FRAUDES DIGITAIS E SEGURANÇA PÚBLICA: A ATUAÇÃO INTEGRADA ENTRE JUIZADOS ESPECIAIS, MINISTÉRIO PÚBLICO E POLÍCIA MILITAR

DIGITAL FRAUD AND PUBLIC SECURITY: INTEGRATED ACTION BETWEEN SPECIAL COURTS, PUBLIC PROSECUTOR'S OFFICE AND MILITARY POLICE

Douglas Angelo Ferrari - Possui Bacharelado em Engenharia de Software pelo Centro Universitário Internacional - UNINTER (2025). Graduação em Gestão Pública pelo Centro Universitário Internacional - UNINTER (2017). Possui especializações em Direito Penal e Processo Penal (Faculdade Unina, 2022), Direito Público (Faculdade Legale, 2020), Segurança Pública (Faculdade Unina, 2020) e Polícia Comunitária (Centro Universitário Leonardo da Vinci UNIASSELVI, 2022). Atualmente é policial militar - Polícia Militar do Paraná.Lattes: http://lattes.cnpq.br/6162042230506144

Marcianita Lopata de Lima - Mestre em Direito Empresarial e Cidadania pelo Centro Universitário Curitiba-UNICURITIBA (2022). Especialização em Gestão Contábil e Tributária pela Universidade Federal do Paraná - UFPR (2019). Especialização em LGPD pela Legale Educacional (2021). Especialização em Direito Empresarial pela Legale Educacional (2021). Especialização em Planejamento Previdenciário pela Legale Educacional (2022). MBA em Gestão de Pessoas pela FACET (2014). Bel. em Direito pela FACEAR (2009). Advogada. Atualmente Coordenadora Financeira e Contábil - Comesp - Consorcio Metropolitano de Serviços do Paraná. Registro no Orcid: https://orcid.org/0000-0002-4300-2968.

Flávia Jeanne Ferrari - Doutoranda e Mestre em Direito Empresarial e Cidadania pelo Centro Universitário Curitiba-UNICURITIBA. Possui especializações nas áreas de Licitações e Contratos; Educação 4.0; Direito Público; Direito Militar; Processo Civil; Direito Ambiental; Direito do Trabalho e Ministério Público - Estado Democrático de Direito pela Fundação Escola do Ministério Público - FEMPAR em parceria com a Universidade Positivo. Técnica em Transações Imobiliárias pela IFPR e Bel. Direito. Pregoeira. Advogada inscrita na OAB-PR. Professora na graduação de Direito na UNIFAEL. Estágio docente na graduação de Direito do Centro Universitário Curitiba - UNICURITIBA. Professora Universitária. Professora Conteudista. Professora de pós graduação. Registro ORCID: 0000-0002-3990-7633. Lattes: //lattes.cnpq.br/1064406440921045

A massificação das tecnologias de informação e comunicação reconfigurou as dinâmicas sociais e, concomitantemente, metamorfoseou o panorama da criminalidade. As fraudes digitais, impulsionadas por mecanismos como engenharia social, phishing e exploração de vulnerabilidades em sistemas de pagamento instantâneo como o PIX, emergiram como um dos principais desafios contemporâneos à segurança pública. Caracterizadas pela transnacionalidade, alta volumetria, baixa percepção de risco pelo agressor e pulverização dos danos, essas infrações tensionam os modelos tradicionais de persecução penal, concebidos para uma realidade analógica e territorializada. O presente artigo científico analisa, sob a ótica jurídico-institucional, a premente necessidade de superação da fragmentação operacional no combate a esse fenômeno. O objetivo central é investigar a viabilidade e a eficácia de um modelo de atuação integrada entre a Polícia Militar, o Ministério Público e os Juizados Especiais Criminais (JECRIM) como resposta sistêmica ao problema. Partindo de uma análise da inadequação dos fluxos procedimentais vigentes – que frequentemente resultam em subnotificação, gargalos investigativos e sensação de impunidade – propõe-se um paradigma de colaboração estruturada. A metodologia empregada baseia-se na análise bibliográfica e documental de doutrina jurídica, legislação pátria (notadamente a Lei 9.099/95, o Código Penal com as alterações da Lei 14.155/2021, e o Marco Civil da Internet), e dados estatísticos de fontes oficiais. Argumenta-se que a Polícia Militar, como órgão de primeira resposta e capilaridade ímpar, deve atuar na coleta qualificada de dados estruturados; o Ministério Público, como dominus litis e titular da política criminal, na análise de padrões e na persecução penal estratégica de grandes massas de dados; e os Juizados Especiais, na aplicação célere e desburocratizada de medidas, alinhadas aos seus princípios fundantes. Conclui-se que apenas a implementação de fluxos operacionais interoperáveis, baseados em tecnologia e inteligência compartilhada, pode conferir ao Estado a capacidade de preservar a ordem pública e a incolumidade patrimonial no emergente e volátil território digital, reafirmando a autoridade estatal e a proteção ao cidadão.

PALAVRAS-CHAVE: Fraudes Digitais. Segurança Pública. Atuação Integrada. Ministério Público. Polícia Militar. Juizados Especiais Criminais**.**

The massification of information and communication technologies has reconfigured social dynamics and, concomitantly, metamorphosed the landscape of crime. Digital fraud, driven by mechanisms such as social engineering, phishing, and the exploitation of vulnerabilities in instant payment systems like PIX, has emerged as one of the primary contemporary challenges to public safety. Characterized by transnationality, high volume, low risk perception by the aggressor, and pulverized damages, these offenses strain traditional models of criminal prosecution, which were designed for an analog and territorialized reality. This scientific article analyzes, from a legal-institutional perspective, the pressing need to overcome operational fragmentation in combating this phenomenon. The main objective is to investigate the feasibility and effectiveness of an integrated action model involving the Military Police, the Public Prosecutor's Office (Ministério Público), and the Special Criminal Courts (JECRIM) as a systemic response to the problem. Starting from an analysis of the inadequacy of current procedural flows – which often result in underreporting, investigative bottlenecks, and a sense of impunity – a paradigm of structured collaboration is proposed. The methodology employed is based on bibliographic and documentary analysis of legal doctrine, national legislation (notably Law 9.099/95, the Penal Code with amendments from Law 14.155/2021, and the Marco Civil da Internet), and statistical data from official sources. It is argued that the Military Police, as the first response body with unparalleled capillarity, should act in the qualified collection of structured data; the Public Prosecutor's Office, as dominus litis and holder of criminal policy, in pattern analysis and strategic criminal prosecution of large data masses; and the Special Courts, in the swift and debureaucratized application of measures, aligned with their founding principles. It is concluded that only

the implementation of interoperable operational flows, based on technology and shared intelligence, can provide the State with the capacity to preserve public order and patrimonial integrity in the emerging and volatile digital territory, reaffirming state authority and citizen protection.

