PBPC
ISSN 2674-9432
Qualis A3 CAPES 2021-2024
DOI - Crossref
Latindex
Indexado no Google Acadêmico

ADMISSIBILIDADE DAS INTERCEPTAÇÕES TELEMÁTICAS ESTRANGEIRAS NO PROCESSO PENAL BRASILEIRO: GARANTISMO PENAL E CONTROLE JURISDICIONAL CONDICIONADO

Marcelo Lacerda Lino, Arlen José da Silva Souza, Sérgio William Domingues Teixeira, Sebastião Pinto

https://doi.org/10.36557/2674-9432.2026v5n5p108-132
Artigo recebido em 3 de Maio e publicado em 3 de Julho de 2026

Análise Doutrinária e Jurisprudencial

RESUMO

A transnacionalização das comunicações digitais impõe ao processo penal contemporâneo uma questão que os sistemas jurídicos clássicos não estão estruturalmente equipados para responder: em que condições dados obtidos por interceptação telemática realizada em jurisdição estrangeira podem ser admitidos como prova válida no processo penal interno, sem violação ao devido processo legal e aos direitos fundamentais constitucionalmente assegurados? Adotou-se método hipotético-dedutivo com abordagem qualitativa, de natureza exploratória-explicativa, mediante pesquisa bibliográfica, análise normativa comparada e análise jurisprudencial qualitativa, examinando as contribuições de Aury Lopes Jr., Gustavo Badaró, Kai Ambos, Luigi Ferrajoli, Mireille Delmas-Marty e Orin Kerr, além do arcabouço normativo da Convenção de Budapeste sobre Cibercrime, promulgada no Brasil pelo Decreto n. 11.491/2023. Os resultados revelam que a admissibilidade dessas provas exige modelo de controle jurisdicional condicionado, articulado em quatro eixos cumulativos: legalidade da obtenção no Estado de origem, compatibilidade material com os direitos fundamentais do Estado destinatário, regularidade da cooperação jurídica internacional e preservação da cadeia de custódia digital. A aplicação do modelo aos casos EncroChat, ANOM e Sky ECC evidenciou perfis diferenciados de vulnerabilidade entre os eixos, confirmando a arquitetura cumulativa e interdependente da proposta. A hipótese foi confirmada: a eficiência investigativa não autoriza a relativização das garantias processuais fundamentais.

Palavras-chave: interceptação telemática. Prova digital transnacional. Admissibilidade probatória. Garantismo penal.

ABSTRACT

The transnationalization of digital communications imposes on contemporary criminal procedure a question that classical legal systems are not structurally equipped to answer: under what conditions may data obtained through telematic interception in a foreign jurisdiction be admitted as valid evidence in domestic criminal proceedings without violating due process and constitutionally guaranteed fundamental rights? A hypothetical-deductive method with qualitative approach and exploratory-explanatory nature was adopted through bibliographical research, comparative normative analysis, and qualitative jurisprudential analysis, examining the contributions of Aury Lopes Jr., Gustavo Badaró, Kai Ambos, Luigi Ferrajoli, Mireille Delmas-Marty, and Orin Kerr, alongside the normative framework of the Budapest Convention on Cybercrime, promulgated in Brazil by Decree No. 11,491/2023. Results reveal that admissibility requires a model of conditioned judicial control structured around four cumulative axes: legality of collection in the state of origin, material compatibility with the receiving state's fundamental rights, regularity of international legal cooperation, and preservation of the digital chain of custody. The application of the model to the EncroChat, ANOM, and Sky ECC cases revealed differentiated vulnerability profiles across the axes, confirming the cumulative and interdependent architecture of the proposal. The hypothesis was confirmed: investigative efficiency does not authorize the relativization of fundamental procedural guarantees.

Keywords: telematic interception. Transnational digital evidence. Evidentiary admissibility. Criminal proceduralism.

1. INTRODUÇÃO

A transnacionalização das comunicações digitais alterou de modo estrutural o campo da prova penal. A fragmentação dos dados por jurisdições distintas, viabilizada por plataformas criptografadas, serviços de armazenamento em nuvem e redes privadas virtuais, dissolve a premissa territorial sobre a qual o processo penal foi historicamente construído. O Estado que pretende utilizar determinada prova criminal pode não ter tido qualquer participação em sua obtenção, realizada por autoridades estrangeiras segundo parâmetros que diferem, às vezes substancialmente, das garantias que o ordenamento constitucional interno assegura ao investigado. Essa dissociação entre o local de produção da prova e o foro de julgamento não constitui contingência tecnológica superável por ajustes incrementais: trata-se de transformação estrutural que exige resposta dogmática articulada.

A urgência prática do problema consolidou-se com as operações internacionais contra as plataformas criptografadas EncroChat, Sky ECC e ANOM, realizadas entre 2020 e 2021, que produziram volumes massivos de dados utilizados em processos penais de dezenas de países simultaneamente. Tribunais alemães divergiram sobre a admissibilidade dos dados do EncroChat: o de Berlim os admitiu; o de Dortmund os rejeitou, por entender que a autorização francesa não atendia ao requisito de suspeita individualizada exigido pelo direito alemão. No Brasil, o Superior Tribunal de Justiça e o Supremo Tribunal Federal foram instados a pronunciar-se sobre questões análogas sem que exista jurisprudência consolidada ou legislação específica que fixe os critérios aplicáveis. Essa lacuna não decorreu de omissão legislativa pontual: ela reflete a incapacidade de um direito processual construído sobre a territorialidade para regular situações probatórias em que nenhuma etapa relevante, seja a captação, o armazenamento, a transmissão ou a apresentação em juízo, ocorre inteiramente em solo nacional.

O problema de pesquisa pode ser formulado nos seguintes termos: quais os critérios jurídico-processuais que condicionam a admissibilidade das interceptações telemáticas obtidas em jurisdições estrangeiras no processo penal brasileiro, de modo a preservar simultaneamente a eficácia da persecução penal transnacional e as garantias fundamentais constitucionalmente asseguradas ao investigado? A hipótese central é a de que essa admissibilidade deve ser submetida a um modelo de controle jurisdicional condicionado, estruturado em quatro eixos cumulativos: legalidade da obtenção no Estado de origem, compatibilidade material com os direitos fundamentais garantidos pela Constituição do

Estado destinatário, regularidade da cooperação jurídica internacional e preservação da cadeia de custódia digital. Sustenta-se que a falha em qualquer desses eixos constitui condição suficiente para a inadmissibilidade da prova, independentemente de sua relevância investigativa, conclusão que o desenvolvimento deste artigo pretende fundamentar dogmaticamente.

O objetivo geral é elaborar modelo dogmático de admissibilidade condicionada para as interceptações telemáticas obtidas em jurisdições estrangeiras, fundamentado nos princípios do garantismo penal e compatível com as exigências da cooperação jurídica internacional contemporânea. Três objetivos específicos desdobram esse propósito: examinar os referenciais teóricos e normativos que balizam o debate sobre prova digital transnacional; construir os quatro eixos do modelo de admissibilidade condicionada e verificar sua operacionalidade mediante aplicação a casos concretos de interceptação transnacional; e discutir os resultados à luz da jurisprudência brasileira e das perspectivas de reforma normativa.

