AGOSTO, 2021

O anteprojeto da LGPD Penal e as regras sobre transferência internacional de dados pessoais

AUTORES

Mario Viola
Leonardo Heringer
Celina Carvalho

EDITORAÇÃO E REVISÃO

Celina Bottino
Christian Perrone

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

ITS
Instituto
de Tecnologia
& Sociedade
do Rio

SUMÁRIO

RESUMO EXECUTIVO	**PG. 1**
INTRODUÇÃO	**PG. 2**
1. O TRATAMENTO DE DADOS PARA FINS DE PERSECUÇÃO PENAL E SEGURANÇA PÚBLICA: A CRIAÇÃO DE NOVO MARCO LEGAL PENAL	**PG. 4**
2. A TRANSFERÊNCIA INTERNACIONAL DE DADOS NO ANTEPROJETO DA LGPD PENAL	**PG. 6**
2.1. O regime jurídico da Diretiva 680/2016	PG. 6
3. MECANISMOS DE TRANSFERÊNCIA INTERNACIONAL DE DADOS E A LGPD PENAL	**PG. 9**
3.1. Decisão de adequação	PG. 10
3.1.1. O processo para a obtenção da decisão de adequação	PG. 11
3.2. Garantias adequadas de proteção	PG.13
3.3. As derrogações específicas	PG. 14
4. DISCUSSÕES E CONTROVÉRSIAS ATUAIS	**PG. 15**
4.1. A Convenção de Budapeste	PG. 15
4.2. ADC 51 e o Acesso a Dados no Exterior	PG.16
CONCLUSÃO	**PG.18**
SOBRE OS AUTORES	**PG.20**
NOTAS	**PG.21**

RESUMO EXECUTIVO

Em um mundo globalizado, onde o fenômeno de Internet das Coisas (*internet of things*) está cada vez mais potencializado, as complexas interações entre territórios exigem cooperação internacional e trocas cada vez mais constantes de informações. Especialmente no âmbito criminal, as autoridades se vêm afetadas diretamente: a investigação e repressão do crime depende cada vez mais da possibilidade de coletar, acessar e transferir informações e dados pessoais mantidos por empresas fora das fronteiras nacionais. Por exemplo, durante o andamento da Operação Lava Jato, ferramentas nesse sentido foram amplamente utilizadas. De forma geral, em matéria penal, os pedidos de cooperação jurídica foram endereçados a 52 países diferentes[1]. O instituto da transferência internacional é, portanto, necessário para possibilitar que um país solicite alguma medida a outro, como, por exemplo, a obtenção de provas.

No intuito de explorar a matéria, o **objetivo** deste relatório é analisar a tutela do ordenamento jurídico brasileiro do instituto da transferência internacional de dados pessoais com foco em investigações criminais e segurança pública. Para tanto, o presente estudo será dividido em **quatro** partes: ***(i)*** exame do tratamento de dados para fins de persecução penal e segurança pública no Brasil e o advento de um novo marco legal penal; ***(ii)*** análise comparativa da transferência internacional de dados no âmbito do regime jurídico europeu em relação ao anteprojeto de **Lei de Proteção de Dados para segurança pública e persecução penal ("LGPD Penal")** submetido no dia 5 de novembro de 2020 à Câmara dos Deputados; ***(iii)*** analisar os mecanismos previstos de transferência internacional de dados no novo anteprojeto penal; ***(iv)*** tecer breves considerações a respeito de controvérsias e discussões atuais que impactam diretamente a matéria estudada, como a possível ratificação da Convenção de Budapeste e o julgamento da Ação Direta de Constitucionalidade nº 51.

A partir dessa análise, espera-se estabelecer o estado da arte do tratamento das transferências internacionais de dados dentro do microssistema de tratamento de dados para fins de segurança pública e investigação criminal. Com o intuito de endossar a implementação de um sistema eficaz de persecução da segurança pública e garantia da proteção de dados, também cumpre o papel de trazer atenção a questões que merecem maior reflexão durante o processo legislativo de maturação do anteprojeto LGPD Penal. Assim, o relatório apresenta aspectos positivos da adoção de soluções que reflitam a lógica internacional de bilateralidade e cooperação mútua. Como se verá, respostas estruturadas bilateralmente e que considerem a interoperabilidade de sistemas e regimes jurídicos parecem ser um caminho interessante a ser explorado.

INTRODUÇÃO

Os fluxos internacionais de dados são hoje uma realidade nos diferentes setores, desde o privado até o público. A natureza global e sem fronteiras obrigatórias do espaço digital permite que inúmeros serviços sejam prestados à distância ou que partes dos mesmos sejam desenvolvidos através de cadeias internacionais que envolvem a transferência internacional de dados. Enviar um e-mail, adentrar uma videoconferência, pedir refeições em serviços de delivery, ou até utilizar sistemas de GPS para se locomover, todas essas atividades podem se beneficiar desse caráter internacional da internet. Nesse sentido, dados do Banco Mundial indicam que 3,000,000,000,000 gigabytes (GB) circulam globalmente através da internet. Isso equivale a 32 Gb por mês e por pessoa de dados, mais de 1 Gb por dia ou 325 milhões de casas assistindo vídeos em "streaming" simultaneamente.[2]

A tendência, portanto, é a circulação transfronteiriça de dados. Em muitos aspectos, os fluxos internacionais de dados podem ser considerados parte do tecido que sustenta a economia global.[3] A OCDE, por exemplo já afirmou que "*cross-border data flows have increased economic efficiency and productivity, raising welfare and standards of living.*"[4]

Evidentemente que, se por um lado, o mundo hiperconectado trás vantagens econômicas, por outro, torna a tutela da proteção de dados mais complexa. Existem claros riscos no que tange a segurança dos dados, mas também quanto à privacidade.[5] Não se trata só da regulação realizada por um ordenamento jurídico, há pelo menos duas jurisdições envolvidas, já que ocorre a exportação e importação de dados. Há a necessidade, então, de ajustes legais que facilitem essa relação e permitam fluxos seguros de dados.

