

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

Admissibility of foreign telematic interceptions in brazilian criminal proceedings: penal garantism and conditional judicial oversight

Arlen Jose Silva de Souza
arlen0402@hotmail.com

Bruna Livia Timbó de Araújo Balthazar
brunaliviatimbo@gmail.com

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, mediante pesquisa bibliográfica e análise normativa comparada, 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 hipótese foi confirmada: a eficiência investigativa não autoriza a relativização das garantias processuais fundamentais.

Palavras-chave: interceptação telemática; admissibilidade probatória; garantismo penal; cooperação jurídica internacional; cadeia de custódia digital.

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 carried out in a foreign jurisdiction be admitted as valid evidence in domestic criminal proceedings, without violating due process of law and the fundamental rights constitutionally guaranteed to the person under investigation? A hypothetical-deductive method with a qualitative approach was adopted, through bibliographical research and comparative

normative analysis, examining the contributions of Aury Lopes Jr., Gustavo Badaró, Kai Ambos, Luigi Ferrajoli, Mireille Delmas-Marty and Orin Kerr, in addition to the normative framework of the Budapest Convention on Cybercrime, promulgated in Brazil by Decree No. 11,491/2023. The results reveal that the admissibility of such evidence requires a model of conditioned judicial control, structured around four cumulative axes: legality of collection in the state of origin, material compatibility with the fundamental rights of the receiving state, regularity of international legal cooperation, and preservation of the digital chain of custody. The hypothesis was confirmed: investigative efficiency does not authorize the relativization of fundamental procedural guarantees.

Keywords: telematic interception; evidentiary admissibility; penal garantism; international legal cooperation; digital chain of custody.

1 INTRODUÇÃO

A transnacionalização das comunicações digitais transformou, de modo estrutural e irreversível, o campo da prova penal. Plataformas criptografadas de uso criminal, serviços de armazenamento em nuvem e redes privadas virtuais fragmentaram o dado digital por continentes inteiros, tornando a localização física da prova uma categoria jurídica de contornos progressivamente imprecisos. O poder punitivo estatal defronta-se, assim, com uma contradição que os instrumentos clássicos do processo penal não foram concebidos para resolver: a prova mais relevante para a persecução criminal existe além das fronteiras do Estado que a pretende utilizar, capturada por autoridades estrangeiras segundo regras que podem diferir substancialmente das garantias que o ordenamento constitucional interno assegura ao investigado.

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 chamados a pronunciar-se sobre questões análogas sem que exista jurisprudência consolidada ou legislação específica que fixe os critérios aplicáveis. Essa lacuna não é acidental: ela é estrutural, pois o direito processual penal brasileiro foi construído sobre a premissa da territorialidade da jurisdição, que a arquitetura distribuída das comunicações digitais contemporâneas desfaz de forma sistemática.

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. A ausência de qualquer desses requisitos conduz, por si só, à inadmissibilidade da prova, independentemente da relevância investigativa dos dados obtidos.

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, cada um vinculado a uma das seções do trabalho: examinar os referenciais teóricos e normativos que balizam o debate sobre prova digital transnacional; analisar os quatro eixos do modelo de admissibilidade condicionada e sua aplicação aos casos concretos; e discutir os resultados à luz da jurisprudência brasileira e das perspectivas de reforma normativa. Adota-se o método hipotético-dedutivo com abordagem qualitativa e natureza exploratório-explicativa, mediante pesquisa bibliográfica em obras doutrinárias nacionais e estrangeiras, análise normativa comparada e exame de decisões judiciais de cortes brasileiras e europeias. As fontes primárias compreendem a Constituição Federal, 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.

2 REFERENCIAIS TEÓRICOS E NORMATIVOS DA PROVA DIGITAL TRANSNACIONAL

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, mas fragmentada. Há convergência em torno do diagnóstico: todos os autores relevantes reconhecem que os modelos clássicos de cooperação são insuficientes para o ambiente digital. Sobre as soluções, a divergência é profunda e reflete posições filosóficas irreduzíveis sobre a hierarquia entre eficiência punitiva e proteção dos direitos fundamentais. A corrente efficientista, de predominância norte-americana, defende vias alternativas aos mecanismos formais de cooperação. A corrente garantista, de influência continental europeia, subordina a admissibilidade a controles judiciais rigorosos em ambos os Estados envolvidos. A corrente harmonizadora busca parâmetros procedimentais mínimos para conciliar eficiência e garantismo. Na literatura brasileira, a lacuna é precisamente a inexistência de modelo dogmático integrado que articule os critérios de admissibilidade aplicáveis às provas digitais de origem estrangeira, o que justifica a construção proposta nesta pesquisa.

