ISSN 2238-9121

7º CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE
EDIÇÃO 2024
MÍDIAS E DIREITOS DA SOCIEDADE EM REDE

Dias 30 e 31 de outubro de 2024 - Santa Maria / RS UFSM - Universidade Federal de Santa Maria

REPORT DO NCMEC: DA ADMISSIBILIDADE COMO PROVA PELO ORDENAMENTO JURÍDICO BRASILEIRO

REPORT FROM NCMEC: ADMISSIBILITY AS EVIDENCE UNDER BRAZILIAN LAW

Eduardo Pacheco de Mello Lima[1]
Anderson Rodrigo Andrade de Lima[2]

RESUMO

O presente estudo tem como norte as provas utilizadas em investigações envolvendo crimes contra a dignidade sexual de crianças e adolescentes praticados pela rede mundial de computadores. Como recorte de pesquisa, busca-se entender a admissibilidade (ou não) das provas produzidas pelo *National Center for Missing & Exploited Children* (NCMEC) quando compartilhadas, via cooperação jurídica internacional, às autoridades brasileiras sem a correspondente autorização da autoridade judiciária competente no Brasil. Observou-se a dificuldade de obtenção de provas virtuais, de maneira célere e eficiente, que façam cessar cibercrimes que afligem crianças e adolescentes. O desafio das polícias judiciárias ainda é maior, uma vez que os crimes cibernéticos transcendem fronteiras, demandando esforço hercúleo na aquisição, manipulação e manutenção dos vestígios digitais. Para tanto, realizou-se uma análise bibliográfica, legal e jurisprudencial acerca do tema. No mais, o método de abordagem foi o hipotético-dedutivo. Dessa forma, entende-se que as provas produzidas tendem a ser admitidas no Brasil pelo STJ. Ainda, faz-se necessário produção legislativa, determinando o envio obrigatório de notícias-crime, sem necessidade de autorização judicial prévia, pelos provedores de aplicação atuantes, no Brasil, quando tenham contato com material de abuso sexual infantojuvenil.

Palavras-chave: licitude; NCMEC; prova; relatório.

ABSTRACT

This study is guided by evidence used in investigations involving crimes against the sexual dignity of children and adolescents committed through the global computer network. The research aims to understand the admissibility (or not) of evidence produced by the National Center for Missing & Exploited Children (NCMEC) when shared, through international legal cooperation, with Brazilian authorities without the corresponding authorization from the competent judicial authority in Brazil. It was observed that obtaining virtual evidence quickly and efficiently to halt cybercrimes affecting children and adolescents is challenging. The difficulties faced by judicial police are even greater, given that cybercrimes transcend borders, requiring tremendous effort in the acquisition, handling, and preservation of digital traces. To address these challenges, a bibliographic, law and case-law analysis on the subject was conducted. Furthermore, the research approach followed the hypothetical-deductive method. Thus, it is understood that the evidence produced tends to be admitted in Brazil by the Superior Court of Justice (STJ). In addition, legislative measures are needed to mandate the obligatory reporting of criminal activities by application providers operating

[1] Eduardo Pacheco de Mello Lima, Delegado de Polícia Federal, realizando especialização em criminalidade cibernética pela Academia Nacional da Polícia Federal, (eduardo_lima_19@hotmail.com).
[2] Anderson Rodrigo Andrade de Lima, Delegado de Polícia Federal, doutorando em ciências sociais pela UFSM, (anderson-ral@hotmail.com).

in Brazil, without prior judicial authorization, whenever they encounter material related to child sexual abuse.

Keywords: legality; NCMEC; evidence; report.

INTRODUÇÃO

Com o avanço da tecnologia, percebe-se que a internet tem sido utilizada como palco de exploração sexual infantojuvenil. Erroneamente visualizada como instrumento que permite absoluto anonimato, o espaço virtual é cenário de produção, divulgação e armazenamento de conteúdo contendo abuso sexual de crianças e adolescentes. Assim, surge a latente necessidade dos órgãos de persecução penal de obtenção célere, análise qualificada e tratamento que garanta a cadeia de custódia dos vestígios digitais produzidos nesse hodierno local de crime.