Nesse sentido, nasce a necessidade de regular adequadamente a transferência internacional de dados quando aplicada às múltiplas atividades que acabam envolvendo esses fluxos transfronteiriços.[6] A segurança pública e investigação criminal acabam ganhando uma dimensão diferente nesse contexto. Hoje é possível que se esteja investigando um crime ocorrido no Brasil, planejado por brasileiros com vítimas brasileiras, mas que dados relevantes para solucioná-lo estejam no exterior, pois o serviço utilizado para orquestrá-lo, por exemplo, armazena dados em outro país.

O legislador brasileiro, atentou-se para as peculiaridades desse cenário. Na construção da Lei Geral de Proteção de Dados ("LGPD"), preferiu deixar de fora o tratamento de dados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais[7]. Designou um sistema diferenciado, outra normativa específica, para tanto. Hoje tem-se o anteprojeto dessa normativa, intitulado como "LGPD Penal".

O sistema europeu, também possui uma dupla normativa, o Regulamento Europeu de Proteção de Dados (conhecida pela sigla "GDPR")[8] e a Diretiva 680/2016[9] que trata de proteção de dados para fins de segurança pública e investigação criminal.[10]

Sendo assim, no que tange também as transferências internacionais de dados podem existir sistemas específicos que buscam regular esses fluxos internacionais de dados para fins de investigações criminais. Essa especificidade justifica uma análise pormenorizada do sistema proposto no anteprojeto "LGPD Penal" brasileiro para verificar a sua compatibilidade com outros sistemas, mormente o europeu.

No primeiro capítulo do presente relatório, iremos tratar da construção de um novo marco legal penal para endereçar o tratamento de dados para fins de persecução penal e segurança pública no Brasil. Será feita uma análise crítica de como a lacuna legislativa pode deixar o agente estatal sem orientações apropriadas em sua atividade de investigação, tal como pode causar prejuízos à proteção dos direitos dos titulares.

No segundo capítulo, passa-se à análise comparativa da transferência internacional de dados no âmbito do regime jurídico europeu em relação ao anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal ("LGPD Penal"). O intuito é comparar a proposta brasileira com o regime jurídico da Diretiva 680/2016 da União Europeia, apreciando a lógica que esteve por trás da construção do modelo europeu.

Na sequência, o capítulo terceiro avalia os mecanismos de transferência internacional de dados previstos no novo anteprojeto penal, quais sejam: a decisão de adequação e o processo para a sua obtenção; as garantias adequadas de proteção; e as derrogações específicas. O relatório busca discutir esses mecanismos à luz da experiência internacional no uso deles ao decorrer dos anos.

Ao final, traça-se considerações sobre discussões atuais que surtem efeito direto na matéria estudada, como a possível ratificação da Convenção de Budapeste e o julgamento da Ação Direta de Constitucionalidade nº 51. O objetivo é apresentar uma visão holística do estado atual das reflexões sobre transferência internacional de dados para os fins de segurança pública, com o fim de orientar a maturação do tema no âmbito nacional.

1. O TRATAMENTO DE DADOS PARA FINS DE PERSECUÇÃO PENAL E SEGURANÇA PÚBLICA: A CRIAÇÃO DE NOVO MARCO LEGAL PENAL

Os incrementos tecnológicos dos últimos anos criaram modelos sofisticados de tratamentos de dados pessoais. A chamada *data-driven society*, uma sociedade orientada por dados, em que no uso de serviços de empresas, no campo da comunicação, do comércio, do turismo ou entretenimento, sujeita-se ao tratamento de dados. Garantir a proteção de dados do indivíduo é fundamental nesse contexto.

Além de zelar pela intimidade e privacidade, a proteção de dados pessoais protege o indivíduo de atos ilegítimos advindos desse grande volume de informações. Veja-se, dados pessoais podem ser utilizados para os mais diversos cibercrimes, que conforme destacado em reunião do G7[11], representam ameaça global[12]. Práticas de *phishing*[13], *identity theft*[14], dentre outras, são cada vez mais comuns e os casos de vazamentos de dados mais emblemáticos. Como consequência, as vítimas desses ataques ficam sujeitas a situações ainda mais perigosas, como, por exemplo, estelionato. Assim, garantir segurança pública e proteção de direitos das vítimas depende justamente do tratamento de dados pessoais[15].

