

A (i)legalidade dos relatórios do NCMEC no Brasil e a jurisprudência do STJ

11/06/2026

No cenário da perseguição penal digital, a cooperação jurídica internacional tradicional tem sido crescentemente complementada por modelos de colaboração privada transnacional. O enfrentamento à exploração sexual infantojuvenil em redes globais ilustra esse novo paradigma, no qual provedores de aplicação, vinculados a deveres legais de jurisdições estrangeiras, passam a atuar como agentes centrais na triagem e no fornecimento de elementos probatórios às autoridades de diversos estados.

Essa privatização da produção de prova, embora impulsionada pela necessidade de celeridade, impõe desafios complexos ao processo penal brasileiro, especialmente no que tange à conciliação entre a eficácia investigativa e o estrito respeito às garantias fundamentais e à reserva de jurisdição.

Papel do NCMEC no combate à exploração sexual infantojuvenil

Um papel central nessa dinâmica cabe ao *National Center for Missing & Exploited Children* — Centro Nacional para Crianças Desaparecidas e Exploradas. Como entidade privada sediada nos Estados Unidos, o NCMEC atua como um *hub* estratégico, centralizando denúncias de exploração sexual infantojuvenil na rede e as distribui globalmente, funcionando como uma ponte entre a vigilância corporativa e a repressão estatal. Esse procedimento é movido por um dever legal, previsto no 18 U.S.C. § 2258A, que impõe aos provedores de serviços eletrônicos a obrigação compulsória de reportar ao centro qualquer conteúdo ilícito de abuso infantil identificado em suas plataformas [1]:

(a) Obrigação de notificação.—

(1) Em geral.—

(A) Obrigação.—A fim de reduzir a proliferação da exploração sexual infantil online e prevenir a exploração sexual de crianças na internet, um provedor—

(i) deve, logo que razoavelmente possível após tomar conhecimento efetivo de quaisquer fatos ou circunstâncias descritos no parágrafo (2)(A), tomar as medidas descritas na alínea (B); e

(ii) poderá, após tomar conhecimento efetivo de quaisquer fatos ou circunstâncias descritos no parágrafo (2)(B), tomar as medidas descritas na alínea (B).

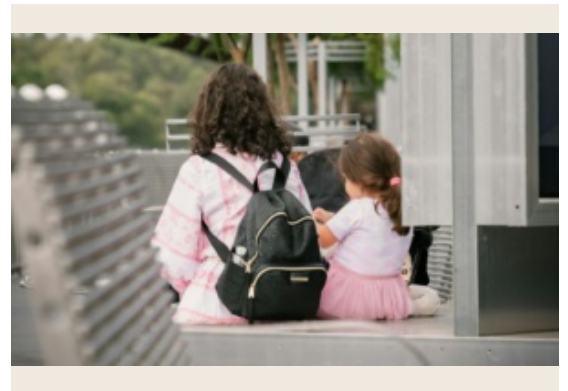
(B) Medidas descritas.—As medidas descritas neste subparágrafo são:

(i) fornecer à CyberTipline do NCMEC, ou a qualquer sucessora da CyberTipline operada pelo NCMEC, o endereço postal, número de telefone, número de fax, endereço de e-mail e ponto de contato específico desse provedor; e

(ii) fazer uma denúncia de tais fatos ou circunstâncias à CyberTipline, ou a qualquer sucessora da CyberTipline operada pelo NCMEC.

Trata-se de um conjunto amplo de informações, descritas no 18 U.S.C. § 2258A(b), que permite ao NCMEC e às autoridades competentes reconstruir o contexto da conduta investigada e identificar seus possíveis autores e vítimas. Assim, os relatórios produzidos pelo NCMEC não decorrem de uma requisição estatal específica dirigida aos provedores, mas do cumprimento de um dever jurídico previamente estabelecido pelo ordenamento norte-americano.

O fluxo operacional inicia-se quando o provedor identifica, por meio de *hash matching*, ferramentas automatizadas de detecção ou denúncias de usuários, conteúdo relacionado à exploração sexual infantojuvenil e o comunica à *CyberTipline* [2] do NCMEC. O relatório pode conter informações cadastrais e técnicas, como endereços IP, registros de acesso, identificadores de contas, *hashes* e, em determinados casos, os próprios arquivos reportados. Após procedimentos preliminares de análise e identificação da jurisdição potencialmente competente, o NCMEC encaminha as informações às autoridades responsáveis, atuando a *CyberTipline* como uma central de recepção, processamento e distribuição de comunicações que conecta órgãos de perseguição penal nos Estados Unidos e em diversos países, conforme a localização dos



usuários e dos fatos investigados.