Ao longo de investigações policiais, constata-se a dificuldade em obtenção de provas por meio de cooperação jurídica internacional, uma vez que é um procedimento lento, complexo e burocrático. Nos crimes cibernéticos, essa árdua tarefa é, particularmente, mais intensa, pois há diversos subterfúgios utilizados para ocultar a autoria delitiva, bem como a sistemática criminosa facilmente transcende fronteiras físicas.

Diante disso, ao longo dessa pesquisa, será feita uma análise embrionária da admissibilidade (ou não) das provas produzidas pelo *National Center for Missing & Exploited Children* (NCMEC), quando compartilhadas às autoridades brasileiras sem a correspondente autorização judicial, no Brasil. Por ter sido vivenciada em diversas investigações, a problemática despertou profundo interesse acadêmico e jurídico por este subscritor, uma vez que se visualiza a possibilidade de nulidades pelo Poder Judiciário das provas internalizadas no processo criminal.

Ao se observar esse contexto, utilizou-se de um estudo bibliográfico, legal e jurisprudencial, especialmente, do julgado do Superior Tribunal de Justiça (STJ), 5. Turma, AREsp nº 701833, para enfrentamento do problema delineado. Nesse panorama, o método de abordagem aplicado foi o hipotético-dedutivo.

Inicialmente, examinou-se a legislação dos Estados Unidos da América (EUA) que regulamenta a exigência de comunicação por parte dos provedores de aplicação acerca de material contendo indicativos de exploração sexual infantojuvenil. Com base nesse norte, chegou-se aos relatórios produzidos pelo NCMEC.

Posteriormente, analisou-se a legislação brasileira que regulamenta o afastamento de sigilo telemático, perpassando-se pelos requisitos necessários para obtenção dos dados privados. Por outro lado, cotejou-se o direito a privacidade com o dever do Estado na garantia da segurança pública.

Por fim, buscou-se compreender a decisão proferida pelo STJ que se debruçou em situação similar, mas não idêntica. No caso aludido, conferiu-se viabilidade de utilização de dados bancários produzidos no exterior sem autorização judicial (porém, com observância do ordenamento alienígena), mas internalizadas, no Brasil, como provas válidas. Destaca-se que o crime apurado era evasão de divisas (art. 22, parágrafo único, da Lei 7.492/82).

Assim, concluiu-se pela tendência de admissão pelo STJ das provas produzidas pelo NCMEC e utilizadas no Brasil. No mais, compreendeu-se a necessidade de produção legislativa, determinando aos provedores de aplicação que comuniquem, independente de ordem judicial, às autoridades investigativas brasileiras os crimes virtuais praticados em detrimento da dignidade sexual de crianças e adolescentes, nos moldes da legislação americana.

1 DOS RELATÓRIOS PRODUZIDOS PELO NCMEC

Nas primeiras linhas, cabe sublinhar que a Polícia Federal vem intensificando e modernizando as investigações com o escopo de enfrentar a divulgação de material contendo violência sexual infantil, na internet, por meio de investigações proativas capazes de apurar, em tempo real, os usuários que compartilham aludidos arquivos ilícitos pela rede mundial de computadores. A competência da Justiça Federal e, por conseguinte, a atribuição investigativa da Polícia Federal, nesses crimes, já foi delimitada pelo Tribunal Pleno do Supremo Tribunal Federal (STF) (RE 628624).

Sendo assim, policiais federais vêm recebendo treinamento, em especial, em parceria com a Polícia Federal Americana (*Federal Bureau of Investigation* - FBI) para a utilização de técnicas destinadas a desenvolver investigações proativas em redes *Peer to Peer* (P2P). Identicamente, há mecanismos de atuação para identificação de grupos de mensageria, nos quais ocorre trocas e disponibilização de material contendo pornografia infantil.

