Capítulo 15

Conectando Pontos: Cooperação Jurídica Internacional e os Desafios Impostos Pelas Redes Distribuídas

Jorge Enrique de Azevedo Tinoco
Pedro Emannuel Medeiros Machado
Marco Bruno Miranda Clementino

RESUMO: O aumento da ocorrência de crimes transnacionais acompanha a crescente integração global das comunicações – principalmente via internet. Com isso em mente, inovações tecnológicas oferecem novas avenidas para a prática de ilícitos que transcendem fronteiras nacionais. Uma das tecnologias que estão em pleno crescimento e possuem alcance global são as redes distribuídas. O presente estudo busca avaliar como os tratados de assistência legal mútua se portam para operacionalizar a persecução de crimes em um contexto transfronteiriço via redes distribuídas e determinar o que é necessário para otimizar a cooperação jurídica internacional nessas situações. Trata-se de uma pesquisa teórica e qualitativa que utiliza a revisão bibliográfica para aferir o estado da arte e as necessidades específicas dos sistemas atuais de cooperação. Como resultado, apresentam-se recomendações de aprimoramento aos atuais modelos de cooperação jurídica internacional – e principalmente aos tratados de assistência legal mútua – no que toca o combate ao crime cibernético via redes distribuídas.
PALAVRAS-CHAVE: Cooperação Jurídica Internacional; Redes Distribuídas; Tratados de Assistência Legal Mútua; Crimes Transnacionais; Cibercrime.

CONNECTING DOTS: INTERNATIONAL JUDICIAL COOPERATION AND THE CHALLENGES POSED BY DISTRIBUTED NETWORKS.

ABSTRACT: *The growth in transnational crime rates follows the ever-growing global integration in communications – mainly through the internet. With this in mind, technological innovations offer new avenues for the practice of illicit behaviour transcending national borders. One of the technologies which are growing rapidly and have a global reach is distributed networks. The present study aims to evaluate how mutual legal assistance treaties behave when operationalizing the persecution of crimes in a cross-border context through distributed networks and determine what is necessary to optimize international judicial cooperation in such situations. It is theoretic and qualitative research made through bibliographic review to determine the state of the art and the specific needs of current systems of cooperation. As a result, recommendations are made to improve the current models of international judicial cooperation – especially regarding mutual legal assistance treaties – in what concerns the fight against cybercrime through distributed networks.*
KEYWORDS: *International Judicial Cooperation; Distributed Networks; Mutual Legal Assistance Treaties; Transnational Crime; Cybercrime.*

INTRODUÇÃO

Poucos avanços tecnológicos trouxeram maiores mudanças à comunicação humana como a *internet*. Mesmo os mais céticos quanto à influência da rede mundial de

computadores já reconhecem sua magnitude[1]. Nesse sentido, uma das maiores disrupções trazidas pela rede mundial de computadores se refere à velocidade de troca e de compartilhamento de informação em nível transnacional.

Como afirmado por Leslie Daigle[2]: "[...] a internet não foi desenhada para reconhecer fronteiras nacionais", e não é difícil confirmar essa afirmação. Nas últimas três décadas, serviços *online* gratuitos vêm permitindo o armazenamento e compartilhamento *online* de arquivos que podem ser visualizados em qualquer país com acesso à internet. Outros serviços, como os de videoconferência, são instrumentais para manter as pessoas conectadas umas às outras tanto doméstica quanto mundialmente – e, em especial, em tempos de pandemia.

Dentre as tecnologias popularizadas pelo crescimento da internet, alguns tipos de arquitetura de redes encontram uma adoção em maior escala. Uma dessas arquiteturas de rede são as conhecidas "redes distribuídas". A arquitetura distribuída permite que diversos *nodes*[3] se comuniquem entre si para executar uma tarefa específica ou para dividir recursos (BALDA; GARG, 2015). É interessante frisar que os *nodes* de uma rede distribuída podem existir dentro de um único prédio e também podem ter alcance transnacional.

Essa distribuição, por conseguinte, permite que as informações de uma rede não estejam concentradas em um único repositório, mas espalhadas por todos os participantes da rede. Dessa maneira, redes distribuídas são naturalmente mais resilientes a qualquer tipo de ataque (BARAN, 1964). Entretanto, essa resiliência tem um custo: não há um ponto centralizado de ataque pelo qual um mandado judicial consiga potencialmente alcançar todos os pontos dessa rede. A depender da extensão e da arquitetura de uma determinada rede distribuída, alguns documentos e arquivos podem estar localizados exclusivamente em outras jurisdições.

Nesse contexto, a determinação unilateral de um país para que diligências policiais ou judiciais sejam tomadas em território estrangeiro (sem prévio tratado que permita tal ação) constituiria uma inequívoca afronta ao princípio da soberania. Nesse sentido, embora ações unilaterais rápidas e incisivas possam ser tidas como mais eficazes para a efetivação do direito, tais medidas colocam em xeque o respeito à igualdade soberana dos Estados, ou seja, o princípio basilar do direito internacional que propicia que cada nação se manifeste na comunidade global com igual reconhecimento (PINTO; OLIVEIRA, 2019).

Para chegar a uma resposta satisfatória ao problema apresentado, a cooperação jurídica internacional é um passo fundamental. De qualquer modo, os mecanismos e procedimentos tradicionais pelos quais essa cooperação normalmente ocorre devem ser questionados e aprimoramentos devem ser propostos. Tais aprimoramentos, por sua vez, além da eficiência *per se*, também devem atentar para o respeito aos direitos humanos e às liberdades fundamentais dos indivíduos (CARLETTI; GUERCIO, 2019).

---

1 Um exemplo disso é o economista vencedor do Prêmio Nobel (2008), Paul Krugman. Em entrevista para o New York Times em 1998, Krugman previu que a importância da internet para a economia não seria maior que a do fax. Recentemente, Krugman se manifestou reconhecendo o erro. Link para matéria sobre o caso (em inglês): https://www.snopes.com/fact-check/paul-krugman-internets-effect-economy/

2 Ex-chefe de tecnologias da internet na Internet Society (ISOC). O texto completo pode ser lido através do link a seguir (em inglês): https://www.internetsociety.org/blog/2013/06/provoking-national-boundaries-on-the-internet-a-chilling-thought/

3 *Node* é um termo em inglês que, nesse contexto, se refere a uma entidade computacional (BALDA; GARG, 2015). Ou seja, um node pode ser um computador, um celular, ou um dispositivo qualquer com memória própria e acesso à internet.

Posto isso, o presente estudo pretende alcançar os seguintes objetivos: (i) averiguar como o sistema tradicional de Acordos de Assistência Legal Mútua (MLAT) responde às demandas por cooperação jurídica em casos nos quais é necessário obter evidências eletrônicas presentes em redes distribuídas, (ii) identificar possíveis gargalos e impedimentos ao bom desenrolar do processo. Em decorrência disso, sugerem-se aprimoramentos aos atuais modelos de cooperação jurídica internacional, em especial aos tratados de assistência legal mútua, no que diz respeito aos crimes cibernéticos executados por meio de redes distribuídas. Trata-se de uma pesquisa qualitativa que utiliza a revisão bibliográfica jurídica e tecnológica, buscando contrapor o material teórico com fenômenos reais.

1. OS MLAT: O ESTADO DA ARTE E AS CRÍTICAS DESSE MECANISMO DE COOPERAÇÃO

A globalização das relações humanas traz, como consequência, a expansão do escopo de condutas ilícitas para além das fronteiras nacionais. O alongado alcance de condutas criminosas, principalmente em espaços essencialmente internacionais (*internet*), impõe um ônus cooperativo aos Estados. Sobre essa afirmativa, Clementino (2013, p.16-17) assevera: "[...] somente a partir da postura cooperativa interestatal é possível que a persecução penal também assuma uma visão global e proceda ao adequado rastreamento das ramificações das organizações criminosas".

Essa cooperação jurídica internacional não depende, necessariamente, da existência de tratados ou instrumentos específicos entre países cooperantes – podendo se pautar no princípio da reciprocidade, por exemplo (GIACOMET JUNIOR, 2019). Dentre os mecanismos de cooperação, um dos mais conhecidos é a carta rogatória. Esse mecanismo é um dos mais clássicos meios para a efetivação da cooperação jurídica internacional. O Reino Unido, por exemplo, instituiu a primeira normativa sobre cartas rogatórias em 1883 a partir da *Order XXXVII, rule 6A*, da Suprema Corte do Reino Unido (SUTHERLAND, 1982).