O referencial teórico estruturante é o garantismo penal de Luigi Ferrajoli. Para Ferrajoli, 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). 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 do processo penal transnacional, critério que Kai Ambos oferece com precisão 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).

Nulla probatio sine lege. 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. A prova ilegal não é apenas prova inadmissível; é prova epistemicamente contaminada. (Ferrajoli, 2002, p. 498).

AperspectivadeMireilleDelmas-Martyacrescentaoenquadramentomacroestrutural indispensável para compreender o problema em sua dimensão política: 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 silenciosa de exceções justificadas por urgência investigativa (Delmas-Marty, 2003). Orin Kerr complementa ao especificar as características tecnológicas que tornam o ambiente digital qualitativamente distinto: 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, o que implica que a admissibilidade não pode ser resolvida pela simples identificação de uma autorização válida em algum ponto do globo (Kerr, 2022).

A admissibilidade da prova obtida no exterior exige análise em dois níveis: em primeiro lugar, a conformidade com o direito do Estado que realizou a coleta; em segundo lugar, a compatibilidade material com os padrões de direitos fundamentais do Estado destinatário. Qualquer um dos dois níveis pode, isoladamente, tornar a prova inadmissível. (Ambos, 2021, p. 217, tradução nossa)

No plano normativo, 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, ressaltando 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. A violação de qualquer das duas dimensões contamina objetivamente a prova (Lopes Jr., 2023).

A inviolabilidade das comunicações telefônicas e telemáticas constitui garantia de primeira grandeza no Estado Democrático de Direito, exigindo reserva jurisdicional absoluta e fundamentação concreta da medida. O sigilo é a regra; a interceptação, a exceção. (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 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 (Lei n. 13.709/2018). Patrícia Peck Pinheiro sustenta que a proteção de dados pessoais integra o núcleo essencial da privacidade e não pode ser sacrificada por conveniências investigativas internacionais (Pinheiro, 2021). O desvio de finalidade probatória, ou seja, a utilização de dados interceptados no exterior para fins distintos dos que justificaram a captação, viola o princípio da finalidade e torna a prova inadmissível, ainda que sua obtenção original tenha sido inteiramente legal. Definidos os referenciais teóricos e constitucionais, cabe examinar o arcabouço normativo internacional que disciplina a obtenção transnacional de provas digitais.

2.2 O regime internacional de obtenção de provas digitais: Budapeste, MLATs e a questão da soberania

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). A adesão brasileira representa avanço normativo significativo; o desafio imediato é a adequação interna às obrigações convencionais assumidas, processo que o legislador ainda não iniciou.

O mecanismo mais relevante para o problema desta pesquisa é a preservação acelerada transfronteiriça do art. 29: 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 apresenta, contudo, limitações estruturais: 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 abre espaço ao fenômeno do *forum shopping* probatório: a seleção estratégica do Estado com menores exigências procedimentais para a obtenção de provas que seriam vedadas no Estado destinatário. Gustavo Badaró denomina esse fenômeno como instrumento de esvaziamento das garantias: quando as autoridades podem escolher livremente de qual jurisdição receberão os dados, o incentivo estrutural é sempre escolher a mais permissiva (Badaró, 2022).

O MLAT representa o equilíbrio possível entre soberania estatal e cooperação penal internacional. Sua lentidão não justifica o abandono das garantias que ele veicula; justifica, antes, a modernização de seus procedimentos. (Badaró, 2022, p. 891).

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. Sua lentidão operacional é o principal argumento para o uso de vias informais. Contudo, como observa Renato Brasileiro de Lima, 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 nesses casos (Lima, 2022). A solução adequada para a lentidão dos Mutual Legal Assistance Treaties é sua modernização com procedimentos eletrônicos e prazos máximos de resposta, não o abandono da formalidade que veiculam.

Em sentido oposto ao modelo dos Mutual Legal Assistance Treaties posiciona-se o Clarifying Lawful Overseas Use of Data Act norte-americano de 2018, que permite às autoridades dos EUA 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 alto 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 EUA sem notificação ao Brasil. Quando esses dados chegam ao processo penal brasileiro por cooperação policial informal, o terceiro eixo do modelo proposto é diretamente comprometido, pois a prova carece de percurso formal verificável.

O panorama normativo internacional revela, em síntese, a tensão estrutural entre o modelo formal, que prioriza soberania e garantias ao custo da celeridade, e o modelo informal, que prioriza eficiência ao custo da previsibilidade jurídica e da proteção dos direitos fundamentais. Essa tensão não se resolve pela escolha de um modelo em detrimento do outro, mas pela construção de critérios dogmáticos de admissibilidade que imponham ao modelo informal o mesmo grau de controle jurisdicional que o modelo formal assegura por design. Os quatro eixos examinados na seção seguinte constituem exatamente essa construção.