Noutro giro, existe uma organização não governamental denominada NCMEC, sem fins lucrativos, fundada em 1984, que recebeu apoio do governo norte-americano para

estabelecer um mecanismo centralizado de recebimento de "denúncias" sobre crimes relacionados a abuso sexual infantil e desaparecimento de crianças. No site oficial, é descrita a missão do Centro Nacional para Crianças Desaparecidas e Exploradas, tendo como lema "toda criança merece uma infância segura":

> O Centro Nacional para Crianças Desaparecidas e Exploradas é uma organização privada sem fins lucrativos, registrada como 501(c)(3), cuja missão é ajudar a encontrar crianças desaparecidas, reduzir a exploração sexual infantil e prevenir a vitimização de crianças. O NCMEC trabalha com famílias, vítimas, o setor privado, autoridades policiais e o público para ajudar na prevenção de sequestros infantis, na recuperação de crianças desaparecidas e na oferta de serviços para combater e prevenir a exploração sexual infantil[3].

Nos Estados Unidos, os prestadores de serviços (de conexão/internet) são obrigados, nos termos do 18 U.S. *Code* § 2258A - *Reporting requirements of providers*[4], a relatarem suspeita de exploração sexual infantil que trafeguem em suas redes ao NCMEC. Essa obrigação é imprescindível ao combate de condutas criminosas, estando prevista expressamente aos provedores:

> (a) Dever de Denunciar. -
> (1) Em geral. -
> (A) Dever. - Com o objetivo de reduzir a proliferação da exploração sexual infantil online e prevenir a exploração sexual infantil na internet, um provedor:
> (i) deve, assim que possível e de forma razoável, após obter conhecimento real de quaisquer fatos ou circunstâncias descritas no parágrafo (2)(A), tomar as ações descritas na alínea (B); e
> (ii) pode, após obter conhecimento real de quaisquer fatos ou circunstâncias descritas no parágrafo (2)(B), tomar as ações descritas na alínea (B).
> (B) Ações descritas
> As ações descritas nesta alínea são:
> (i) fornecer à CyberTipline do NCMEC (ou qualquer sucessora da CyberTipline operada pelo NCMEC) o endereço postal, número de telefone,

[3] CHILDREN. National Center for Missing and Exploited. **About Us.** 2024. Disponível em: https://www.missingkids.org/footer/about. Acesso em: 15 out. 2024.
The National Center for Missing & Exploited Children is a private, non-profit 501(c)(3) corporation whose mission is to help find missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC works with families, victims, private industry, law enforcement, and the public to assist with preventing child abductions, recovering missing children, and providing services to deter and combat child sexual exploitation.
[4] EUA. **Reporting requirements of providers**. 18 USC 2258ª. Disponível em: https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2258A&num=0&edition=prelim. Acesso em: 29 ago. 2024.

> número de fax, endereço de e-mail e ponto de contato individual do provedor; e
> (ii) fazer um relatório desses fatos ou circunstâncias à CyberTipline, ou a qualquer sucessora da CyberTipline operada pelo NCMEC.[5]

Em destaque, é dever dos provedores reportarem ao NCMEC diversas informações de natureza privada, por exemplo, localização geográfica, imagens de aparente pornografia infantil e qualquer outra informação de identificação pessoal, inclusive informações fornecidas voluntariamente pelo próprio usuário. Nesse sentido, transcreve-se o texto legal:

> Com o objetivo de prevenir a futura vitimização sexual de crianças e, na medida em que as informações estejam sob custódia ou controle de um provedor, os fatos e circunstâncias incluídos em cada relatório, conforme a subseção (a)(1), poderão, a critério exclusivo do provedor, incluir as seguintes informações:
> (1) Informações sobre o indivíduo envolvido: informações relacionadas à identidade de qualquer indivíduo que pareça ter violado ou planeja violar uma lei federal descrita na subseção (a)(2). Essas informações podem incluir, na medida do razoavelmente possível: endereço de e-mail, Endereço de Protocolo de Internet (IP), Localizador Uniforme de Recursos (URL);
> (2) Informações de pagamento (excluindo informações pessoalmente identificáveis) ou qualquer outra informação identificadora, incluindo informações auto-relatadas;
> (3) Referência histórica: informações sobre quando e como um cliente ou assinante de um provedor carregou, transmitiu ou recebeu conteúdo relacionado ao relatório, ou quando e como esse conteúdo foi reportado ou descoberto pelo provedor. Isso pode incluir: carimbo de data e hora, fuso horário;
> (4) Informações de localização geográfica: informações sobre a localização geográfica do indivíduo envolvido ou do site, que podem incluir endereço IP ou endereço verificado, ou, caso não esteja razoavelmente disponível, pelo menos uma forma de informação geográfica identificadora, como o código de área ou código postal fornecido pelo cliente ou assinante, ou armazenado/obtido pelo provedor;

