SOBERANIA DIGITAL E LIMITES CONSTITUCIONAIS À INVESTIGAÇÃO PENAL NO AMBIENTE VIRTUAL

DIGITAL SOVEREIGNTY AND CONSTITUTIONAL LIMITS TO CRIMINAL INVESTIGATION IN THE VIRTUAL ENVIRONMENT

Helton Carlos de Albuquerque Ferreira[1]
Glebson Weslley Bezerra da Silva[2]
Renato Fazio[3]

RESUMO

O presente trabalho tem como objetivo analisar os desafios enfrentados pelo Estado brasileiro na persecução penal de crimes cibernéticos, especialmente diante da necessidade de obtenção de provas armazenadas por grandes plataformas tecnológicas estrangeiras, como Google, Meta, Apple e Microsoft. A pesquisa busca compreender de que forma é possível compatibilizar a eficiência da investigação criminal com o respeito aos direitos fundamentais consagrados na Constituição Federal de 1988, especialmente após a Emenda Constitucional nº 115/2022, que consagrou o direito à proteção de dados pessoais como garantia constitucional.
Nesse contexto, o estudo explora o conceito de soberania digital e os limites constitucionais da atuação estatal no ambiente virtual, com ênfase nos princípios da legalidade, proporcionalidade, devido processo legal, inviolabilidade da intimidade e autodeterminação informativa. São examinados os marcos legais brasileiros, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, bem como os instrumentos de cooperação internacional, como o MLAT e a recente adesão do Brasil à Convenção de Budapeste sobre o Cibercrime. Além da análise repressiva, o trabalho também aborda a importância da atuação preventiva por meio da inteligência cibernética, da integração interinstitucional e da capacitação técnica dos operadores do direito. Conclui-se que a construção de um modelo de persecução penal digital eficiente exige respeito rigoroso aos direitos fundamentais, articulação multidisciplinar e cooperação jurídica internacional efetiva, de modo a garantir a legitimidade do poder punitivo estatal sem comprometer os pilares do Estado Democrático de Direito.

Palavras-chave: Soberania digital; Crimes cibernéticos; Direitos fundamentais; Investigação penal; Privacidade; Proteção de dados.

ABSTRACT

The present work aims to analyze the challenges faced by the Brazilian State in the criminal prosecution of cybercrimes, especially given the need to obtain evidence stored by large foreign technological platforms, such as Google, Meta, Apple and Microsoft. The research seeks to understand how it is possible to reconcile the efficiency of criminal investigation with respect for the fundamental rights enshrined in the 1988 Federal Constitution, especially after Constitutional Amendment No. 115/2022, which enshrined the right to personal data protection

[1] Bacharelando em Direito pelo Centro Universitário UNIFBV. E-mail: helton_carlosaf@hotmail.com.
[2] Doutorando e Mestre em Direito - Universidade Católica de Pernambuco. Especialista em Criminologia. Advogado. Pesquisador do Grupo Asa Branca Criminologia (UNICAP/CNPq). Coordenador dos cursos de Direito e Relações Internacionais do Centro Universitário Estácio do Recife - Unidade Abdias de Carvalho. Docente do Curso de Direito da Estácio Recife. Docente do Curso de Direito do Centro Universitário UNIFBV Wyden.
[3] Mestrando em Perícias Forenses pela Universidade de Pernambuco, Especialista em Penal e Processo Penal pela OAB-ESA, Advogado Criminalista e Professor Universitário.

as a constitutional guarantee.
In this context, the study explores the concept of digital sovereignty and the constitutional limits of state action in the virtual environment, with an emphasis on the principles of legality, proportionality, due legal process, inviolability of privacy and informational self-determination. Brazilian legal frameworks are examined, such as the Marco Civil da Internet and the General Data Protection Law, as well as international cooperation instruments, such as the MLAT and Brazil's recent accession to the Budapest Convention on Cybercrime. In addition to repressive analysis, the work also addresses the importance of preventive action through cyber intelligence, interinstitutional integration and technical training of legal operators. It is concluded that the construction of an efficient digital criminal prosecution model requires strict respect for fundamental rights, multidisciplinary coordination and effective international legal cooperation, in order to guarantee the legitimacy of state punitive power without compromising the pillars of the Democratic Rule of Law.

Keywords: Digital sovereignty; Cybercrimes; Fundamental rights; Criminal investigation; Privacy; Data protection.

1 INTRODUÇÃO

A revolução tecnológica e a expansão exponencial da internet transformaram profundamente as relações sociais, econômicas e jurídicas no século XXI. Nesse cenário, o ciberespaço se consolidou como novo ambiente de interação humana, onde direitos são exercidos, deveres se manifestam e, inevitavelmente, condutas criminosas também se desenvolvem (Faustino, 2020). O direito penal, historicamente vinculado a elementos físicos e territoriais, encontra-se agora diante de desafios inéditos, impostos por um mundo digital marcado pela fluidez das informações, pela atuação transnacional de agentes e pelo controle concentrado de dados por grandes corporações tecnológicas estrangeiras (Castells, 2003).

Como bem observa Castells (2003, p. 16), “a internet é, acima de tudo, uma rede de comunicação interativa, que se desenvolve como a espinha dorsal da nova forma de organização social característica da era da informação: a sociedade em rede.” Nesse novo cenário, crimes cibernéticos desafiam a lógica territorial do direito penal tradicional, exigindo do Estado novas formas de atuação que respeitem os direitos fundamentais sem perder sua eficácia.

A persecução penal de crimes digitais, como fraudes eletrônicas, invasão de dispositivos informáticos, cyberbullying, estelionato virtual, pornografia infantil e disseminação não autorizada de conteúdo íntimo, exige respostas rápidas e tecnicamente adequadas (Caiado; Caiado, 2018; Torres et al., 2022). Contudo, essa necessidade de eficiência investigativa não pode prescindir do respeito aos direitos e garantias fundamentais consagrados na Constituição Federal de 1988, tais como o devido processo legal, a inviolabilidade da intimidade e o sigilo das comunicações (Brasil, 1988, art. 5º, incisos X, XII, LIV e LV). O dilema entre segurança

pública e proteção das liberdades individuais impõe um debate profundo sobre os limites legítimos da atuação estatal no ambiente digital (De Carvalho, 2018

A questão se torna ainda mais complexa quando se considera que parte significativa dos dados necessários às investigações está sob a guarda de empresas internacionais, como Google, Meta (Facebook, Instagram, WhatsApp), Apple e Microsoft, cujos servidores muitas vezes se localizam fora do território nacional. Nessa perspectiva, surgem impasses relacionados à jurisdição, à soberania estatal e à eficácia da legislação interna diante de interesses e normativos estrangeiros (Rodrigues, 2021; Guerra; Bertholini, 2023). O conceito de soberania digital, compreendido como a capacidade do Estado de regular o uso de dados e a atuação de plataformas digitais conforme suas próprias leis e instituições, emerge como elemento central desse debate (Bioni, 2019).