Adota-se o método hipotético-dedutivo, partindo da hipótese central submetida a teste pelo confronto com o referencial teórico, o arcabouço normativo e os casos concretos examinados. A abordagem é qualitativa, orientada pela interpretação de fenômenos jurídicos complexos em seu contexto normativo e doutrinário, sem pretensão de mensuração estatística. Quanto aos objetivos, a pesquisa é exploratória no que se refere à sistematização de campo ainda carente de parâmetros consolidados na literatura brasileira, e explicativa na medida em que identifica e articula os critérios que condicionam a admissibilidade das provas digitais transnacionais. Os procedimentos técnicos compreendem pesquisa bibliográfica em obras doutrinárias nacionais e estrangeiras, análise normativa comparada entre o ordenamento constitucional brasileiro e os instrumentos internacionais aplicáveis, e análise jurisprudencial qualitativa de decisões de cortes brasileiras e europeias. O arcabouço normativo primário é constituído pela Constituição Federal de 1988, pela Lei n. 9.296/1996, pela Lei n. 13.964/2019 e pela Convenção de Budapeste sobre Cibercrime, promulgada no Brasil pelo Decreto n. 11.491/2023, cuja adesão recente confere ao tema particular relevância para a prática jurídica nacional.

2. REFERENCIAIS TEÓRICOS E NORMATIVOS DA PROVA DIGITAL TRANSNACIONAL

A construção de um modelo dogmático de admissibilidade condicionada para as interceptações telemáticas de origem estrangeira pressupõe dois planos analíticos distintos e complementares. O primeiro é teórico: identificar os referenciais que fundamentam axiologicamente a exigência de controle jurisdicional sobre a prova digital transnacional e que oferecem os critérios operacionais para sua verificação. O segundo é normativo: examinar o arcabouço internacional que disciplina a obtenção e o compartilhamento dessas provas, avaliando em que medida os instrumentos disponíveis satisfazem ou comprometem os parâmetros de admissibilidade que o ordenamento constitucional brasileiro impõe. A subseção 2.1 desenvolve o referencial teórico estruturante, articulando as contribuições do garantismo penal de Luigi Ferrajoli, do critério da dupla licitude de Kai Ambos, da análise macroestrutural de Mireille Delmas-Marty e da especificação tecnológica de Orin Kerr, além do quadro normativo constitucional interno. A subseção 2.2 examina o regime internacional de obtenção de provas digitais, com ênfase na Convenção de Budapeste sobre Cibercrime, nos Mutual Legal Assistance Treaties e no modelo unilateral norte-americano, identificando as insuficiências de cada instrumento frente às exigências do modelo proposto.

2.1. Garantismo Penal, Dupla Licitude e Desterritorialização: Fundamentos para a Análise

O debate doutrinário sobre admissibilidade de provas digitais transnacionais desenvolveu-se de forma acelerada, porém sem convergência sobre as soluções. Há consenso apenas no diagnóstico: os modelos clássicos de cooperação internacional são insuficientes para o ambiente digital. As divergências refletem posições filosóficas substantivas sobre a hierarquia entre eficiência punitiva e proteção dos direitos fundamentais. A corrente eficientista, predominante na literatura norte-americana, defende vias alternativas aos mecanismos formais de cooperação, priorizando a celeridade investigativa. A corrente garantista, de influência continental europeia, subordina a admissibilidade a controles judiciais rigorosos nos dois Estados envolvidos. A corrente harmonizadora, por sua vez, busca parâmetros procedimentais mínimos que conciliem eficiência e garantismo sem sacrificar nenhum dos dois inteiramente. Na literatura brasileira, a ausência de modelo dogmático integrado que articule critérios de admissibilidade aplicáveis às provas digitais de origem estrangeira é a lacuna central que esta pesquisa se propõe a preencher.

O referencial teórico estruturante é o garantismo penal de Luigi Ferrajoli. Para o autor, o processo penal democrático tem por função primária a limitação do poder punitivo

mediante garantias epistêmicas e procedimentais rigorosas. Uma condenação fundada em prova ilegalmente obtida é ilegítima não porque o condenado seja necessariamente inocente, mas porque viola as regras que conferem ao Estado o direito de punir (Ferrajoli, 2002). O autor sustenta que não basta que a prova exista: é necessário que sua produção tenha obedecido a formas legais precisas, verificáveis e controláveis pelo acusado e pelo juiz, pois a prova ilegal não é apenas inadmissível, mas epistemicamente contaminada (Ferrajoli, 2002, p. 498). Transferida ao campo das interceptações transnacionais, essa premissa implica que a legalidade estrangeira não cria, por si só, legitimidade interna: o Estado brasileiro não pode condenar com base em prova compatível com o direito de origem, mas incompatível com os valores constitucionais brasileiros.

Dessa premissa decorre a necessidade de um critério que operacionalize a exigência ferrajoliana no plano transnacional. Kai Ambos oferece esse critério ao propor o exame em dois níveis independentes e cumulativos: conformidade com o direito do Estado de origem e compatibilidade material com os direitos fundamentais do Estado destinatário, sendo que a falha em qualquer dos níveis é suficiente, por si só, para tornar a prova inadmissível (Ambos, 2021, p. 217). Essa estrutura analítica em dois níveis é o instrumento de operacionalização do garantismo ferrajoliano no contexto das provas de origem estrangeira, e constitui o núcleo do modelo proposto nesta pesquisa. A perspectiva de Ambos, contudo, não abrange a dimensão política do problema, razão pela qual o referencial precisa ser complementado.

Mireille Delmas-Marty oferece o enquadramento político e macroestrutural necessário para compreender o problema em sua amplitude. A globalização da criminalidade produziu uma globalização da prova que os sistemas processuais nacionais, construídos sobre a premissa da territorialidade, não estão preparados para absorver. O resultado é um espaço de assimetrias em que a eficácia punitiva avança enquanto a proteção dos direitos fundamentais recua pela acumulação progressiva de exceções justificadas por urgência investigativa, até que as exceções se tornem o regime ordinário (Delmas-Marty, 2003). Esse fenômeno é precisamente o risco que o modelo de controle jurisdicional condicionado busca neutralizar ao impor parâmetros verificáveis independentemente da via pela qual a prova foi obtida.

Orin Kerr especifica as características tecnológicas que tornam o ambiente digital qualitativamente distinto de qualquer cenário probatório anterior. Os dados podem estar fragmentados em múltiplos países simultaneamente, dissolvendo o pressuposto clássico de

que a prova ocupa um local físico sujeito a uma única soberania. Isso implica que a admissibilidade não pode ser resolvida pela simples identificação de uma autorização válida em algum ponto do globo, pois cada fragmento do dado pode ter sido capturado sob regime jurídico distinto (Kerr, 2022). Ferrajoli fundamenta axiologicamente a inadmissibilidade de provas ilegais; Ambos operacionaliza esse fundamento em parâmetros verificáveis; Delmas-Marty contextualiza os riscos políticos da cooperação informal; e Kerr demonstra por que a tecnologia impede soluções baseadas em territorialidade. Esses quatro referenciais, tomados em conjunto, fornecem a base teórica sobre a qual o modelo dogmático proposto se sustenta.