No contexto virtual, contudo, juristas têm demonstrado elevado grau de insatisfação com a carta rogatória em função da lentidão pela qual esse mecanismo é processado (BRENNER; SCHWERHA, 2004). No Brasil, o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), órgão do Ministério da Justiça, vem notando um aumento no uso de outros mecanismos para além das cartas rogatórias (BRASIL, 2019).

Segundo o DRCI, em matéria penal, alguns dos fatores que causam esse novo modelo de cooperação incluem: (i) o direito internacional costumeiro, (ii) diversos tratados bilaterais, regionais e multilaterais firmados pelo Brasil e (iii) previsão expressa de regras para o auxílio direto pelo art. 216-O, § 2º do Regimento Interno do Superior Tribunal de Justiça (BRASIL, 2019).

Nesse contexto, os Tratados de Assistência Jurídica Mútua (MLAT), por mais utilizados que sejam, são passíveis de uma análise crítica do seu funcionamento e eficácia. Os MLAT surgiram como um mecanismo de colaboração e cooperação entre os povos com o fito de se alcançarem soluções pacíficas e adequadas aos casos de interação entre duas jurisdições internacionais distintas. Nesse sentido, tais tratados permitem a troca de evidências e informações, por meio da comunicação entre autoridades centrais, com o intuito de operacionalizar a assistência técnica necessária entre duas jurisdições interna-

cionais. Além disso, acordos de assistência legal mútua encontram-se em vigor em mais de sessenta países, incluindo os Estados Unidos, o Brasil e a União Europeia (US DEPARTMENT OF STATE, 2014).

Importa saber, ainda, que esses mecanismos de cooperação representam uma resposta encontrada pelo Direito Internacional para tentar solucionar problemas relativos à territorialidade para o andamento de processos domésticos. A cooperação depende do reconhecimento da juridicidade e soberania de um outro país para que, com a assistência do país requerido, o requerente possa cumprir as diligências cabíveis. Essa situação envolve, normalmente, a obtenção de arquivos físicos localizados em território estrangeiro. A *internet*, contudo, permite o acesso remoto – o que traz novos parâmetros para os procedimentos de cooperação que ainda se baseiam na realidade física (STF, 2020). Essa realidade pode estimular países a adotarem medidas unilaterais, pautando-se em um ideal de eficácia que, em tese, deveria se sobrepor ao procedimento moroso.

Essa postura unilateral que preza por um ideal de "eficiência" em desfavor da soberania e dos interesses de outros Estados não representa uma novidade. Em 1983, a Corte Federal de Apelações dos Estados Unidos para o Décimo Primeiro Circuito determinou que a instituição financeira *Bank of Nova Scotia* divulgasse dados financeiros localizados em uma filial nas Bahamas em clara violação às leis bahamenses de proteção dos dados bancários. Dois anos depois, em um novo caso envolvendo a *Bank of Nova Scotia*, a mesma corte ignorou o pedido escrito de um oficial estrangeiro que ressaltava a importância de se observarem as leis de proteção aos dados bancários (ERWIN, 1992). Essas decisões do Décimo Primeiro Circuito deram início a uma doutrina legal estadunidense, conhecida como *Nova Scotia Subpoenas* (MADRUGA; FELDENS, 2016).

Tendo esse contexto em mente, é mister reconhecer que os MLAT proporcionam um caminho viável para a obtenção de dados, elementos probatórios e para a execução de diligências processuais de maneira a respeitar a soberania estrangeira. Medidas unilaterais, no que lhes concerne, por mais que sejam empregadas com o objetivo de maior "eficiência", acabam ignorando a juridicidade de um outro Estado. Em assim sendo, segundo Madruga e Feldens (2016), sob a ótica da reciprocidade, admitir a possibilidade de ação unilateral por parte do Brasil significaria admitir que outros países fizessem o mesmo – o que implicaria clara violação à Constituição Federal de 1988. Ademais, caso não seja seguida a ótica da reciprocidade, a unilateralidade pode acarretar problemas futuros de ordem legal ou diplomática.

O Brasil, por exemplo, é um país que adota MLAT com diversos países e, em matéria penal, é estado-parte de quatorze acordos multilaterais de assistência legal mútua (BRASIL, 2021b). Esse número aumenta consideravelmente ao se tratar de acordos bilaterais – sendo, atualmente, signatário de vinte e um tratados bilaterais, dentre os quais, o mais recente é o MLAT estabelecido com o Reino Hachemita da Jordânia em março de 2019 (BRASIL, 2021a).

Levando em consideração as informações apresentadas, por mais que o uso dos MLAT seja crescente (BRASIL, 2019) e ofereça resultados mais ágeis que cartas rogatórias pautadas na reciprocidade (BRENNER; SCHWERHA, 2004), é importante analisar as críticas a esses instrumentos de cooperação e quais os fundamentos que as consubstanciam.

Nessa perspectiva, no ano de 2017, o Supremo Tribunal Federal (STF) foi instado a se pronunciar sobre o tema. A razão pela qual se solicitou a manifestação do STF foi

a proposição da Ação Declaratória de Constitucionalidade (ADC) nº 51 por parte da Federação das Associações das Empresas Brasileiras de Tecnologia da Informação – ASSESPRO. Um dos objetivos da ADC 51 é declarar a constitucionalidade do Decreto nº 3.810, de 2 de maio de 2002, que promulga o MLAT entre Brasil e Estados Unidos (BRASIL, 2020).

Na audiência pública sobre o controle de dados de usuários por provedores de *internet* no exterior, da ADC 51, foram suscitados alguns dos aspectos negativos documentados do MLAT entre o Brasil e os Estados Unidos. Segundo dados do Ministério da Justiça e Segurança Pública do Brasil, o acordo de assistência mútua entre os países não seria um instrumento de cooperação efetivo. Durante essa audiência pública, o à época Ministro da Justiça e Segurança Pública Sérgio Moro fez as seguintes afirmações acerca da efetividade do MLAT Brasil-Estados Unidos:

> [...] o Ministério da Justiça fez um levantamento de pedidos de cooperação entre 2016 a 2019, envolvendo obtenção de dados ou comunicações telemáticas do Brasil e Estados Unidos, e foi verificado que apenas 26% deles teriam sido cumpridos total ou parcialmente, ou seja, 74% deles não teriam sido cumpridos. Por outro lado, foi também destacado que o tempo de cumprimento médio desses pedidos tem sido 10 meses, quando são cumpridos, o que, em termos de investigação criminal, que muitas vezes envolve questões urgentes, pode significar uma investigação criminal destituída de utilidade (STF, 2020, p.38).

Os números trazidos pelo Ministério da Justiça e Segurança Pública são incisivos. Como é notado por Brenner e Schwerha (2004), uma das principais vantagens de um MLAT é a celeridade quando comparado a outros mecanismos. É seguro afirmar, pois, que o prazo médio de dez meses para o cumprimento de um pedido esvazia, em partes, o sentido de ter um tratado de assistência e desencoraja a cooperação, uma vez que seria mais efetivo confiar em medidas unilaterais ou informais.

A cooperação jurídica, principalmente no que diz respeito a cibercrimes, é especialmente difícil por conta de fatores específicos ao espaço digital, como as diferenças legislativas (princípio da dupla incriminação) e diferentes capacidades tecnológicas para a investigação (CEREZO; LOPEZ; PATEL, 2007). Colocar mais barreiras ao processo cooperativo significa não atender ao objetivo final: combater a criminalidade transnacional.

Isso posto, as críticas aos MLAT não se restringem à lentidão ou ao baixo número de casos atendidos. Organizações voltadas à defesa dos direitos humanos na *internet*, como a *Access Now*, expressaram desaprovação à atual forma pela qual se operacionalizam os tratados de assistência legal. Dentre as falhas apontadas, podem ser citadas: (i) demora na efetivação da cooperação; (ii) pouco investimento nos departamentos de cooperação das autoridades centrais; (iii) falta de uma rede de proteção aos direitos humanos; e (iv) demandas desproporcionais por questões geográficas[4] (MITNICK, 2017).

Lentidão e ineficácia não se harmonizam com o universo do Direito na perspectiva de obtenção de um julgamento justo, célere e compatível com o devido processo legal. Cientes de que a cooperação interestatal tem por finalidade a obtenção de provas e a

[4] Um exemplo dessa desproporcionalidade geográfica pode ser visto nos Estados Unidos, que recebem muitos pedidos de cooperação, uma vez que as maiores empresas de tecnologia estão sediadas no território americano (MITNICK, 2017).

execução de diligências necessárias ao processo, o tempo de execução dessa atividade cooperativa é essencial para que se mantenha a finalidade e utilidade do processo.