Além disso, a promulgação da Emenda Constitucional nº 115/2022, que incluiu expressamente o direito à proteção de dados pessoais no rol dos direitos e garantias fundamentais (Brasil, 2022, art. 5º, LXXIX), reafirma a necessidade de uma abordagem jurídica que concilie a repressão eficiente à criminalidade com a tutela da privacidade, da liberdade de expressão, do sigilo das comunicações e do devido processo legal. O direito à autodeterminação informativa, já reconhecido pelo Supremo Tribunal Federal (STF) no julgamento da ADI 6387, que questionava a constitucionalidade da Medida Provisória nº 954/2020, Medida que previa o compartilhamento de dados pessoais de usuários de telefonia móvel com o IBGE para fins de pesquisas estatísticas durante a pandemia de COVID-19, ganha contornos constitucionais robustos, impondo limites objetivos à atuação estatal e estabelecendo novos parâmetros para a atividade investigativa no ambiente virtual (STF, 2020).

Diante desse contexto, o presente trabalho teve por objetivo analisar, sob a perspectiva do ordenamento jurídico brasileiro, como compatibilizar a necessidade de uma persecução penal eficaz dos crimes cibernéticos com a proteção dos direitos fundamentais, à luz dos desafios impostos pela soberania digital e pela atuação de plataformas tecnológicas estrangeiras. Para tanto, foram abordadas as bases normativas vigentes, os princípios constitucionais aplicáveis, as práticas investigativas adotadas pelas autoridades brasileiras e os mecanismos de cooperação internacional, com especial atenção aos riscos de arbitrariedades e violações de direitos no processo de obtenção de provas digitais.

Desse modo, a pesquisa propõe-se a contribuir com a construção de uma abordagem equilibrada, que reconheça os limites legítimos do poder punitivo do Estado no ciberespaço, ao mesmo tempo em que assegure os instrumentos necessários à repressão da criminalidade digital, respeitando os fundamentos democráticos e constitucionais do Estado de Direito.

2 EFICIÊNCIA NA PERSECUÇÃO PENAL: A necessidade de uma análise técnica e em tempo hábil

O avanço da tecnologia e a consolidação da sociedade da informação transformaram radicalmente a dinâmica da criminalidade, especialmente no meio digital. Os crimes cibernéticos possuem características próprias que exigem do Estado uma atuação célere, técnica e especializada. O tempo é fator crítico, e a eficácia da investigação penal depende, muitas vezes, da capacidade de resposta em tempo real. Dados voláteis, conexões criptografadas e múltiplas camadas de anonimato impõem à persecução penal um novo paradigma, que desafia os métodos tradicionais de apuração.

Segundo Torres et al. (2022, p. S33):

> …a estrutura clássica da investigação criminal revela-se ineficiente para responder às novas formas de criminalidade digital, sendo imprescindível o desenvolvimento de práticas investigativas tecnológicas e colaborativas, tanto no plano nacional quanto internacional.

Crimes como fraudes bancárias online, invasão de dispositivos informáticos, extorsões virtuais, pornografia infantil e vazamento de dados pessoais exigem atuação imediata. Muitas vezes, os rastros digitais desaparecem rapidamente em questão de horas. A obtenção de provas, especialmente aquelas armazenadas em servidores de empresas estrangeiras, depende da agilidade da autoridade investigativa, sob pena de comprometimento da eficácia penal. Caiado e Caiado (2018, p. 12) afirmam que:

> A dinâmica da criminalidade cibernética exige resposta ágil por parte das autoridades investigativas, pois a prova digital é por natureza efêmera, sujeita à exclusão automática, à criptografia ou ao simples deslocamento transnacional em questão de segundos. Perder o timing equivale a comprometer a persecução penal.

Essa realidade impõe a reestruturação da atuação do Ministério Público e das polícias, que devem investir em núcleos especializados em crimes cibernéticos, com equipes multidisciplinares e ferramentas de inteligência digital. Além disso, é essencial fomentar a cooperação entre os órgãos de investigação e os provedores de serviços, de modo a facilitar a obtenção de dados mediante requisições fundamentadas.

2.1 Marco Civil da Internet e a Produção de Provas Digitais

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, constitui o principal marco normativo brasileiro para o uso da internet e a proteção de direitos no ambiente digital.

Ela define princípios, garantias, direitos e deveres dos usuários, além de regras claras para a atuação dos provedores de conexão e de aplicações.

O artigo 10 do Marco Civil estabelece que o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, o que reforça a necessidade de atuação célere e fundamentada por parte das autoridades investigadoras. Trata-se de uma proteção constitucional à intimidade, à vida privada e ao sigilo das comunicações, conforme previsto no artigo 5º, incisos X e XII da Constituição Federal de 1988. A exigência de ordem judicial protege os indivíduos contra a obtenção arbitrária de dados pessoais e limita a atuação do Estado a hipóteses de real necessidade, devidamente justificadas.

Além disso, o artigo 13 da referida lei determina que os provedores de conexão devem armazenar os registros de conexão à internet por um ano, enquanto os provedores de aplicações são obrigados a manter os registros de acesso por seis meses. Esses prazos são considerados o "tempo de vida útil" da prova digital no Brasil, mas muitas vezes mostram-se insuficientes diante da lentidão dos trâmites judiciais ou da resistência de plataformas tecnológicas em colaborar com rapidez.

Rodrigues (2021, p. 185) adverte que:

> A obtenção de dados no exterior é um dos principais gargalos da investigação penal brasileira, pois muitas plataformas, como Google, Meta e Apple, exigem cumprimento de tratados internacionais, como o MLAT, o que acarreta demora de meses e até anos para o acesso às informações.

Esse cenário de morosidade processual compromete a efetividade da persecução penal e pode levar à perda de provas cruciais, especialmente em casos que exigem resposta urgente, como crimes contra a dignidade sexual de crianças e adolescentes, sequestros virtuais, fraudes eletrônicas bancárias e vazamentos de dados pessoais sensíveis.

A situação se agrava pelo fato de que muitas dessas empresas mantêm servidores fora do território nacional e alegam que não estão juridicamente sujeitas à legislação brasileira. Contudo, o parágrafo 1º do artigo 11 do Marco Civil é claro ao dispor que:

> Empresas responsáveis pela oferta de serviços por meio da internet no Brasil devem obedecer à legislação brasileira quanto aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas, mesmo que tenham sede no exterior.