***Keywords**: Digital Fraud. Public Safety. Integrated Action. Public Prosecutor's Office. Military Police. Special Criminal Courts*

INTRODUÇÃO

A sociedade contemporânea assiste a uma digitalização exponencial das relações humanas. O ciberespaço, antes um domínio restrito à vanguarda tecnológica, consolidou-se como a principal arena para transações comerciais, interações sociais e o exercício da cidadania. Esta migração, acelerada por eventos globais e pela conveniência de ferramentas como os pagamentos instantâneos – notadamente o sistema PIX no Brasil, que revolucionou a dinâmica financeira –, trouxe consigo não apenas progresso, mas a sofisticação e a massificação de condutas criminosas. As fraudes digitais, em suas múltiplas roupagens (como *phishing*, *pharming*, engenharia social e golpes de falsa central de atendimento), deixaram de ser incidentes isolados para se tornarem um fenômeno endêmico, com profundo impacto na estabilidade econômica e na sensação de segurança da população.

Conforme dados da Federação Brasileira de Bancos (FEBRABAN), os golpes e fraudes digitais cresceram exponencialmente nos últimos anos, acompanhando a digitalização bancária. O Anuário Brasileiro de Segurança Pública (2023) corrobora essa percepção, indicando que o estelionato, em grande parte impulsionado por sua modalidade virtual, é um dos crimes patrimoniais com maior índice de crescimento no país. Este cenário revela uma dura realidade: o aparato estatal de persecução penal, historicamente moldado para combater o crime físico e territorializado, encontra-se em severa dificuldade para responder a esta nova modalidade delitiva. A velocidade, o anonimato relativo, a transnacionalidade e, principalmente, a escala industrial das fraudes digitais impõem um desafio sistêmico.

O problema central que este artigo enfrenta é a ineficácia do modelo atual de persecução penal para lidar com crimes de fraude digital de alta volumetria e baixo valor individual. A estrutura tradicional é fragmentada: a vítima, muitas vezes desorientada, registra um Boletim de Ocorrência (BO) – seja em uma delegacia da Polícia Civil ou, frequentemente, junto à Polícia Militar, a primeira porta de acesso ao Estado. Esse registro, por vezes incompleto e não padronizado, inicia um inquérito policial (quando o faz) que raramente avança, soterrado pela complexidade da coleta de provas digitais voláteis (como dados de conexão ou rastreamento de transações). O Ministério Público, destinatário final desses inquéritos, recebe peças informativas deficientes e pulverizadas, impossibilitando uma atuação estratégica. Por fim, os Juizados Especiais Criminais (JECRIM), idealizados pela Lei 9.099/95 para a resolução célere de infrações de menor potencial ofensivo – categoria na qual muitas dessas fraudes se enquadram –, não conseguem absorver essa demanda massificada ou oferecer

soluções efetivas que transcendam o caso individual.

Este ciclo de fragmentação gera um custo social devastador: a impunidade. O cidadão vê o Estado como incapaz de proteger seu patrimônio e de punir os responsáveis, erodindo a confiança nas instituições de segurança pública e justiça. A questão, portanto, transcende a esfera do ilícito patrimonial individual e se eleva a um problema de Segurança Pública. O Artigo 144 da Constituição Federal de 1988, ao definir a segurança como dever do Estado, não se restringe à desordem física, mas à preservação da "ordem pública e da incolumidade das pessoas e do patrimônio". A ordem pública, em seu sentido contemporâneo, abrange a própria estabilidade das relações sociais e econômicas, que hoje são predominantemente digitais. Como leciona o mestre José Afonso da Silva (2005, p. 764) sobre a amplitude do conceito:

> A segurança pública consiste numa situação de garantia e proteção dos direitos individuais e coletivos, assegurando a tranquilidade e a paz social. Não se trata apenas da ausência de criminalidade, mas de um estado de convivência ordenada e pacífica, onde o Estado atua para prevenir e reprimir ilícitos que perturbem essa convivência, seja no espaço físico ou, por extensão lógica, no ambiente digital que a ele se equivale funcionalmente. (SILVA, 2005, p. 764).

Diante desse diagnóstico, o objetivo deste trabalho é analisar a viabilidade jurídica e a necessidade operacional da implementação de um modelo de *atuação integrada* entre a Polícia Militar, o Ministério Público e os Juizados Especiais Criminais. A hipótese central é que a superação do modelo de silos institucionais, através da criação de fluxos de informação padronizados, interoperáveis e tecnologicamente assistidos, é a única resposta estratégica capaz de conferir eficiência à persecução penal dessa modalidade criminosa.

A justificativa para focar nesta tríade (PM-MP-JECRIM) reside em suas competências e características complementares. A Polícia Militar possui a capilaridade e a prontidão para ser o ponto de coleta qualificada da informação primária. O Ministério Público detém a titularidade da ação penal e a visão macroscópica necessária para identificar padrões e orquestrar a persecução de forma estratégica. Os Juizados Especiais, por sua vez, oferecem o arcabouço legal da celeridade, informalidade e desburocratização (GRINOVER et al., 2005), essencial para lidar com a demanda em massa.

Para desenvolver essa tese, o artigo utilizará uma metodologia de análise bibliográfica e documental, explorando a doutrina jurídica especializada em Direito Digital, Processo Penal e Segurança Pública, bem como a legislação pertinente. A abordagem será analítico-propositiva, iniciando com a caracterização do fenômeno (Seção 2) e a análise do arcabouço legal (Seção 3), passando pela crítica ao modelo fragmentado atual (Seção 4), para então detalhar a proposta de um fluxo operacional integrado (Seção 5) e os desafios à sua implementação (Seção 6). Espera-se, com isso, contribuir para o debate acadêmico e institucional sobre a modernização da segurança pública e do sistema

de justiça criminal, adequando-os aos desafios inadiáveis do século XXI.

2 O FENÔMENO DAS FRAUDES DIGITAIS: CARACTERIZAÇÃO E IMPACTO NA SEGURANÇA PÚBLICA

A compreensão da necessidade de integração institucional exige, primeiramente, um diagnóstico preciso da natureza do fenômeno a ser combatido. As fraudes digitais não são meramente a transposição de crimes patrimoniais tradicionais para um novo meio; elas representam uma nova categoria de ilícito com características próprias que desafiam fundamentalmente os pilares da investigação e da jurisdição.