Partindo dessa ótica, ao encarar a realidade de um Estado que busca a obtenção de dados telemáticos para fins de construção de elementos probatórios robustos durante uma persecução penal e esses dados encontram-se armazenados sob a jurisdição de outro Estado, o MLAT, pelas razões citadas, não corresponde à maneira ótima de cooperação. A situação se agrava, ainda mais, quando se depara com uma configuração distribuída de dados, na qual um só arquivo, ou conjunto de dados, é fragmentado e espalhado por vários locais distintos ao redor do mundo através das redes distribuídas. A obtenção do dado não está sujeita, nesse contexto, a apenas uma jurisdição, mas a várias.

Portanto, o pensar jurídico nesses casos não requer apenas noções de cooperação internacional mas também de soberania, de autodeterminação nacional, do princípio da territorialidade. Requer também receptividade para uma abordagem interdisciplinar, uma vez que os desafios trazidos pelos cibercrimes envolvem expertises incomuns aos juristas. Na configuração distribuída, principalmente, esses elementos se fazem ainda mais necessários, uma vez que não se trata mais de uma relação mútua entre apenas dois Estados, pois os "fragmentos" desses dados estão, ao mesmo tempo, em vários locais distintos. Por essa razão, entender a conceituação e o funcionamento dessa rede é o próximo passo a se seguir.

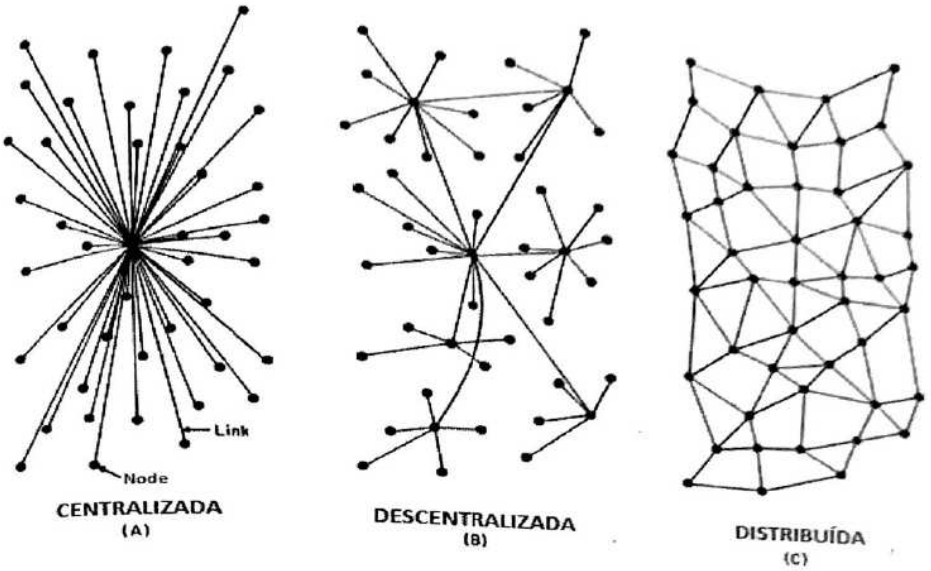
2. AS REDES DISTRIBUÍDAS: COMO FAZER COM QUE UM ARQUIVO ESTEJA EM DOIS LUGARES AO MESMO TEMPO

Um dos primeiros usos do conceito de "redes distribuídas" no contexto de sistemas de comunicação surgiu com o relatório de Paul Baran (1964) para a força aérea dos Estados Unidos. Nesse relatório, esse autor demonstra algumas das peculiaridades e vantagens das comunicações em redes distribuídas. Mesmo três décadas depois da publicação do relatório de Baran (1964), a ideia de distribuição de redes continua a influenciar a tecnologia da informação. Segundo Coulouris et al. (1994), as redes distribuídas podem ser conceituadas nos seguintes termos:

> [...] um sistema que consiste em uma coleção de máquinas autônomas conectadas por redes de comunicação e equipados com sistemas de *software* desenhados para produzir um ambiente computacional consistente e integrado. Sistemas distribuídos permitem que pessoas cooperem e coordenem suas atividades de forma mais eficiente e efetiva. Os propósitos principais dos sistemas distribuídos podem ser elencados como: compartilhamento de recursos, abertura, concorrência, escalabilidade, tolerância a erros e transparência (COULOURIS et al., 1994, apud JIA; ZHOU, 2005, p.1, tradução nossa).

A conceituação de Coulouris et al. (1994) permite entender as redes distribuídas como um conjunto de máquinas pertencentes a uma rede que se comunicam entre si sem precisar da intermediação de um ponto central. Para auxiliar a compreensão da definição trazida, vale a pena fazer uso dos diagramas de Paul Baran (1964).

FIGURA 1
Diagramas de Paul Baran (1964)



Fonte: BARAN (1964, p.2, tradução nossa).
Disponível em: https://www.rand.org/pubs/research_memoranda/RM3420.html

Os diagramas apresentados na Figura 1 trazem três arquiteturas de rede distintas: (A) uma rede centralizada; (B) uma rede descentralizada; e (C) uma rede distribuída. Nesses diagramas, os pontos são idênticos e estão distribuídos geograficamente da mesma maneira. Cada uma das arquiteturas apresentadas traz vantagens e desvantagens para um sistema específico.

Sistemas nos quais há necessidade de acesso singularizado e controle rigoroso de arquivos podem adotar a configuração centralizada (modelo A). Uma das principais vantagens de sistemas centralizados é o grau mais elevado de controle sobre a rede. Um exemplo de sistema centralizado pode ser encontrado em um servidor de hospital. Dentro do servidor em questão, existem diversos arquivos com informações sensíveis. Essas informações podem, em um modelo centralizado, ser disponibilizadas apenas para pessoas com permissões específicas[5].

Entretanto, o modelo centralizado também possui algumas desvantagens. Dada a sua arquitetura aglutinadora, a centralização tornaria uma rede "obviamente vulnerável, uma vez que a destruição de um único *node* destruiria a comunicação entre estações-fim" (BARAN, 1964, p.1, tradução nossa). Em outras palavras, se o *node* central do modelo A for removido, nenhum dos outros pontos conseguirá se comunicar ou acessar os arquivos contidos no ponto central. Nesse sentido, arquiteturas centralizadas são, por definição, mais suscetíveis a ataques como, por exemplo, o *Denial of Service Attack*[6] (DoS) (KAVITHA; RAMALAKSHMI; MURUGESWARI, 2019).

5 Em um cenário hipotético, um médico pode ter acesso ao diagnóstico da enfermidade do paciente, enquanto um funcionário administrativo pode ter acesso apenas aos dados referentes ao plano de saúde do paciente. Essas permissões seriam validadas e o acesso aos arquivos correspondentes seria dado por um servidor central que disponibilizaria os arquivos.

6 Um ataque DoS pode ser caracterizado como um ataque à disponibilidade do sistema. Enquanto diversos tipos de ataque podem buscar a coleta e armazenamento de dados (e.g.: cartões de crédito, dados bancários), o ataque DoS

O modelo B soluciona, em parte, a vulnerabilidade mencionada. Ao formar *clusters*[7], a rede garante que não há um ponto central e único de fragilidade, mas diversos pontos centrais – um para cada *cluster* formado. Dessa forma, a arquitetura descentralizada previne a dependência integral em um ponto único de rede, contudo, ainda assim, não há como prevenir a sujeição à centralização, mesmo que em nível menor. Embora esse modelo propicie um grau de resiliência maior à rede, o padrão descentralizado ainda requer, ao contrário do que sua nomeação indica, um certo grau de centralização.

Por sua vez, um sistema distribuído (modelo C) não possui qualquer ponto central. Todos os *nodes* pertencentes à rede podem se comunicar livremente. Esse modelo é, sem dúvidas, o mais resiliente, uma vez que um ataque à rede terá de afetar não apenas um ou alguns pontos, mas absolutamente todos os *nodes* da rede. Entretanto, o sistema distribuído não permite o mesmo controle que é tradicional de um sistema centralizado. Enquanto a arquitetura centralizada permite saber qual o armazenamento central e a via necessária de comunicação entre dois pontos, as redes distribuídas não funcionam dessa maneira.

Por não depender de intermediários, usuários da rede podem compartilhar arquivos entre si sem depender de um repositório central. Entretanto, os desafios jurídicos começam a ficar aparentes ao se perceber que, embora essa arquitetura proporcione eficiência e resiliência para o sistema nela pautado, a distribuição também significa que um mandado judicial não conseguiria alcançar de forma eficaz uma rede sem repositório central. As características mencionadas fazem das redes distribuídas uma ferramenta viável para propiciar atividades ilícitas de caráter transnacional.