No plano normativo interno, o ordenamento constitucional brasileiro fornece os parâmetros de controle sobre as interceptações telemáticas domésticas e, por extensão interpretativa, sobre as estrangeiras. O art. 5º, inciso XII, da Constituição Federal protege a inviolabilidade do sigilo das comunicações, ressalvando a possibilidade de interceptação por ordem judicial. A Lei n. 9.296/1996 regulamentou essa ressalva para as comunicações telefônicas e, por extensão progressiva da jurisprudência, para as telemáticas, exigindo autorização judicial fundamentada, indicação dos investigados e dos fatos que justificam a medida, prazo máximo de quinze dias renovável e impossibilidade de deferimento quando inexistir indício razoável de autoria em infrações puníveis com reclusão. Aury Lopes Jr. identifica nesse regime dois planos de proteção: a dimensão formal, que tutela o sigilo do ato comunicativo, e a dimensão material, que protege o conteúdo da comunicação contra usos distintos daqueles que justificaram a captação, de modo que a violação de qualquer das duas dimensões contamina objetivamente a prova (Lopes Jr., 2023, p. 512).

A Emenda Constitucional n. 115/2022, ao consagrar a proteção de dados pessoais como direito fundamental autônomo no art. 5º, inciso LXXIX, da Constituição Federal, acrescentou terceiro vetor normativo de controle sobre as provas digitais transnacionais. Além da legalidade formal e da compatibilidade constitucional clássica, o tratamento dos dados obtidos mediante interceptação, incluindo seu compartilhamento internacional, deve observar os princípios da finalidade, adequação e necessidade previstos na Lei Geral de Proteção de Dados. Patrícia Peck Pinheiro sustenta que a proteção de dados pessoais integra o núcleo essencial da privacidade e não pode ser afastada por razões investigativas de conveniência internacional (Pinheiro, 2021). Para os fins deste referencial, importa registrar que o princípio da finalidade opera como critério autônomo de admissibilidade: dados interceptados no exterior e utilizados para fins distintos dos que justificaram a captação

original são inadmissíveis independentemente da legalidade da obtenção, questão que será desenvolvida na análise do segundo eixo do modelo.

2.2. O Regime Internacional de Obtenção de Provas Digitais: Budapeste, MLATs e a Questão da Soberania

O arcabouço normativo internacional que disciplina a obtenção transnacional de provas digitais apresenta tensão estrutural entre eficiência e garantismo que o referencial teórico da subseção anterior permite compreender em suas implicações dogmáticas. A análise desse arcabouço é, portanto, etapa necessária para identificar em que medida os instrumentos disponíveis satisfazem ou comprometem os critérios de admissibilidade que o modelo proposto exige.

A Convenção de Budapeste sobre Cibercrime, adotada em 2001 e promulgada no Brasil pelo Decreto n. 11.491/2023, constitui o instrumento normativo internacional mais abrangente sobre obtenção transnacional de provas digitais. Seu texto organiza-se em torno de três pilares: harmonização das tipificações penais relativas a crimes cibernéticos; criação de poderes investigativos específicos para o ambiente digital, com reserva jurisdicional para as medidas mais intrusivas; e mecanismos de cooperação internacional para obtenção e compartilhamento de provas. No plano dos poderes investigativos internos, a Convenção impõe aos signatários a previsão de instrumentos como a preservação rápida de dados armazenados (art. 16), a preservação de dados de tráfego (art. 17), a apresentação coercitiva de dados de assinantes (art. 18) e a interceptação de conteúdo (art. 21). Para o modelo proposto, o mecanismo mais relevante é a preservação acelerada transfronteiriça do art. 29, pelo qual o Estado requerente solicita ao requerido a preservação imediata dos dados enquanto o pedido formal tramita pelos canais diplomáticos, combinando celeridade investigativa com formalismo procedimental.

A Convenção de Budapeste apresenta, contudo, limitação estrutural diretamente relevante para o primeiro eixo do modelo de admissibilidade: não estabelece padrão uniforme de controle judicial para as interceptações, remetendo aos direitos internos a definição dos requisitos concretos de autorização. Isso gera assimetria protetiva entre jurisdições e cria condições para o fenômeno denominado por Gustavo Badaró de forum shopping probatório, que consiste na seleção estratégica do Estado com menores exigências procedimentais para obtenção de provas que seriam vedadas no Estado destinatário. Quando as autoridades

podem escolher livremente de qual jurisdição receberão os dados, o incentivo estrutural é sempre a escolha pela jurisdição mais permissiva, esvaziando materialmente as garantias do Estado destinatário (Badaró, 2022, p. 891). A adesão brasileira à Convenção representa avanço normativo significativo, mas o desafio imediato é a adequação interna às obrigações convencionais assumidas, processo que o legislador ainda não iniciou.

Os Mutual Legal Assistance Treaties constituem o mecanismo clássico e mais consolidado de obtenção formal de provas em outro Estado. Submetem a solicitação ao controle judicial interno do Estado requerido e asseguram legitimidade processual em ambas as jurisdições, atendendo simultaneamente ao primeiro e ao terceiro eixos do modelo proposto. A lentidão operacional desses tratados é o principal argumento apresentado para a utilização de vias informais. Renato Brasileiro de Lima observa que, mesmo na ausência de tratado bilateral específico, a cooperação deve processar-se segundo as regras do direito internacional costumeiro e dos princípios gerais de assistência mútua, que também impõem formalidade, transparência e reciprocidade, sendo o controle judicial interno ainda mais rigoroso nessas situações (Lima, 2022). A solução adequada para a lentidão dos Mutual Legal Assistance Treaties é sua modernização mediante procedimentos eletrônicos e prazos máximos de resposta, e não o abandono do formalismo que lhes é inerente.

Em sentido oposto posiciona-se o Clarifying Lawful Overseas Use of Data Act norte-americano de 2018, que permite às autoridades dos Estados Unidos requisitar diretamente a empresas de tecnologia sediadas no país dados armazenados em qualquer parte do mundo, independentemente do país de residência do investigado. Essa extensão unilateral da jurisdição gerou conflito direto com o Regulamento Geral de Proteção de Dados da União Europeia e com as legislações de privacidade de múltiplos países, evidenciando que a disputa sobre jurisdição probatória digital não é apenas questão dogmática, mas problema de soberania com relevante grau de litigiosidade internacional. Para o Brasil, cujos cidadãos utilizam intensamente plataformas de empresas norte-americanas, dados de brasileiros podem ser acessados pelas autoridades dos Estados Unidos sem notificação ao Estado brasileiro. Quando esses dados chegam ao processo penal por cooperação policial informal, o percurso formal verificável, que o terceiro eixo do modelo exige como condição de admissibilidade, encontra-se comprometido de origem, por razão estrutural e não acidental.