[5] *Ibid.*
(a) Duty To Report.-
(1) In general.-
(A) Duty.-In order to reduce the proliferation of online child sexual exploitation and to prevent the online sexual exploitation of children, a provider-
(i) shall, as soon as reasonably possible after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(A), take the actions described in subparagraph (B); and
(ii) may, after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(B), take the actions described in subparagraph (B).
(B) Actions described.-The actions described in this subparagraph are-
(i) providing to the CyberTipline of NCMEC, or any successor to the CyberTipline operated by NCMEC, the mailing address, telephone number, facsimile number, electronic mailing address of, and individual point of contact for, such provider; and
(ii) making a report of such facts or circumstances to the CyberTipline, or any successor to the CyberTipline operated by NCMEC.

ISSN 2238-9121

> (5) Representações visuais de aparente pornografia infantil: qualquer representação visual de aparente pornografia infantil ou outro conteúdo relacionado ao incidente sobre o qual o relatório se refere;
> (6) Comunicação completa: a comunicação completa contendo qualquer representação visual de aparente pornografia infantil ou outro conteúdo, incluindo:
> (A) Quaisquer dados ou informações sobre a transmissão da comunicação; e
> (B) Quaisquer representações visuais, dados ou outros arquivos digitais contidos na comunicação ou anexados a ela[6].

Poder-se-ia indagar se as aludidas informações estão albergadas por cláusula de reserva de jurisdição. No entanto, no mesmo dispositivo legal alienígena, existe previsão expressa que permite a difusão dos "*reports*" para órgãos de persecução penal, inclusive, de outros países, utilizando-se, por exemplo, da *International Criminal Police Organization* (Interpol):

> (c) Encaminhamento de Relatório para aplicação da lei. – De acordo com seu papel de central de informações como uma organização privada e sem fins lucrativos, e ao término de sua análise em prol de sua missão social, o NCMEC (Centro Nacional para Crianças Desaparecidas e Exploradas) deverá disponibilizar cada relatório feito nos termos do parágrafo (a)(1) para uma ou mais das seguintes agências de aplicação da lei:
> (1) Qualquer agência federal de aplicação da lei envolvida na investigação de exploração sexual infantil, sequestro ou crimes de aliciamento;

---

[6] *Ibid*.
(b) Contents of Report.-In an effort to prevent the future sexual victimization of children, and to the extent the information is within the custody or control of a provider, the facts and circumstances included in each report under subsection (a)(1) may, at the sole discretion of the provider, include the following information:
(1) Information about the involved individual.-Information relating to the identity of any individual who appears to have violated or plans to violate a Federal law described in subsection (a)(2), which may, to the extent reasonably practicable, include the electronic mail address, Internet Protocol address, uniform resource locator, payment information (excluding personally identifiable information), or any other identifying information, including self-reported identifying information.
(2) Historical reference.-Information relating to when and how a customer or subscriber of a provider uploaded, transmitted, or received content relating to the report or when and how content relating to the report was reported to, or discovered by the provider, including a date and time stamp and time zone.
(3) Geographic location information.-Information relating to the geographic location of the involved individual or website, which may include the Internet Protocol address or verified address, or, if not reasonably available, at least one form of geographic identifying information, including area code or zip code, provided by the customer or subscriber, or stored or obtained by the provider.
(4) Visual depictions of apparent child pornography.-Any visual depiction of apparent child pornography or other content relating to the incident such report is regarding.
(5) Complete communication.-The complete communication containing any visual depiction of apparent child pornography or other content, including-
(A) any data or information regarding the transmission of the communication; and
(B) any visual depictions, data, or other digital files contained in, or attached to, the communication.