A título de exemplo, a arquitetura distribuída – e em especial o protocolo *peer-to-peer* (P2P)[8] – é comumente creditada como instrumental para sites que agregam arquivos pirateados (FETSCHERIN, 2005). Se um arquivo ilegal se encontra em diversos nodes de uma mesma rede, os quais se comunicam entre si, não há como pretender parar a circulação desse arquivo sem remover absolutamente todos os pontos de contato. Objetivar a apreensão de cada node de uma determinada rede P2P, além de demandar enormes recursos, também necessitaria a cooperação célere e coordenada de diversas jurisdições.

De qualquer modo, não é apenas o protocolo P2P que traz desafios no contexto das redes distribuídas. O uso de um artifício chamado *sharding*[9] também pode adicionar barreiras à obtenção de determinados documentos. O diferencial do *sharding* é que ele

---

busca causar uma enxurrada de pedidos de acesso à uma única rede ao mesmo tempo, causando a queda do sistema e a indisponibilidade da rede (JIA; ZHOU, 2005).

7 O termo *cluster* pode ser definido como uma espécie de "aglutinação de computadores conectados (*nodes*) que trabalham de forma conjunta como se fossem uma única (e muito mais poderosa) máquina" (SUSE, 2021, s/p, tradução nossa). De qualquer maneira, para os fins do presente trabalho, não se usará o termo *cluster* no sentido de propiciar a produção de um esforço conjunto de processamento, mas no sentido de ser uma aglutinação de *nodes* em um mesmo espaço em uma rede.

8 A definição mais básica e comumente aceita para o protocolo *peer-to-peer* é a seguinte: "Uma rede distribuída pode ser chamada de *peer-to-peer* [...] caso os participantes dividam uma parte de seus próprios recursos de hardware [...]. Esses recursos compartilhados são necessários para operacionalizar o serviço e conteúdo oferecidos pela rede [...]. Eles são acessíveis por outros *nodes* diretamente, sem passar por entidades intermediárias. Os participantes dessa rede são tanto provedores [...] quanto usuários [...] dos recursos" (SCHOLLMEIER, 2001, p.1, tradução nossa).

9 *Sharding* pode ser definido como "um método de dividir e armazenar um único grupo lógico de dados em múltiplas bases de dados" (KIM, 2014, s/p, tradução nossa). Um exemplo que pode ajudar na assimilação do conceito apresentado é o de uma tabela (*i.e.:* grupo lógico de dados) cujos conteúdos (*i.e.:* os dados) foram divididos em diversos servidores físicos (*i.e.:* bases de dados).

permite que um mesmo arquivo seja repartido em pequenas partes e espalhado em diversos *nodes* que compõem a rede. Dessa maneira, se um arquivo contendo uma tabela é considerado fundamental para a instrução de um determinado caso, e essa tabela está repartida por meio de *sharding*, isso significa que partes do documento completo podem estar espalhadas por diversas jurisdições. Essa situação fica mais complicada se o arquivo que se busca só interessa à instrução se for obtido integralmente, o que ensejaria cooperação entre múltiplas jurisdições.

3. OS ILÍCITOS TRANSNACIONAIS E COOPERAÇÃO ENTRE JURISDIÇÕES NO CONTEXTO DAS REDES DISTRIBUÍDAS

A evolução tecnológica, somada aos inúmeros desenvolvimentos técnicos, sociais, econômicos, culturais e políticos das últimas décadas, aceleraram significativamente e intensificaram todo o processo de fluxo de informações ao redor do mundo, tornando a sociedade cada vez mais interligada, cada vez mais globalizada. Essas mudanças, especialmente o progresso técnico no transporte de pessoas, bens e dados, aproximam ainda mais rápida e intimamente os habitantes de diferentes sociedades. Tal aproximação favorece o progresso econômico e cultural em muitas áreas mas também impõe certos custos (SIEBER, 2010).

Nesse sentido, a *internet* e o ciberespaço global simbolizam a nova qualidade de interação mundial na sociedade moderna da informação, ao mesmo tempo em que os vírus de computador e os web-ataques exemplificam o resultado dos riscos da interdependência dos usuários desse espaço (SIEBER, 2010). A partir dessa perspectiva, é possível entender a *internet* como a representação máxima da globalização, uma vez que se refere ao espaço no qual os indivíduos interagem sem interferência de qualquer fronteira física ou política.

Sob esse raciocínio, a vida em sociedade nos ambientes *online* ganha uma dimensão inerentemente internacional. Isso se deve, sobretudo, à instantânea transmissão de *bytes* que compõem mensagens, documentos, mídias e demais arquivos incorpóreos, transmitidos de um país ao outro, sem a necessidade de procedimentos migratórios, autorização de importação de dados, selos postais ou pagamento de impostos.

Como direta consequência da transnacionalização de atividades sujeitas à regulamentação legal, questões jurídicas que transcendem fronteiras crescem em volume e importância. No contexto de direito privado, sujeitos em diferentes países assinam contratos de venda, empresas multinacionais formam cartéis que limitam a concorrência que afetam no mercado mundial e – por meio da disseminação de arquivos na *internet* – as violações de direitos autorais ocorrem em vários Estados simultaneamente (SIEBER, 2010).

Urge, então, a importância da Cooperação Jurídica Internacional, a fim de promover a participação colaborativa entre Estados para garantir a maior efetividade na investigação por meio da assistência entre as jurisdições para a obtenção de dados que possam servir como elementos probatórios para a persecução penal. Afinal, os dados que importam ao processo podem estar localizados em servidores sediados em territórios estrangeiros e, para acessar tais informações, é necessário o consentimento do Estado sede.

3.1. A RELAÇÃO ENTRE SOBERANIA, TERRITÓRIO E COOPERAÇÃO JURÍDICA INTERNACIONAL

A cooperação jurídica internacional decorre de dois conceitos inerentes ao Estado: soberania e território. Segundo Carreau e Bichara (2016), a primeira noção de "soberania" surgiu com o pensamento de Jean Bodin, na França do Século XVI. A soberania, para Bodin, seria a essência do Estado – uma qualidade *sine qua non* para que pudesse haver um ente estatal. A soberania, para esse autor, significaria imputar ao soberano a possibilidade de criar leis, mesmo que ele não estivesse, necessariamente, adstrito às normas criadas. Bodin, contudo, não entendia que o soberano estivesse acima de todas as leis – o Estado permaneceria subordinado às leis divinas, da natureza e às comuns a todas as nações. Dessa maneira, para Bodin, a soberania não seria uma negação de qualquer norma aplicável ao Estado, mas "[...] um princípio essencial de direito interno, destinado a ordenar a sociedade política" (CARREAU; BICHARA, 2016, p.10).

A conceituação de soberania passou por diversas transformações ao longo do tempo, desde interpretações como a de Hobbes, que a entendiam como um poder absoluto do Estado (CARREAU; BICHARA, 2016), até Ferrajoli, que propõe uma análise tripartite pautada em aspectos: (i) filosóficos, (ii) histórico-práticos e (iii) ligados à legitimidade conceitual-jurídica (CLEMENTINO, 2013). Invariavelmente, qualquer que seja a proposição sobre o conceito de soberania, uma questão se mantém – nas palavras de Clementino (2013, p.51):

> Sendo absoluta e autossuficiente, não se submete, a princípio, a nenhuma limitação no seu exercício, o que termina por pressupor um espaço territorial delimitado de incidência, até porque, se esse atributo é reconhecido a todas entidades estatais, é de se supor a igualdade entre estas e sua consequente independência recíproca.

Dessa ideia decorre que a soberania está necessariamente ligada ao território. É importante, assim, entender a relação simbiótica entre soberania e territorialidade. Levando em consideração o exercício da soberania sobre determinado território, é possível dizer que há um alcance geográfico sobre as relações pertencentes a um dado ordenamento jurídico, ou seja, existe uma limitação para a aplicação das normas estatais. Sobre a territorialidade aplicada ao direito tributário, Torres (2003) disserta:

> O conceito de territorialidade é imprescindível para o tratamento de qualquer elemento do direito Internacional. Nenhum conceito pode ter maior interesse no direito tributário internacional do que este, pois serve como fundamento para todos os demais contornos dos regimes jurídicos aplicáveis, e em particular pelos vínculos que mantém com a noção de soberania, em face do poder de tributar dos Estados (TORRES, 2003, p.72, apud EL KHATIB, 2012, s/p).