O panorama normativo internacional revela, em síntese, que nenhum dos instrumentos disponíveis satisfaz integralmente os critérios de admissibilidade que o

problema de pesquisa exige. A Convenção de Budapeste avança na harmonização, mas não uniformiza o controle judicial. Os Mutual Legal Assistance Treaties asseguram formalismo, mas carecem de celeridade. O modelo unilateral norte-americano prioriza a eficiência ao custo da soberania e das garantias dos investigados. Essa insuficiência não se resolve pela escolha de um instrumento em detrimento dos demais, mas pela construção de critérios dogmáticos de admissibilidade que imponham, em qualquer hipótese, o mesmo grau de controle jurisdicional que o ordenamento constitucional brasileiro exige. Os quatro eixos desenvolvidos na seção seguinte constituem essa construção.

3. METODOLOGIA

A pesquisa classifica-se, quanto ao método de abordagem, como hipotético-dedutiva. Parte-se de uma hipótese central — a de que a admissibilidade das interceptações telemáticas obtidas em jurisdições estrangeiras deve ser submetida a modelo de controle jurisdicional condicionado, estruturado em quatro eixos cumulativos — e busca-se, pelo confronto dessa hipótese com o referencial teórico, o arcabouço normativo e os casos concretos examinados, verificar sua sustentação ou refutação. Esse percurso é próprio do método hipotético-dedutivo, no qual o conhecimento científico avança pela formulação de hipóteses que, submetidas a teste, são corroboradas ou abandonadas (Lakatos; Marconi, 2021). A escolha por esse método é coerente com o objetivo geral do artigo, que não é descrever o estado da arte, mas elaborar e testar um modelo dogmático original.

Quanto à abordagem, a pesquisa é qualitativa. Não se pretende mensurar variáveis nem produzir generalizações estatísticas, mas compreender, interpretar e sistematizar fenômenos jurídicos complexos a partir de seus significados normativos, doutrinários e jurisprudenciais. A pesquisa qualitativa, conforme Creswell e Creswell (2021), caracteriza-se pela ênfase na interpretação de fenômenos em seu contexto, pela valorização das fontes primárias e pela construção indutiva e dedutiva de sentido a partir dos dados coletados. No campo jurídico, essa abordagem é especialmente adequada quando o objeto de investigação envolve lacunas normativas, tensões entre princípios e categorias dogmáticas em construção, como é o caso da admissibilidade probatória transnacional.

Quanto aos objetivos, a pesquisa é simultaneamente exploratória e explicativa. É exploratória porque o tema da admissibilidade das interceptações telemáticas estrangeiras no processo penal brasileiro carece de tratamento sistemático na literatura nacional,

configurando campo em que a investigação científica ainda não produziu parâmetros consolidados. Gil (2022) situa a pesquisa exploratória como aquela que visa proporcionar maior familiaridade com o problema, tornando-o mais explícito ou permitindo a construção de hipóteses. É explicativa porque não se limita a descrever o fenômeno: busca identificar os fatores que determinam ou condicionam a admissibilidade dessas provas, articulando relações de causalidade normativa entre os critérios propostos e as exigências constitucionais. A dimensão explicativa é, nesse sentido, o plano em que a contribuição científica se concretiza.

Quanto aos procedimentos técnicos, a pesquisa combina três estratégias complementares. A primeira é a pesquisa bibliográfica, desenvolvida a partir de obras doutrinárias nacionais e estrangeiras nos campos do processo penal, do direito internacional, da teoria do garantismo e do direito digital. Conforme Fonseca (2002), a pesquisa bibliográfica permite ao investigador cobrir uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente, sendo indispensável quando o problema de pesquisa requer o domínio de posições teóricas consolidadas em diferentes tradições jurídicas. A segunda é a análise normativa comparada, que examina o ordenamento constitucional brasileiro, a legislação infraconstitucional pertinente e os instrumentos internacionais aplicáveis, em cotejo com sistemas jurídicos estrangeiros relevantes para o problema investigado. Essa estratégia permite identificar convergências, divergências e lacunas entre os regimes normativos, fornecendo o substrato para a construção dos critérios dogmáticos de admissibilidade. A terceira é a análise jurisprudencial qualitativa, que examina decisões de cortes brasileiras e europeias sobre admissibilidade de provas digitais transnacionais, com ênfase nos casos envolvendo as operações EncroChat, Sky ECC e ANOM. Essa análise não tem pretensão de exaustividade quantitativa: seu propósito é identificar padrões argumentativos, divergências interpretativas e lacunas decisórias que o modelo proposto pretende suprir.

As fontes primárias que integram o corpus normativo da pesquisa são a Constituição Federal de 1988, a Lei n. 9.296/1996, a Lei n. 13.964/2019 e a Convenção de Budapeste sobre Cibercrime, promulgada no Brasil pelo Decreto n. 11.491/2023. As fontes secundárias compreendem a doutrina especializada nacional e estrangeira referenciada ao longo do trabalho. A seleção das fontes obedeceu a dois critérios: relevância direta para o problema de pesquisa e representatividade das principais correntes doutrinárias identificadas no estado da arte. Não foram estabelecidos recortes temporais rígidos para a pesquisa bibliográfica, dado

que obras seminais mais antigas, como as de Ferrajoli (2002) e Delmas-Marty (2003), mantêm plena pertinência teórica para o objeto investigado. O recorte temporal aplicado à análise jurisprudencial e normativa é predominantemente o período posterior a 2020, que marca o início das grandes operações internacionais contra plataformas criptografadas e, com elas, a emergência prática do problema examinado.

4. OS QUATRO EIXOS DE CONTROLE JURISDICIONAL: CRITÉRIOS E APLICAÇÃO

A construção do modelo de admissibilidade condicionada proposto neste artigo articula-se em dois momentos analíticos sucessivos. O primeiro consiste na formulação dogmática dos quatro eixos que compõem o modelo, a partir dos referenciais teóricos e normativos examinados na Seção 2. O segundo consiste na aplicação desses eixos aos casos concretos que evidenciaram, na prática internacional recente, os limites dos instrumentos de cooperação atualmente disponíveis. A subseção 4.1 desenvolve o primeiro momento; as subseções 4.2 e 4.3 desenvolvem o segundo, examinando respectivamente os casos EncroChat e ANOM, e o caso Sky ECC, com a síntese comparativa dos três casos ao final.

4.1. Construção Dogmática dos Quatro Eixos

O primeiro eixo exige que a interceptação telemática tenha sido produzida em conformidade com os requisitos legais da jurisdição responsável pela captação. Esse critério compreende autorização judicial prévia de juiz ou tribunal competente segundo o direito do Estado de origem, delimitação concreta do objeto com identificação dos investigados e das infrações em apuração, prazo determinado, fundamentação sobre necessidade e proporcionalidade, e supervisão judicial durante a execução. O exame não se restringe ao aspecto formal, à mera existência de autorização judicial, mas alcança o aspecto material da decisão. Quando as autoridades estrangeiras invocam sigilo de Estado para não revelar os documentos que instruíram a autorização judicial, a impossibilidade de verificação é, ela própria, causa de inadmissibilidade, pois o garantismo de Ferrajoli exige que a legalidade da prova seja demonstrável e contestável, não apenas afirmada pelas autoridades que a produziram (Ferrajoli, 2002). Uma decisão estrangeira que autoriza a captação em massa de todos os usuários de uma plataforma sem individualização de suspeitos ilustra essa exigência: ela pode ser formalmente válida segundo o direito de origem e, ainda assim, carecer da fundamentação concreta que o modelo exige.

