

Polido: Brasil deve urgentemente aderir à Convenção de Budapeste

Na última quinta-feira (30/6), o Escritório do Programa de Crimes Cibernéticos do Conselho da Europa (C-PROC) publicou a atualização da situação das leis de crimes cibernéticos ao redor do globo. Em perspectiva geral, o conselho verificou progresso significativo desde 2013, considerando que 124 membros das Nações Unidas (64%) já contam com leis e regimes especiais para combate à criminalidade cibernética transnacional, em grande medida em conformidade com a [Convenção de Budapeste sobre Crime Cibernético de 2001](#). De fato, o aumento expressivo do que eu chamaria de evolução qualitativa de leis e regulamentos da internet no domínio geral dos ilícitos cibernéticos oferece uma preciosa pista. Tendo em mente que delitos criminais passaram a ser praticados exponencialmente por intermédio de ferramentas computacionais e informáticas desde o advento da internet na década de 1990 para fins civis e comerciais, incluindo práticas de ataques cibernéticos, a discussão reforçada em foros multilaterais, como no Conselho da Europa, apenas endossa a preocupação de política normativa. Hoje, 92 membros das Nações (48%) já contam com regras vigentes e consistentes com os artigos 16 a 21 da Convenção de Budapeste, que estabelecem poderes processuais às autoridades de aplicação das digitais (*e-evidences*).



A posição brasileira, em especial, é preocupante até hoje. Em

2006 era iniciado movimento no Congresso reforçando a importância de nosso Estado de aderir à convenção, e o país foi já convidado a integrar o grupo de países que não são membros do Conselho da Europa, como Guatemala, México, Nova Zelândia, África do Sul e Tunísia. O caminho das propostas legislativas no Congresso, contudo, também oscilou entre projetos inovadores e de intensa participação democrática, como o que resultou no Marco Civil da Internet, e iniciativas repressivas de criminalização de usos e usuários da internet, como no precedente aberto pela malfadada Lei Azeredo (chamado também de AI-5 Digital). Veiculado no Projeto de Lei nº 84/1999, apresentado pelo ex-parlamentar Eduardo Azeredo, a proposta originalmente criava regras para criminalizar certas condutas no ambiente digital. Entre os tipos penais, estavam os crimes de acesso e obtenção de informações em sistemas restritos, a transferência não autorizada de dados ou informações particulares e a destruição de banco de dados e terceiros. Depois de várias emendas, o projeto levou à promulgação da Lei 12.735/2012, cuja maior contribuição tenha sido a de determinar que órgãos da polícia judiciária brasileira pudessem estruturar "*setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado*".

O que mais chamava a atenção de especialistas, sem dúvidas, era a falta de integração das discussões congressuais no Brasil para os avanços multilaterais e política externa de *cooperação internacional em matéria digital e prevenção aos crimes cibernéticos* travados no Conselho da Europa. com os

procedimentos de revisão da Convenção de Budapeste de 2001. Somente em 22/7/2020 o texto do tratado foi encaminhado pela presidência da República ao Congresso Nacional (Mensagem 412/2020) para fins de adesão brasileira ao instrumento, nos termos do artigo 49, inciso I, da Constituição [\[1\]](#). Passados tantos apertos com o funcionamento de suas comissões, agora em 17 de junho, a Câmara, por meio da Comissão de Relações Exteriores, deu o pontapé ao procedimento com a tramitação de urgência do Projeto de Decreto Legislativo 255, que tem hoje o senador Vitor Hugo (PSL-GO) como relator [\[2\]](#). De acordo com os dados da Estratégia Nacional de Segurança Cibernética, em 2017 já contabilizada mais de 70 milhões de vítimas de crimes cibernéticos no Brasil. No ano seguinte, 89% dos executivos do país foram vítimas de fraudes cibernéticas. O Brasil é o segundo país com as maiores perdas causadas por esse tipo de ataque.

Em vigor desde 2004, a Convenção de Budapeste de 2001 é um dos mais importantes instrumentos a lidar com aspectos penais substantivos, processuais e cooperativos no combate aos crimes cibernéticos e envolve mais de 60 países. Por seu caráter multilateral global e específico, ela reconhece o respeito às soberanias dos Estados signatários, preservação dos direitos e garantias fundamentais das partes e interesses das autoridades nacionais de aplicação da lei, em especial quanto ao objetivo de investigação e persecução de crimes praticados na internet e/ou com intermédio de ferramentas de internet e tecnologias digitais.