A partir desse conceito, pode-se perceber a importância da noção de espaço e, principalmente, do conceito de territorialidade para o Direito Internacional como um todo, tendo em vista, também, o debate acerca da soberania dos Estados. Por esse motivo, o estudo da aplicabilidade dos regimes jurídicos e dos poderes estatais mostra-se tão essencial para a atualidade, na qual enxerga-se cada vez menos os limites fronteiriços entre sociedades e se enxerga uma realidade tão conectada e próxima.

Com efeito, a redução das distâncias propiciada pelo surgimento da *internet*, bem como pela sua popularização, incrementou também o número de crimes cibernéticos e de delitos transnacionais (CEREZO; LOPEZ; PATEL, 2007). Isso significa que a presença física do perpetrador no local do crime deixa de ser um requisito necessário para a consumação.

Tendo isso em mente, vale analisar a conceituação de ilícito transnacional trazida pela Convenção das Nações Unidas contra o Crime Organizado Transnacional, adotada em Nova York, em 15 de novembro de 2000, e incorporada no ordenamento jurídico brasileiro por meio do Decreto nº 5.015, de 12 de março de 2004. A Convenção estabelece que "infrações transnacionais" serão: (i) aquelas cometidas em mais de um Estado; (ii) as que forem cometidas em um só Estado, mas que parte substancial da sua preparação, planejamento, direção e controle tenha lugar em outro Estado; (iii) as que forem cometidas em um só Estado, mas envolvam a participação de um grupo criminoso organizado que pratique atividades criminosas em mais de um Estado; ou ainda (iv) as que forem cometidas em um só Estado, mas produzam efeitos substanciais noutro Estado (BRASIL, 2004).

Esse cenário se mostra ainda mais delicado no tocante às investigações e à aplicação de diferentes jurisdições nesses tipos de delitos – para promover esses objetivos, a cooperação entre Estados se faz essencial. Nesse viés, a mesma Convenção trouxe em seu artigo 19 que, ao tratar das investigações conjuntas, os Estados Partes devem considerar a possibilidade de celebração de acordos ou protocolos bilaterais a fim de atuarem conjuntamente nas investigações dos processos judiciais, como se pode observar no dispositivo:

> Artigo 19
> Investigações conjuntas
> Os Estados Partes considerarão a possibilidade de celebrar acordos ou protocolos bilaterais ou multilaterais em virtude dos quais, com respeito a matérias que sejam objeto de investigação, processos ou ações judiciais em um ou mais Estados, as autoridades competentes possam estabelecer órgãos mistos de investigação. Na ausência de tais acordos ou protocolos, poderá ser decidida casuisticamente a realização de investigações conjuntas. Os Estados Partes envolvidos agirão de modo a que a soberania do Estado Parte em cujo território decorra a investigação seja plenamente respeitada (BRASIL, 2004).

Posto isso, é seguro afirmar que a Cooperação Jurídica Internacional representa o meio adequado para assegurar o devido processo legal das ações judiciais, enquanto, ao mesmo tempo, mantêm-se o respeito à soberania e à jurisdição dos diferentes Estados envolvidos. Não é possível, dessa forma, tomar medidas judiciais extraterritoriais sem minimizar a soberania alheia, tal qual ocorreu no caso *Nova Scotia* trazido na primeira seção do presente trabalho.

Contudo, atentando para o contexto de redes distribuídas e transnacionais, questiona-se sobre a permanência dos MLAT como mecanismos efetivos para promover a execução de diligências judiciais em diversas jurisdições. Isso se deve não só às críticas ao estado da arte dos MLAT, como também à própria natureza da arquitetura de dados em redes distribuídas. Nesse sentido, a ausência de um ponto central como base para o armazenamento de um determinado arquivo mostra-se como uma barreira para o bom funcionamento de um acordo bilateral de assistência mútua, uma vez que o Estado

que tenha interesse nesse dado não teria um único Estado específico para o qual pedir auxílio, mas vários.

3.2. TERRITORIALIDADE E REDES DISTRIBUÍDAS

Ao trazer a discussão da territorialidade para o contexto das redes distribuídas, desafios começam a ficar aparentes. Nessas redes, dois *nodes* têm acesso direto entre si e podem estar localizados em pontos opostos no planeta. O acesso direto de um *node* ao outro significa que não há intermediários necessários para a troca de arquivos. A falta de um intermediário complica ações cooperativas que seriam, anteriormente, mais simples.

Se uma atividade ilegal está sendo operacionalizada entre um ponto A e um ponto C por intermédio de um ponto B, o passo lógico seria direcionar a demanda por cooperação ao ponto B. Na ausência desse intermediário, seriam necessárias tantas ações de cooperação quanto houvessem jurisdições envolvidas – se, para além dos pontos A e C, também existirem pontos D, E, F, G e H, o volume de cooperações necessárias aumentaria proporcionalmente. Em função disso, questiona-se quanto à efetividade de instrumentos bilaterais de cooperação para um problema que é, por natureza, multilateral.

Essa multiplicidade de territórios nos quais há o desenvolvimento de atividades criminosas cria um ônus cooperativo para que se proceda ao combate das condutas ilícitas. Esse ônus cooperativo pode ser visto por alguns como um impedimento à boa condução de investigações e à celeridade processual. Contudo, essa possível frustração não justifica a imposição de medidas unilaterais e o consequente menosprezo às jurisdições terceiras. Apesar disso, a unilateralidade preconizada por medidas como as *Nova Scotia Subpoenas* estão sendo adotadas em algumas jurisdições, como Reino Unido, Paquistão e Bélgica em nome de um padrão mais elevado de "eficiência" (MITNICK, 2017).

Todavia, mesmo no contexto das redes distribuídas, a cooperação jurídica internacional demonstrou alguns casos de sucesso. Recentemente, a Agência da União Europeia para a Justiça Criminal (Eurojust) coordenou ações de cooperação com diversos países para a apreensão de equipamento usado na distribuição de material protegido por direitos autorais (VAN LIEROP, 2020). Esse caso será considerado em maior detalhe na seção a seguir.

3.3 CASO DE SUCESSO: A EUROJUST E REDES P2P

Em agosto de 2020, a Eurojust comunicou a apreensão de sessenta servidores na Europa e na América do Norte, pertencentes a uma organização acusada de promover a pirataria de mídia protegida por direitos autorais. Esse esforço conjunto foi operacionalizado a partir da cooperação entre dezenove países e da coordenação da Eurojust (VAN LIEROP, 2020).

A atividade de pirataria executada pelo grupo de crime organizado consistia na obtenção fraudulenta de arquivos de mídia e sua posterior propagação em redes P2P via *torrent* (uma tecnologia que permite a transferência de arquivos pelo protocolo P2P). Algumas das mídias divulgadas pela organização criminosa não haviam sequer sido disponibilizadas para compra no mercado legítimo. Essa situação causou um prejuízo estimado superior a dez milhões de dólares americanos para a indústria do entretenimento (VAN LIEROP, 2020).

O caso em questão surgiu a partir de um pedido da promotora-de-ligação dos Estados Unidos para a Eurojust. Segundo Van Lierop (2020), dada a natureza transnacional do crime em questão, a cooperação e a ação coordenada entre jurisdições seriam imprescindíveis. Nesse sentido, a ação da agência europeia envolveu a execução de mais de trinta pedidos de cooperação via MLAT, além do alinhamento conjunto de operações pelo centro de coordenação da Eurojust. O sucesso da agência europeia em ações como essa já ganhou o reconhecimento do vice-presidente da Motion Picture Association (MPA) em carta de reconhecimento ao trabalho da Eurojust, na qual afirma que "[a organização da operação executada] é, sem dúvidas, o melhor modelo possível para o trabalho excelente executado pelas organizações europeias" (VAN VOORN, 2020, p.1, tradução nossa).

Considerando a operação retratada, fica evidente a importância de uma outra dimensão que vai além da cooperação interestatal: a coordenação das atividades. Em função da multiplicidade de territórios e autoridades envolvidas, assim como da resiliência inerente às redes distribuídas, é imperativo que as ações de cooperação sejam coordenadas para que ensejem bons resultados. Na seção seguinte, a importância da coordenação para ações cooperativas em redes distribuídas será analisada em maior minúcia.

4. O DILEMA DA DISTRIBUIÇÃO: COMO COORDENAR A AÇÃO DE AGENTES ESTATAIS?

Com vistas ao cenário apresentado na seção anterior, é possível entender que ilícitos transnacionais operacionalizados por meio de redes distribuídas impõem um ônus cooperativo às jurisdições envolvidas em função das diferenças de territorialidade. Nesse contexto, a cooperação jurídica internacional não se apresenta como uma alternativa, mas como uma necessidade. Para que se promova o combate a ilícitos transnacionais pela *internet*, é necessário que arquivos consigam ser obtidos e/ou removidos dos servidores originais. Isso não pode ocorrer, respeitadas a legalidade e a soberania nacional, sem que haja consenso e a participação das jurisdições cooperantes.