Ocorre que, no intuito de promover a segurança pública e investigação criminal, a troca de informações, na era da comunicação, passa a ser medida essencial de inteligência para o controle da atividade criminosa[16]. O acesso a dados pessoais pelas chamadas *law enforcement agencies* (agentes de cumprimento da lei) pode servir para a elucidação de crimes e a prevenção de delitos violentos, inclusive o terrorismo, ou extremamente repugnantes, como a violência sexual contra menores na Internet. Frisa-se que o raciocínio é aplicável tanto a crimes cibernéticos, mas também a infrações que fora desse escopo, mas que para reunir o arcabouço probatório necessário é indispensável recorrer às informações obtidas por provedores e servidores.

A lógica exposta evidencia a necessidade de regras que equilibrem os interesses postos na relação: os direitos dos titulares e a necessidade de investigação do agente estatal. Nesse sentido, as atuais regras de proteção de dados podem não ser apropriadas para orientar o agente estatal em sua atividade de investigação ou segurança pública. Há a necessidade que se proteja os direitos dos titulares (precipuamente sua privacidade) e, ao mesmo tempo, possibilitar que se atinja os objetivos finais dos agentes públicos envolvidos.

Para exemplificar os questionamentos que poderão surgir da falta de regras precisas sobre os tratamentos de dados no âmbito da persecução penal, basta termos em mente os desafios jurisprudenciais existentes quanto à admissibilidade da prova obtida através de interceptação telefônica antes do advento da Lei nº 9.296/96. Entendia-se, à época, que nem mesmo a autorização judicial (reserva de jurisdição) era capaz de validar essa prova, dada a inexistência de legislação regulamentando-a. A reserva de lei é que deveria reger a atividade dos agentes públicos, impedindo de agir sem lei específica que autorizasse a ação.

Em julgado do Supremo Tribunal Federal, por exemplo, tem-se que *"sem a edição de lei definidora das hipóteses e da forma indicada no art. 5º, inc. XII, da Constituição não pode o Juiz autorizar a interceptação de comunicação telefônica para fins de investigação criminal"*.[17]

Essa situação, ilustra o que a falta de uma lei para regulamentar a ação estatal pode impactar no exercício da atividade de agentes públicos. Similar, então, é a situação da proteção de dados pessoais no contexto analisado, pois na falta de uma norma específica, tem-se insegurança jurídica que pode prejudicar não apenas o indivíduo, mas o interesse público, porque *"o Estado também tem a obrigação de utilizar, diligentemente, todos os meios à sua disposição para realizar uma investigação, dentro de um prazo razoável, que sirva de base para o processamento, o esclarecimento dos fatos, o julgamento e a sanção dos autores"*.[18]

No que tange a prevenção e repressão à criminalidade, na situação atual de fluxos internacionais de dados, em que as provas - dados eletrônicos - podem estar em outros países, a concertação de ações estatais, particularmente pela via da cooperação jurídica internacional, exige a transferência internacional de dados pessoais. Neste particular, como adverte o professor Vladmir Aras, que também é membro do Ministério Público Federal e já ocupou o cargo de secretário de cooperação internacional da Procuradoria Geral da República (PGR), a falta de uma lei nacional versando sobre proteção de dados pessoais em matéria penal já vem prejudicando a atuação do Estado brasileiro no combate à criminalidade.[19]

Conforme elucida o professor, "o Estado brasileiro enfrenta dificuldades para obter acesso a dados de cidadãos europeus ou de estrangeiros residentes na União Europeia, quando tais dados são necessários à segurança pública, ao controle migratório ou à persecução criminal no Brasil". Ainda, destaca a articulação da Polícia Federal com a Europol[20] que exigiu a formalização de acordo específico entre o Brasil e o Serviço Europeu de Polícia para atividades de inteligência estratégica, conduto, **sem a possibilidade de transferência de dados pessoais**[21].

Em resumo, para que sejam respeitados os direitos fundamentais do indivíduo e, ao mesmo tempo, não seja inviabilizado o exercício do poder/dever estatal de prevenir, investigar e reprimir atos criminosos, é importante que exista uma lei que regule os tratamentos de dados pessoais para fins de segurança pública e persecução penal. Mais particularmente sobre o tema desta análise, é preciso que esta normativa defina as regras que deverão nortear as transferências de dados pessoais.

É justamente para elaborar um anteprojeto de lei com esse fim que o então Presidente da Câmara dos Deputados, entendendo "que os órgãos de segurança pública e de investigação e repressão de infrações penais não podem prescindir de uma legislação que assegure a circulação de dados pessoais entre autoridades", expediu, em novembro de 2019, ato[22] instituindo uma comissão de juristas. Também justificou a edição do ato, dentre outros motivos, o entendimento de que "dados pessoais traduzem projeção da personalidade do indivíduo, seu

tratamento por meio de ferramentas de tecnologia da informação deve sempre observar a preservação da privacidade dos cidadãos, tanto o mais quando o risco recai sobre o *status libertatis*."

Após um ano de trabalho, a comissão de juristas entregou o anteprojeto de lei de proteção de dados para segurança pública e persecução penal, que ficou conhecido como LGPD Penal.

2. A TRANSFERÊNCIA INTERNACIONAL DE DADOS NO ANTEPROJETO DA LGPD PENAL

Como visto, de forma semelhante ao modelo europeu, a LGPD[23] excluiu do seu escopo a sua aplicação ao tratamento de dados realizados para os fins de segurança pública (art. 4, III, LGPD). Em ambos regimes, a saída encontrada foi previsão de norma específica para regulamentar a proteção e transferência de dados pessoais para fins de persecução penal.