A proporcionalidade constitui requisito material autônomo dentro do primeiro eixo, com dupla incidência: a medida deve ser proporcional segundo os parâmetros do Estado de origem e, cumulativamente, segundo o ordenamento brasileiro. Interceptações autorizadas no exterior para investigar crimes que no Brasil não alcançariam o patamar de gravidade do art. 2º, inciso III, da Lei n. 9.296/1996 não satisfazem o critério, mesmo que perfeitamente legais no Estado de origem. A vedação constitucional às provas ilícitas não distingue, em seu suporte normativo, entre provas produzidas no Brasil e provas produzidas no exterior, pois a ilicitude é condição objetiva da prova, e não consequência territorial de sua obtenção (Badaró, 2022, p. 578). Quando o exame revela autorização genérica, desproporcional ou inexistente, a prova é inadmissível sem necessidade de exame dos demais eixos.

O segundo eixo opera de forma independente e cumulativa ao primeiro. Ainda que a interceptação tenha sido validamente realizada segundo o direito do Estado de origem, o processo penal brasileiro exige verificação adicional da compatibilidade material entre o procedimento de obtenção e os direitos fundamentais constitucionalmente assegurados. Tratá-lo como condição subsidiária ao primeiro eixo seria converter a cooperação internacional em mecanismo de contorno das garantias constitucionais, fenômeno que a doutrina denomina laundering evidence. Os direitos tutelados incluem intimidade e vida privada (art. 5º, X, CF), sigilo das comunicações (art. 5º, XII, CF), devido processo legal (art. 5º, LIV, CF), contraditório e ampla defesa (art. 5º, LV, CF), proibição de provas ilícitas (art. 5º, LVI, CF) e proteção de dados pessoais (art. 5º, LXXIX, CF). A violação de qualquer desses direitos contamina objetivamente a prova, pois o processo penal não existe para facilitar a condenação de culpados, mas para assegurar que somente culpados sejam condenados, e somente mediante provas validamente obtidas (Lopes Jr., 2023, p. 78).

O critério do contraditório diferido é especialmente relevante no segundo eixo. O processo penal brasileiro admite que a interceptação ocorra sem o conhecimento prévio do investigado, mas exige que ele possa contestar os elementos probatórios em momento oportuno. Interceptações estrangeiras cujos métodos técnicos o Estado de origem se recusa a revelar criam obstáculo estrutural a essa exigência, pois o investigado não pode contestar a autenticidade de dados quando não sabe como foram capturados. Soma-se a isso o desvio de finalidade probatória, que consiste na utilização de dados interceptados para fins distintos dos que justificaram a captação: essa prática viola o princípio da finalidade da Lei Geral de Proteção de Dados e torna a prova inadmissível mesmo que sua obtenção original tenha sido

inteiramente legal. A análise de compatibilidade constitucional é necessariamente mais complexa do que a verificação de legalidade no Estado de origem, porque envolve aplicar parâmetros do Estado destinatário a procedimentos executados segundo outra lógica jurídica. O julgador brasileiro deve examinar não apenas se o procedimento estrangeiro violou alguma norma constitucional interna em sua literalidade, mas se os valores que essas normas tutelam foram respeitados na substância. Essa distinção entre conformidade formal e compatibilidade material constitui o núcleo operacional do critério da dupla licitude de ambos aplicados ao contexto constitucional brasileiro.

O terceiro eixo trata da regularidade procedimental da transferência internacional da prova. A obtenção e a transmissão dos dados digitais devem observar os tratados internacionais aplicáveis, os acordos bilaterais de cooperação jurídica e os mecanismos formais de assistência mútua. A distinção entre cooperação policial para fins investigativos e cooperação jurídica para fins probatórios é dogmaticamente decisiva e frequentemente ignorada na prática: a primeira pode operar com menor formalismo quando seus produtos não se destinam a fundar condenações, ao passo que a segunda exige rigor procedimental pleno, porque o produto será apresentado em juízo como fundamento de decisões que podem resultar na privação de liberdade do acusado. A cooperação policial informal pode servir a fins legítimos de agilização das investigações, mas não pode substituir os mecanismos formais de assistência jurídica para fins probatórios, pois a prova que ingressa no processo deve ter percurso formal verificável, e não apenas resultado investigativo relevante (Ambos, 2021, p. 284). O ingresso no processo penal de informações obtidas por canais informais, sem conversão em prova processualmente válida pelos mecanismos formais de cooperação, compromete a admissibilidade do elemento probatório, independentemente de sua relevância investigativa.

A intensidade do controle jurisdicional deve ser inversamente proporcional à formalidade da via de cooperação utilizada: provas obtidas por *Mutual Legal Assistance Treaty* regularmente tramitado apresentam nível de controle prévio que reduz o ônus do exame a posteriori, ao passo que provas obtidas por cooperação policial informal exigem controle de intensidade máxima sobre todos os aspectos das condições de captação e transmissão. Essa regra opera como desincentivo ao uso de vias informais: quanto mais informal a via, mais rigoroso o controle e maior a probabilidade de exclusão da prova. O percurso da prova desde sua captação no Estado de origem até sua apresentação no processo penal brasileiro deve ser

integralmente documentado, verificando-se se foram utilizados canais formais previstos em tratados ou acordos bilaterais e se as autoridades transmissoras tinham competência segundo seu próprio direito.

O quarto eixo é o mais específico ao domínio da prova digital e o que mais distingue a análise probatória contemporânea da dogmática processual tradicional. Dados digitais são modificáveis sem deixar rastros perceptíveis ao exame ordinário, de modo que um arquivo adulterado com competência técnica pode ser indistinguível do original. Apenas o registro criptográfico de integridade, o hash, permite verificar a posteriori se o conteúdo foi alterado desde a captação. Sem esse registro, a prova digital carece de verificabilidade epistêmica, não sendo possível afirmar, com o grau de certeza que o processo penal exige, que ela representa fielmente o que a autoridade afirma. A cadeia de custódia digital não é mera formalidade burocrática, mas garantia epistêmica fundamental: sem ela, não é possível afirmar com segurança que a prova apresentada em juízo é a mesma prova que foi originalmente obtida, no estado em que foi obtida (Badaró, 2022, p. 609). A cadeia de custódia de provas digitais transnacionais é ainda mais exigente do que a doméstica, pois envolve múltiplas transferências entre jurisdições distintas; sua documentação adequada deve abranger o registro técnico do processo de captação com os métodos utilizados, os valores de hash calculados no momento da obtenção e confirmados em cada transferência, e a certificação pelo Estado de origem da autenticidade e integridade dos dados transmitidos.

No Brasil, a Lei n. 13.964/2019 reforçou as exigências de cadeia de custódia nos arts. 158-A a 158-F do Código de Processo Penal, cujos princípios, integridade, autenticidade, rastreabilidade e verificabilidade, são plenamente aplicáveis, por extensão interpretativa, às provas digitais transnacionais. A questão das consequências da ruptura da cadeia de custódia digital é controvertida: o Superior Tribunal de Justiça a trata como nulidade relativa, dependente de demonstração de prejuízo, ao passo que Badaró sustenta que ela gera nulidade absoluta, por comprometer a própria possibilidade de aferição da autenticidade da prova e, portanto, o exercício pleno do contraditório (Badaró, 2022). A posição mais coerente com o garantismo de Ferrajoli é a segunda: quando não é possível demonstrar que os dados apresentados são idênticos aos captados, a prova perde sua verificabilidade epistêmica e não pode fundar condenação.