ISSN 2238-9121

> (2) Qualquer agência estadual ou local de aplicação da lei envolvida na investigação de exploração sexual infantil;
> (3) Uma agência estrangeira de aplicação da lei designada pelo Procurador-Geral sob o parágrafo (d)(3) ou uma agência estrangeira que tenha uma relação estabelecida com o FBI, o Serviço de Imigração e Controle de Alfândega (ICE) ou a INTERPOL, e que esteja envolvida na investigação de exploração sexual infantil, sequestro ou crimes de aliciamento[7].

Logo, tais provedores (*Facebook, Instagram, WhatsApp, Reddit* inc., *Google, Microsoft*, entre outros) reportam o armazenamento, disseminação e divulgação de conteúdo alusivo a abuso sexual infantojuvenil de que tiverem conhecimento, detectados nos seus sistemas. Esses dados têm sido obtidos a partir ferramentas automatizadas, como, a citar, a inteligência artificial.

No Brasil, não há previsão legal similar determinando aos provedores a comunicação espontânea de notícia-crime, quando tiverem contato com material que viole a dignidade de crianças e adolescentes em suas plataformas. Nesse ponto, entende-se como salutar a importação legislativa com as devidas adaptações ao solo pátrio.

Concluindo, quando se trata de suspeitos provavelmente com residência no Brasil, o NCMEC encaminha as notícias de crime à Polícia Federal (órgão de ligação da Interpol no Brasil) para que entabule investigação formal. A partir desse momento, instaura-se inquérito policial com o objetivo de apurar a autoria delitiva e suas circunstâncias, tendo em vista o compartilhamento da materialidade do crime (e.g., fotos, vídeos e áudios). Tais investigações policiais, no âmbito da Polícia Federal, são, comumente, denominadas como "operação rapina".

2 DO DIREITO À PRIVACIDADE AO DEVER DO ESTADO EM GARANTIR A SEGURANÇA PÚBLICA

[7] *Ibid.*
c) Forwarding of Report to Law Enforcement.-Pursuant to its clearinghouse role as a private, nonprofit organization, and at the conclusion of its review in furtherance of its nonprofit mission, NCMEC shall make available each report made under subsection (a)(1) to one or more of the following law enforcement agencies:
(1) Any Federal law enforcement agency that is involved in the investigation of child sexual exploitation, kidnapping, or enticement crimes.
(2) Any State or local law enforcement agency that is involved in the investigation of child sexual exploitation.
(3) A foreign law enforcement agency designated by the Attorney General under subsection (d)(3) or a foreign law enforcement agency that has an established relationship with the Federal Bureau of Investigation, Immigration and Customs Enforcement, or INTERPOL, and is involved in the investigation of child sexual exploitation, kidnapping, or enticement crimes.

Salienta-se que o crime cibernético é desafiador de investigar devido às múltiplas etapas envolvidas, como intrusão inicial, escalonamento de privilégios e exfiltração de dados. Os serviços de cibercrime estão amplamente disponíveis, na *dark web*, com alta especialização e colaboração entre provedores ilícitos. Esses serviços incluem corretores de acesso inicial (IABs), *crypters*, e serviços de contra antivírus (CAV), além do uso de VPNs para ocultar atividades criminosas. Nesse sentido, Wendt e Martins ensina que:

> A lei não necessariamente acompanhou e acompanha o ritmo da tecnologia e essa desconexão [temporal] tem criado significativo problema para os integrantes do sistema de Segurança Pública e, especialmente, do sistema de persecução criminal. Se, por um lado, as autoridades públicas se encontram cada vez mais no escuro, crimes graves – como terrorismo, pedofilia online, tráfico de drogas etc. – são cometidos, invariavelmente, com um importante componente tecnológico[8].

Todo esse aparelhamento tecnológico em prol do cibercriminoso dificulta o papel investigativo do Estado. Identicamente, abarreirar o compartilhamento de vestígios digitais entre Estados soberanos cria empecilhos para as forças de segurança pública.

Ad argumentandum, destaca-se que o acesso direto, independentemente de decisão judicial, a dados de conexão foi discutido em audiência pública da Comissão de Comunicação da Câmara dos Deputados, no âmbito do PL 2514/15[9]. Essa discussão sinaliza a dificuldade na obtenção de vestígios digitais, no espectro investigativo de crimes cibernéticos.