Cabe afirmar, portanto, que a localização de *nodes* de uma rede distribuída em múltiplos territórios cria elementos de estraneidade em tantas jurisdições quanto houver territórios envolvidos. O desafio criado a partir dessa diversidade de locais se pauta na multiplicidade de soberanias que precisarão cooperar e na forma como se dará essa cooperação. Mesmo que diversos Estados estejam dispostos a cooperar para obter uma prova ou executar uma ordem judicial estrangeira, o modo pelo qual essa cooperação será executada pode significar o sucesso ou a falha da ação.

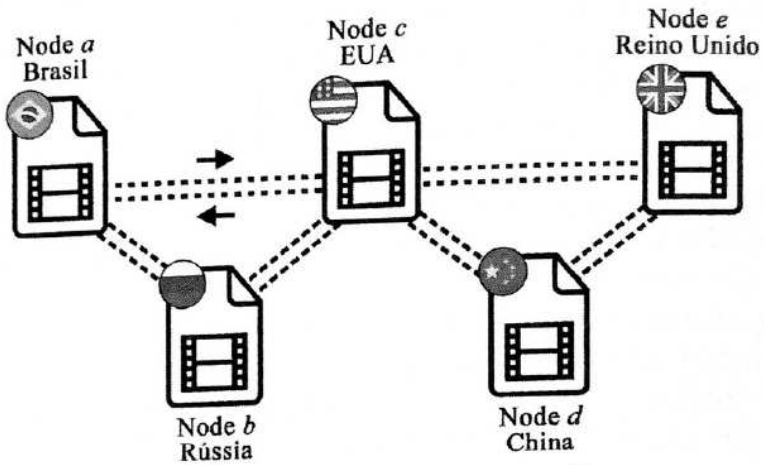
Caso um Estado cooperante não venha a agir em tempo hábil, é possível que a ordem judicial perca o sentido – um arquivo pode ser realocado, repartido, ou replicado em outro *node* participante da rede. Em assim sendo, a cooperação por si só não basta para operacionalizar a execução de uma ordem judicial, sendo necessária, também, a coordenação das ações interestatais.

A imprescindibilidade da coordenação decorre da própria natureza das redes distribuídas e dos objetivos que se quer atingir por meio da ação de cooperação. Tendo em vista o livre acesso que *nodes* da rede têm entre si, não dependendo de *clusters* centralizadores, um ataque precisa ser direcionado a *nodes* ou *links* específicos em uma rede de uma só vez. Com essa ação simultânea, evita-se que a informação seja repartida, realocada ou repetida para outros servidores.

Para entender os desafios apresentados pela arquitetura distribuída, é importante explorar o funcionamento de dois artifícios descritos nas seções anteriores, em contextos de cooperação jurídica: o P2P e o *sharding*.

O protocolo P2P propõe uma rede distribuída e compartilhada na qual todos os *nodes* interagem livremente entre si – cada ponto da rede funciona simultaneamente como provedor e usuário de um recurso (SCHOLLMEIER, 2001). Exemplos de ilícitos praticados por redes P2P incluem o compartilhamento de mídia pirateada, mas não estão restritos a essa prática, podendo envolver condutas criminosas mais gravosas[10].

FIGURA 2
Exemplo de ilícito *cross-border* por meio de uma rede P2P



Fonte: ilustração proposta pelos autores[11].

A Figura 2 ilustra uma rede P2P cujos participantes disponibilizam um arquivo pirateado entre si. Cada um dos pontos da rede está em um país diferente (*nodes a*, *b*, *c*, *d* e *e*) e pode se comunicar direta e livremente. Uma decisão judicial que objetivasse remover o arquivo compartilhado da *internet* precisaria, em virtude do princípio da territorialidade e do respeito à soberania nacional, promover uma cooperação entre Brasil, Rússia, Estados Unidos da América, China e Reino Unido.

Todavia, caso essa cooperação não seja coordenada, os responsáveis pela rede podem ter tempo para adicionar novos *nodes* à rede ou criar outras formas de *backup* do arquivo pirateado. De maneira ideal, essa ação precisaria ser executada de forma coordenada em cada jurisdição – não permitindo que a conduta ilícita persistisse.

Essa necessidade de coordenar a execução de ações que pretendem atacar uma rede distribuída reflete uma das mais proeminentes características dessa arquitetura: a

[10] Essas práticas ilícitas foram famosamente utilizadas por usuários de alguns sites de compartilhamento P2P como o Napster e o Kazaa (MOONEY; SAMANTA; ZADEH, 2010). Contudo, o mesmo protocolo já se mostrou viável para a prática de outros atos ilícitos, tais como compartilhamento de pornografia infantil (BRENNAN; HAMMOND, 2017) involving illegal or non-consensual activities associated with the sexual victimisation of children. This work extends an earlier typal analysis carried out by Hammond et al. (2009. An examination of problematic paraphilic use of peer to peer facilities. In Advances in the analysis of online paedophile activity (pp. 65–73.

[11] Alguns dos elementos visuais usados na confecção da figura foram obtidos a partir do site https://freeicons.io/ utilizando uma licença aberta.

resiliência. Por não possuir um ponto central de ataque, a efetividade de uma ação que se propõe a remover arquivos de uma rede distribuída depende do ataque simultâneo a diversos *nodes* ou *links* que a compõem.

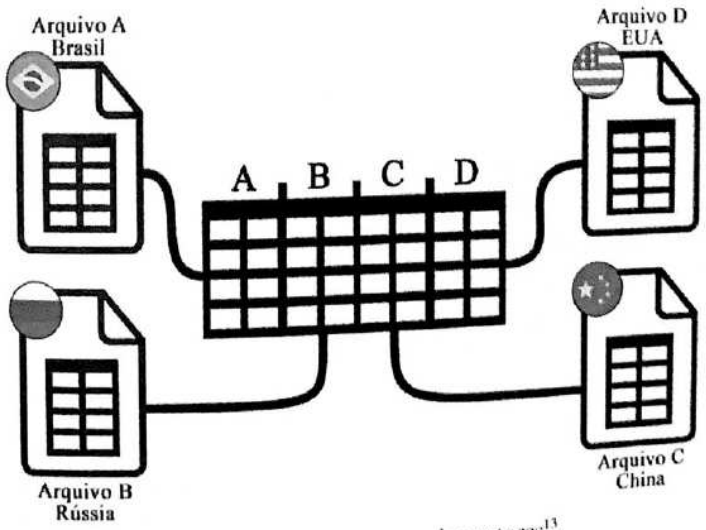
A resiliência dessas redes, assim como o ar de anonimato dos participantes e a própria normalização cultural da pirataria virtual (SAHNI; GUPTA, 2019), gera um ambiente convidativo para a criação de "culturas pirata". Principalmente no que tange a entretenimento, não é incomum observar o compartilhamento de mídias protegidas por direitos autorais em redes P2P, comumente obras cinematográficas (FETSCHERIN, 2005) ou musicais (MOONEY; SAMANTA; ZADEH, 2010).

De qualquer maneira, não é apenas o compartilhamento de material protegido por direitos autorais que é propiciado por meio de redes P2P. Em estudo sobre uma rede chamada "Gnutella", Hughes *et al.* (2006) apontam para a existência de um volume preocupante de procuras por pornografia ilegal entre usuários. Segundo Hughes *et al.* (2006), em um período de três semanas, do total de buscas na rede, em média 1,6% desse material correspondia a pornografia ilegal[12]. Essa realidade chamou a atenção de acadêmicos da psicologia que estão desenvolvendo modelos de padrões comportamentais predatórios em comunidades *online* que usam o compartilhamento de arquivos via protocolo P2P (BRENNAN; HAMMOND, 2017).

Para além da resiliência oferecida pelo modelo P2P, o uso do *sharding* também pode afetar o resultado de uma cooperação jurídica envolvendo a obtenção de arquivos em uma rede distribuída. Enquanto a multiplicidade de *nodes* dificulta a execução de uma medida judicial que envolva a retirada de conteúdos da *internet*, o *sharding* pode afetar até mesmo a obtenção de provas para a instrução processual.

FIGURA 3

Exemplo de uso do *sharding* para dificultar a obtenção de uma prova



Fonte: ilustração proposta pelos autores[13].