A possibilidade de compartilhamento internacional dessas comunicações encontra respaldo expresso no 18 U.S.C. § 2258A(c)(3), dispositivo que permite ao NCMEC transmitir os relatórios recebidos a autoridades estrangeiras encarregadas da aplicação da lei que mantenham vínculos institucionais com o FBI, o ICE ou a Interpol. De acordo com estatísticas divulgadas pelo próprio NCMEC, aproximadamente 77% das comunicações atualmente processadas referem-se a ocorrências situadas fora do território norte-americano, sendo encaminhadas a órgãos competentes de cerca de 170 países e territórios [3]. Em determinadas situações, a Interpol também atua como canal de difusão dessas informações. Quando os dados constantes do *report* indicam conexão com o Brasil, o material costuma ser direcionado à Polícia Federal por meio dos mecanismos de cooperação policial internacional, podendo subsidiar a abertura de procedimentos investigatórios.

Os *reports* do NCMEC inserem-se em um fenômeno de privatização da prova transnacional, no qual particulares assumem funções tradicionalmente desempenhadas pelo Estado na obtenção e circulação de elementos probatórios. Embora o Brasil possa exercer jurisdição extraterritorial probatória sobre provedores de serviços de internet – inclusive com requisição direta, conforme reconhecido pelo STF na ADC 51 [4] –, nos *reports* do NCMEC, não há requisição estatal direta, mas compartilhamento decorrente de dever legal. Como resultado, a identificação e transmissão inicial dos elementos probatórios passam a ser realizadas por agentes privados, reduzindo a intervenção dos mecanismos formais de cooperação e dos controles judiciais.

Como observa Paula Ritzmann Torres, a produção de prova transnacional mediante jurisdição extraterritorial implica uma delegação parcial do controle sobre direitos fundamentais à esfera privada, privilegiando a eficiência na obtenção da prova em detrimento das garantias fundamentais [5], o que também parece ser uma realidade no caso dos *reports* fornecidos pelo NCMEC.

Discussão sobre a (i)legalidade das provas decorrentes dos *reports* do NCMEC no Brasil

Em maio de 2026, o STJ julgou o AgRg nos EDcl no AREsp 3.091.178/SP, no qual expressamente tratou, pela primeira vez em decisão colegiada, da validade dos *reports* do NCMEC no Brasil. No caso concreto, a Corte reconheceu o *report* fornecido como legítima *notitia criminis*, dado que “a proteção constitucional não pode ser invocada para salvaguardar a prática de atos ilícitos graves como a pornografia infantil” [6]. Justificou ainda que não haveria ilegalidade na prova baseada no relatório do organismo NCMEC, porque a “obtenção de dados cadastrais vinculados a endereços de IP pela autoridade policial diretamente junto aos provedores prescinde de autorização judicial prévia”, tendo em vista o artigo 10, § 3º, do Marco Civil da Internet.

Porém, consta expressamente da fundamentação do voto da ministra relatora que a “identificação do endereço de IP e a requisição de dados cadastrais (como nome, endereço e filiação)” não configurariam quebra de sigilo telemático sujeita à reserva de jurisdição. Trata-se de entendimento que não parece ser referendado na jurisprudência do STF, que reconhece que dados de IP estão protegidos sob o manto da reserva de jurisdição (v.g. ADI 5.642).

Desse modo, além de fundamentar a validade da medida em premissa que aparenta conflitar com a jurisprudência do STF acerca da tutela constitucional dos dados de IP, a decisão sustenta que as garantias constitucionais não poderiam ser opostas à persecução de delitos de elevada gravidade. Tal raciocínio, entretanto, suscita objeções relevantes. A incidência dos direitos e garantias fundamentais não se condiciona à menor ou maior reprovabilidade da conduta investigada, tampouco pode ser afastada em razão da gravidade do crime apurado. Em um Estado de Direito, a legitimidade da atuação estatal não decorre da natureza da infração, mas do respeito aos parâmetros constitucionais que disciplinam e limitam intervenções na área de proteção dos direitos fundamentais.

Para todo efeito, o STJ já reconheceu a possibilidade de utilização, no Brasil, de provas produzidas lícitamente no exterior segundo a legislação do país de origem, ainda que sem observância dos requisitos previstos no direito brasileiro. No AREsp 701.833/SP, a 5ª Turma admitiu o uso de informações bancárias obtidas nos Estados Unidos sem autorização judicial, mas em conformidade com a legislação local. Em sentido semelhante, no RHC 210.067, a 6ª Turma validou dados extraídos da plataforma Sky ECC pelas autoridades francesas e posteriormente compartilhados com o Brasil, destacando a incidência do princípio da *lex diligentiae*, previsto no artigo 13 da Lindb. Segundo esse entendimento, os meios de obtenção da prova submetem-se à lei do país onde a diligência foi realizada, ressalvada a hipótese de afronta à ordem pública nacional, na qual há prevalência da *lex loci*.