3 OS QUATRO EIXOS DE CONTROLE JURISDICIONAL: CRITÉRIOS E APLICAÇÃO

3.1 Legalidade da obtenção e compatibilidade constitucional: Os dois primeiros 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: uma decisão estrangeira que autoriza a captação em massa de todos os usuários de uma plataforma sem individualização de suspeitos pode ser formalmente válida segundo o direito de origem e, ainda assim, carecer da fundamentação concreta que o modelo exige. 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: o garantismo de Ferrajoli exige que a legalidade da prova seja demonstrável e contestável, não apenas afirmada pelas autoridades que a produziram (Ferrajoli, 2002).

A proporcionalidade constitui requisito material autônomo 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. O caso EncroChat exemplifica as tensões do primeiro eixo: a autorização francesa para captação em massa sem individualização foi aceita pelo Tribunal Regional de Berlim, mas rejeitada pelo de Dortmund, que entendeu não atender ao requisito de suspeita individualizada do direito alemão. A operação ANOM aprofunda o problema ao nível máximo: o FBI criou e operou secretamente a própria plataforma

como instrumento de interceptação, sem autorização judicial individualizada prévia, configurando engano estrutural sem precedentes no processo penal democrático. Quando o exame revela autorização genérica, desproporcional ou inexistente, a prova é inadmissível sem necessidade de exame dos demais eixos.

A vedação constitucional às provas ilícitas não distingue, em seu suporte normativo, entre provas produzidas no Brasil e provas produzidas no exterior. A ilicitude é condição objetiva da prova, não consequência territorial de sua obtenção. (Badaró, 2022, p. 578)

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 seria converter a cooperação internacional em mecanismo de contorno das garantias constitucionais, o 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), *due process of law* (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 a contaminação decorre da natureza do vício, não da intenção das autoridades que o praticaram.

O processo penal não existe para facilitar a condenação de culpados; existe para assegurar que somente culpados sejam condenados, e somente mediante provas validamente obtidas. Quando a prova é ilegal, o processo perde seu fundamento de legitimidade, qualquer que seja a culpabilidade do acusado. (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: o investigado não pode contestar a autenticidade de dados quando não sabe como foram capturados. A operação Sky ECC configura dupla desvantagem processual: os dados foram distribuídos a mais de uma dezena de países sem que nenhum deles participasse da autorização judicial belga-holandesa, deixando os investigados sem acesso ao juízo do Estado de origem e sem autorização judicial no Estado destinatário. O desvio de finalidade probatória, que consiste na utilização de dados interceptados para fins distintos dos que justificaram a captação, 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. Uma interceptação realizada com autorização judicial formal, mas sem prazo determinado, sem individualização de suspeitos ou sem qualquer possibilidade de contestação posterior pelo investigado, pode ser formalmente conforme ao direito estrangeiro e, ainda assim, materialmente incompatível com os valores constitucionais brasileiros. Essa distinção entre conformidade formal e compatibilidade material constitui o núcleo operacional do critério da dupla licitude de Ambos aplicado ao contexto constitucional brasileiro.

3.2 Regularidade da cooperação e cadeia de custódia digital: Os dois eixos procedimentais

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; 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. 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 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. A prova que ingressa no processo deve ter percurso formal verificável, não apenas resultado investigativo relevante. (Ambos, 2021, p. 284).

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; 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 caso Sky ECC exemplifica os efeitos do compartilhamento unilateral: os dados foram distribuídos a mais de uma dezena de países sem que nenhum participasse da autorização judicial belga-holandesa nem obtivesse autorização própria, convertendo a legalidade belga em habilitação universal sem filtro judicial intermediário. O percurso da prova desde sua captação no Estado de origem até sua apresentação no processo penal brasileiro deve ser integralmente documentado, verificando 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: 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 é 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 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.

A cadeia de custódia digital não é mera formalidade burocrática; é 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).

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; Badaró sustenta que 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.

4 RESULTADOS, LIMITES DA JURISPRUDÊNCIA E CAMINHOS DE REFORMA

4.1 Confirmação da hipótese e operacionalização do modelo

A pesquisa confirma a hipótese central: 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 análise crítica dos casos concretos 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. 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 quatro fases sequenciais, com decisão fundamentada especificamente em relação a cada eixo.