Não se desconhece que o afastamento do sigilo dos dados telemáticos, no Brasil, depende de ordem judicial expressa (art. 5º, inciso XII, da CF/88). O sigilo de dados telemáticos é garantido pela Constituição como um direito fundamental de primeira geração vinculado à privacidade.

No entanto, o afastamento desse sigilo é permitido, mediante reserva jurisdicional, nas situações legalmente previstas, especialmente, para investigação criminal e instrução penal, de modo a equilibrar o direito à privacidade com o interesse público na apuração de infrações penais. Esse dever se baseia na ideia de que a sociedade tem o direito de ser protegida contra a criminalidade e que o Estado deve agir para garantir a ordem, a segurança e a justiça (art. 144 da CF/88).

---

[8] MARTINS, Tiago Misael de Jesus. WENDT, Emerson. **Hacking legal ou investigativo/lawful hacking: perspectivas a partir da legislação brasileira.** Em publicação. P. 4.

[9] SOUZA, Murilo. **Autoridades defendem acesso direto a dados de conexão de abusadores de crianças**. Agência Câmara Notícias. 2024. Disponível em: https://www.camara.leg.br/noticias/1056016-AUTORIDADES-DEFENDEM-ACESSO-DIRETO-A-DADOS-DE-CONEXAO-DE-ABUSADORES-DE-CRIANCAS. Acesso em: 27 ago. 2024.

Nesse contexto, a Lei nº 9.296/1996 regula a interceptação de comunicações telefônicas e, por analogia, é utilizada, em parte, para regulamentar pedidos judiciais de interceptação (fluxo) de dados telemáticos e registros digitais em investigações (comunicações por *e-mail*, mensagens instantâneas, entre outros). Essa legislação estabelece as condições em que as autoridades judiciais podem afastar o sigilo telemático, tais como, prazo de duração (15 dias, podendo ser prorrogados); demonstração de indícios razoáveis da autoria ou participação em infração penal; não ser possível obter a prova por outros meios (excepcionalidade da medida) e a infração penal ser punida, no mínimo, com pena de reclusão.

Da mesma forma, a Lei nº 12.965/2014 (Marco Civil da Internet) prevê a proteção da privacidade e estabelece que o conteúdo de comunicações privadas será disponibilizado mediante ordem judicial (art. 10, § 2º). O pedido de acesso a dados deve ser fundamentado e específico, demonstrando a necessidade e proporcionalidade da medida.

Ainda, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) estabelece princípios para o tratamento de dados pessoais, garantindo a proteção da privacidade dos indivíduos. Assim, a Lei contém diretrizes que buscam proteger a privacidade e garantir a transparência no uso de dados pessoais.

Diante disso, indaga-se se a internalização das provas obtidas, nos EUA, obedecendo-se à legislação daquele país, poderão ser aproveitadas, no Brasil, sem a correspondente ordem judicial de afastamento de sigilo telemático. Em resposta, será analisada, a seguir, decisão judicial do STJ em caso similar.

3 DA LICITUDE DAS PROVAS PRODUZIDAS PELO NCMEC

Para fins de otimizar a persecução penal, observa-se que os dados obtidos pelo NCMEC, nos EUA, são decorrentes de comunicação dos provedores de aplicação sem necessidade de ordem judicial. Em posse desses vestígios digitais, o NCMEC encaminha-os às autoridades brasileiras que direcionam esforços para identificação da autoria delitiva.

Em situação envolvendo cooperação direta entre agências investigativas, a quinta turma do STJ (STJ, 5. Turma, AREsp nº 701833) entendeu que “as diligências feitas em países estrangeiros conforme as leis locais são válidas no Brasil mesmo se não houver prévia autorização judicial ou participação das autoridades centrais”[10]. No caso concreto,

[10] JUSTIÇA, Superior Tribunal de. **Quinta Turma admite prova bancária obtida no exterior conforme a lei local e sem autorização judicial.** 2021. Secretaria de Comunicação Social.

o Ministério Público Federal (MPF) denunciou Hamilcar Schiavetti pela prática de evasão de divisas (art. 22, parágrafo único, da Lei nº 7.492/1986), uma vez que teria mantido dinheiro em uma conta, no *Delta National Bank*, em Nova Iorque, entre 1999 e 2005, sem declarar os valores à Receita Federal do Brasil (RFB) e ao Banco Central (BACEN). Nessa conjuntura, em 2003, a Procuradoria de Nova Iorque compartilhou com a Polícia Federal do Brasil dados e extratos bancários com movimentações financeiras consideradas suspeitas.

