos estados da Região Norte.

Dados do Fórum Brasileiro de Segurança Pública (2024) revelam crescimento expressivo dos estelionatos praticados por meio eletrônico, com taxas elevadas em estados como Rondônia e Roraima, o que evidencia a urgência da criação de delegacias especializadas em crimes cibernéticos nas unidades federativas que ainda não dispõem dessas estruturas, bem como a descentralização dessas unidades para municípios estratégicos.

A concentração de recursos nas capitais mostra-se incompatível com a natureza difusa, ubíqua e frequentemente transnacional dos delitos digitais. Tais iniciativas devem ser acompanhadas de investimentos em infraestrutura tecnológica, aquisição de ferramentas de análise forense digital e implementação de programas permanentes de capacitação técnica dos agentes públicos.

Iniciativas institucionais já existentes podem servir de parâmetro para a formulação dessas políticas públicas. (Chesney; Citron, 2019 apud Ferreira; Leme, 2023) mencionam a Resolução TSE nº 742/2021 como exemplo de resposta institucional articulada ao fenômeno da desinformação digital. Embora direcionada à proteção do processo eleitoral, a medida evidencia a viabilidade de estratégias coordenadas entre diferentes órgãos do sistema de justiça para o enfrentamento de fenômenos complexos, como as *deepfakes*, indicando a necessidade de expansão desse modelo para outras esferas da tutela jurídica.

Em síntese, a efetividade da tutela penal no ambiente digital depende menos de reformas legislativas isoladas e mais da implementação de uma política pública integrada, que contemple simultaneamente o aprimoramento normativo, o fortalecimento institucional e a redução das desigualdades regionais. Sem esse enfoque multidimensional, novas alterações legislativas tenderão a reproduzir o descompasso já identificado entre a sofisticação normativa e a capacidade operacional do Estado, mantendo a resposta penal aos crimes digitais, como até o presente momento, em um plano predominantemente simbólico.

CONSIDERAÇÕES FINAIS

A presente pesquisa analisou a evolução normativa dos crimes cibernéticos no Brasil, com foco na Lei nº 14.155/2021, no enquadramento das *deepfakes* e nos desafios da persecução penal na Região Norte. Os resultados confirmaram a hipótese inicial: embora haja relevante avanço legislativo com as Leis nº 12.737/2012 e nº 14.155/2021, a efetividade prática permanece limitada por déficits estruturais, tecnológicos e institucionais, agravados por assimetrias regionais.

Verificou-se que o avanço normativo não acompanha a velocidade da inteligência artificial generativa. Ante a ausência de tipificação específica, as *deepfakes* exigem adequação típica indireta aos crimes já existentes, o que gera fragilidades interpretativas e insegurança jurídica na proteção da honra, da imagem, da privacidade e da estabilidade institucional.

No âmbito processual, sobressaem-se barreiras como a transnacionalidade, o anonimato e a volatilidade probatória. Na Região Norte, esse quadro é acentuado pela escassez de delegacias especializadas, concentração de recursos nas capitais e insuficiência de capacitação técnica, resultando em reduzida taxa de elucidação, expressiva subnotificação, diluição estatística das *deepfakes* e formação de uma vasta “cifra negra”. Constatou-se, ainda, assimetria institucional: casos envolvendo figuras

públicas tendem a receber maior atenção institucional, enquanto os crimes patrimoniais cotidianos contra vítimas anônimas permanecem invisibilizados.

Conclui-se que a efetividade da tutela penal no ambiente digital não decorre do mero recrudescimento punitivo, mas de uma política criminal integrada que articule aprimoramento normativo, fortalecimento institucional e redução das desigualdades regionais no acesso à tecnologia e à justiça. Sem a integração entre Direito, tecnologia e políticas públicas, o sistema penal permanecerá formalmente sofisticado, porém materialmente limitado a uma eficácia simbólica. A invisibilidade estatística das *deepfakes* na Região Norte é o sintoma de um aparato estatal ainda não equipado para a criminalidade do século XXI nas periferias do país, revelando que a promessa de tutela penal igualitária permanece inconclusa.

REFERÊNCIAS

BASTOS, J. T. **Crime cibernético e o estelionato virtual**. 2016. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Regional Integrada do Alto Uruguai e das Missões, Erechim, 2016. Disponível em: https://www.uricer.edu.br/cursos/arq_trabalhos_usuario/4259.pdf. Acesso em: 21 set. 2025.

BOTELHO, Thaís Helena Falcão; NÖTH, Winfried. **Deepfake**: inteligência artificial para discriminação e geração de conteúdos. TECCOGS – Revista Digital de Tecnologias Cognitivas, n. 23, p. 69–78, jan./jun. 2021.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. **Diário Oficial da União**: Rio de Janeiro, 31 dez. 1940.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**: Rio de Janeiro, 13 out. 1941.