A ausência de parâmetros hermenêuticos consolidados sobre a admissibilidade da prova digital transnacional é uma das vulnerabilidades mais sérias do processo penal brasileiro contemporâneo. Decisões casuísticas e contraditórias comprometem tanto a segurança jurídica dos investigados quanto a eficácia das investigações. (Lopes Jr., 2023, p. 627)

A aplicação do modelo aos três casos concretos examinados revela perfis distintos de vulnerabilidade. O EncroChat concentra problemas no primeiro eixo, pela ausência de individualização na autorização francesa, e no quarto eixo, pelo sigilo sobre os métodos técnicos de captação; o segundo eixo é comprometido secundariamente pela impossibilidade de contraditório efetivo. A ANOM apresenta vulnerabilidades em todos os quatro eixos: inexistência de autorização judicial individualizada prévia no primeiro; método de engano estrutural incompatível com o *due process* no segundo; ausência de cooperação formal com os países destinatários no terceiro; e sigilo parcial sobre os métodos técnicos no quarto. O Sky ECC tem o terceiro eixo como ponto de ruptura mais evidente, pelo compartilhamento unilateral sem autorização judicial nos países destinatários, com efeito direto sobre o quarto eixo, pois a ausência de cooperação formal impede a documentação adequada do percurso dos dados. Os três objetivos específicos foram integralmente alcançados: os referenciais teóricos e normativos foram examinados; os quatro eixos foram analisados com aplicação aos casos concretos; e os resultados foram discutidos à luz da jurisprudência e das perspectivas de reforma.

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 quatro questões que ainda aguardam resposta definitiva: aplicabilidade da proibição de provas ilícitas às provas de autoridades estrangeiras; requisitos mínimos de compatibilidade constitucional; contaminação pela cooperação policial informal; e nulidade absoluta pela ruptura da cadeia de custódia digital. 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.

4.2 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: se a proibição constitucional de provas ilícitas se aplica às provas obtidas por autoridades estrangeiras segundo seu próprio direito; quais os requisitos mínimos de compatibilidade constitucional; se o ingresso de dados por cooperação policial informal contamina a prova para fins de admissibilidade; e se a ruptura da cadeia de custódia digital gera nulidade absoluta ou relativa.

A erosão das garantias processuais penais não ocorre, em geral, por supressão formal de direitos. Ocorre pela acumulação de exceções justificadas por urgência, eficiência ou necessidade securitária, até que as exceções se tornem o regime ordinário. (Delmas-Marty, 2003, p. 112).

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 efficientista, de que o rigor dos critérios tornará impossível a condenação de criminosos transnacionais, confunde o problema: o modelo não impede a cooperação internacional nem o uso de provas estrangeiras; 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: é o padrão constitucional brasileiro, que fez escolha normativa expressa sobre a hierarquia de valores no processo penal.

A dimensão transnacional dos direitos fundamentais fornece o argumento mais profundo em favor do modelo: ao utilizar o produto de uma violação praticada no exterior, o Estado brasileiro torna-se cúmplice funcional dessa violação (Ferrajoli, 2002), e a vedação constitucional às provas ilícitas é, nessa perspectiva, não apenas regra de exclusão processual, mas expressão do dever estatal de não instrumentalizar violações de direitos, sejam domésticas ou estrangeiras. A construção de parâmetros hermenêuticos coerentes para a admissibilidade das interceptações telemáticas transnacionais é, em última análise, uma questão de identidade constitucional: o tipo de processo penal que o Brasil quer ter revela-se nas escolhas que o sistema jurídico faz nos casos em que a prova mais relevante foi obtida por meios que comprometem os direitos do investigado.

5 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 confronto entre o referencial teórico e os dados normativos, doutrinários e jurisprudenciais analisados: o garantismo de Ferrajoli forneceu os fundamentos axiológicos; a dupla licitude de Ambos operacionalizou-os em parâmetros verificáveis; a desterritorialização de Delmas-Marty contextualizou os riscos da cooperação informal; e a análise de Kerr especificou as características tecnológicas que tornam os instrumentos clássicos estruturalmente insuficientes.

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 analisados com densidade analítica suficiente para uso prático pelo operador do direito, incluindo a aplicação sobre os casos concretos do EncroChat, da ANOM e do Sky ECC. 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 irreduzível, 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. **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal, para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais do cidadão e para fixar a competência privativa da União para legislar e organizar a proteção e o tratamento de dados pessoais. Brasília, DF: Congresso Nacional, 2022.
- 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. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.
- 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 nov. 2001. (CETS n. 185).
- DELMAS-MARTY, Mireille. **Três Desafios para um Direito Mundial**. Tradução de Fauzi Hassan Choukr. Rio de Janeiro: Lumen Juris, 2003.
- FERRAJOLI, Luigi. **Direito e Razão: Teoria do Garantismo Penal**. Tradução de Ana Paula Zomer et al. São Paulo: Revista dos Tribunais, 2002.
- KERR, Orin S. **Computer Crime Law**. 5. ed. St. Paul: West Academic Publishing, 2022.
- 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.