Isso significa que, mesmo sendo multinacionais, tais empresas estão sujeitas à jurisdição nacional quando oferecem serviços no país ou coletam dados de usuários brasileiros. A

inobservância desse comando legal pode caracterizar violação da soberania brasileira e obstrução à justiça, o que tem gerado embates jurídicos recorrentes nos tribunais.

A jurisprudência também tem evoluído no sentido de afirmar a obrigação das plataformas em cooperar com a Justiça.

Para contornar essas dificuldades, têm sido propostas estratégias como a criação de canais diretos de comunicação entre autoridades brasileiras e representantes legais das empresas no Brasil, a padronização de formulários de requisição de dados e a capacitação dos operadores do direito para redigir pedidos tecnicamente adequados, contendo informações claras, específicas e juridicamente fundamentadas.

Além disso, a adesão do Brasil à Convenção de Budapeste sobre o Cibercrime (formalizada em 2023) representa um passo importante na cooperação internacional para a produção de provas digitais. O tratado permite a realização de pedidos rápidos de preservação de dados e estabelece bases jurídicas comuns entre os países signatários, o que tende a reduzir os prazos e obstáculos enfrentados em investigações transnacionais.

Contudo, mesmo com esses avanços normativos e internacionais, é imprescindível que a atuação investigativa se mantenha fiel aos princípios constitucionais da proporcionalidade, legalidade e razoabilidade, para evitar abusos e garantir a admissibilidade da prova em juízo. A agilidade não pode se sobrepor à legalidade, e a produção da prova digital deve ser orientada por parâmetros técnicos, processuais e éticos, sob pena de se comprometer não apenas a legitimidade da investigação, mas também os direitos fundamentais dos cidadãos.

2.2 Inteligência Cibernética e Atuação Preventiva

Além da repressão, a atuação estatal no combate à criminalidade digital deve se concentrar cada vez mais em estratégias preventivas, baseadas em inteligência cibernética, análise preditiva e integração de dados. O objetivo principal da atuação preventiva é a antecipação de condutas ilícitas, por meio do monitoramento de comportamentos suspeitos, da detecção de vulnerabilidades em sistemas e da identificação de agentes ou organizações que atuam de maneira recorrente no ambiente virtual.

A inteligência cibernética refere-se ao conjunto de ferramentas, técnicas e processos voltados à coleta, tratamento e análise de informações disponíveis no ciberespaço, com o intuito de gerar conhecimento estratégico para a tomada de decisões pelas autoridades de segurança pública. Essa atividade não se confunde com vigilância indiscriminada: ela deve ser orientada

por critérios técnicos e jurídicos, assegurando que o processamento de dados respeite os princípios da legalidade, da proporcionalidade e da finalidade legítima.

Nesse contexto, a adoção de ferramentas de big data, inteligência artificial (IA) e machine learning tem se tornado uma tendência nos sistemas modernos de persecução penal. Algoritmos podem ser usados para identificar padrões anômalos de comportamento, cruzar grandes volumes de dados e gerar alertas em tempo real para investigações mais eficientes. Entretanto, como adverte Bioni (2019, p. 115):

> A automação do processo de tomada de decisão pelo Estado, especialmente em contextos que envolvem direitos fundamentais, requer extrema cautela. Os sistemas baseados em algoritmos precisam ser auditáveis, transparentes e submetidos a mecanismos de controle institucional.

O uso responsável da tecnologia exige, portanto, transparência algorítmica, ou seja, a possibilidade de fiscalização pública sobre como as ferramentas tecnológicas são construídas e aplicadas, especialmente se influenciam decisões que impactam diretamente a esfera privada dos cidadãos. Sistemas de pontuação de risco, por exemplo, já são utilizados em alguns países para fins de triagem investigativa, mas enfrentam críticas por possíveis vieses e violações ao princípio da presunção de inocência.

A atuação preventiva também requer integração entre órgãos públicos. A criação de bancos de dados interligados, como cadastros de incidentes cibernéticos, histórico de denúncias, perfis de comportamento e registros técnicos de ataques, é uma forma eficaz de antecipar ameaças e construir uma base robusta de inteligência estratégica. Essa integração, contudo, precisa observar a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), especialmente no que diz respeito à anonimização, à segurança da informação e à limitação da coleta ao mínimo necessário para os fins legítimos da investigação.

A cooperação com a iniciativa privada também se mostra essencial. Provedores de aplicação, redes sociais e plataformas de hospedagem detêm parte significativa das informações que podem subsidiar uma resposta preventiva à criminalidade digital. Para isso, é fundamental que existam protocolos de resposta rápida, canais de comunicação direta e incentivos à conformidade regulatória das empresas com as leis brasileiras.

Ademais, a atuação preventiva deve incluir educação digital da população, campanhas de conscientização sobre segurança na internet e programas de formação para operadores do direito e da segurança pública. A prevenção da criminalidade não se limita à tecnologia: ela

começa com a formação crítica e cidadã dos usuários, especialmente os mais vulneráveis, como crianças, adolescentes e idosos.

Faustino (2020, p. 64) pontua com precisão:

> A eficiência investigativa não pode ser construída às custas da privacidade generalizada da população. A coleta e o tratamento de dados, ainda que com fins de segurança pública, devem respeitar a finalidade, necessidade e proporcionalidade, sob pena de se transformar em controle social abusivo.

Dessa forma, a construção de um modelo eficiente e legítimo de atuação preventiva no ambiente digital exige um tripé institucional: (i) infraestrutura tecnológica pública, com investimento constante em sistemas e plataformas de análise de dados; (ii) capacitação técnica e jurídica dos profissionais envolvidos, para garantir segurança jurídica e eficácia probatória; e (iii) respeito estrito aos direitos fundamentais, sob pena de converter a prevenção em instrumento autoritário.

Em resumo, a inteligência cibernética não substitui a investigação tradicional, mas a complementa de forma estratégica, permitindo que o Estado atue com mais previsibilidade, seletividade e responsabilidade na repressão qualificada de crimes digitais, sem abrir mão dos princípios do Estado de Direito.

2.3 Cooperação Interinstitucional e Internacional

Outro aspecto essencial para uma persecução penal eficaz no ambiente digital é a cooperação entre diferentes esferas do poder público nacional**,** bem como a articulação com instituições internacionais. A natureza transnacional da criminalidade digital desafia os limites da soberania territorial, exigindo respostas coordenadas, céleres e juridicamente harmonizadas entre países.

Crimes cibernéticos, como pornografia infantil, fraudes bancárias, extorsões virtuais, ataques de ransomware e roubo de dados sensíveis, são frequentemente praticados por agentes situados fora do território brasileiro, utilizando infraestruturas tecnológicas distribuídas em diversas jurisdições. Isso torna a investigação criminal dependente da colaboração internacional, tanto para identificar os autores quanto para acessar as provas armazenadas em servidores estrangeiros.