Os quatro eixos operam de forma cumulativa e interdependente. A satisfação de três não compensa a falha no quarto, problemas em um eixo revelam frequentemente problemas

nos demais, e o modelo constitui sistema integrado de controle, não lista de requisitos independentes. É justamente essa interdependência que a aplicação aos casos concretos, desenvolvida nas subseções seguintes, permite evidenciar com precisão.

4.2. Aplicação do Modelo aos Casos EncroChat e ANOM

A aplicação dos quatro eixos aos casos concretos selecionados permite verificar a operacionalidade do modelo proposto e evidenciar, de forma empírica, a interdependência entre os critérios que o compõem. O EncroChat e a ANOM constituem operações internacionais de interceptação em massa de comunicações criptografadas, conduzidas entre 2020 e 2021, que produziram volumes expressivos de dados utilizados em processos penais de dezenas de países simultaneamente. Ambas as operações concentram vulnerabilidades no primeiro eixo, mas divergem quanto à extensão do comprometimento dos demais critérios.

O caso EncroChat ilustra com precisão as tensões do primeiro eixo. A autorização francesa para a captação em massa dos dados da plataforma, sem individualização prévia de suspeitos, foi aceita pelo Tribunal Regional de Berlim, que considerou válida a transmissão dos dados às autoridades alemãs com fundamento na cooperação policial europeia. O Tribunal Regional de Dortmund, ao examinar a mesma matéria, chegou a conclusão oposta, por entender que a ausência de suspeita individualizada na autorização francesa não atendia ao requisito de individualização exigido pelo direito processual penal alemão para medidas dessa natureza. Essa divergência entre cortes do mesmo país, aplicando o mesmo conjunto de dados, demonstra que a ausência de parâmetros uniformes de controle judicial no plano internacional produz incerteza jurídica mesmo dentro de um único ordenamento. Submetido ao primeiro eixo do modelo proposto, o caso revela exatamente o tipo de autorização genérica que o critério exige sejam examinadas em sua dimensão material, e não apenas formal: a validade da autorização segundo o direito francês não dispensa o exame de proporcionalidade e individualização exigido pelo Estado destinatário. O segundo eixo é comprometido secundariamente, pois o sigilo mantido pelas autoridades francesas sobre os métodos técnicos de captação compromete a possibilidade de contraditório efetivo por parte dos investigados, que não têm acesso aos elementos necessários para contestar a autenticidade dos dados.

A operação ANOM aprofunda o problema ao nível máximo de comprometimento do modelo. Nesse caso, o Federal Bureau of Investigation criou e operou secretamente a própria

plataforma de comunicação criptografada, distribuída entre organizações criminosas como suposta alternativa segura às plataformas já comprometidas, sem qualquer autorização judicial individualizada prévia que legitimasse a captação massiva de comunicações. A aplicação do modelo ao caso ANOM revela vulnerabilidade em todos os quatro eixos simultaneamente. No primeiro eixo, inexiste autorização judicial individualizada que preceda a captação, pois a própria criação da plataforma pelas autoridades investigativas dispensou qualquer controle jurisdicional prévio sobre a medida.

No segundo eixo, o método de engano estrutural empregado, no qual o investigado comunica-se livremente por acreditar estar protegido por criptografia segura, quando na realidade todas as comunicações são monitoradas desde a origem, é incompatível com as garantias do devido processo legal, na medida em que captura a manifestação da vontade do investigado sob falsa premissa de sigilo.

No terceiro eixo, a ausência de cooperação formal com os países destinatários dos dados compromete a regularidade procedimental da transferência internacional da prova, pois os Estados que receberam informações da operação não participaram de qualquer mecanismo formal de assistência mútua em sua fase de captação.

No quarto eixo, o sigilo mantido sobre os métodos técnicos de operação da plataforma dificulta a verificação da cadeia de custódia digital, pois não é possível auditar de forma independente os procedimentos empregados para garantir a integridade dos dados capturados.

O contraste entre os dois casos é instrutivo para a compreensão da arquitetura cumulativa do modelo. O EncroChat representa hipótese em que a falha se concentra predominantemente em um eixo, com repercussão limitada sobre os demais, ao passo que a ANOM representa o limite máximo de incompatibilidade entre meio de obtenção da prova e garantias processuais, na medida em que nenhuma das condições de admissibilidade examinadas neste artigo se verifica, ainda que parcialmente, em qualquer etapa da operação. Em ambos os casos, contudo, a aplicação do modelo conduz à mesma conclusão normativa: a inadmissibilidade da prova não depende da gravidade dos crimes investigados nem da relevância dos dados obtidos, mas exclusivamente da verificação objetiva dos critérios que compõem cada eixo.

4.3. Aplicação do Modelo ao Caso Sky ECC e Síntese Comparativa

O caso Sky ECC apresenta configuração distinta dos dois anteriores, na medida em que seu ponto de ruptura se concentra predominantemente no terceiro eixo do modelo, com repercussão direta sobre o quarto. A investigação foi conduzida por autoridades belgas e neerlandesas, que obtiveram acesso ao conteúdo das comunicações trafegadas pela plataforma mediante autorização judicial belga-holandesa, e posteriormente compartilharam os dados obtidos com mais de uma dezena de outros países, entre os quais o Brasil, sem que nenhum desses Estados destinatários tivesse participado da autorização judicial original ou obtido autorização própria para a recepção e utilização processual dos dados.

Submetido ao terceiro eixo, o caso evidencia com clareza o fenômeno da habilitação universal sem filtro judicial intermediário: a legalidade da captação segundo o direito belga e neerlandês não se estende automaticamente aos Estados que receberam os dados por via de cooperação informal, pois a regularidade procedimental exigida pelo modelo pressupõe que cada Estado destinatário verifique, por seus próprios mecanismos formais de assistência mútua, a legitimidade do percurso pelo qual a prova chegou ao seu território. A ausência desse filtro compromete diretamente o quarto eixo, pois a documentação da cadeia de custódia digital depende da cooperação formal entre as autoridades envolvidas em cada etapa da transferência. Quando o compartilhamento ocorre por canais informais, sem registro sistemático das condições de transmissão, a verificação da integridade dos dados desde sua captação original até sua apresentação em juízo no Estado destinatário torna-se substancialmente comprometida. O segundo eixo é igualmente afetado, ainda que de forma secundária: os investigados nos países destinatários, entre eles o Brasil, não dispuseram de acesso ao juízo do Estado de origem para contestar a autorização original, nem contaram com autorização judicial própria no Estado destinatário que submetesse a recepção dos dados a controle jurisdicional específico, configurando dupla desvantagem processual quanto ao exercício do contraditório.