No que diz respeito à transferência internacional de dados pessoais[24], tem estrutura e conteúdo inspirados na já mencionada Diretiva UE 680/2016 (*Law Enforcement Directive*, "LED")[25], concebidos a partir da compreensão de que **"a construção de uma arquitetura regulatória compatível com modelos internacionais amplia as capacidades de integração e parcerias a nível internacional do Brasil."**[26]

Em linhas gerais, o regulamento europeu, GDPR[27], também permite a transferência de dados[28] quando se reconhece que o ordenamento jurídico do país recipiente oferece nível de proteção adequado, ou quando o controlador dispõe de salvaguardas apropriadas. Contudo, como se adiantou, a transmissão de dados para fins de persecução penal entre países regidos pelo GDPR e outros deverá observar a normativa específica. Assim, na Diretiva (EU) 680/2016 existe uma estrutura específica para transferências internacionais.

2.1. O regime jurídico da Diretiva 680/2016

O regime da Diretiva 680/2016 é baseado na lógica de que a coleta e tratamento de dados voltados à segurança pública devem seguir um regime específico. Nos termos do "item" (4) da exposição de motivos, a livre circulação de dados pessoais entre as autoridades competentes para efeitos de prevenção e investigação deve ser facilitada, de forma a assegurar simultaneamente um elevado nível de proteção de dados pessoais e a atividade a ser realizada pelo agente. A fluidez desse intercâmbio de dados é crítico para garantir a eficácia em matéria penal no que tange à cooperação policial, conforme o "item" (7) da exposição de motivos.

Veja-se, se no âmbito de uma investigação penal as autoridades competentes fossem obrigadas a buscar o consentimento do titular para realizar o tratamento, este poderia representar óbice à própria eficiência na manutenção da ordem e segurança pública. Assim, a saída encontrada pela Diretiva é estabelecer que a segurança de dados pessoais no domínio da cooperação jurídica em matéria penal e da cooperação policial assenta-se em garantir que as autoridades estran-

geiras e/ou organismos internacionais dispensarão aos dados compartilhados o mesmo nível de proteção e tratamento que lhes é dispensado pelas autoridades que os detêm.[29]

Sob esse raciocínio, a normativa estabelece três mecanismos disponíveis para efetuar a transferência internacional de dados (art. 35, d):

- **Decisão de adequação**, que reconhece no país terceiro, no organismo internacional ou em um ou mais setores específicos desse país terceiro um nível de proteção de dados pessoais adequado.
- **Oferecimento de garantias adequadas** para a proteção mediante um instrumento juridicamente vinculativo.
- **Derrogação das regras da diretiva** no caso de situações específicas: se a transferência for necessária para proteger interesses vitais do titular dos dados e/ou seus legítimos interesses, para prevenir ameaça iminente e grave contra a segurança pública de um Estado-membro ou país terceiro, e em outros em que haja justificativa, inclusive exercício ou defesa de um direito num processo judicial.

A lógica do dispositivo é de prescrever múltiplas possibilidades para facilitar a transferência para esses fins. Aqui tem-se um sistema de comportas, em que dados pessoais só devem sair da UE (abrem-se as comportas) através de um desses três mecanismos.[30]

O primeiro mecanismo conecta países com sistemas de proteção de dados - nesse contexto de segurança pública e persecução criminal - essencialmente equivalentes. De fato, no Considerando 67 da Diretiva, os seguintes pontos que devem ser avaliados para a concessão de uma decisão de adequação:

A adoção de uma decisão de adequação relativa a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias de assegurar um nível adequado de proteção, essencialmente equivalente ao assegurado na União, em particular quando os dados são tratados num ou em vários setores específicos. Em especial, o país terceiro deverá garantir o controle efetivo e independente da proteção dos dados e estabelecer mecanismos de cooperação com as autoridades s de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.[31]

Nesse sentido, o que permite a transferência internacional é uma decisão prévia da Comissão Europeia que estabelece que o país (ou o setor) para o qual se transfere dados tem esse grau de proteção equivalente. O mecanismo visa a relação entre os Estados e não a relação específica entre as partes a que transfere e a que recebe dados.

Percebe-se que essa situação se modifica na falta de uma decisão de adequação. A interação entre as partes ganha destaque, pois nos outros meca-

nismos as “comportas” para a saída dos dados pessoais somente se abrem se existem garantias específicas ou a situação permite - seja porque há uma diminuição do risco para o titular, seja porque as exigências do interesse público o demandam.

No segundo mecanismo, então, tem-se que os agentes públicos do país que necessita dos dados, podem apresentar garantias *adequadas* para a transferência, nos termos do art. 37 do regulamento[32]. Por último, na falta de ambos, confere-se a transferência se foram aplicáveis as derrogações a situações específicas, na forma do art. 38 do diploma.