Não obstante, os precedentes do STJ relativos à aplicação da *lex diligentiae* versavam sobre hipóteses em que a infração penal investigada apresentava elementos de conexão com o exterior, circunstância que justificava a incidência do artigo 13 da Lindb. Diversamente, nos *reports* encaminhados pelo NCMEC, o processamento e o encaminhamento das informações podem ocorrer nos Estados Unidos, sem que isso implique a localização do fato delituoso naquele país. Sob essa ótica, a referência aos “fatos ocorridos em país estrangeiro”, constante do artigo 13 da Lindb, deve ser compreendida como alusiva à própria infração penal objeto da investigação, e não ao simples tratamento ou trânsito internacional dos dados.

Nesse contexto, mostra-se pertinente o entendimento firmado pelo STF no RE 628.624, segundo o qual a transnacionalidade dos delitos previstos nos artigos 241, 241-A e 241-B do ECA pressupõe a existência de projeção internacional, ainda que potencial, do resultado, inexistente quando a conduta permanece integralmente circunscrita ao território nacional, como quando há publicação do material em conversas privadas na internet sem estrangeiro envolvido. Nas hipóteses em que tal elemento transnacional se faz presente, contudo, a adoção da teoria da ubiquidade pelo artigo 6º do Código Penal permite reconhecer a ocorrência do delito também em território estrangeiro, o que pode justificar a incidência da *lex diligentiae*. Afinal, a dimensão transnacional da infração tende a envolver fatos probatoriamente relevantes ocorridos fora do Brasil, atraindo a aplicação do artigo 13 da Lindb, segundo o qual a prova desses fatos submete-se à legislação vigente no local de sua ocorrência.

A conclusão, contudo, não pode ser generalizada para todos os *reports* encaminhados pelo NCMEC. Há inúmeras situações em que os delitos previstos nos artigos 241, 241-A e 241-B do ECA são integralmente praticados em território brasileiro, envolvendo usuários localizados no Brasil e submetidos exclusivamente à jurisdição nacional. Nesses casos, o mero fato de os dados terem sido processados ou encaminhados a partir dos Estados Unidos não é suficiente para conferir caráter transnacional à infração penal. Ausente qualquer elemento relevante de conexão do fato investigado com o exterior, a validade dos *reports* não parece poder ser fundamentada, ao menos com base no artigo 13 da Lindb, na incidência da *lex diligentiae*, uma vez que os fatos objeto da persecução ocorreram integralmente sob a égide do ordenamento jurídico brasileiro.

Ainda assim, diante da orientação atualmente adotada pelo STJ quanto à legalidade das provas derivadas dos *reports* do NCMEC — ao menos no que se refere às categorias de dados que a Corte considere não submetidas à reserva de jurisdição —, caso esse entendimento venha a se consolidar, impõe-se reconhecer que tais comunicações devem ser compreendidas como meras notícias-crime aptas a desencadear a atividade investigativa, mas insuficientes, por si sós, para fundamentar uma condenação. Ademais, a licitude da obtenção ou do compartilhamento da informação no exterior não afasta a necessidade de observância das garantias constitucionais que regem a persecução penal no Brasil. A utilização subsequente desses dados permanece sujeita aos limites impostos pela reserva de jurisdição, pela reserva de lei e pela proporcionalidade, de modo que a validade da origem da informação não se projeta automaticamente sobre os atos investigativos dela decorrentes, tampouco possui o condão de convalidar eventual intervenção em direitos fundamentais praticadas em território nacional sem a correspondente autorização constitucional ou legal.

[1] Disponível [aqui](#).

[2] O *CyberTipline* recebeu o número de 21,3 milhões de *reports* no ano de 2025. NCMEC. 2025 CyberTipline Report. Disponível [aqui](#).

[3] NCMEC. 2025 CyberTipline Report. Disponível [aqui](#).

[4] STF, ADC 51/DF, rel. min. Gilmar Mendes, Pleno, j. em 23/02/2023, DJe de 28/4/2023.

[5] TORRES, Paulo Ritzmann. Métodos de obtenção da prova transnacional: cooperação jurídica internacional e jurisdição extraterritorial. 2024. 549 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, 2024, p. 232-233.

[6] STJ, AgRg nos EDcl no AREsp 3.091.178/SP, rel. min. Maria Marluce Caldas, 5ª Turma, j. 12/05/2026, DJe de 19/5/2026. Não é, porém, a primeira vez que o STJ reconhece a validade de dados fornecidos a partir do exterior em persecução quanto aos delitos previstos nos arts. 241-A e 241-B do ECA, como no caso do HC 828.743/RS, no qual a investigação se iniciou por informações compartilhadas pelo Reino Unido.