12 Para conceituar o que seria "pornografia ilegal", Hughes *et al.* (2006, p.4, tradução nossa) considerou "práticas que são claramente ilegais sob a lei do Reino Unido e de normas internacionais: estupro, incesto, bestialidade e o abuso sexual de crianças".

13 Alguns dos elementos visuais usados na confecção da figura foram obtidos a partir do site https://freeicons.io/ utilizando uma licença aberta.

A Figura 3 ilustra um arquivo único (tabela ABCD no centro da imagem) que foi repartido, e cada partição está localizada em uma jurisdição diferente. Essa situação cria um impasse que depende da cooperação jurídica para sua solução. Entretanto, assim como ocorre com o exemplo anterior, a coordenação da ação de agentes estatais será essencial para que se obtenham todas as partições.

O motivo para tal está, novamente, no *timing* da ação. Caso o Arquivo A seja obtido no Brasil sem que sejam obtidos os Arquivos B, C e D, nas demais jurisdições, os responsáveis pela rede podem criar outras partições ou realocar os fragmentos já existentes para outros servidores. Essa situação fica ainda mais gravosa caso o arquivo que se busca obter (tabela ABCD) só interessar à instrução em sua integralidade – hipótese na qual a cooperação e a coordenação entre todas as jurisdições envolvidas são indispensáveis.

Tendo isso em mente, alguns sistemas já fazem uso de *sharding* e P2P em conjunto para criar sistemas distribuídos e com alto grau de segurança de arquivos – é o caso do Layr, um sistema de armazenamento de arquivos *online* e distribuído (BARNARD; LIANG; ALLARD, 2018). Vale ressaltar que esse tipo de recurso não se limita à partição de tabelas, também podendo ser usado para particionar imagens, vídeos e diversos outros tipos de arquivo.

A natureza distribuída dessa arquitetura de rede traz problemas para os quais o atual sistema de cooperação jurídica internacional não possui respostas satisfatórias. Por se tratar de sistemas distribuídos, não parece possível que o mero desenvolvimento de instrumentos bilaterais de assistência mútua seja suficiente. A resolução de ilícitos executados por redes distribuídas depende da cooperação coordenada entre diversas jurisdições, a qual, embora já tenha se mostrado possível (VAN LIEROP, 2020), precisa ser expandida e mais bem institucionalizada.

O que se extrai da situação e dos exemplos apresentados é a necessidade de cooperações amplas, multilaterais, coordenadas e orientadas a resultados. Esses valores entram em conflito com as críticas feitas ao *status quo* da cooperação jurídica internacional que é, por vezes, vista como lenta e ineficaz (VALENTE, 2020). Contudo, também não se mostram razoáveis propostas que privilegiem soluções unilaterais em detrimento da soberania de outros países (MADRUGA; FELDENS, 2016).

Sobre esse contexto, internacionalistas são deixados com uma árdua tarefa: encontrar modos de operacionalizar a prestação jurisdicional em um mundo que segue a arquitetura distribuída independentemente dos arranjos jurídicos. Vale salientar que essa tarefa precisa equilibrar, também, interesses estratégicos nacionais, além da proteção e do cuidado pelos direitos humanos (CARLETTI; GUERCIO, 2019).

CONCLUSÃO

O mundo das tecnologias e o mundo jurídico trabalham em velocidades diferentes. Enquanto as tecnologias objetivam ser cada vez mais disruptivas, a lei precisa se pautar em protocolos e garantias. Essa disparidade pode causar frustração com o *status quo*: crimes transnacionais sendo combatidos lentamente por meio de morosas cooperações. Contudo, vale lembrar que o processo e as garantias inerentes ao direito são essenciais para que um sistema jurídico seja legítimo, democrático e promova a justiça – principalmente ao se tratar do direito penal.

Os MLAT oferecem um caminho para que se operacionalize uma cooperação jurídica e, portanto, proporcionam uma maneira de prosseguir às diligências necessárias ao processo enquanto se mantém o respeito à soberania do país cooperante. Contudo, embora existam casos de sucesso, eles se devem à ação célere e coordenada entre jurisdições cooperantes. Os MLAT, nesse sentido, não são, *per se*, meios ineficazes de se obterem provas ou de se executarem diligências em territórios estrangeiros, mas o modo e o tempo no qual são operacionalizados pode ser ineficaz e esvaziar o sentido da cooperação.

Em assim sendo, para fazer com que a cooperação jurídica internacional seja eficaz em um mundo que emprega a arquitetura distribuída, alguns desafios precisam ser superados. A princípio, países devem ampliar a gama de jurisdições com as quais podem estabelecer cooperações, uma vez que arquivos circulam por diversos territórios. Dada a necessidade de essas atividades cooperativas serem coordenadas entre diversas jurisdições, faz sentido que entidades internacionais de grande alcance sejam responsáveis por operacionalizar esse arranjo. Por fim, também é necessário medir e monitorar o sucesso e o insucesso das cooperações em curso e estabelecer quais são os motivos que as fazem exitosas ou não. Sem atentar para esses desafios, é natural admitir que medidas unilaterais se tornem cada vez mais atrativas – em flagrante desrespeito às soberanias nacionais.

Em suma, cabe fazer algumas recomendações para o futuro dos MLAT – principalmente no contexto de crimes operacionalizados por redes distribuídas: (i) prestigiar soluções multilaterais para o estabelecimento de tratados de assistência legal mútua; (ii) incentivar e apoiar a criação de entidades de coordenação de atividades cooperativas com enfoque global; (iii) estimular a criação de meios de monitoramento e aferição de resultados das cooperações (ativas e passivas) em curso.

REFERÊNCIAS

BALDA, Praveen; GARG, Matish. Security Enhancement in Distributed Networking. **International Journal of Computer Science and Mobile Computing**, v. 4, n. 4, p. 761–767, abr. 2015. .

BARAN, Paul. **On Distributed Communications: I. Introduction to Distributed Communications Networks**, n. RM-3420-PR. Santa Monica: The RAND Corporation, ago. 1964. Disponível em: https://www.rand.org/pubs/research_memoranda/RM3420.html. Acesso em: 30 abr. 2021.

BARNARD, Dylan; LIANG, Florence; ALLARD, Tannr. Layr. 2018. **Layr - A decentralized cloud storage system**. Disponível em: http://layr-team.github.io/layr-project/. Acesso em: 9 maio 2021.

BRASIL. **Ação Declaratória de Constitucionalidade nº 51. Ministro Gilmar Mendes**. [*S. l.*: *s. n.*], 10 dez. 2020. Disponível em: https://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5320379. Acesso em: 12 maio 2021.

BRASIL. Acordos Bilaterais. 2021a. **Ministério da Justiça e Segurança Pública**. Disponível em: https://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais/acordos-bilaterais-1. Acesso em: 12 maio 2021.

BRASIL. Acordos Multilaterais. 2021b. **Ministério da Justiça e Segurança Pública**. Disponível em: https://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais/acordos-multilaterais-1. Acesso em: 12 maio 2021.

BRASIL. Decreto nº 5.015, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. 12 mar. 2004. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em: 13 maio 2021.

BRASIL. **Manual de Cooperação Jurídica Internacional: Matéria Penal e Recuperação de Ativos**. 4. ed. Brasília: Ministério da Justiça, 2019. Disponível em: https://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/manual-penal-online-final-2.pdf. Acesso em: 11 maio 2021.

BRENNAN, Margaret; HAMMOND, Sean. A methodology for profiling paraphilic interest in Child Sexual Exploitation Material users on peer-to-peer networks. **Journal of Sexual Aggression**, v. 23, n. 1, p. 90–103, 2 jan. 2017. https://doi.org/10.1080/13552600.2016.1241308.

BRENNER, Susan W.; SCHWERHA, Joseph J. Introduction—Cybercrime: A Note on International Issues. **Information Systems Frontiers**, v. 6, n. 2, p. 111–114, 1 jun. 2004. https://doi.org/10.1023/B:ISFI.0000025779.42497.30.

CARLETTI, Cristiana; GUERCIO, Laura. New Frontiers, New Actors, New Rules: Global Commons, Human Rights, Business. How to Improve Judicial Cooperation and International Development. **Boletim da Sociedade Brasileira de Direito Internacional**, v. 106, n. 141–145, p. 213–244, jun. 2019. .

CARREAU, Dominique; BICHARA, Jahyr-Philippe. **Direito Internacional**. 2. ed. Rio de Janeiro: Lumen Juris, 2016.