A aplicação do modelo aos três casos examinados revela perfis distintos de vulnerabilidade, cuja comparação evidencia a utilidade analítica da estrutura cumulativa proposta. O EncroChat concentra problemas no primeiro eixo, pela ausência de individualização na autorização francesa, com comprometimento secundário do segundo eixo pelo sigilo sobre os métodos técnicos de captação. A ANOM apresenta vulnerabilidades simultâneas nos quatro eixos, configurando o caso de comprometimento mais extenso entre os três exemplos analisados: inexistência de autorização judicial individualizada prévia no

primeiro eixo, método de engano estrutural incompatível com o devido processo legal no segundo, ausência de cooperação formal com os países destinatários no terceiro, e sigilo sobre os métodos técnicos de operação no quarto. O Sky ECC, por sua vez, tem no terceiro eixo seu ponto de ruptura mais evidente, com efeito direto sobre o quarto eixo e comprometimento secundário do segundo.

Essa distribuição diferenciada de vulnerabilidades confirma a arquitetura cumulativa e interdependente do modelo proposto. Nenhum dos três casos apresenta falha isolada e circunscrita a um único eixo sem qualquer repercussão sobre os demais, o que corrobora a tese de que os quatro critérios não constituem lista de requisitos independentes, mas sistema integrado no qual a fragilidade em um ponto tende a se propagar para os demais. A aplicação empírica confirma, assim, a hipótese central da pesquisa: a admissibilidade das interceptações telemáticas obtidas em jurisdições estrangeiras não pode ser aferida por critério único, mas exige verificação cumulativa que examine, de forma articulada, a legalidade da obtenção, a compatibilidade constitucional, a regularidade da cooperação e a integridade da cadeia de custódia digital.

5. RESULTADOS, LIMITES DA JURISPRUDÊNCIA E CAMINHOS DE REFORMA

A discussão dos resultados desta pesquisa organiza-se em dois planos complementares. O primeiro consiste em interpretar o que a confirmação da hipótese central, evidenciada pela aplicação do modelo aos casos examinados na seção anterior, significa para a compreensão do problema de admissibilidade probatória transnacional e para a operacionalização prática do modelo proposto. O segundo consiste em confrontar essa confirmação com o estado atual da jurisprudência brasileira, identificando os limites que a ausência de parâmetros hermenêuticos consolidados impõe à segurança jurídica, e em indicar os caminhos de reforma normativa capazes de superar essas limitações. A subseção 5.1 desenvolve o primeiro plano; a subseção 5.2 desenvolve o segundo, examinando a postura do Superior Tribunal de Justiça e do Supremo Tribunal Federal diante das questões que o modelo proposto contribui para esclarecer.

5.1. Confirmação da Hipótese e Operacionalização do Modelo

A aplicação do modelo aos casos EncroChat, ANOM e Sky ECC, desenvolvida na seção anterior, confirma a hipótese central desta pesquisa: a admissibilidade probatória das

interceptações telemáticas obtidas em jurisdições estrangeiras deve ser submetida a modelo de controle jurisdicional condicionado, estruturado nos quatro eixos cumulativos propostos. A convergência entre o referencial teórico garantista, as exigências constitucionais do art. 5º da Constituição Federal e a verificação empírica realizada conduz à mesma conclusão: sem controle jurisdicional rigoroso articulado em parâmetros verificáveis, a admissibilidade das provas digitais transnacionais torna-se campo de erosão sistemática das garantias fundamentais. A diversidade de perfis de vulnerabilidade identificada nos três casos, ao invés de enfraquecer o modelo, reforça sua utilidade analítica: justamente por não depender de um critério único, o modelo permanece operacional diante de configurações fáticas distintas, capturando tanto falhas concentradas em um único eixo quanto comprometimentos estruturais simultâneos.

O modelo é operacionalizável sem necessidade de reforma legislativa imediata. O juiz criminal pode, com fundamento direto na Constituição Federal, aplicar os quatro eixos mediante exame em fases sequenciais, com decisão fundamentada especificamente em relação a cada critério. Essa característica é relevante para a contribuição prática do artigo, pois desvincula a efetividade do modelo da aprovação de legislação específica, que tende a ser processo moroso e sujeito a incertezas políticas. A ausência de parâmetros hermenêuticos consolidados sobre a admissibilidade da prova digital transnacional constitui uma das vulnerabilidades mais sérias do processo penal brasileiro contemporâneo, pois decisões casuísticas e contraditórias comprometem tanto a segurança jurídica dos investigados quanto a eficácia das investigações (Lopes Jr., 2023, p. 627). É exatamente essa lacuna hermenêutica que o modelo proposto busca preencher, oferecendo ao julgador parâmetros verificáveis que substituem a análise casuística por critério sistemático.

A contribuição científica pode ser sintetizada em três planos. No plano dogmático, oferece modelo de admissibilidade condicionada com quatro eixos verificáveis, aplicável com fundamento direto na Constituição Federal. No plano jurisprudencial, fornece parâmetros hermenêuticos que podem orientar o Supremo Tribunal Federal e o Superior Tribunal de Justiça na consolidação de jurisprudência coerente, respondendo às questões que ainda aguardam resposta definitiva, examinadas na subseção seguinte. No plano legislativo, identifica as reformas necessárias, em especial a adequação às obrigações da Convenção de Budapeste, já promulgada, e a modernização dos Mutual Legal Assistance Treaties com procedimentos eletrônicos e prazos máximos de resposta.

5.2. Limites da Jurisprudência Brasileira e a Necessidade de Reforma Normativa

A jurisprudência brasileira sobre admissibilidade de provas digitais transnacionais encontra-se em estágio embrionário, marcado pela fragmentação e pela ausência de parâmetros hermenêuticos sistematizados. O Superior Tribunal de Justiça tem admitido provas obtidas por cooperação internacional condicionando-as genericamente ao respeito dos tratados e das garantias fundamentais, sem especificar quais garantias são exigíveis nem em que condições se consideram satisfeitas. O Supremo Tribunal Federal afirmou o caráter objetivo da vedação às provas ilícitas, mas não enfrentou em caráter definitivo a questão específica das interceptações estrangeiras compartilhadas sem supervisão judicial nacional.

Para a consolidação de jurisprudência coerente, quatro questões centrais precisam ser respondidas. A primeira diz respeito à aplicabilidade da proibição constitucional de provas ilícitas às provas obtidas por autoridades estrangeiras segundo seu próprio direito, questão diretamente respondida pelo modelo proposto mediante o primeiro e o segundo eixos. A segunda refere-se aos requisitos mínimos de compatibilidade constitucional exigíveis dessas provas, tratada pelo segundo eixo do modelo. A terceira concerne à contaminação da prova pelo ingresso de dados por cooperação policial informal, examinada pelo terceiro eixo. A quarta envolve a natureza da nulidade decorrente da ruptura da cadeia de custódia digital, absoluta ou relativa, tratada pelo quarto eixo. A jurisprudência ainda não convergiu sobre nenhuma dessas quatro questões, e essa indefinição prolongada favorece a erosão progressiva das garantias processuais, fenômeno que não costuma ocorrer por supressão formal de direitos, mas pela acumulação de exceções justificadas por urgência, eficiência ou necessidade securitária, até que as exceções se tornem o regime ordinário (Delmas-Marty, 2003).