Nesse sentido, a cooperação interinstitucional no plano interno é igualmente indispensável. Polícia Federal, Ministério Público, Judiciário, Autoridade Nacional de Proteção de Dados (ANPD), Ministério da Justiça e agências de inteligência devem atuar de forma

articulada, com fluxos bem definidos de comunicação, integração de bases de dados e protocolos operacionais conjuntos. A fragmentação entre instituições, sem diálogo técnico ou divisão clara de competências, compromete não apenas a eficiência investigativa, mas também a segurança jurídica das medidas adotadas.

No plano internacional, o ingresso do Brasil como país signatário da Convenção de Budapeste sobre o Cibercrime, formalizado em 2023, representa um marco na consolidação de uma política de segurança cibernética baseada na legalidade e na cooperação global. A Convenção fornece instrumentos legais padronizados para facilitar a produção e o compartilhamento de provas digitais entre os países-membros, tais como:

a) Solicitações de preservação de dados eletrônicos antes mesmo de formalizar um pedido completo;
b) Procedimentos simplificados de envio e resposta de dados de identificação de usuários**;**
c) Normas harmonizadas para a tipificação de delitos cibernéticos, como acesso não autorizado a sistemas, fraudes online, crimes contra menores, entre outros.

No entanto, como bem destacam Guerra e Bertholini (2023, p. 147):

> A cooperação jurídica internacional no combate aos crimes digitais deve ser pautada pela celeridade, pelo respeito aos direitos fundamentais e pela superação de entraves burocráticos que historicamente comprometem a efetividade das investigações transnacionais.

Ou seja, a simples assinatura de tratados não basta. É necessário implementar mecanismos internos eficazes que garantam a operacionalização dos instrumentos jurídicos previstos. Isso inclui:

a) Criação de autoridades centrais com estrutura e pessoal técnico-jurídico qualificado para processar pedidos internacionais;
b) Treinamento dos magistrados, promotores e delegados sobre como formular e executar pedidos de cooperação com base na Convenção;
c) Estabelecimento de pontos de contato 24/7, conforme previsto no artigo 35 da Convenção, para atender situações de urgência envolvendo provas digitais voláteis;
d) Inclusão de cláusulas de respeito aos direitos humanos e à legislação nacional nos acordos de execução direta com provedores estrangeiros.

Outro avanço importante seria o fortalecimento de acordos diretos com empresas de tecnologia que operam no Brasil e armazenam dados de usuários, como Google, Meta, Apple e Microsoft. A criação de memorandos de entendimento (MoUs) ou termos de cooperação técnica, ainda que sem força vinculante equivalente a tratados, pode facilitar a comunicação institucional e reduzir o tempo de resposta a pedidos de preservação e fornecimento de dados — desde que sempre observados os limites da legislação nacional e os direitos fundamentais dos indivíduos envolvidos.

Ainda no campo da cooperação, destaca-se o papel de redes internacionais de segurança, como Interpol, Europol e GAFIC (Grupo de Ação Financeira da América do Sul), que promovem o intercâmbio de informações, a elaboração de alertas conjuntos e até a emissão de mandados internacionais de prisão. Essas redes, apesar de não possuírem poder normativo ou coercitivo direto, funcionam como plataformas de inteligência colaborativa que contribuem significativamente para a celeridade da investigação penal no ciberespaço.

Por fim, é preciso enfatizar que a coleta de dados pessoais por meio da cooperação internacional deve respeitar integralmente a Lei Geral de Proteção de Dados (LGPD) e a Emenda Constitucional nº 115/2022, que consagra o direito à proteção de dados como direito fundamental. O compartilhamento de informações entre países e empresas deve ser proporcional, limitado à finalidade da investigação e cercado de garantias de segurança jurídica, evitando abusos ou usos indevidos das informações obtidas.

Assim, a construção de uma política eficiente de cooperação interinstitucional e internacional exige uma postura ativa do Estado brasileiro, que deve conciliar seu compromisso com a persecução penal à observância do devido processo legal e à proteção das liberdades individuais, mesmo diante dos desafios do ciberespaço.

3 A ATUAÇÃO ESTATAL E OS LIMITES CONSTITUCIONAIS IMPOSTOS À LUZ DOS DIREITOS FUNDAMENTAIS

A atuação estatal no campo da investigação penal digital exige uma reflexão cuidadosa sobre os limites que a Constituição Federal de 1988 impõe ao exercício do poder punitivo, sobretudo quando se trata da proteção dos direitos e garantias fundamentais. A persecução penal de crimes cibernéticos, embora demande respostas céleres e eficazes, não pode se sobrepor aos princípios constitucionais que estruturam o Estado Democrático de Direito.

3.1 Princípio da Legalidade

O princípio da legalidade penal, previsto no artigo 5º, inciso II da Constituição Federal de 1988, estabelece que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". No âmbito penal, esse princípio também se traduz na máxima nullum crimen, nulla poena sine lege, ou seja, não há crime nem pena sem prévia cominação legal. Trata-se de um dos pilares do Estado Democrático de Direito, cujo objetivo é proteger o indivíduo contra arbitrariedades e garantir previsibilidade jurídica na atuação estatal.

No contexto da investigação penal digital, a legalidade impõe um marco normativo claro e específico para a adoção de medidas invasivas, como interceptações telemáticas, acesso a dados de navegação, geolocalização e quebras de sigilo de comunicações. Tais medidas representam restrições significativas a direitos fundamentais e, portanto, só podem ser admitidas com base em lei formal, expressa e previamente estabelecida.

A Lei nº 9.296/1996, que regulamenta as interceptações telefônicas e telemáticas, exige ordem judicial motivada, hipóteses de investigação criminal e a indispensabilidade da medida para o esclarecimento dos fatos. Já o Marco Civil da Internet (Lei nº 12.965/2014) introduz salvaguardas específicas para o ambiente digital, como a exigência de autorização judicial para o acesso a conteúdos de comunicações privadas e a previsão de prazos mínimos para a guarda de registros de conexão e aplicação.

Além disso, o artigo 11 do Marco Civil estabelece que as empresas estrangeiras com atuação no Brasil estão sujeitas à legislação nacional, reforçando o alcance da legalidade mesmo no contexto transnacional da internet. Assim, a legalidade não se limita à existência da norma, mas também à sua efetiva aplicação dentro de um modelo constitucional garantista.

A ausência de previsão legal específica para determinadas medidas investigativas digitais, como o acesso a dados em nuvem, ainda é tema controverso, o que torna essencial a atuação prudente das autoridades, evitando abusos e fortalecendo a confiança na Justiça. Portanto, a legalidade é o alicerce sobre o qual se deve construir qualquer ação investigativa legítima no ciberespaço.