A convenção também é destacável por alguns aspectos que a posicionam entre os instrumentos predominantes na cooperação internacional digital. Em primeiro lugar, abre espaço para instrumentos de cooperação facilitada e reforçada entre atores estatais e não estatais em questões relacionadas a internet, sistemas informáticos e computacionais, Trata-se de um acordo bastante arrojado se comparado aos mecanismos tradicionais de cooperação jurídica internacional e assistência jurídica mútua, como os MLATs (por exemplo, o [Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos de 1997](#); o [Tratado de Cooperação em Matéria Penal entre Brasil e Suíça de 2004](#)). Em segundo lugar, contempla estratégias conjuntas entre os países membros para a tipificação, combate e prevenção de crimes praticados pela internet, os delitos cibernéticos, e medidas de cooperação específicas para acesso a dados e informações digitais. Por fim, pela convenção e seu regime facilitado, os Estados signatários se alinham para facilitar a cooperação internacional para a obtenção transfronteiriça de provas digitais (*e-evidences*) no curso de investigações e persecução criminais (artigo 19). Elas dizem respeito às provas relacionadas a fraudes financeiras, tráfico internacional de drogas, lavagem de dinheiro, pornografia infantil e outros crimes praticados com apoio de ferramentas tecnológicas e da internet.

Apesar de o Brasil contar com instituições representativas de um sólido *marco legal digital*, em larga medida alcançadas pela gradual consolidação de regras e princípios do Marco Civil da Internet de 2014, das normas gerais de comércio eletrônico e proteção do consumidor online, além das recentes Lei Geral de Proteção de Dados-LGPD e Estratégia de Segurança Cibernética (Decreto nº 10.222/2020), agentes dos Poderes Executivo e Judiciário têm se posicionado em práticas isolacionistas que enfraquecem a cooperação internacional em matéria digital. Elas rompem, inclusive, com esforços existentes de fortalecimento de iniciativas em redes, foros especializados e negociações na área tecnológica. Demonstram enormes descompassos com as bases do Direito Internacional, além da perda de oportunidade de conferir ao Brasil maior presença e engajamento nas instituições de combate à criminalidade transnacional.

Assim como o exemplo dado por decisões anteriores em matéria criminal com repercussão internacional, como no Inquérito 4781 do STF, em que o ministro Alexandre de Moraes determinava bloqueio de contas de usuários da internet por grandes empresas de internet em múltiplas jurisdições, o comportamento reincidente de autoridades de aplicação da lei tem sido preocupante. Instrumentos de cooperação internacional em processos judiciais no Brasil têm sido rejeitados como se representassem violação da soberania nacional. Esse tema de repercussão geral, inclusive, será objeto de discussão pelo Plenário do STF, na Ação Direta de Constitucionalidade 51/2017, em setembro próximo, oportunidade em que a corte decide sobre a aplicação dos instrumentos de cooperação jurídica e assistência mútua em casos envolvendo dados localizados no estrangeiro.

Uma correção de rota, contudo, contribuirá para retirar o ambiente legal e institucional brasileiro no campo digital, proteção de dados e direitos fundamentais online de uma zona de penumbra. Isso porque essa mudança representará o alinhamento aos princípios que estão estampados no negligenciado artigo 4º da Constituição da República, em que respeito às jurisdições estrangeiras e cooperação internacional são imperativos para o Estado brasileiro. Autoridades de aplicação da lei, por sua vez, insistem no argumento de que os mecanismos de cooperação jurídica internacional por tratados e convenções processuais para acesso a provas digitais ou telemáticas são lentas e ineficientes. O fundamento de utilitarismo pela simples celeridade para acesso a conteúdos de comunicação privada entre usuários de internet ou cumprimento de medidas de bloqueio ou suspensão de acesso a sites e contas de usuários não poderia se sobrepor aos direitos e liberdades fundamentais, em que garantias processuais e devido processo também devem ser observadas.

Em todos esses eventos, existem graves sintomas de uma narrativa deletéria que também estava a contaminar o Congresso Nacional na discussão mais recente do controvertido [Projeto de Lei 2.630/2020](#) (Lei Brasileira sobre Liberdade, Responsabilidade, Transparência na Internet, ou PL das Fake News). Existe uma linha argumentativa que busca alterar o direito vigente no Brasil e o sentido do artigo 4º da Constituição da República, particularmente sob dois aspectos. O primeiro reside na interpretação rasteira de "dados empíricos" sobre baixo número de respostas de autoridades de cooperação de outros países em pedidos de cooperação penal solicitados pelo Brasil. O segundo diz respeito ao desejo de demonstrar que decisões da Justiça brasileira podem ser direcionadas a qualquer pessoa "dentro e fora do Brasil" indistintamente (ou seja, teriam algo como efeitos "transponíveis ou "transgressores" à jurisdição de outros Estados). Parlamentares descuidados, no entanto, apenas conferem aparência de legitimidade para soluções manifestamente ilegais do ponto de vista

internacional. Isso porque deixam de respeitar princípios relativos à soberania, não ingerência nos assuntos internos de outros Estados, assim como a cooperação necessária para solução de questões ou controvérsias (inclusive as de natureza civil e comercial) que tenham repercussão internacional.

O exemplo mais gritante, entre vários, está no artigo 32 do PL 2630. Ele determina que empresas provedoras de serviços de redes sociais e comunicações interpessoais estabeleçam uma espécie de canal direto para banco de dados contendo informações de usuários brasileiros, localizado no país da sede das empresas, para fins de cumprimento de ordens da "autoridade judicial brasileira" [3].