2.1 A Nova Face do Estelionato: Conceituação e Tipologias

O núcleo da fraude digital reside na conduta tipificada, em sua maioria, no Artigo 171 do Código Penal brasileiro: o estelionato, definido como "obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento". O meio digital potencializa o "artifício, ardil" a níveis sem precedentes. As tipologias são vastas e mutáveis, adaptando-se rapidamente às novas tecnologias e comportamentos sociais.

Entre as mais disseminadas estão o *phishing* (pescaria digital), onde o criminoso se passa por uma entidade confiável para "pescar" dados sensíveis da vítima; o *pharming*, uma técnica mais sofisticada que redireciona o tráfego de um site legítimo para um servidor fraudulento; os golpes de engenharia social, que manipulam a psicologia da vítima (como o "golpe do WhatsApp" ou a "falsa central bancária"); e, mais recentemente, os golpes explorando o sistema PIX, que combinam a velocidade da transação instantânea com a engenharia social para induzir transferências irreversíveis. Tarcísio Teixeira (2020), ao discutir a criminalidade informática, destaca que o elemento central é a desmaterialização da conduta.

> O crime informático ou digital caracteriza-se, essencialmente, pela sua natureza intangível e pela sua capacidade de ser cometido à distância, rompendo com as barreiras geográficas tradicionais. O 'artifício' ou 'ardil' do estelionato migra do mundo físico para o ambiente virtual, potencializado pela escalabilidade da rede e pela dificuldade de rastreamento imediato do agente. (TEIXEIRA, 2020, p. 115).

A fraude não exige mais a presença física, a falsificação de um documento tangível ou a superação de uma barreira física. O "meio fraudulento" é um e-mail, um link, uma mensagem de texto. Essa desmaterialização torna o crime mais "limpo" e, para o agressor, aparentemente menos arriscado. O legislador buscou endereçar essa especificidade, como será visto, mas a velocidade da inovação criminosa supera em muito o ciclo legislativo.

2.2 A Criminologia do Ciberespaço: Fatores Impulsionadores

Quatro fatores criminológicos principais explicam a explosão das fraudes digitais:

escalabilidade, anonimato relativo, transnacionalidade e baixo custo.

Primeiro, a *escalabilidade*. Um fraudador não precisa mais enganar uma vítima por vez. Com um único disparo de e-mail de *phishing* ou a criação de um único site falso, ele pode atingir milhões de potenciais vítimas simultaneamente. O custo marginal de "atacar" a segunda ou a milionésima vítima é próximo de zero. Isso transforma a fraude de uma atividade "artesanal" para uma "industrial".

Segundo, o *anonimato relativo*. Embora a rastreabilidade digital seja tecnicamente possível, ela é complexa e exige cooperação de múltiplos atores (provedores de conexão, de aplicação, instituições financeiras). O uso de VPNs, redes *proxy*, criptografia e moedas digitais (embora menos comum em fraudes de varejo) dificulta a identificação da autoria. Como bem apontam Blum e Bruno (2021, p. 231), a prova digital é volátil e sua complexidade técnica serve como um escudo inicial para o delinquente.

Terceiro, a *transnacionalidade*. O servidor que hospeda o site falso pode estar na Rússia, o fraudador operando do Sudeste Asiático, a conta de "laranja" receptora dos valores no Brasil, e a vítima em qualquer lugar do território nacional. Essa pulverização geográfica quebra o pilar da territorialidade do processo penal, exigindo mecanismos de cooperação internacional (como os *Mutual Legal Assistance Treaties* - MLATs) que são notoriamente lentos e inadequados para a velocidade do crime digital.

Quarto, o *baixo custo e a percepção de risco*. O "investimento" para cometer a fraude é baixo – muitas vezes, apenas o acesso à internet e o conhecimento de técnicas básicas de engenharia social. A percepção de risco de ser pego e efetivamente punido é baixíssima, criando um desequilíbrio na equação racional do crime: a recompensa potencial é alta e o risco percebido é mínimo.

2.3 O Transbordamento da Esfera Privada: A Fraude Digital como Ameaça à Ordem Pública

Por muito tempo, o estelionato foi visto como um crime estritamente patrimonial, de interesse predominantemente privado. A própria legislação, com a alteração promovida pela Lei 13.964/2019 (Pacote Anticrime), tornou a ação penal para o estelionato, em regra, pública condicionada à representação da vítima, reforçando essa visão. Contudo, a massificação da fraude digital obriga a uma releitura desse paradigma.

Quando dezenas de milhares de cidadãos são fraudados diariamente, quando a confiança no principal sistema de pagamento instantâneo do país (PIX) é abalada, quando a sensação de insegurança migra do espaço físico (a rua) para o espaço virtual (o aplicativo bancário), não se está mais diante de uma soma de litígios privados. Está-se diante de uma ameaça sistêmica à *ordem pública* e à *incolumidade patrimonial* coletiva.

O Artigo 144 da Constituição Federal de 1988 estabelece a segurança pública como um dever do Estado, exercida para a preservação desses dois pilares. A interpretação desse artigo não pode ficar restrita ao século XX. A "ordem

pública" hoje inclui a estabilidade e a confiabilidade do ambiente digital onde a vida econômica e social se desenrola. A "incolumidade do patrimônio" não se refere apenas à carteira no bolso, mas aos dados e aos fundos armazenados digitalmente. Alexandre de Moraes (2023, p. 711), ao comentar o referido artigo, é enfático ao ligar a segurança pública à proteção de todos os direitos fundamentais, o que, por conseguinte, inclui o patrimônio em sua acepção digital:

> A segurança pública é a garantia de proteção aos direitos fundamentais (vida, liberdade, patrimônio), devendo o Estado, por meio de seus órgãos, neutralizar as ações criminosas que pretendam ou venham a lesar tais direitos, independentemente do meio utilizado para a prática do ilícito. (MORAES, 2023, p. 711).

A omissão ou a ineficácia do Estado em proteger o patrimônio dos cidadãos no ambiente digital representa, portanto, um fracasso no cumprimento de seu dever constitucional. A fraude digital em massa não é um problema de polícia judiciária ou de juizado; é, em sua essência, um problema de Segurança Pública que demanda a atuação sinérgica de *todos* os órgãos listados no Art. 144, incluindo a Polícia Militar, em sua função de preservação da ordem pública.

Negar essa natureza é relegar o cidadão a um vácuo de proteção estatal, onde o crime, embora massificado, é tratado de forma pulverizada e ineficiente, gerando a perigosa sensação de que o ciberespaço é uma "terra sem lei", o que corrói a própria legitimidade do monopólio estatal da força e da justiça.