Nos Estados Unidos, a proteção ao sigilo bancário é menor do que em países como o Brasil. Embora existam leis que resguardem a privacidade financeira, não é sempre necessária uma autorização judicial para acessar dados bancários em certas investigações. A quebra do sigilo pode ser feita por meio de diferentes procedimentos administrativos, dependendo da natureza e da finalidade da investigação.

Diante disso, a 5ª Turma do STJ analisou se o uso de provas bancárias obtidas diretamente por autoridades estrangeiras, sem autorização judicial, viola a ordem jurídica brasileira. O caso envolvia a cooperação jurídica internacional entre Brasil e Estados Unidos, regulada pelo Acordo de Assistência Judiciária em Matéria Penal (MLAT), internalizado pelo Decreto nº 3.810, de 2 de maio de 2001.

O MLAT tem como objetivo facilitar a troca de informações e provas entre Estados signatários em processos penais, como investigações, ações judiciais ou medidas de prevenção criminal. O Acordo permite não apenas cooperação formal feita pela autoridade central do país requerente (art. 4º), mas também outras formas de assistência direta entre autoridades investigativas, conforme previsto no art. 1º, n. 2, "h":

> Alcance da Assistência
> 1. As Partes se obrigam a prestar assistência mútua, nos termos do presente Acordo, em matéria de investigação, inquérito, ação penal, prevenção de crimes e processos relacionados a delitos de natureza criminal.
> 2. A assistência incluirá:
> h) qualquer outra forma de assistência não proibida pelas leis do Estado Requerido[11].

Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/13052021-Quinta-Turma-admite-prova-bancaria-obtida-no-exterior-conforme-a-lei-local-e-sem-autorizacao-judicial.aspx. Acesso em: 29 ago. 2024.

[11] BRASIL. **Acordo de Assistência Judiciária em Matéria Penal.** Brasília, DF: Presidente da República, 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm. Acesso em 30 ago. 2024.

Já no art. 17, reforça-se que qualquer acordo, ajuste ou outra prática bilateral cabível também podem ser adotados pelas partes. Nesse sentido, descreve o dispositivo legal:

> Os termos de assistência e demais procedimentos contidos neste Acordo não constituirão impedimento a que uma Parte preste assistência à outra com base em dispositivos de outros acordos internacionais aplicáveis, ou de conformidade com suas leis nacionais. As Partes podem também prestar-se assistência nos termos de qualquer acordo, ajuste ou outra prática bilateral cabível[12].

Embora o MLAT facilite a cooperação, ele não obriga o uso exclusivo de um procedimento formal para todas as situações. A cooperação direta entre agências policiais ou investigativas é permitida e válida, desde que respeite as leis de cada país e não viole garantias fundamentais.

A controvérsia girou em torno da legalidade de informações obtidas, nos EUA, em conformidade com a legislação local, mas sem a intermediação das autoridades centrais (Ministério da Justiça, no Brasil, e Procurador-Geral dos EUA). A Corte Superior concluiu que tal procedimento não compromete a validade das provas, pois o Acordo permite tanto a solicitação formal, via autoridades centrais, quanto a cooperação direta entre órgãos investigativos.

A decisão destacou que o MLAT não estabelece a nulidade das provas obtidas sem esse trâmite formal. Assim, desde que as informações sejam adquiridas de acordo com as leis do país de origem, elas podem ser utilizadas legalmente no processo brasileiro. Além disso, o contraditório e a ampla defesa não são violados, uma vez que podem ser garantidos durante o julgamento no Brasil.

Sendo assim, a 5ª Turma negou o recurso, reafirmando que exigir uniformidade entre os procedimentos legais de diferentes países poderia inviabilizar investigações internacionais. Portanto, a prova coletada, no exterior, mesmo sem autorização judicial, é válida e não infringe o devido processo legal, no Brasil.