3.2 Ampla Defesa e Contraditório

O devido processo legal, previsto no artigo 5º, incisos LIV e LV da Constituição Federal, assegura a todo acusado o direito à ampla defesa e ao contraditório, princípios que se aplicam integralmente à investigação penal, inclusive em sua fase preliminar. A ampla defesa envolve tanto a defesa técnica (por advogado) quanto a autodefesa, enquanto o contraditório garante a

possibilidade de manifestação sobre todas as provas e decisões que afetem a esfera jurídica do investigado.

No ambiente digital, esses direitos ganham ainda mais relevância diante do caráter técnico e sigiloso das provas eletrônicas. O acusado, por vezes, sequer tem conhecimento de que está sendo investigado por meio de ferramentas tecnológicas altamente complexas, como interceptações de mensagens criptografadas, rastreamento de IPs ou acesso a dados armazenados em servidores no exterior. Isso exige do Estado uma atuação ainda mais transparente e fundamentada, sob pena de nulidade processual.

Além disso, a jurisprudência do STF tem reconhecido a necessidade de que a defesa tenha acesso amplo aos elementos probatórios colhidos durante a investigação, ainda que ela esteja em curso, desde que isso não comprometa o êxito da diligência ou exponha terceiros de forma desproporcional.

Como bem destaca Barroso (2019):

> O processo penal não é apenas um instrumento para apurar a verdade material, mas também um espaço de proteção dos direitos fundamentais do acusado, sendo a ampla defesa um dos pilares da legitimidade do exercício do poder punitivo.

A partir disso, conclui-se que a utilização de provas digitais não pode ser feita de forma unilateral, secreta e arbitrária. É dever do Estado garantir que todas as medidas adotadas durante a investigação respeitem o equilíbrio entre acusação e defesa, permitindo o exercício pleno da ampla defesa com todas as garantias a ela inerentes.

3.3 Inviolabilidade da Intimidade, Vida Privada e Sigilo de Dados

Os incisos X e XII do artigo 5º da Constituição Federal asseguram expressamente a inviolabilidade da intimidade, da vida privada e do sigilo das comunicações, sendo que qualquer restrição a esses direitos deve obedecer aos critérios de excepcionalidade, legalidade e controle judicial. No ambiente digital, esses direitos assumem nova dimensão, tendo em vista a enorme quantidade de informações pessoais armazenadas em dispositivos eletrônicos e em servidores de provedores de aplicação e conexão.

O simples uso cotidiano de aplicativos, redes sociais, e-mail e serviços em nuvem gera um rastro digital que revela hábitos, preferências, localização, interações sociais e até convicções ideológicas ou religiosas dos usuários. Isso torna o ambiente digital um espaço

extremamente sensível do ponto de vista da privacidade, sendo indispensável uma atuação estatal criteriosa e limitada ao estritamente necessário.

Com a promulgação da Emenda Constitucional nº 115/2022, o direito à proteção de dados pessoais passou a integrar o rol dos direitos fundamentais (art. 5º, LXXIX), conferindo status constitucional ao princípio da autodeterminação informativa, que garante ao indivíduo o controle sobre suas próprias informações. Essa inovação fortalece os parâmetros constitucionais para a atuação estatal na coleta, tratamento e compartilhamento de dados pessoais, inclusive para fins investigativos.

Bioni (2019, p. 84) ressalta que:

> A proteção de dados pessoais representa, no contexto contemporâneo, um desdobramento lógico dos direitos à privacidade e à autodeterminação informativa. O Estado, ao acessar tais informações, deve observar os princípios da finalidade, adequação e necessidade, sob pena de configurar desvio de finalidade e violação constitucional.

Nesse sentido, as medidas de investigação que envolvem acesso a dados sensíveis, como mensagens privadas, conteúdos de nuvem, localização em tempo real ou registros de acesso, devem ser submetidas a rigoroso controle judicial e técnico, garantindo que a obtenção da prova seja proporcional ao grau de lesão investigado e indispensável à apuração da verdade.

A atuação investigativa que desconsidera esses limites coloca em risco não apenas a validade da prova obtida, mas também a legitimidade do sistema de justiça criminal. Em um Estado Democrático de Direito, a proteção da intimidade e dos dados pessoais deve caminhar lado a lado com a repressão qualificada da criminalidade, especialmente nos meios digitais.

3.4 Proporcionalidade e Razoabilidade na Investigação

A aplicação dos princípios da proporcionalidade e da razoabilidade constitui parâmetro indispensável para aferir a legitimidade das medidas investigativas no ambiente virtual. Esses princípios, embora não expressamente previstos no texto constitucional, são reconhecidos pela doutrina e pela jurisprudência como fundamentos implícitos do Estado Democrático de Direito. Segundo Gilmar Mendes (2022), a proporcionalidade “atua como baliza para o controle da atividade estatal, especialmente em contextos de conflito entre direitos fundamentais, como ocorre frequentemente em investigações criminais de natureza digital”. Dessa forma, medidas como a interceptação de comunicações, a quebra de sigilo de dados e a solicitação de informações a provedores estrangeiros devem ser empregadas apenas quando forem indispensáveis para o esclarecimento dos fatos e desde que autorizadas judicialmente, mediante

justificativa concreta de sua necessidade e adequação. O quadro 1 apresenta uma síntese das medidas Investigativas no ambiente digital e seus limites constitucionais.

Quadro 1 - Medidas Investigativas no Ambiente Digital e seus Limites Constitucionais

Medida Investigativa	Fundamento Legal	Direito Fundamental Afetado	Exigência Constitucional
Interceptação de comunicações eletrônicas	Lei nº 9.296/1996; CF/88, art. 5º, XII	Sigilo das comunicações (CF/88, art. 5º, XII)	Necessária autorização judicial, com decisão fundamentada e por tempo determinado
Acesso a registros de conexão ou de aplicação	Marco Civil da Internet (Lei nº 12.965/2014), art. 10 e 13	Privacidade e dados pessoais (CF/88, art. 5º, X e LXXIX)	Autorização judicial; observância da finalidade, necessidade e proporcionalidade
Busca e apreensão de dispositivos eletrônicos	CPP, art. 240 e seguintes; jurisprudência do STF	Inviolabilidade da intimidade (CF/88, art. 5º, X)	Mandado judicial específico; vedação à devassa generalizada de dados
Solicitação de dados a provedores estrangeiros	MLAT; Convenção de Budapeste; Marco Civil da Internet, art. 11	Soberania nacional e autodeterminação informativa	Cooperação internacional formalizada ou autorização judicial fundamentada
Geolocalização e rastreamento em tempo real	Jurisprudência do STF (HC 166.373/PR; RE 1048841)	Direito à privacidade e locomoção	Autorização judicial com justificativa da urgência e relevância da medida

Fonte: Elaboração própria com base na CF/88, Marco Civil da Internet, Lei nº 9.296/1996, jurisprudência do STF e autores referenciados.