3 O ARSENAL JURÍDICO-INSTITUCIONAL BRASILEIRO: LIMITES E POSSIBILIDADES

A resposta estatal ao avanço da criminalidade digital tem se dado, principalmente, em duas frentes: a legislativa, buscando atualizar os tipos penais e as ferramentas de investigação; e a jurisdicional, interpretando as novas dinâmicas à luz das garantias constitucionais. Contudo, a eficácia desse arsenal é limitada pela complexidade da investigação e pela estrutura processual vigente.

3.1 O Ajuste Legislativo: As Inovações da Lei nº 14.155/2021

O ordenamento jurídico brasileiro tentou responder ao desafio. Leis como a nº 12.737/2012 (Lei "Carolina Dieckmann"), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) criaram o arcabouço para a regulação do ambiente digital. No entanto, no campo específico das fraudes, a inovação mais significativa foi a Lei nº 14.155, de 27 de maio de 2021.

Esta lei alterou drasticamente o Artigo 171 do Código Penal, inserindo tipos qualificados específicos para o ambiente digital. Ela criou a qualificadora da "Fraude eletrônica" (§ 2º-A), com pena de reclusão de 4 a 8 anos, nos seguintes termos:

> Art. 171...
> 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. (BRASIL, 2021).

Além disso, no § 2º-B, estabeleceu a mesma pena (4 a 8 anos) se o crime for praticado "mediante a utilização de servidor de computador (...) localizado fora do território nacional".

A lei também buscou resolver um dos maiores gargalos investigativos: a definição da competência territorial. O novo § 4º do Art. 70 do Código de Processo Penal passou a estabelecer que, nos crimes de estelionato praticados por meio eletrônico, a competência é definida "pelo local do domicílio da vítima". Essa alteração foi vital, pois antes dela, a jurisprudência majoritária fixava a competência no local da obtenção da vantagem (onde estava a conta do fraudador), o que pulverizava as investigações por todo o país e dificultava o acesso da vítima à justiça.

Contudo, a Lei 14.155/2021 gerou um efeito colateral complexo para o sistema que este artigo analisa. Ao elevar a pena *mínima* para 4 anos de reclusão, ela, em tese, retirou a fraude eletrônica da esfera de competência dos Juizados Especiais Criminais, que só processam crimes com pena máxima não superior a 2 anos (Art. 61 da Lei 9.099/95). Além disso, impediu a aplicação do Acordo de Não Persecução Penal (ANPP), que exige pena mínima inferior a 4 anos (Art. 28-A do CPP). Esta decisão legislativa, embora buscasse maior repressão, pode ter inadvertidamente engessado o sistema, jogando essa massa de crimes complexos e de difícil solução na vala comum da Justiça Criminal ordinária, notoriamente mais lenta e sobrecarregada, potencializando a impunidade.

3.2 A Problemática Probatória e a Volatilidade da Evidência Digital

Independentemente da pena ou da competência, o maior desafio da persecução penal digital é a prova. A prova da autoria e da materialidade em um crime digital não está em um local físico, mas em dados voláteis e distribuídos. Para comprovar uma fraude, é necessário rastrear o fluxo do dinheiro, identificar os titulares das contas (muitas vezes "laranjas"), quebrar o sigilo de dados de conexão (registros de IP) para identificar a origem do ataque, e quebrar o sigilo de dados de aplicação (conteúdo de mensagens) para provar o dolo.

O Marco Civil da Internet (Lei 12.965/2014) estabelece, em seu Artigo 10º, que o provedor de conexão deve guardar os registros de conexão pelo prazo de um ano, e os provedores de aplicação (redes sociais, e-mails) devem guardar os registros de acesso por seis meses. A obtenção desses dados, contudo, exige autorização judicial. Esse é um ponto crítico de gargalo. Em um sistema fragmentado, a vítima registra o BO; o BO vira um inquérito; o delegado representa pela quebra do sigilo; o MP opina; o juiz defere. Esse trâmite pode levar semanas ou meses. No tempo do crime digital, isso é uma eternidade. Muitas vezes, quando a ordem judicial chega ao provedor, o prazo de guarda legal dos dados já expirou.

A doutrina especializada é uníssona quanto a essa dificuldade. Patrícia Peck Pinheiro (2021) adverte que a ausência de uma cadeia de custódia digital robusta, desde a coleta inicial pela vítima ou pela autoridade policial, é a

principal causa de nulidade processual ou de absolvição por falta de provas. A prova digital é, por definição, facilmente alterável.

> A prova digital é volátil por natureza. A sua coleta e preservação exigem um rigor técnico e procedimental absoluto, desde a preservação de logs de servidores até a correta espelhagem de dispositivos, sob pena de nulidade e da impossibilidade de se estabelecer a autoria e a materialidade delitiva no ambiente cibernético. A ausência de padronização na coleta inicial é o calcanhar de Aquiles da persecução penal digital. (BLUM; BRUNO, 2021, p. 231).

Essa complexidade probatória, somada ao volume, cria um cenário onde a investigação individualizada de cada fraude digital se torna economicamente inviável para o Estado.

3.3 A Tensão entre Eficiência Repressiva e Garantias Fundamentais no Ambiente Digital

A busca pela eficiência na investigação digital invariavelmente colide com garantias constitucionais, notadamente a privacidade, a intimidade (Art. 5º, X, CF) e o sigilo de dados e comunicações (Art. 5º, XII, CF). A Constituição Federal protege esses direitos, permitindo sua relativização apenas por ordem judicial fundamentada e para fins de investigação criminal ou instrução processual penal.

O Supremo Tribunal Federal (STF) tem sido chamado a balizar essa tensão, como no julgamento do Marco Civil da Internet (ADI 5527), onde se discutiu a constitucionalidade da guarda de registros. A chamada "jurisprudência da ponderação" se faz presente. Contudo, na prática da persecução das fraudes, o desafio é outro: como investigar crimes em massa sem promover uma devassa generalizada?

O Ministério Público, por exemplo, ao identificar um padrão de fraude (um mesmo site falso ou uma mesma conta receptora), não pode obter uma "ordem de quebra de sigilo genérica" ou prospectiva. A necessidade de individualização das condutas, pilar do Direito Penal e Processual Penal, é um obstáculo à investigação de crimes que são, por natureza, massificados e despersonalizados. A integração proposta neste artigo deve, portanto, ser desenhada de forma a respeitar incondicionalmente essas garantias, sob pena de ser declarada ilegal e ineficaz, tornando nula toda a prova colhida. A eficiência não pode ser alcançada ao custo da supressão de direitos fundamentais.