CEREZO, Ana I.; LOPEZ, Javier; PATEL, Ahmed. International Cooperation to Fight Transnational Cybercrime. *In*: SECOND INTERNATIONAL WORKSHOP ON DIGITAL FORENSICS AND INCIDENT ANALYSIS (WDFIA 2007), ago. 2007. **Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007)** [...]. Karlovassi: IEEE Computer Society, ago. 2007. p. 13–27. DOI 10.1109/WDFIA.2007.4299369. Disponível em: https://ieeexplore.ieee.org/abstract/document/4299369. Acesso em: 12 maio 2021.

CLEMENTINO, Marco Bruno Miranda. **A Cooperação Jurídica Internacional em Matéria Penal-Tributária como Instrumento de Repressão à Criminalidade Organizada Transnacional: Globalização e Novos Espaços de Juridicidade**. 2013. 375 f. Universidade Federal de Pernambuco, Recife, 2013. Disponível em: https://attena.ufpe.br/bitstream/123456789/11080/1/TESE%20Marco%20Bruno%20Miranda%20Clementino.pdf. Acesso em: 11 maio 2021.

EL KHATIB, Tamer Mahmoud Abd Ellatif Mahmoud. **Aspectos gerais dos Princípios da Territorialidade e Universalidade no ordenamento jurídico.** 1 dez. 2012. **Âmbito Jurídico**. Disponível em: https://ambitojuridico.com.br/cadernos/direito-tributario/aspectos-gerais-dos-principios-da-territorialidade-e-universalidade-no-ordenamento-juridico/. Acesso em: 13 maio 2021.

ERWIN, Philip O. The International Securities Enforcement Cooperation Act of 1990: Increasing International Cooperation in Extraterritorial Discovery? **Boston College International and Comparative Law Review**, v. 15, n. 3, p. 31, 1 ago. 1992. .

FETSCHERIN, Marc. Movie piracy on peer-to-peer networks—the case of KaZaA. **Telematics and Informatics**, Copyright: rights-holders, user and innovators. v. 22, n. 1, p. 57–70, 1 fev. 2005. https://doi.org/10.1016/j.tele.2004.06.005.

GIACOMET JUNIOR, Isalino Antonio. Como Elaborar um Pedido de Cooperação Jurídica Internacional em Matéria Penal. **Manual de Cooperação Jurídica Internacional: Matéria Penal e Recuperação de Ativos**. 4. ed. Brasília: Ministério da Justiça, 2019. p. 10–19. Disponível em: https://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/manual-penal-online-final-2.pdf. Acesso em: 11 maio 2021.

HUGHES, D.; WALKERDINE, J.; COULSON, G.; GIBSON, S. Peer-to-peer: is deviant behavior the norm on P2P file-sharing networks? **IEEE Distributed Systems Online**, v. 7, n. 2, fev. 2006. https://doi.org/10.1109/MDSO.2006.13.

JIA, Weijia; ZHOU, Wanlei. **Distributed network systems: from concepts to implementations**. New York: Springer, 2005. v. 15, (Network theory and applications, v. 15).

KAVITHA, D.; RAMALAKSHMI, R.; MURUGESWARI, R. The Detection and Mitigation of Distributed Denial-of-Service (DDOS) Attacks in Software Defined Networks using Distributed Controllers. *In*: 2019 IEEE INTERNATIONAL CONFERENCE ON CLEAN ENERGY AND ENERGY EFFICIENT ELECTRONICS CIRCUIT FOR SUSTAINABLE DEVELOPMENT (INCCES), dez. 2019. **2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES)** [...]. Krishnankoil: [*s. n.*], dez. 2019. p. 1–5. DOI 10.1109/INCCES47820.2019.9167698. Disponível em: https://doi.org/10.1109/INCCES47820.2019.9167698. Acesso em: 30 abr. 2021.

KIM, Jeeyoung. How Sharding Works. 5 dez. 2014. **Medium**. Disponível em: https://medium.com/@jeeyoungk/how-sharding-works-b4dec46b3f6. Acesso em: 30 abr. 2021.

MADRUGA, Antenor; FELDENS, Luciano. Dados eletrônicos e cooperação internacional: limites jurisdicionais. **Temas de Cooperação Internacional**. Coleção MPF Internacional. 2. ed. Brasília: Ministério Público Federal, 2016. p. 49–70. Disponível em: https://memorial.mpf.mp.br/cc/vitrine-virtual/publicacoes/temas-de-cooperacao-internacional-2a-edicao-revista-e-ampliada/view. Acesso em: 9 maio 2021.

MITNICK, Drew. **What's wrong with the system for cross-border access to data**. 25 abr. 2017. **Access Now**. Disponível em: https://www.accessnow.org/whats-wrong-system-cross-border-access-data/. Acesso em: 10 maio 2021.

MOONEY, Patrick; SAMANTA, Subarna; ZADEH, Ali. Napster and its Effects on the Music Industry: An Empirical Analysis. **Journal of Social Sciences**, v. 6, n. 3, p. 303–309, 1 jan. 2010. https://doi.org/10.3844/jssp.2010.303.309.

PINTO, Maira Arcoverde Barreto; OLIVEIRA, Diogo Pignataro de. A Venda Internacional de Dados Para Fins de Manipulação Eleitoral por Meio de Algoritmos: Um caso de interferência interestatal? In: Wagner Menezes. (Org.). **Direito Internacional em Expansão**. 1. ed. Belo Horizonte: Arraes Editores, 2019. v. XVI, p. 692–702.

SAHNI, Sanjeev P.; GUPTA, Indranath. Peer Group Association Promotes Digital Piracy. *In*: SAHNI, Sanjeev P.; GUPTA, Indranath (orgs.). **Piracy in the Digital Era: Psychosocial, Criminological and Cultural Factors**. Singapore: Springer, 2019. p. 81–97. DOI 10.1007/978-981-13-7173-8_6. Disponível em: https://doi.org/10.1007/978-981-13-7173-8_6. Acesso em: 9 maio 2021.

SCHOLLMEIER, R. A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications. *In*: FIRST INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING, 1., 1 ago. 2001. **Proceedings First International Conference on Peer-to-Peer Computing** [...]. Linköping: IEEE Computer Society, 1 ago. 2001. v. 1, p. 0101–0101. DOI 10.1109/P2P.2001.990434. Disponível em: https://www.computer.org/csdl/proceedings-article/p2p/2001/15030101/12OmNxecS94. Acesso em: 30 abr. 2021.

SIEBER, Ulrich. Legal Order in a Global World – The Development of a Fragmented System of National, International, and Private Norms –. **Max Planck Yearbook of United Nations Law Online**, v. 14, n. 1, p. 1–49, 2010. https://doi.org/10.1163/18757413-90000048.

STF. ADC 51 - Audiência Pública sobre Controle de Dados de Usuários por Provedores de Internet no Exterior. p. 242, 10 fev. 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf. Acesso em: 12 maio 2021.

SUSE. Computer Cluster. 2021. **SUSE**. Disponível em: https://susedefines.suse.com/definition/computer-cluster/. Acesso em: 30 abr. 2021.

SUTHERLAND, Philip F. The Use of the Letter of Request (Or Letter Rogatory) for the Purpose of Obtaining Evidence for Proceedings in England and Abroad. **The International and Comparative Law Quarterly**, v. 31, n. 4, p. 784–839, 1982. .

US DEPARTMENT OF STATE. **2014 International Narcotics Control Strategy Report: Volume II**, n. INCSR 2014. Washington, DC: Bureau for International Narcotics and Law Enforcement Affairs, mar. 2014. Disponível em: https://2009-2017.state.gov/documents/organization/222880.pdf. Acesso em: 12 maio 2021.

VALENTE, Fernanda. Para Moro, cooperação jurídica com EUA para produzir provas é muito demorada. 10 fev. 2020. **Consultor Jurídico**. Disponível em: https://www.conjur.com.br/2020-fev-10/cooperacao-juridica-eua-produzir-provas-demorada. Acesso em: 9 maio 2021.

VAN LIEROP, Ton. New major crackdown on one of the biggest online piracy groups in the world: international coordination led by Eurojust | Eurojust | European Union Agency for Criminal Justice Cooperation. 26 ago. 2020. **EuroJust**. Disponível em: https://www.eurojust.europa.eu/new-major-crackdown-one-biggest-online-piracy-groups-world-international-coordination-led-eurojust. Acesso em: 10 maio 2021.

VAN VOORN, Jan. **Recognition Letter - MPA**. [*S. l.*: *s. n.*], 10 jun. 2020. Disponível em: https://www.eurojust.europa.eu/sites/default/files/2020-06/2020-06-10_Recognition-letter-MPA.pdf. Acesso em: 13 maio 2021.