3.5 O Devido Processo Legal no Ciberespaço

O ciberespaço não pode ser compreendido como um território de exceção normativa. Mesmo em face dos desafios impostos pela tecnologia, como a volatilidade dos dados e a atuação transnacional de criminosos, o Estado não está autorizado a flexibilizar as garantias processuais previstas na Constituição. Isso inclui o respeito ao juízo natural, à publicidade dos atos, à motivação das decisões e à paridade de armas entre as partes.

O Supremo Tribunal Federal, no julgamento da ADI 6387, reforçou a importância da proteção dos dados pessoais, reconhecendo que:

> A Constituição de 1988 impõe limites materiais e procedimentais à coleta e ao tratamento de dados pessoais, exigindo, para tanto, base legal legítima, finalidade clara e respeito à autodeterminação informativa do titular dos dados. (STF, ADI 6387, Rel. Min. Edson Fachin, 2020)

Nesse julgamento, foi suspensa a eficácia da Medida Provisória nº 954/2020, que permitia o compartilhamento massivo de dados de usuários de telefonia com o IBGE, evidenciando que, mesmo diante de finalidades públicas relevantes, a proteção da privacidade deve prevalecer.

4 A ATUAÇÃO MULTIDISCIPLINAR E TRANSNACIONAL PARA UMA PERSECUÇÃO PENAL EFICIENTE

A complexidade dos crimes cibernéticos impõe novos desafios à atuação do Estado, exigindo uma abordagem que vá além das fronteiras nacionais e das disciplinas jurídicas tradicionais. A persecução penal eficiente no ambiente virtual requer uma atuação integrada entre diferentes áreas do conhecimento (direito, tecnologia da informação, investigação criminal, psicologia forense, entre outras), bem como uma forte articulação internacional. O cibercrime é, por natureza, transnacional e técnico. Assim, a resposta estatal também precisa ser técnica, ágil e colaborativa.

A revolução digital impôs novas competências às instituições jurídicas. Juízes, promotores, delegados e advogados precisam compreender minimamente o funcionamento dos sistemas informáticos, das redes e dos mecanismos de armazenamento e criptografia de dados. A atuação eficiente depende da tradução de elementos técnicos para o processo penal, sem violar os direitos e garantias constitucionais dos investigados. Torres et al. (2022, p. S38) afirmam que:

> A atuação eficaz no combate à criminalidade cibernética exige do operador do direito conhecimentos básicos sobre tecnologia da informação, redes, servidores, algoritmos de busca, linguagens de programação e, principalmente, sobre a dinâmica da prova digital e sua cadeia de custódia.

Essa capacitação, contudo, não se restringe ao campo jurídico. Ela deve envolver também peritos, técnicos de informática e especialistas em segurança da informação. Trata-se de uma atuação multidisciplinar que permite a coleta, preservação e análise de dados digitais com rigor técnico e processual.

4.1 O Papel da Atuação Judicial na Garantia dos Direitos Fundamentais

Embora a eficiência investigativa seja uma demanda legítima diante da sofisticação da criminalidade digital, ela não pode ser alcançada ao custo da erosão de direitos e garantias constitucionais. O Poder Judiciário, como garantidor do devido processo legal, assume papel decisivo no equilíbrio entre a repressão penal e a preservação das liberdades fundamentais. Sua atuação funciona como um freio legítimo ao exercício arbitrário do poder estatal, especialmente em contextos de alta sensibilidade informacional, como ocorre nas investigações envolvendo dados digitais.

Medidas investigativas invasivas, como interceptações telemáticas, quebras de sigilo de comunicações, apreensão de dispositivos eletrônicos, geolocalização e acesso a conteúdos em nuvem – afetam diretamente os direitos à intimidade, privacidade, sigilo de dados e liberdade individual. Por essa razão, devem necessariamente ser submetidas ao crivo do Judiciário, que deve avaliar, com base nos princípios da legalidade, necessidade, adequação e proporcionalidade, se a medida é justificada diante dos elementos apresentados.

A atuação judicial, portanto, não pode ser meramente homologatória ou protocolar, mas exige uma análise rigorosa dos fundamentos fáticos e jurídicos apresentados pela autoridade policial ou pelo Ministério Público. O juiz deve verificar a presença de indícios razoáveis de autoria e materialidade, bem como a indispensabilidade da medida para o sucesso da investigação. A inexistência desses requisitos pode acarretar não apenas a nulidade da prova colhida, mas também a responsabilização do Estado por violação de direitos fundamentais.

Como bem adverte Gilmar Mendes (2022, p. 472): "A jurisdição constitucional não pode permitir a construção de um Estado de vigilância permanente, no qual a tecnologia sirva para fragilizar os direitos individuais em nome de uma suposta segurança coletiva."

Essa advertência ganha especial relevância no contexto da era digital, em que o volume e a profundidade dos dados disponíveis tornam os cidadãos vulneráveis a formas inéditas de controle estatal. A atuação judicial deve ser, portanto, contrapeso institucional ao poder investigativo, evitando que a eficiência se transforme em abuso e que o combate ao crime justifique práticas incompatíveis com o Estado Democrático de Direito.

Além disso, decisões como a que suspendeu a eficácia da Medida Provisória nº 954/2020, no julgamento da ADI 6387, reforçam que mesmo medidas com aparente finalidade pública não podem desconsiderar o direito fundamental à proteção de dados pessoais. O STF entendeu que o compartilhamento compulsório de dados de usuários com o IBGE, sem consentimento ou controle judicial, violava os princípios da proporcionalidade e da finalidade, e impunha risco à autodeterminação informativa dos cidadãos.

Nesse contexto, o Judiciário tem um papel duplo: (i) proteger o núcleo essencial dos direitos fundamentais, garantindo que nenhuma medida investigativa ultrapasse os limites do razoável; e (ii) legitimar a atuação investigativa, desde que observados os parâmetros legais e constitucionais. Trata-se de uma atuação que exige preparo técnico, sensibilidade jurídica e responsabilidade institucional.

Cabe destacar, ainda, que a efetividade desse controle judicial passa pela capacitação dos magistrados em temas relacionados à tecnologia da informação, segurança cibernética e privacidade digital. É indispensável que o juiz compreenda os impactos técnicos e sociais de

medidas como a quebra de criptografia, o espelhamento de celulares, ou o rastreamento por meio de cookies e metadados. Só assim será possível exercer uma jurisdição informada, prudente e compatível com a complexidade dos desafios contemporâneos.