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.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). **Diário Oficial da União**: Brasília, DF, 24 abr. 2014. Disponível em: <https://>

www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 ago. 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal e o Código de Processo Penal para dispor sobre crimes eletrônicos. **Diário Oficial da União**: Brasília, DF, 28 maio de 2021.

BRASIL. Lei nº 14.197, de 1º de setembro de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para dispor sobre os crimes contra o Estado Democrático de Direito. **Diário Oficial da União**: Brasília, DF, 2 set. 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14197.htm. Acesso em: 28 ago. 2026.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. **Dispõe sobre o desenvolvimento, a implementação e o uso responsável de sistemas de inteligência artificial no Brasil**. Brasília, DF: Senado Federal, 2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 28 ago. 2026.

BRASIL. Supremo Tribunal Federal. **Guia ilustrado contra as deepfakes**. Brasília: STF, Coordenadoria de Combate à Desinformação, 2024.

BRASIL. Tribunal de Justiça do Estado do Acre. **Agravo de Instrumento nº 1001508-23.2024.8.01.0000**. Relatora: Des^a. Waldirene Cordeiro. Segunda Câmara Cível. Julgado em 10 set. 2024. Disponível em: <https://esaj.tjac.jus.br/cjsg/resultadoCompleta.do>. Acesso em: 5 abr. 2026.

BRASIL. Tribunal de Justiça do Estado do Acre. **Agravo de Instrumento nº 1001933-50.2024.8.01.0000**. Relatora: Des^a. Waldirene Cordeiro. Segunda Câmara Cível. Julgado em 22 dez. 2024. Disponível em: <https://esaj.tjac.jus.br/cjsg/resultadoCompleta.do>. Acesso em: 2 abr. 2026.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 742, de 10 de agosto de 2021**. Dispõe sobre o enfrentamento à desinformação no processo eleitoral. Brasília, DF: TSE, 2021. Disponível em: <https://www.tse.jus.br/legislacao/resolucoes>. Acesso em: 28 ago. 2026.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital**: primeiras impressões e reflexos no CP e no CPP. Meu Site Jurídico, 2021. Disponível em: <https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimes-de-fraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/>. Acesso em: 2 abr. 2026.

DELMANTO, Celso. **Código Penal comentado**. São Paulo: Saraiva, 2016.

DIAS, Vera Marques. A problemática da investigação do cibercrime. **Data Venia — Revista Jurídica Digital**, ano 1, n. 1, p. 63-88, jul./dez. 2012. Disponível em: <https://www.datavenia.pt/edicoes/DataVenia01.pdf>. Acesso em: 5 abr. 2026.

FERREIRA, Amanda Passos; LEME, Carolina da Silva. **O fenômeno da deepfake no contexto eleitoral e seus efeitos no Estado Democrático de Direito**. Boletim IBCCRIM, São Paulo, v. 31, n. 363, p. 21–23, 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1573. Acesso em: 1 abr. 2026.

FERREIRA, Jhonatan Fernando. **Dos crimes contra o Estado Democrático de Direito e da tutela penal aos bens jurídicos essenciais**. 2024. Dissertação (Mestrado em Direito Político e Econômico) – Universidade Presbiteriana Mackenzie, São Paulo, 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário brasileiro de segurança pública 2024**. São Paulo, 2024.

GRECO, Rogério. **Curso de Direito Penal: parte especial**. 11. ed. Niterói: Impetus, 2014. v. 2.

HASSEMER, Winfried. **Direito Penal: Fundamentos, estrutura, política**. Porto Alegre: Editora Sérgio Antonio Fabris, 2008.

LIMA, Renato Sérgio de; BUENO, Samira. **As novas configurações dos crimes patrimoniais no Brasil**. In: Anuário Brasileiro de Segurança Pública. São Paulo, 2023.

OLIVEIRA, Giovanna Aleixo Gonçalves; ÁVILA, Gustavo Noronha de. *Deepfake*, direitos da personalidade e o direito penal: uma análise dos impactos tecnológicos na era digital. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 19, 2024. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/85239>. Acesso em: 2 abr. 2026.

SOUZA, Vinícius Cunha de. **Crimes cibernéticos e os desafios investigativos na Região Norte do Brasil**. 2025. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Tocantins, Palmas, 2025. Disponível em: <https://umbu.uft.edu.br/bitstream/11612/8166/1/TCC%20-%20Monografia%20Direito%20-%20Vin%C3%ADcius%20Cunha%20de%20Souza.pdf>. Acesso em: 5 abr. 2026.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Cria regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial). **Jornal Oficial da União Europeia**, Bruxelas, 12 jul. 2024. Disponível em: <https://artificialintelligenceact.eu/article/50/>. Acesso em: 12 mai. 2026.