4 A ATUAÇÃO FRAGMENTADA DOS ATORES INSTITUCIONAIS

O principal entrave à efetividade da resposta estatal às fraudes digitais não é, paradoxalmente, a falta de leis ou de institutions, mas a ausência de *processos* integrados. Cada ator institucional – Polícia Militar, Ministério Público e Juizados Especiais – atua dentro de sua esfera de competência de forma isolada, criando "silos" de informação e gargalos decisórios que, somados, resultam na ineficiência sistêmica.

4.1 A Polícia Militar como Porta de Entrada: O Desafio do Registro Qualificado

Em grande parte do território nacional, a Polícia Militar é a instituição de maior capilaridade e a primeira a quem o cidadão recorre. Mesmo em crimes não-emergenciais como a fraude digital, muitas vítimas, por desorientação ou pela indisponibilidade de delegacias especializadas, buscam o 190 ou uma viatura para relatar o ocorrido. Além disso, muitas PMs mantêm sistemas de registro de ocorrência *online* ou em seus quartéis, absorvendo parte da demanda que seria da Polícia Judiciária.

A PM, em sua missão constitucional de "polícia ostensiva e a preservação da ordem pública" (Art. 144, § 5º, CF), desempenha um papel crucial. O registro da fraude, mesmo que não seja um crime de sua atribuição investigativa direta, é um ato de preservação da ordem pública, pois documenta a quebra da incolumidade patrimonial. O problema reside na *qualidade* desse registro.

Frequentemente, o Boletim de Ocorrência é registrado como um mero relato textual dos fatos narrados pela vítima. Faltam campos estruturados para dados técnicos essenciais à investigação digital: chave PIX do destinatário, URL do site falso, número de IP (se a vítima tiver), *prints* de tela com metadados, *hash* de arquivos, etc. O policial militar na ponta da linha, treinado para a ocorrência física, muitas vezes não está capacitado para extrair ou orientar a preservação desses dados voláteis. Essa falha no registro inicial é um ponto cego do sistema, como adverte a doutrina sobre o ciclo completo de polícia:

> A eficiência da segurança pública depende da integração de todo o ciclo de atividade policial – do policiamento ostensivo à investigação e ao processamento. A falha em qualquer etapa, como um registro de ocorrência deficiente, compromete irremediavelmente as fases subsequentes, pois a informação primária é a matéria-prima de toda a persecução penal. (MIRANDA; LIMA, 2021, p. 45).

O resultado é um registro que, embora cumpra a função estatística, possui baixíssimo valor investigativo. Esse "BO" é, muitas vezes, encaminhado à Polícia Civil, onde se torna mais um em uma pilha de inquéritos que não avançarão por falta de elementos mínimos. A PM, sem perceber, funciona como um "filtro às avessas": ao invés de qualificar a informação para a investigação, ela apenas a registra de forma burocrática e incompleta, desperdiçando o potencial de sua capilaridade.

4.2 O Ministério Público: *Dominus Litis* Diante de um Dilúvio de Dados

O Ministério Público é, por excelência, o titular da ação penal (Art. 129, I, CF) e o destinatário final das investigações. É ao MP que cabe analisar a justa causa e decidir pelo oferecimento da denúncia, pelo arquivamento ou pela requisição de novas diligências. Hugo Nigro Mazzilli (2008), um dos maiores doutrinadores sobre a instituição, ressalta o papel do MP como defensor da ordem jurídica e dos interesses sociais.

> O Ministério Público é o defensor da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis,

> não se limitando à figura do acusador, mas atuando como um verdadeiro fiscal da lei e da justiça, inclusive na esfera cível e na tutela dos interesses difusos e coletivos. (MAZZILLI, 2008, p. 55).

No contexto das fraudes digitais, o MP enfrenta um dilema. Recebendo milhares de inquéritos pulverizados sobre golpes de R$ 100,00 ou R$ 500,00, a instituição é forçada a uma atuação reativa e ineficiente. A análise individual de cada caso é inviável e de baixo impacto. O promotor de justiça se vê diante da escolha de assoberbar a Justiça com milhares de denúncias de baixa complexidade ou arquivar em massa por "insignificância" ou falta de provas, ambas soluções insatisfatórias.

A verdadeira força do MP, que seria a atuação estratégica, é neutralizada pela fragmentação dos dados. O MP possui unidades especializadas (como os GAECOs ou promotorias de crimes cibernéticos), mas estas não recebem os dados de forma estruturada. Elas não conseguem "ver" que 500 Boletins de Ocorrência registrados em 50 cidades diferentes apontam para a *mesma* conta receptora ou para o *mesmo* servidor de *phishing*. Cada caso é um caso. Essa falta de visão sistêmica impede o MP de focar no "peixe grande" – a organização criminosa por trás da fraude industrial – e o obriga a lidar apenas com os "peixinhos" (as vítimas) ou os "laranjas".

4.3 Os Juizados Especiais Criminais e o Dilema do "Menor Potencial Ofensivo" em Massa

Os Juizados Especiais Criminais (JECRIM) foram criados pela Lei 9.099/95 para serem uma válvula de escape do sistema penal tradicional. Seus princípios basilares são a oralidade, informalidade, economia processual e celeridade (Art. 62). A ideia, como brilhantemente defendida por Ada Pellegrini Grinover e outros (2005), era criar uma justiça criminal ágil para as "infrações de menor potencial ofensivo" (IMPO) – contravenções e crimes com pena máxima não superior a 2 anos.

> O escopo principal da Lei 9.099/95 foi o de criar uma justiça criminal mais célere, informal e desburocratizada, voltada à conciliação e à reparação do dano, para as infrações de menor potencial ofensivo, buscando evitar o encarceramento e promover a pacificação social através de medidas como a transação penal e a composição civil dos danos. (GRINOVER et al., 2005, p. 78).

O estelionato "simples" (Art. 171, *caput*), antes das recentes alterações, se enquadrava perfeitamente nesse escopo, especialmente em golpes de pequeno valor. O JECRIM seria o local ideal para a vítima buscar a reparação do dano e para o autor do fato (se identificado) aceitar uma transação penal (multa ou restrição de direitos), evitando o moroso processo ordinário.

Contudo, como visto, a Lei 14.155/2021, ao qualificar a fraude eletrônica com pena mínima de 4 anos, criou um paradoxo. Ela "promoveu" o crime digital mais comum à justiça comum, retirando-o da esfera célere do JECRIM. Isso gerou um debate jurídico: o estelionato simples (pena de 1 a 5 anos), mesmo que praticado por meio eletrônico, mas sem os elementos específicos do § 2º-A (como indução por rede

social), ainda seria JECRIM? A jurisprudência tem se mostrado dividida.