O Poder Judiciário deve ser visto não como um obstáculo à investigação penal eficiente, mas como garantidor da sua legitimidade. Uma decisão judicial bem fundamentada, pautada nos princípios constitucionais, fortalece o sistema de justiça criminal, assegura a confiança da sociedade nas instituições e evita retrocessos autoritários mascarados de modernização tecnológica.

4.2 Cooperação Jurídica Internacional e o Combate à Criminalidade Transnacional

Diante da globalização da informação, boa parte das provas necessárias à investigação de crimes cibernéticos encontra-se em poder de empresas estrangeiras ou armazenadas em servidores localizados fora do Brasil. Nessa perspectiva, torna-se fundamental o uso de instrumentos de cooperação internacional, como: Cartas rogatórias**;** Tratados de assistência mútua (MLATs)**;** Adesão à Convenção de Budapeste sobre o Cibercrime **e** Acordos bilaterais diretos com provedores e plataformas internacionais**.**

A recente adesão do Brasil à Convenção de Budapeste, formalizada em 2023, representa um marco importante, pois facilita o intercâmbio rápido de informações e a padronização de procedimentos entre países signatários. Entretanto, como alertam Guerra e Bertholini (2023, p. 146):

> O simples ingresso do Brasil na Convenção de Budapeste não resolve os entraves burocráticos e jurídicos da cooperação internacional. É necessário que o país desenvolva canais institucionais eficientes, com autoridade central ágil e mecanismos de resposta em tempo real.

Esse ponto é essencial: não basta assinar tratados, é preciso implementar estruturas internas que deem efetividade à cooperação. O Ministério da Justiça, o Ministério Público Federal e a Polícia Federal devem atuar de forma coordenada, com núcleos de cooperação internacional capacitados e articulados com as autoridades de outros países.

Quadro 2 – Principais Instrumentos de Cooperação Internacional Utilizados na Investigação Penal de Crimes Digitais

Instrumento Jurídico	Abrangência	Utilização na Prática	Vantagens	Limitações
MLAT (Mutual Legal Assistance Treaty)	Acordos bilaterais entre países	Solicitação de dados armazenados por empresas no exterior	Segurança jurídica e formalidade	Lento, burocrático e dependente da reciprocidade
Carta Rogatória	Cooperação	Citação ou intimação	Legitimidade	Alto custo e

	judicial entre autoridades nacionais e estrangeiras	de pessoa no exterior; obtenção de provas formais	processual e reconhecimento judicial internacional	tempo de tramitação elevado
Convenção de Budapeste (2001)	Tratado multilateral sobre cibercrime (Brasil signatário desde 2023)	Troca de informações em tempo real; preservação de dados eletrônicos	Cooperação rápida, base normativa padronizada	Ainda em implementação prática no Brasil
Acordos diretos com provedores (ex: Google, Meta)	Aplicação informal ou extrajudicial	Requisições diretas com base em termos de serviço das plataformas	Celeridade na resposta em casos urgentes	Dependência da boa vontade e políticas internas das empresas estrangeiras
Redes de cooperação internacional (Interpol, GAFIC, Europol)	Estruturas colaborativas de inteligência	Compartilhamento de dados, alertas de segurança e mandados de prisão internacionais	Agilidade e alcance operacional global	Sem poder vinculante legal direto; exige articulação entre autoridades

Fonte: Elaboração própria com base em Rodrigues (2021), Guerra e Bertholini (2023), Convenção de Budapeste e prática de cooperação internacional do Ministério da Justiça.

4.3 EXEMPLO PRÁTICO: Invasão de Dispositivo Eletrônico

A investigação de crimes como a invasão de dispositivos eletrônicos, prevista no artigo 154-A do Código Penal, exige uma abordagem tecnicamente especializada e juridicamente segura. Trata-se de um crime que se caracteriza pelo acesso não autorizado a dispositivos informáticos alheios, com o fim de obter, adulterar ou destruir dados sem o consentimento do titular, podendo ser agravado caso haja divulgação de conteúdo ou prejuízo à vítima.

Dada a natureza do delito — muitas vezes praticado de forma remota, utilizando redes privadas virtuais (VPNs), proxies, e técnicas de mascaramento de IP — a identificação do autor demanda a correlação de múltiplos dados técnicos, como:

a) Endereços IP utilizados em momentos específicos;
b) Registros de conexão e de acesso a aplicações;
c) Metadados associados às ações do invasor;
d) Logs de servidor;
e) Informações de dispositivos vinculados à mesma atividade (ex: MAC Address, identificadores de hardware);
f) Perícia forense em computadores, celulares e mídias removíveis da vítima e do suspeito.

Importante destacar que o simples rastreamento do IP não é suficiente para determinar a autoria, uma vez que esse dado pode estar vinculado a redes públicas, uso coletivo ou mesmo ser falsificado por técnicas como o IP spoofing. É por isso que a jurisprudência tem exigido

uma construção probatória robusta, baseada em cadeia de custódia formal, análises técnicas qualificadas e autorização judicial para todas as etapas que impliquem restrição de direitos fundamentais**.**

A autorização judicial prévia é indispensável, por exemplo, para:

a) A obtenção dos registros de IP junto aos provedores de conexão e aplicação (nos termos do Marco Civil da Internet, art. 10 e 13);
b) O acesso a dados de localização e comunicações trocadas pelo investigado;
c) A busca e apreensão de dispositivos eletrônicos, como smartphones, laptops ou HDs externos;
d) A realização de perícia técnica nos dados armazenados ou deletados.

Caso qualquer dessas etapas seja realizada sem o devido respaldo judicial ou sem respeito à cadeia de custódia (registro completo e contínuo da origem e tratamento da prova digital), o material obtido poderá ser considerado ilícito, gerando sua exclusão do processo com base no artigo 157 do Código de Processo Penal.

Diversas decisões judiciais já reconheceram nulidades processuais quando houve violação à reserva de jurisdição ou uso indevido de dados pessoais sem justificativa adequada**.** Um exemplo paradigmático é o do Tribunal de Justiça de São Paulo (TJSP), que anulou a condenação de um réu por invasão de dispositivo eletrônico porque a polícia obteve dados do roteador da residência do acusado sem ordem judicial e sem qualquer registro da cadeia de custódia. No acórdão, a corte enfatizou que "o acesso informal e não autorizado a equipamentos de informática compromete a confiabilidade da prova e viola frontalmente os princípios do devido processo legal e da legalidade estrita".

Nesse sentido, como enfatiza Bioni (2019, p. 152):

> A legitimidade da atuação estatal no ciberespaço depende de sua conformidade com os direitos fundamentais. A eficácia investigativa não se mede apenas pela obtenção da prova, mas também pela regularidade de sua obtenção e admissibilidade judicial.