Diante disso, a norma busca conferir um certo espaço de adequação entre seu regime jurídico e dos países estrangeiros. Isso porque através de mecanismos, sejam as decisões de adequação, o oferecimento de garantias ou as derrogações, possibilitar-se-ia a transferência de dados para fins de persecução penal.

ica evidente o intuito do modelo europeu de conferir um espaço de adequação, quando comparado a outros países. Apenas a título exemplificativo, o Vietnã, para garantir a possibilidade de acesso a dados para esses fins, exige que empresas de telecomunicações *offshore* e provedores de serviços de Internet com mais de 10.000 usuários que tenham sedes ou escritórios de representação no Vietnã e armazenem dados pessoais de usuários de Vietnã dentro do país.[33] A lógica por trás do modelo é garantir que os dados fiquem suscetíveis a requerimentos das autoridades.[34]

Em sentido semelhante, o Projeto de Lei nº 4728/2020[35], que após análise técnica foi retirado pelo próprio autor, havia sido proposto para determinar que os dados pessoais dos brasileiros fossem armazenados e mantidos fisicamente em repositório situado em território nacional. Apesar da exigência buscar facilitar o *enforcement* das autoridades, obrigações como esta detém o potencial de comprometer o caráter global da rede e o desenvolvimento de serviços online [36].

A restrição adotada pelo país advém da tensão entre a necessidade dos países de implementar e garantir o *enforcement* de suas legislações nacionais frente ao caráter global da Internet. Nesse diapasão, países buscaram, por meio de previsões legais, ampliar o alcance territorial de suas jurisdições[37], ainda que a atividade de tratamento seja realizada por agente no exterior[38]. Não basta, todavia, haver a expansão da jurisdição no papel, sem ser possível a cooperação do país estrangeiro. Por esse motivo, especialistas apontam que acordos reginais podem ser mais eficazes, ao invés de leis unilateralmente impostas[39]. Nesse ponto, a Diretiva 680/2016 parece, de certa forma, fornecer mecanismos de adequação entre seu regime jurídico e o estrangeiro.

Cabe, por fim, ressaltar que a Diretiva 680/2016, assegurou a eficácia dos acordos internacionais de cooperação jurídica internacional em vigor que implicam a transferência internacional de dados pessoais até que sejam alterados, substituídos ou revogados.[40] Essa disposição permite a continuidade da troca de informações no âmbito da cooperação policial e da cooperação judiciária interna-

cional,[41] mesmo na ausência de uma decisão de adequação e sem utilização dos outros dois mecanismos. Sublinha-se aqui que a interação para troca de provas entre países tende historicamente a ser feita através desses regimes especiais estabelecidos por tratados de cooperação jurídica internacional, como é o caso da Convenção sobre Cibercrime (Convenção de Budapeste) ou os tratados do sistema MLA (*"mutual legal assistance"* - acordos de assistência judicial mútua).

3. MECANISMOS DE TRANSFERÊNCIA INTERNACIONAL DE DADOS E A LGPD PENAL

Como mencionado anteriormente, o sistema de proteção de dados adotado no Brasil segue de certa forma o modelo europeu. Nesse sentido, as previsões do anteprojeto da LGPD Penal no que diz respeito à transferência internacional de dados ecoam lógica similar a da Diretiva 680/2016.

No que interessa a essa análise, as hipóteses para transferência internacional e cooperação internacional encontradas no art. 53, inciso II do diploma correspondem às mesmas apresentadas anteriormente, veja: ***(i)*** a obtenção de uma decisão de adequação; ***(ii)*** o oferecimento de garantias adequadas de proteção; e ***(iii)*** a incidência de derrogações excepcionais.

De fato, aproveitar-se da experiência internacional parece ser uma decisão acertada e que provavelmente irá facilitar que o Brasil esteja integrado aos principais fluxos internacionais de transferências de dados pessoais,[42] resultando (espera-se) em uma maior efetividade no combate ao crime em conjunto com uma proteção de direitos adequada. Esse, contudo, é apenas um dos aspectos a ser considerado.

Não é possível se desviar do ideal de que existe um desafio de adequação a ser analisado aqui. Até o presente momento, somente quatorze países possuem decisões de adequação nos termos do GDPR, tendo o Reino Unido se juntado a esse número apenas recentemente[43]. Dentre esses países, o Reino Unido foi o primeiro - e até agora único - que possui uma decisão de adequação[44] também para fins de segurança pública e investigação criminal, nos termos da Diretiva 680/2016, não apenas ao GDPR, como é o caso dos demais.

Cumpre indicar então que, mesmo com os mecanismos fornecidos e o espaço de adequação, garantir parâmetros mínimos e comuns entre as diferentes jurisdições é tarefa complexa. Ao se utilizar de bases similares a do modelo europeu - tanto no que tange ao GDPR como na Diretiva 680/2016, o ordenamento brasileiro parece dar um passo para facilitar os fluxos internacionais de dados, mas **não se pode ignorar que há um caminho a ser percorrido para garantir a efetividade desses mecanismos de adequação**.

A potencial integração com o sistema europeu de proteção de dados é um dos elementos nesse processo de participação nos fluxos internacionais de dados. Outro ponto é a estar compatível e/ou interoperável com os padrões internacionais de fluxos seguros e confiáveis de dados. Trata-se então de se tornar membro, por

exemplo, das estruturas da organização internacional OCDE ou mesmo de mecanismos de cooperação jurídica internacional como a Convenção de Budapeste.[45]

Nesse trajeto de compatibilização e interoperabilidade com outros sistemas de proteção de dados para fins de segurança pública e persecução criminal, deve-se ter claro que no centro da questão está o fato de a proteção de dados escudar diversos outros direitos (privacidade, intimidade, presunção de inocência, devido processo legal etc) - o que impõe um dever de abstenção estatal, que só pode tratar os dados pessoais em situações autorizadas em lei;[46] ao mesmo tempo, também que existe um dever de ação, no sentido de garantir a proteção dos dados que são tratados sob a sua responsabilidade.