Percebe-se que a origem da prova é lícita, conforme as regras do país que a produziu. Logo, seria um contrassenso considerar como prova ilícita, no Brasil, quando compartilhada via canais oficiais da Interpol.

Nesse diapasão, não se desconhece a importância da proteção do direito à privacidade, albergado pelo art. 5º, X, XI e XII da CF/88. No entanto, partindo do ponto de

[12] *Ibid.*

que inexiste direto absoluto, deve-se analisar de forma harmônica com outros direitos também protegidos por um Estado Democrático de Direito, em particular, o princípio da integral proteção da criança e adolescente um dos pilares fundamentais do Estatuto da Criança e do Adolescente (ECA), bem como da Constituição Federal de 1988 (art. 227).

CONCLUSÃO

Novos debates precisam ser travados, no âmbito legislativo, a fim de que os provedores de aplicação (por exemplo, *Google*) sejam compelidos a comunicar às autoridades policiais brasileiras, sem necessidade de ordem judicial, quando identificarem o armazenamento e compartilhamento de dados digitais, contendo abuso de criança e adolescente. Logo, adotar-se-ia a mesma sistemática já consolidada na legislação norte americana.

Em relação às provas compartilhadas à Polícia Federal, via Interpol, pelo NCMAC, ainda não há jurisprudência das cortes superiores abordando sua validade. No entanto, em caso similar, mas não idêntico, o STJ sinalizou apreço pela licitude das provas obtidas com base na legislação alienígena e importadas ao solo pátrio, por meio de cooperação internacional direta entre órgãos investigativos, embora sem autorização de afastamento de sigilo por autoridade judiciária competente no Brasil.

Com o aumento de investigações policiais, questionamentos tendem a surgir, visando a provocar o entendimento nas cortes superiores. Assim, cabe ao operador do direito ter consciência das dificuldades enfrentadas, no combate aos crimes cibernéticos, em especial, os impactos transnacionais das condutas de armazenamento, disseminação e divulgação de conteúdo relativo a abuso sexual infantojuvenil.

REFERÊNCIAS

BRASIL. **Acordo de Assistência Judiciária em Matéria Penal.** Brasília, DF: Presidente da República, 2001. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm. Acesso em 30 ago. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 30 ago. 2024.

BRASIL, **Superior Tribunal de Justiça (5. Turma). AREsp nº 701833 / SP (2015/0105835-2).** Relator Exmo. Sr. Ministro RIBEIRO DANTAS. Julgado em 04/05/2021. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2

ISSN 2238-9121

050914&num_registro=201501058352&data=20210510&peticao_numero=-1&formato=PDF. Acesso em: 30 ago. 2024.

CHILDREN. National Center for Missing and Exploited. **About Us**. 2024. Disponível em: https://www.missingkids.org/footer/about. Acesso em: 15 out. 2024.

EUA. **Reporting requirements of providers**. 18 USC 2258ª. Disponível em: https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18section2258A&num=0&edition=prelim. Acesso em: 29 ago. 2024.

JUSTIÇA, Superior Tribunal de. **Quinta Turma admite prova bancária obtida no exterior conforme a lei local e sem autorização judicial.** 2021. Secretaria de Comunicação Social. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/13052021-Quinta-Turma-admite-prova-bancaria-obtida-no-exterior-conforme-a-lei-local-e-sem-autorizacao-judicial.aspx. Acesso em: 29 ago. 2024.

MARTINS, Tiago Misael de Jesus. WENDT, Emerson; **Hacking legal ou investigativo/lawful hacking: perspectivas a partir da legislação brasileira.** Em publicação.

SOUZA, Murilo. **Autoridades defendem acesso direto a dados de conexão de abusadores de crianças**. Agência Câmara Notícias. 2024. Disponível em: https://www.camara.leg.br/noticias/1056016-AUTORIDADES-DEFENDEM-ACESSO-DIRETO-A-DADOS-DE-CONEXAO-DE-ABUSADORES-DE-CRIANCAS. Acesso em: 29 ago. 2024.