Mesmo nos casos que permanecem no JECRIM, o sistema não foi desenhado para a "massa". O JECRIM é ágil para o "um a um" (um furto simples, uma lesão corporal leve). Ele não possui ferramentas para uma audiência de conciliação com 500 vítimas e um único fraudador. O sistema de citação, intimação e realização de audiências, mesmo que virtualizado pós-pandemia, ainda é individualizado. A fraude digital em massa "quebra" a lógica do JECRIM, transformando o que deveria ser célere em um novo foco de sobrecarga e prescrição.

A fragmentação é, portanto, completa: a PM registra mal, o MP não tem visão estratégica e o JECRIM não tem capacidade processual para a escala do problema, quando sequer é competente para ele.

5 O IMPERATIVO DA ATUAÇÃO INTEGRADA: DESENHANDO UM NOVO PARADIGMA OPERACIONAL

A ineficiência do modelo fragmentado não é uma falha de competência das instituições, mas uma falha de *design* sistêmico. A solução para um problema complexo e massificado como a fraude digital não reside em mais leis ou na sobrecarga de uma única instituição, mas na reengenharia dos processos e na criação de fluxos de trabalho inteligentes e integrados. A resposta deve ser sistêmica, e a tríade PM-MP-JECRIM oferece a estrutura basilar para essa revolução operacional.

5.1 Fundamentos da Integração: Superando os "Silos" Institucionais

A integração não significa sobreposição de funções ou usurpação de competências. A PM não passará a investigar, o MP não passará a policiar ostensivamente e o Juizado não se tornará um órgão de persecução. A integração significa *interoperabilidade* de dados e *coordenação* de ações. O pilar dessa integração é a informação. O crime digital é um crime de informação, e deve ser combatido com informação.

O modelo tradicional de "passagem de bastão" – onde a PM registra, a PC investiga, o MP denuncia e o Judiciário julga, cada um em seu tempo e com seus sistemas – é anacrônico. O novo paradigma deve ser o de uma "rede neural", onde a informação coletada na ponta (PM) alimenta em tempo real um cérebro analítico (MP), que por sua vez aciona o braço resolutivo (JECRIM ou Justiça Comum) de forma precisa e estratégica.

Este modelo se baseia em três fundamentos interdependentes que precisam ser desenvolvidos de forma coesa: a padronização da coleta de dados, a centralização da análise de inteligência e a desburocratização da resposta judicial. O elo que une esses três pilares é, invariavelmente, a tecnologia.

5.2 Proposta de um Fluxo Operacional Integrado (PM-MP-JECRIM)

O desenho de um fluxo integrado é o núcleo desta proposta. Ele visa transformar o volume,

hoje um problema, em uma vantagem estratégica – o que em tecnologia se conhece como *Big Data*.

5.2.1 Fase 1: O Registro Estruturado e a Triagem Qualificada pela Polícia Militar

A revolução começa na porta de entrada. A Polícia Militar, com sua capilaridade ímpar, deve ser capacitada para ser o *coletor qualificado* da informação. Isso implica, fundamentalmente, duas mudanças estruturais e simultâneas.

A primeira mudança é a *capacitação* contínua do efetivo. O policial militar que atende a ocorrência ou o operador do sistema de registro *online* da corporação deve ser treinado para entender os dados essenciais da fraude digital. A vítima precisa ser orientada, já neste primeiro contato, a preservar os dados corretos e voláteis, como, por exemplo, não apenas o "print" da tela, mas como salvar um e-mail com seus metadados, como identificar a URL correta e como preservar o ID de uma transação PIX.

A segunda mudança, indissociável da primeira, é a reestruturação dos *sistemas de registro (BO)*. O Boletim de Ocorrência deve deixar de ser um campo de "texto livre" para se tornar um *formulário estruturado* e dinâmico. Ao selecionar a tipologia "Fraude Digital - PIX", o sistema deve, obrigatoriamente, abrir campos específicos e mandatórios, tais como: [Chave PIX Destino], [Banco Destino], [Valor], [Data/Hora], [Chave PIX Origem], [Telefone Usado no Golpe], https://nordvpn.com/pt/blog/sites-de-burlas/, e [ID da Transação].

Esse registro estruturado, feito pela PM, não tem valor investigativo imediato, mas tem um valor de *inteligência* incalculável. Esse banco de dados, ao ser preenchido por milhares de vítimas em todo o estado, torna-se a principal fonte de dados para a próxima fase. A PM cumpre sua função de preservação da ordem pública ao registrar o fato e *qualificar* a informação para o próximo ator do sistema.

5.2.2 Fase 2: A Central de Análise de Padrões e a Atuação Estratégica do Ministério Público

Aqui reside a mudança de paradigma. O banco de dados estruturado, alimentado em tempo real pelos registros da PM, deve ser acessível (respeitadas as normas de sigilo) por uma unidade central de análise, preferencialmente dentro do Ministério Público, que já possui estruturas de inteligência e análise de dados (como os GAECOs ou promotorias especializadas).

O papel dessa Central de Análise (MP + Inteligência da PM/PC) não é investigar o golpe de R$ 50,00 da vítima A, mas sim rodar algoritmos de *data mining* e *Business Intelligence* (BI) para encontrar padrões. O sistema deve ser capaz de responder automaticamente a perguntas estratégicas: Quantos B.O.s das últimas 24 horas apontam para a *mesma* Chave PIX "laranja"? Quantas vítimas em cidades diferentes relataram o *mesmo* número de telefone de "falsa central"? Quantos golpes foram originados do *mesmo* bloco de endereços IP?

Ao invés de 1000 inquéritos pulverizados, o MP passa a ter um "dossiê de inteligência" que aponta para um *único* alvo (o titular da conta laranja principal) ou uma *única* infraestrutura (o servidor do site falso). A atuação do MP deixa de ser reativa e pulverizada para ser *proativa e estratégica*.

Detentor dessa inteligência, o Ministério Público passa a ter um leque de ações estratégicas de alto impacto. Primeiramente, pode requisitar à Polícia Civil uma investigação direcionada e qualificada, focada no "nó" da rede criminosa, e não na vítima individual. Em segundo lugar, pode representar judicialmente por medidas cautelares complexas, como a quebra de sigilo bancário da conta central ou o sigilo telemático do servidor, fazendo-o de forma robusta e fundamentada ao demonstrar ao Judiciário a *escala* da atividade criminosa. Finalmente, essa visão macro permite ao *Parquet* identificar o "varejo" e o "atacado" do crime, direcionando os valiosos e limitados recursos investigativos para onde o impacto social e repressivo é maior.

5.2.3 Fase 3: A Resolução Célere e Massificada no Âmbito dos Juizados Especiais Criminais

Uma vez que o MP e a Polícia Judiciária (acionada pelo MP) identificam a autoria – seja do "laranja" ou do operador principal – o sistema enfrenta o desafio da resolução. Como processar o autor de um golpe que vitimou 1000 pessoas?