O regramento sobre transferência internacional de dados pessoais previsto na LGPD Penal deve ser enxergado, portanto, como um meio de viabilizar a integração do Brasil aos fluxos de transferências internacionais, além de ser uma garantia de respeito aos direitos fundamentais dos cidadãos brasileiros e dos estrangeiros que vivem no país. O indivíduo não deve ser instrumentalizado em nome de atender interesses coletivos, por mais relevantes que estes sejam. Entende-se, portanto, que há ferramentas que podem auxiliar na harmonização entre o dever legítimo das autoridades com os direitos fundamentais dos indivíduos e o alcance global da Internet - sem desconsiderar as dificuldades de garantir a efetividade dessa.

A partir dessas premissas é que se passa à análise específica das supramencionadas hipóteses autorizativas do anteprojeto.

3.1. Decisão de adequação:

Do ponto de vista brasileiro, a decisão de adequação, que é de natureza administrativa e não jurisdicional, é o pronunciamento da autoridade brasileira de proteção de dados[47] que reconhece que um país estrangeiro ou uma organização internacional oferece nível de proteção compatível (não necessariamente idêntico[48]) àquele que é conferido pelo Direito Interno. Trata-se de uma permissão ampla, que permite que a transferência internacional de dados, desde que devidamente justificada, ocorra sem a necessidade de oferecimento de garantias e sem precisar de uma autorização específica para cada transferência. É, de certo modo, equivalente a que se estivesse ocorrendo um compartilhamento interno.

As transferências de dados pessoais baseadas em decisão de adequação estão disciplinadas da seguinte forma no anteprojeto:

> Art. 54. A transferência de dados pessoais para um país estrangeiro ou para uma organização internacional pode ser efetuada com base em **decisão de adequação** que determine que aquele país, território ou uma de suas unidades subnacionais, ou a organização internacional destinatária, asseguram nível de proteção adequado.

> § 1º A transferência de dados pessoais com base em decisão de adequação deve observar o artigo 34 da Lei nº 13.709/2018 e dispensa autorização específica, sem prejuízo dos demais requisitos legais.
> § 2º O Conselho Nacional de Justiça poderá estabelecer procedimento simplificado para a tomada de decisão sobre o nível de adequação de um país, quando este for um Estado Parte da Convenção do Conselho da Europa, de 1981 (CETS 108) e de seus protocolos.
> § 3º Os atos do Conselho Nacional de Justiça que revoguem, alterem ou suspendam a decisão de adequação não prejudicam as transferências de dados pessoais para outro país, território ou uma unidade subnacional, ou para organização internacional, quando efetuadas nos termos dos artigos 55 e 56.

Como se percebe, uma decisão de adequação deve ser precedida de uma análise baseada nos critérios previamente estabelecidos pela lei. Para entendermos os critérios que deverão ser considerados pela autoridade brasileira de proteção de dados nessa análise, temos que observar a remissão do anteprojeto[49] feita ao artigo 34 da LGPD[50]. Ou seja, será preciso avaliar ***(i)*** a legislação vigente no país de destino ou no organismo internacional; ***(ii)*** a natureza dos dados que se pretende transferir; ***(iii)*** a observância dos princípios gerais e os direitos dos titulares previstos no ordenamento brasileiro; ***(iv)*** a adoção de determinadas medidas segurança; ***(v)*** a existência de garantias judiciais e institucionais que assegurem o respeito aos direitos de proteção de dados; e ***(vi)*** outras circunstâncias específicas.

Embora de modo bem menos detalhado, esses critérios são semelhantes aos indicados na Diretiva UE 680/2016[51].

Outro aspecto importante a esclarecer é que a decisão de adequação não é imutável. Ela está sujeita à revogação, alteração ou suspensão, o que, claro, sempre precisará ser devidamente motivado. A grande questão aqui é a preservação das circunstâncias de proteção equivalente. Pode ser que a decisão de adequação já não mais se mantenha, devido a mudanças.

Dessa forma, então, que a transferência internacional de dados pessoais fundada em uma decisão de adequação deve significar para o titular dos dados pessoais a garantia de que os seus dados receberão proteção equivalente a que lhe é dispensada pelo direito interno. Por outro lado, para a autoridade responsável pelo tratamento representará a permissão de transferência de dados sem a necessidade de oferecimento de garantia ou de autorização específica, desde que, é claro, haja um fundamento jurídico válido.

3.1.1. O processo para a obtenção da decisão de adequação

Quando analisado na prática, sob a ótica do ordenamento europeu, o processo até a decisão de adequação pode ser efetivamente complexo. Basta notar que a Diretiva, em vigor desde o ano de 2016, tão somente teve a primeira decisão de adequação em 28 de junho de 2021. Como já mencionado, e, em relação ao

GDPR, somente quatorze países possuem decisões de adequação. Qual seria o motivo da dificuldade de obter uma decisão de adequação?