O respeito ao devido processo legal não é apenas uma formalidade jurídica, mas um requisito essencial à própria validade do processo penal. A atuação da polícia judiciária e do Ministério Público deve estar em sintonia com os princípios constitucionais, sob pena de transformar a investigação em um procedimento arbitrário e suscetível à responsabilização do Estado — inclusive por meio de ações indenizatórias fundadas em dano moral, abuso de autoridade ou violação à intimidade e à privacidade.

Por fim, é importante ressaltar que o uso de perícia digital forense certificada é uma garantia não apenas para a acusação, mas também para a defesa e para o Judiciário. O laudo técnico é o elo entre o dado bruto e a prova judicialmente válida, sendo fundamental que o perito atue com independência, impessoalidade e fundamentação técnica.

Em resumo, no contexto da investigação de crimes informáticos como a invasão de dispositivos, o respeito aos direitos fundamentais não é um obstáculo à eficácia da persecução penal, é o que a torna legítima, sólida e compatível com o Estado de Direito.

5 CONCLUSÃO

A era digital trouxe transformações profundas nas relações sociais, econômicas e jurídicas, impondo ao Direito Penal o desafio de adaptar seus mecanismos investigativos a uma realidade virtual marcada pela fluidez informacional, pela descentralização territorial e pelo protagonismo de grandes corporações tecnológicas. Nesse contexto, a persecução penal de crimes cibernéticos exige um novo paradigma: aquele que compatibiliza eficiência investigativa com o respeito estrito aos direitos fundamentais garantidos pela Constituição Federal de 1988.

O presente trabalho demonstrou que a atuação estatal no ciberespaço, embora legítima e necessária diante do crescimento exponencial da criminalidade digital, encontra limites jurídicos bem definidos, especialmente após a promulgação da Emenda Constitucional nº 115/2022, que incorporou expressamente a proteção de dados pessoais ao rol de direitos fundamentais. A investigação penal digital não pode, portanto, justificar a adoção de medidas arbitrárias, invasivas ou desproporcionais. A legalidade, o devido processo legal, a ampla defesa, o contraditório, a inviolabilidade da intimidade e o sigilo das comunicações continuam a ser balizas indispensáveis para a legitimidade do agir estatal.

Verificou-se, ainda, que a eficiência investigativa no ambiente virtual depende diretamente de três pilares fundamentais: (i) a celeridade e tecnicidade na coleta e preservação de provas digitais; (ii) o respeito rigoroso aos limites constitucionais, especialmente no tocante à privacidade e autodeterminação informativa; e (iii) a atuação multidisciplinar e transnacional, que inclui a capacitação técnica dos operadores do Direito, o uso de ferramentas de inteligência cibernética e a articulação com mecanismos internacionais de cooperação jurídica.

A adesão do Brasil à Convenção de Budapeste e o fortalecimento da Autoridade Nacional de Proteção de Dados (ANPD) são passos importantes na construção de um modelo jurídico que respeite a soberania digital e, ao mesmo tempo, promova a responsabilização efetiva de condutas criminosas praticadas no ciberespaço. No entanto, para que esses avanços

normativos se traduzam em eficácia concreta, é necessário investimento institucional, reformulação de práticas processuais e, sobretudo, compromisso político com os fundamentos do Estado Democrático de Direito.

Por fim, conclui-se que é possível, e necessário, construir uma persecução penal no ambiente virtual que seja ao mesmo tempo eficaz e constitucional. A soberania digital não pode servir de pretexto para autoritarismos tecnológicos, mas tampouco pode ser um obstáculo intransponível para a repressão de crimes graves. O equilíbrio entre segurança pública e liberdade individual é o maior desafio jurídico da contemporaneidade – e será o critério que distinguirá os sistemas de justiça comprometidos com a democracia daqueles que cedem ao apelo da vigilância desenfreada.

REFERÊNCIAS

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**. 8. ed. São Paulo: Saraiva Educação, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 maio 2025.

BRASIL. **Decreto nº 3.810, de 2 de maio de 2001**. Promulga o Tratado entre a República Federativa do Brasil e os Estados Unidos da América sobre assistência judiciária mútua em matéria penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm. Acesso em: 23 maio 2025.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 20 maio 2025.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Dispõe sobre a interceptação de comunicações telefônicas. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 20 maio 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet: estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 maio 2025.

CAIADO, Felipe B.; CAIADO, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. In: DOMINGOS, Fernanda T. S. et al. **Crimes cibernéticos: coletânea de artigos**. Brasília: Ministério Público Federal, 2018. p. 8–25.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Jorge Zahar, 2003.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime (Convenção de Budapeste)**. Budapeste, 2001. Disponível em: https://www.coe.int/en/web/cybercrime. Acesso em: 23 maio 2025.

DE CARVALHO, Lucas Borges. Soberania digital: legitimidade e eficácia da aplicação da lei na internet. **Revista Brasileira de Direito**, v. 14, n. 2, p. 213–235, 2018.

FAUSTINO, André. **Fake news: a liberdade de expressão nas redes sociais na sociedade da informação**. São Paulo: Lura Editorial, 2020.

GUERRA, Carolina; BERTHOLINI, João. Novos desafios regulatórios: a recém-criada Autoridade Nacional de Proteção de Dados (ANPD) em face da investigação do compartilhamento de dados entre WhatsApp e Facebook. **Aurora: Revista de Arte, Mídia e Política**, v. 16, n. 47, p. 134–151, 2023.

MECABÔ, Alex. Proteção de dados pessoais: a função e os limites do consentimento, de Bruno Bioni. **Revista de Direito Civil Contemporâneo**, v. 28, p. 427–443, 2021.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 18. ed. São Paulo: Saraiva, 2022.

RODRIGUES, Cristina Barbosa. Dados pessoais na economia digital: análise dos impactos da proteção de dados no uso de big data pelo GAFA. **Revista de Direito Internacional e Globalização Econômica**, v. 8, n. 8, p. 179–197, 2021.

SUPREMO TRIBUNAL FEDERAL (Brasil). **Ação Direta de Inconstitucionalidade nº 6387**. Relator: Min. Edson Fachin. Julgamento em: 7 maio 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 20 maio 2025.

SUPREMO TRIBUNAL FEDERAL (Brasil). **Habeas Corpus nº 166.373/SP**. Relator: Min. Gilmar Mendes. Julgamento em: 3 set. 2019. Disponível em: https://jurisprudencia.stf.jus.br. Acesso em: 20 maio 2025.

TORRES, Hugo Pereira Ferraz et al. Prevenção e combate à criminalidade virtual: contribuições da justiça consensual. **Revista Multidisciplinar do Sertão**, v. 1, n. 1, p. S30–S56, 2022.