No plano normativo, a reforma legislativa adequada deve incorporar os quatro eixos como critérios expressos de admissibilidade, criar exigências específicas de cadeia de custódia para provas transnacionais, regulamentar a verificação judicial das condições de obtenção estrangeira e estabelecer prazos máximos para cooperações formais. A objeção eficientista, segundo a qual o rigor dos critérios tornaria impossível a condenação de criminosos transnacionais, confunde o problema: o modelo não impede a cooperação internacional nem o uso de provas estrangeiras, mas condiciona-as ao cumprimento de requisitos verificáveis que Estados com mecanismos formais modernizados produzirão naturalmente. A objeção comparatística, que aponta sistemas democráticos com padrões menos exigentes, é

factualmente correta, mas o parâmetro de controle não é o menor denominador comum do direito comparado, e sim o padrão constitucional brasileiro, que fez escolha normativa expressa sobre a hierarquia de valores no processo penal.

A reforma dos Mutual Legal Assistance Treaties, em particular, beneficiaria diretamente o terceiro eixo do modelo, ao reduzir o incentivo estrutural ao uso de vias informais de cooperação que hoje comprometem a regularidade procedimental da transferência de provas. A adequação interna às obrigações da Convenção de Budapeste, por sua vez, forneceria parâmetros normativos mais precisos para o primeiro eixo, ao exigir dos signatários requisitos mínimos de controle judicial sobre as medidas investigativas mais intrusivas. Essas reformas, embora desejáveis, não são pressuposto para a aplicação imediata do modelo proposto. Isso ocorre porque os quatro eixos derivam diretamente de normas constitucionais já vigentes, o sigilo das comunicações, o devido processo legal, a vedação às provas ilícitas e a proteção de dados pessoais, e não de dispositivos infraconstitucionais ainda inexistentes. O juiz criminal já dispõe, portanto, do fundamento normativo necessário para aplicar o modelo independentemente de qualquer alteração legislativa, de modo que a reforma normativa sugerida tem função de consolidação e segurança jurídica, não de viabilização do modelo.

6. CONSIDERAÇÕES FINAIS

O problema que organizou esta pesquisa, quais os critérios jurídico-processuais que condicionam a admissibilidade das interceptações telemáticas obtidas em jurisdições estrangeiras no processo penal brasileiro, foi efetivamente enfrentado pela construção de parâmetros normativos que o sistema jurídico brasileiro não oferece de forma consolidada, preenchendo a lacuna dogmática identificada no estado da arte. A hipótese foi confirmada: a admissibilidade deve ser submetida a modelo de controle jurisdicional condicionado, estruturado nos quatro eixos cumulativos propostos. Essa confirmação não derivou de dedução apriorística, mas do percurso metodológico hipotético-dedutivo adotado, que submeteu a hipótese central ao confronto sistemático entre o referencial teórico, o arcabouço normativo e os casos concretos analisados. Os quatro referenciais mobilizados na Seção 2, fundamento axiológico, critério operacional, contextualização política e especificação tecnológica, convergiram para sustentar a mesma conclusão normativa, demonstrando a coerência interna do modelo construído.

Os três objetivos específicos foram integralmente alcançados. Os referenciais teóricos e normativos que balizam o debate foram examinados com a identificação das três correntes doutrinárias internacionais, das lacunas da literatura brasileira e da divergência crítica sobre as operações de infiltração tecnológica em servidores estrangeiros. Os quatro eixos do modelo de admissibilidade condicionada foram construídos com densidade analítica suficiente para uso prático pelo operador do direito e, em etapa subsequente e distinta, aplicados aos casos concretos do EncroChat, da ANOM e do Sky ECC, cuja comparação evidenciou perfis diferenciados de vulnerabilidade e confirmou a arquitetura cumulativa do modelo. Os resultados foram discutidos criticamente, confrontando o modelo com a jurisprudência existente, identificando as reformas necessárias, em especial a adequação interna às obrigações da Convenção de Budapeste, promulgada pelo Decreto n. 11.491/2023, e a modernização dos Mutual Legal Assistance Treaties.

A posição do autor sobre o problema central é a seguinte: quando o conflito entre eficiência investigativa e garantismo penal é irredutível, o modelo constitucional brasileiro determina que o garantismo prevaleça, não porque a eficiência seja valor menor, mas porque a legitimidade do poder punitivo democrático depende de que o Estado se submeta às regras que ele mesmo criou para limitar sua própria ação. Um processo penal que admite provas ilegalmente obtidas, no Brasil ou no exterior, sob o argumento da necessidade investigativa, não é processo penal democrático: é processo penal de exceção com aparência de legalidade. A Constituição de 1988, ao consagrar a inadmissibilidade das provas ilícitas como garantia fundamental, fez escolha deliberada sobre a identidade do Estado brasileiro, escolha que não se enfraquece porque a prova vem do exterior, porque o crime é grave ou porque a condenação seria conveniente. Honrá-la também no domínio das provas digitais transnacionais é dever que recai sobre o legislador, o juiz e o doutrinador.

REFERÊNCIAS

AMBOS, Kai. Treatise on International Criminal Law. Oxford: Oxford University Press, 2021.

BADARÓ, Gustavo Henrique. Processo Penal. 10. ed. São Paulo: Thomson Reuters Brasil, 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988.

BRASIL. Decreto n. 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético. Brasília, DF: Presidência da República, 2023.

BRASIL. Lei n. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Brasília, DF: Presidência da República, 1996.

BRASIL. Lei n. 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019.

CONSELHO DA EUROPA. Convenção sobre o Cibercrime. Budapeste, 23 de novembro de 2001. (CETS n. 185).

CRESWELL, John W.; CRESWELL, J. David. Projeto de pesquisa: métodos qualitativo, quantitativo e misto. 5. ed. Porto Alegre: Penso, 2021.

DELMAS-MARTY, Mireille. Três Desafios para um Direito Mundial. Tradução de Fauzi Hassan Choukr. Rio de Janeiro: Lumen Juris, 2003.

ESTADOS UNIDOS. Clarifying Lawful Overseas Use of Data Act. Public Law 115-141, Div. V, 132 Stat. 1213-1225, 23 mar. 2018.

FERRAJOLI, Luigi. Direito e Razão: Teoria do Garantismo Penal. Tradução de Ana Paula Zomer et al. São Paulo: Revista dos Tribunais, 2002.

FONSECA, João José Saraiva da. Metodologia da pesquisa científica. Fortaleza: UEC, 2002.

GIL, Antonio Carlos. Como elaborar projetos de pesquisa. 6. ed. São Paulo: Atlas, 2017.

KERR, Orin S. Computer Crime Law. 5. ed. St. Paul: West Academic Publishing, 2022.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 9. ed. São Paulo: Atlas, 2021.

LIMA, Renato Brasileiro de. Legislação Criminal Especial Comentada. 10. ed. Salvador: JusPodivm, 2022.

LOPES JR., Aury. Direito Processual Penal. 20. ed. São Paulo: SaraivaJur, 2023.

PINHEIRO, Patrícia Peck. Direito Digital. 7. ed. São Paulo: SaraivaJur, 2021.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016: relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, L 119, 4 maio 2016. p. 1-88.