Um primeiro elemento é que nem todos os países possuem os padrões de proteção de dados semelhantes. A decisão de adequação considera justamente a equivalência desses padrões em relação ao sistema europeu, ou seja, se são "adequados". Com isso, o conceito "ser adequado" precisou ser esclarecido pelo Tribunal de Justiça da União Europeia (*Court of Justice of the European Union*, "TJUE").

Em 2015, no julgamento do caso *Maximillian Schrems v. Data Protection Commissioner (Ireland) ('Schrems')*[52], o TJUE invalidou o acordo entre os EUA e a UE, alterando o padrão do que representava a adequação.[53] Prevalecia então a interpretação de que um país terceiro oferecesse nível de proteção semelhante.

O TJUE no julgamento do Caso *Schrems* I considerou que, embora a legislação de um país não tenha de ser idêntica à legislação da UE para ser considerada adequada, deve assegurar um nível de proteção dos dados pessoais e dos direitos dos titulares dos dados que seja «essencialmente equivalente» ao garantido na UE. Posteriormente, com a entrada em vigor do GDPR, essa definição foi codificada no Considerando 104 (*Recital 104*)[54] do Regulamento.

Nesse sentido, o *European Data Protection Board*, publicou Recomendações 01/2021 sobre o referencial de adequação sob a Diretiva 680/2016[55], segundo o qual a interpretação sobre o conceito de "nível adequado de proteção", conforme especificado nos entendimentos do Tribunal de Justiça da União Europeia no caso *Schrems* I, deve ser "essencialmente equivalente ao garantido na UE". De forma que, os meios aos quais o país pode recorrer para o fim de alcançar tal nível de proteção pode diferir daqueles empregados dentro da União Europeia, todavia, na prática, esses meios devem se revelar eficazes[56].

Como consequência, a análise da adequação passa a ser mais rígida e não se limita a verificar a legislação e jurisprudência do país. Em suma, a adequação pode ser alcançada por meio de uma combinação de direitos para os titulares dos dados e obrigações daqueles que processam os dados ou que exercem controle sobre esse processamento e supervisão por órgãos independentes. No entanto, as regras de proteção de dados só são eficazes se forem aplicáveis e seguidas na prática. É, portanto, necessário considerar não apenas o conteúdo das regras aplicáveis aos dados pessoais transferidos, mas também o sistema em vigor para garantir a eficácia de tais regras. Assim, mecanismos que garantam cumprimento (mecanismos de *"enforcement"*) eficientes são de suma importância para a eficácia das regras de proteção de dados.[57]

Como se vê, a prática europeia indica que o processo de adequação envolve elementos complexos. Para o contexto brasileiro, compreender as consequências práticas advindas da legislação é fundamental, quando se tem um ordenamento cuja fonte é similar e, especialmente, tendo em vista o anteprojeto da LGPD Penal.

A partir da experiência internacional, quais seriam os mecanismos que poderiam ser implementados para facilitar um eventual processo de adequação? O texto proposto à Câmara remete a observância do art. 34 da LGPD e foca na atuação do Conselho Nacional de Justiça - como autoridade de supervisão - para estabelecer os referidos atos de adequação.

Cumpre mencionar que, apesar das disposições do art. 34 serem similares ao ordenamento europeu, são relativamente menos detalhadas. Em linhas gerais, a Diretiva UE 680/2016 exige a necessidade de analisar ***(i)*** o Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais; ***(ii)*** existência e o funcionamento efetivo de uma ou mais autoridades de controlo independentes no país; e ***(iii)*** os compromissos internacionais assumidos pelo país. Ainda assim, persistem os desafios a implementação e frequentemente as transferências ocorrerem por meio do oferecimento de garantias adequadas de proteção de dados, objeto de análise do item 4.2.

Nesse sentido, tem-se duas consequências práticas. Enquanto não estiver em voga o sistema proposto no anteprojeto, há uma zona cinzenta sobre as regras específicas para a possibilidade de envio de dados pessoais para o exterior. Mas, de fato, não é possível a estruturação de zonas seguras de transferências internacionais de dados pessoais através de decisões de adequação, sendo necessário recorrer a outros institutos. Mais relevante do ponto de vista das autoridades brasileiras de segurança pública e persecução criminal é que se torna mais complexo requerer a instauração de processos para a decisão de adequação, particularmente quanto ao sistema europeu: primeiro, por dificilmente cumprir com o elemento de equivalência; e, segundo, o interesse em uma decisão mútua de adequação diminui, por não ser difícil estabelecer a reciprocidade.

3.2. Garantias adequadas de proteção

Quando não for possível obter uma decisão de adequação, a transferência internacional de dados pessoais poderá se basear no oferecimento de garantias de que os dados transferidos serão adequadamente protegidos. Nesse caso, diferentemente do que ocorre quando há uma decisão de adequação, não se tem uma autorização ampla para o fluxo de dados. As transferências são controladas e devem se limitar aos **tipos de dados, às partes e às finalidades previamente ajustadas em um instrumento juridicamente vinculativo; se tiverem sido avaliadas pelo agente responsável.**

Eis a forma como o anteprojeto disciplina a questão, as condições para a transferência internacional são indicadas nos incisos do art. 55, que dispõe tanto sobre a necessidade de instrumento juridicamente vinculativo, ou da avaliação de um agente responsável a respeito das circunstâncias referentes à transferência no sentido de estabelecer essa garantia.