Aqui, o JECRIM deve ser resgatado, mesmo diante do debate sobre a pena. Primeiramente, é defensável que muitos golpes "simples" não se enquadram na qualificadora de 4 anos (Lei 14.155/2021), permanecendo na esfera da Lei 9.099/95. Segundo, mesmo que não seja JECRIM, os princípios da celeridade e da economia processual devem ser importados para a Justiça Comum para esses casos.

A integração permite uma *resolução em massa*. O MP, ao invés de 1000 denúncias, oferece *uma* denúncia em concurso de crimes (continuidade delitiva ou concurso formal/material) ou, mais eficazmente, propõe um *Acordo de Não Persecução Penal (ANPP)* ou *Transação Penal* coletiva.

O JECRIM (ou a Vara Criminal) pode usar a tecnologia para reverter o jogo, implementando soluções de resolução em escala. Uma dessas soluções seria a realização de *audiências virtuais coletivas*, permitindo que, através de videoconferência, o autor do fato (o "laranja", por exemplo) seja confrontado não com uma, mas com dezenas de vítimas de forma simultânea, otimizando a pauta.

Outra medida crucial seria a *composição de danos facilitada*. A integração do sistema de justiça com o sistema bancário (via SISBAJUD ou mecanismos mais ágeis) pode permitir o bloqueio rápido de valores na conta do fraudador e sua distribuição proporcional e automatizada às vítimas cadastradas no "banco de dados de BOs" da PM.

Por fim, a resposta penal deve ser repensada, como através de uma *transação penal estratégica*. A multa ou a medida restritiva de direitos proposta na transação penal pode ser calculada com base no *somatório* dos danos

causados a todas as vítimas identificadas pela Central de Análise, e não apenas em um único delito, tornando a medida efetivamente desestimulante e alinhada à real gravidade da conduta massificada.

Os Juizados Especiais, assim, cumpririam sua vocação original de desburocratização e pacificação social, não tratando o caso individualmente, mas o *evento* criminoso de forma integral.

5.3 A Tecnologia como Vértice da Integração: Interoperabilidade e Inteligência Artificial

Este modelo integrado só é viável com um forte alicerce tecnológico. A "cola" que une PM, MP e JECRIM é a *interoperabilidade* dos sistemas. Não é realista que a PM mude seu sistema de BO para se adequar ao sistema de inquérito digital do MP. O que é necessário é a criação de *APIs* (*Application Programming Interfaces*) que permitam que os sistemas "conversem".

O BO estruturado da PM deve gerar, automaticamente, um "evento" no sistema do MP. O MP, ao analisar os dados, deve conseguir "puxar" os registros relevantes sem necessidade de ofícios de papel. A decisão do JECRIM deve, por sua vez, alimentar o banco de dados original da PM, informando à vítima que seu caso teve uma resolução.

Além da interoperabilidade, o uso de *Inteligência Artificial (IA)* e *Machine Learning* na Fase 2 (Análise pelo MP) é fundamental. Algoritmos de IA podem analisar milhões de registros de ocorrência em segundos, identificando padrões que um analista humano levaria meses para encontrar. A IA pode prever "hotspots" de fraude, identificar novas tipologias de golpe assim que elas emergem e correlacionar dados aparentemente desconexos (ex: um BO de fraude no Paraná com outro em Pernambuco que usaram o mesmo prefixo de telefone). A adoção de tecnologia preditiva e analítica não é uma opção, mas uma condição de sobrevivência para o sistema de justiça no século XXI.

> A Inteligência Artificial aplicada ao sistema de justiça não visa substituir o julgador ou o promotor, mas sim potencializar sua capacidade de análise em cenários de alta complexidade e volumetria de dados. Em crimes de massa, como fraudes digitais, a IA é a única ferramenta capaz de correlacionar padrões ocultos e fornecer a inteligência estratégica necessária para uma atuação estatal efetiva e não meramente simbólica. (PASCHOAL, 2022, p. 89).

6 DESAFIOS À IMPLEMENTAÇÃO DO MODELO INTEGRADO

A proposta de um fluxo integrado, embora logicamente robusta, enfrenta barreiras significativas em sua implementação prática. Esses desafios não são intransponíveis, mas exigem vontade política, investimento e, acima de tudo, uma mudança de cultura institucional.

6.1 Desafios Culturais e a Resistência à Mudança Institucional

O maior obstáculo é, frequentemente, o cultural. As instituições de segurança e justiça historicamente se desenvolveram em "silos",

com forte senso de autonomia e delimitação de competências. A Polícia Militar, o Ministério Público e o Judiciário possuem culturas organizacionais distintas, e por vezes, antagônicas.

A ideia de um banco de dados de ocorrências da PM alimentando diretamente a análise de inteligência do MP pode gerar resistências. Questionamentos sobre "quem é o dono do dado", "quem comanda a investigação" e "invasão de competência" são inevitáveis. A PM pode resistir a se tornar uma "coletora de dados" para o MP; o MP pode resistir a atuar com base em dados "policiais" não filtrados pela investigação da Polícia Civil; e o Judiciário pode ver com desconfiança a "massificação" de processos que ferem a lógica da análise individualizada.

Superar essa barreira exige a construção de *confiança*, que se dá através de protocolos claros (Acordos de Cooperação Técnica), definição precisa de papéis, e a criação de comitês gestores interinstitucionais. A liderança de cada órgão deve abraçar a integração não como uma perda de autonomia, mas como um ganho de *eficiência* para a sociedade.

6.2 Desafios Tecnológicos, Orçamentários e de Capacitação

A interoperabilidade sistêmica é tecnologicamente complexa e cara. As instituições utilizam sistemas legados, desenvolvidos em plataformas diferentes. A construção das APIs, a garantia da segurança da informação (para evitar vazamento dos dados dos cidadãos) e a criação de um *dashboard* de análise unificado exigem investimento financeiro substancial.

Em um cenário de restrição orçamentária, justificar a alocação de recursos para "sistemas" em detrimento de "viaturas" ou "novos fóruns" é um desafio político. É preciso demonstrar o *retorno sobre o investimento* (ROI), que no caso, se mede em aumento da taxa de resolução, recuperação de ativos e, principalmente, aumento da confiança do cidadão no Estado.

Paralelamente, há o desafio da *capacitação*. O policial militar na ponta deve ser treinado para o registro qualificado. O promotor de justiça e o juiz devem ser treinados para entender a prova digital e as ferramentas de análise de dados. A cultura do "processo de papel" digitalizado precisa ser substituída pela cultura da "gestão de dados". Isso exige um esforço contínuo e profundo em todas as escolas de formação e aperfeiçoamento das carreiras.