Em uma primeira análise, a fórmula do artigo 32 do PL 2630/2020, além de romper com garantias e procedimentos específicos segundo os Artigos 10, 11 e 15 do Marco Civil, praticamente busca burlar ou elidir quaisquer procedimentos de cooperação jurídica internacional acionáveis também em respeito à jurisdição do Estado estrangeiro, particularmente o país da sede do controlador. Esses procedimentos incluem os que seriam necessários para cumprimento de pedidos relativos a dados de usuários de redes sociais e de serviços de mensagens, residentes no Brasil (nacionais ou estrangeiros residentes), para autoridades do Estado onde o controlador desses dados esteja sediado, ou mesmo para execução de decisões da Justiça brasileira perante tribunais de outros Estados eventualmente vinculados às questões em controvérsia. Há dados de usuários, como os relativos a comunicações privadas, que são protegidos e regidos tanto pela lei brasileira como pela lei estrangeira e entrelaçados pela incidência de normas imperativas e de proteção de direitos e garantias fundamentais — algo que não seria novidade para o jogo e regras do direito internacional privado, da Constituição e tratados e convenções. E de modo mais espetaculoso, a fórmula do artigo 32 do projeto pretende alcançar dados "referentes a usuários brasileiros", que podem tecnicamente residir no Brasil ou em outro país.

Não seria mais oportuna e necessária, portanto, a apreciação urgente do Congresso Nacional do texto da Convenção de Budapeste no PDL 255/2021. Em 11/12/2019, o Brasil havia sido convidado pelo Conselho da Europa a integrar o conjunto de partes signatárias do tratado. O segundo protocolo da convenção encontra-se em negociações. No documento, há posicionamento claro sobre a oportunidade de o Brasil ingressar em regime de cooperação facilitado para acesso a provas eletrônicas. Esse tema é também retomado na detalhada [nota técnica](#) do Grupo de Apoio sobre Criminalidade Cibernética sobre a Convenção de Budapeste, do Ministério Público Federal, de 28/8/2020. Aliás, o [Alto Painel para Cooperação Digital das Nações Unidas](#) reforçou que a *interdependência digital* é necessária à compreensão dos desafios postos à consecução de objetivos de justiça e adjudicação de litígios entre atores estatais e não estatais envolvendo a internet e novas tecnologias.

Vale a pena, portanto, o Congresso Nacional considerar o momento para a efetiva adesão do Brasil à Convenção de Budapeste. Em 12/7/2020, o Conselho da Europa publicou [relatório](#) sobre os benefícios e impactos do tratado em escala global, tanto para Estados signatários, como para outros países [4]. Alguns indicadores são relevantes em temas de cooperação para acesso transfronteiriço a dados. Em fevereiro de 2020, cerca de 177 países (92%) estavam em processo de reformar suas legislações internas, ou o fizeram nos últimos anos em matéria penal para se ajustar às demandas digitais e novas tecnologias. As partes não apenas se basearam na Convenção de Budapeste quando reformaram suas legislações internas, mas também cerca de 153 (79%) dos membros da Organização das Nações Unidas se utilizaram dos dispositivos do tratado como guia ou uma fonte de inspiração para basear suas reformas legislativas domésticas. Por fim, cerca de 106 (55%) países da ONU já tem adotado normas, em seus direitos internos, equivalentes aos dispositivos da Convenção de Budapeste. Um terço de países adotou, ao menos, algumas regras específicas de Direito Penal segundo a convenção, incrementando

seus sistemas jurídicos domésticos [\[5\]](#).

[\[1\]](#) Este ato formal procedeu à Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública, publicada em 11 de dezembro de 2019, que sinalizou, pela primeira vez, a intenção do Brasil aderir à convenção, unindo-se "a grupo internacional que inclui países como Argentina, Austrália, Canadá, Chile, Costa Rica, Estados Unidos, Japão, Paraguai, República Dominicana e membros da União Europeia".

[\[2\]](#) <<https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2287513&ord=1>>.

[\[3\]](#) "artigo32: *Os provedores de redes sociais e de serviços de mensageria privada deverão ter sede e nomear representantes legais no Brasil, informações que serão disponibilizadas em seus sítios na internet, bem como manter acesso remoto, a partir do Brasil, aos seus bancos de dados, os quais conterão informações referentes aos usuários brasileiros e servirão para a guarda de conteúdos nas situações previstas em lei, especialmente para atendimento de ordens de autoridade judicial brasileira*".

[\[4\]](#) COE, *The Budapest Convention on Cybercrime: benefits and impact in practice*. Council of Europe: Strasbourg. 2020. Disponível em: <<https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>>.

[\[5\]](#) COE, *The Budapest Convention on Cybercrime: benefits and impact in practice*. Council of Europe: Strasbourg. 2020, esp.p.5. Disponível em: <<https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>>.

Date Created

05/07/2021