6.3 Desafios Jurídico-Procedimentais: A Cadeia de Custódia Digital e o Compartilhamento de Dados

O compartilhamento de dados entre PM e MP, e destes com o Judiciário, deve ser feito com rigoroso respeito à legalidade. A Lei Geral de Proteção de Dados (LGPD) se aplica, embora com as exceções previstas para a segurança pública (Art. 4º, III). O principal desafio é garantir a *cadeia de custódia* da prova digital (prevista no Art. 158-A e seguintes do CPP).

Como garantir que o *print* de tela anexado ao BO da PM tem integridade e autenticidade para ser usado como prova pelo MP? O registro

estruturado deve ser pensado para isso, talvez com a implementação de coleta via sistemas que garantam o *hash* (assinatura digital) do arquivo no momento do *upload*.

Além disso, o acesso do MP ao banco de dados "bruto" da PM não pode ser um "fishing expedition" (pesca probatória). O acesso deve ser regulado por protocolos que definam o escopo da análise (focada em padrões de fraude) e que preservem o sigilo dos dados das vítimas que não se enquadram na investigação em curso. A atuação deve ser cirúrgica, baseada em inteligência, e não em devassa. O respeito às garantias constitucionais (Art. 5º, X e XII) é a linha mestra que, se violada, derruba todo o modelo.

CONSIDERAÇÕES FINAIS

A ascensão das fraudes digitais como o crime patrimonial de massa do século XXI expôs a obsolescência do modelo de persecução penal analógico, fragmentado e reativo. A arquitetura institucional brasileira, composta por órgãos de excelência como a Polícia Militar, o Ministério Público e os Juizados Especiais, é subutilizada quando forçada a operar em "silos", incapaz de responder à velocidade, escala e complexidade do crime cibernético. O resultado é um cenário socialmente desastroso: a impunidade dos criminosos, a vitimização contínua dos cidadãos e a erosão da confiança no Estado como garantidor da ordem pública e da incolumidade patrimonial.

Este artigo demonstrou que a resposta a esse desafio não está na edição de mais leis punitivas – que, como visto no caso da Lei 14.155/2021, podem até gerar efeitos colaterais indesejados, como o engessamento do sistema – nem na sobrecarga de uma única instituição. A resposta é sistêmica, e reside na *integração operacional*.

A proposta de um fluxo integrado (PM-MP-JECRIM) não é uma utopia, mas uma necessidade pragmática. Ela transforma o maior problema atual – o volume – na maior solução. Ao tratar os milhares de registros de ocorrência não como processos individuais, mas como um *Big Data* a ser analisado, o Estado inverte a lógica do jogo.

Neste modelo, a Polícia Militar transcende o mero registro e se torna o ponto de coleta qualificada de inteligência, usando sua capilaridade ímpar. O Ministério Público deixa de ser um homologador de arquivamentos ou um acusador pulverizado e se torna o cérebro estratégico do sistema, focando seus recursos na desarticulação das redes criminosas. Os Juizados Especiais (ou a Justiça Comum adaptada) deixam de ser um gargalo processual e se tornam uma plataforma ágil de resolução em massa, focada na reparação do dano e na rápida aplicação da lei, restaurando a vocação de celeridade da Lei 9.099/95.

A implementação deste paradigma, como visto, não é trivial. Ela exige a superação de barreiras culturais, investimentos em tecnologia interoperável e um rigoroso respeito aos procedimentos legais e às garantias fundamentais. A tecnologia, da IA à simples padronização de formulários, é a ferramenta-chave, mas a *vontade política* e a *colaboração interinstitucional* são os motores da mudança.

A alternativa a este esforço de integração é a aceitação tácita da falência do Estado na

proteção do cidadão no ambiente digital. É assistir passivamente à consolidação do ciberespaço como um território sem lei, onde o crime compensa. As instituições que compõem o sistema de segurança pública e justiça, pilares da democracia brasileira, têm o dever constitucional e a responsabilidade histórica de se adaptar, evoluir e, sobretudo, cooperar. A integração não é mais uma opção; é o único caminho viável para que a ordem pública e a incolumidade do patrimônio sejam, de fato, preservadas na era digital.

REFERÊNCIAS BIBLIOGRÁFICAS

ANUÁRIO BRASILEIRO DE SEGURANÇA PÚBLICA. *17º Anuário Brasileiro de Segurança Pública*. Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://www.google.com/search?q=https://forumseguranca.org.br/anuario-brasileiro-seguranca-publica/. Acesso em: 10 nov. 2025.

BLUM, Renato Opice; BRUNO, Bruno. *Direito Digital: Novas Teses Jurídicas*. 2. ed. São Paulo: Thomson Reuters, 2021.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 nov. 2025.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Rio de Janeiro, RJ, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 10 nov. 2025.

BRASIL. *Decreto-Lei nº 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Rio de Janeiro, RJ, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 10 nov. 2025.

BRASIL. *Lei nº 9.099, de 26 de setembro de 1995*. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, DF, 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9099.htm. Acesso em: 10 nov. 2025.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 nov. 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 nov. 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 nov. 2025.

BRASIL. *Lei nº 13.964, de 24 de dezembro de 2019*. Aperfeiçoa a legislação penal e processual penal. Brasília, DF, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 10 nov. 2025.

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 tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Brasília, DF, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 10 nov. 2025.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). *Pesquisa FEBRABAN de Tecnologia Bancária 2023*. São Paulo: FEBRABAN, 2023. Disponível em: https://www.google.com/search?q=https://portal.febraban.org.br/pesquisa-febraban-de-tecnologia-bancaria-2023/. Acesso em: 10 nov. 2025.

GRINOVER, Ada Pellegrini et al. *Juizados Especiais Criminais: comentários à Lei 9.099/95*. 5. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2005.

MAZZILLI, Hugo Nigro. *O Ministério Público na Constituição de 1988*. 2. ed. São Paulo: Saraiva, 2008.

MIRANDA, Fabrício; LIMA, Renato Sérgio de. *Ciclo Completo de Polícia: Uma Análise da Proposta no Brasil*. São Paulo: Fórum Brasileiro de Segurança Pública, 2021.

MORAES, Alexandre de. *Direito Constitucional*. 39. ed. São Paulo: Atlas, 2023.

PASCHOAL, Fernando. *Inteligência Artificial e Direito: Fundamentos e Aplicações*. São Paulo: Almedina, 2022.

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

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 25. ed. São Paulo: Malheiros Editores, 2005.

TEIXEIRA, Tarcísio. *Direito Digital e Processo Eletrônico*. 4. ed. São Paulo: Juspodivm, 2020.