Mais especificamente, a transferência internacional de dados justificada no oferecimento de garantias exige do **agente responsável pelo tratamento a avaliação quanto às circunstâncias da transferência e a suficiência (adequação) das garantias existentes**. Ao agente responsável pelo tratamento também é atribuída

a obrigação de manter o registro documental das transferências realizadas (art. 55, §2º). O que se estabelece é uma análise específica de uma "adequação" das circunstâncias, tendo em vista garantias existentes.

Essas medidas devem ser entendidas como salvaguardas que, somadas às garantias adequadas, irão estabelecer um ambiente de efetiva proteção para os dados pessoais transferidos.

A respeito do dispositivo, cabe tecer comentários sobre um ponto em particular: há uma ausência de referência sobre a *forma* do oferecimento de garantia adequada. No geral, ainda que se reconheça a relevância de deixar espaços para serem ajustados ou preenchidos no processo de implementação, por outro lado, gera um grau de incerteza até que a autoridade competente aborde os devidos pontos e esclareça os parâmetros aceitáveis. Considerando a complexidade envolvendo a decisão de adequação, faz-se importante métodos claros e seguros para a eficiência das garantias.

Vale notar que, em comparação à LGPD, o anteprojeto oferece poucos detalhes a respeito dessas opções de garantias adequadas. Ao estabelecer a possibilidade de transferência internacional de dados quando forem oferecidas garantias adequadas, a LGPD indica as formas para que isso seja feito; quais sejam: cláusulas contratuais – padrão ou específicas –, normas corporativas globais, ou selos, certificados e códigos de conduta regularmente emitidos.

Esse ponto é especialmente importante quando comparado a experiência europeia. Uma das críticas direcionadas à hipótese de oferecimento de garantias adequadas é que podem ser insuficientes para a proteção dos direitos fundamentais. No âmbito da hipótese de avaliação, as garantias parecem receber pouco escrutínio em comparação com as decisões de adequação, devido à quantidade reduzida de avaliações *ex ante* ou *ex post*. Sem a referida avaliação, há um receio de que autoridades de segurança pública (*"law enforcement"*) poderiam ficar sob pressão para autorizar transferências, mesmo sem as devidas salvaguardas presentes. O receio é de que interesses possam ficar mais alinhados para permitir ou facilitar investigações do que proteger os direitos dos titulares.

Desse ponto de vista, vale ressaltar que fica a encargo da autoridade estabelecer estruturas formais com os parâmetros a serem seguidos, as quais devem ser enquadradas por si só como salvaguardas e garantias. Além de ser importante restar clara a responsabilidade para auferir essas salvaguardas e garantias.

3.3. As derrogações específicas

Não havendo uma decisão de adequação e mesmo não havendo uma oferta de garantias, o anteprojeto da LGPD Penal contempla a possibilidade de ocorrerem transferências internacionais, quando atender *relevante interesse público ou individual*. E mesmo nessas situações, será preciso levar em consideração os direitos, as liberdades e as garantias fundamentais do titular dos dados.

O regramento proposto pelo anteprojeto contemplou as seguintes hipóteses de derrogação em seu art. 56: (i) para proteger os *interesses vitais* do titu-

lar dos dados ou de outra pessoa; (ii) para salvaguardar os *legítimos interesses do titular* dos dados; (iii) para *prevenir uma ameaça imediata e grave* contra a segurança pública no Brasil ou em país estrangeiro; (iv) em casos específicos, para exercer *direitos de defesa* no âmbito de processo judicial ou administrativo punitivo, sem prejuízo das demais exigências legais; ou (v) em casos específicos, para a *cooperação jurídica internacional*, de acordo com regras e instrumentos de direito internacional.

Ainda que se verifiquem os fundamentos previstos no inciso IV, os dados pessoais não serão transferidos se a autoridade competente para proceder à transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados em causa prevalecem sobre as finalidades que motivariam a transferência por interesse público.

As transferências de dados efetuadas com base neste artigo serão limitadas aos dados *estritamente necessários* para a finalidade almejada. Princípio este de caráter fundamental com origem na base do pensamento de minimizar o tratamento de dados pessoais.

A previsão dessas hipóteses de derrogação é muito importante para contornar barreiras que poderiam ser intransponíveis e levariam a uma aplicação desarrazoada do Direito. Em nome da proteção dos dados pessoais, poder-se-ia estar prejudicando outros direitos. Nesses casos, sempre excepcionais, aplica-se a autorização legal para viabilizar a transferência internacional dos dados.

É preciso, contudo, que essas regras de derrogação sejam aplicadas de modo parcimonioso. **São exceções à regra geral de proteção de dados e não podem ser usadas de modo irresponsável**. A lógica para as derrogações seria idealmente para situações de menor potencial de dano. A banalização do uso dessa permissão legal poderá fragilizar o sistema de proteção de dados.

Novamente, a atuação da autoridade de supervisão será fundamental para determinar os casos específicos em que seria possível e apropriado o uso dessa exceção. O importante de se notar é que sem a aprovação desse anteprojeto, há também nesses casos uma situação lacunar em que atualmente, em sentido estrito, somente os instrumentos diplomáticos ou de cooperação jurídica internacional é que dão base legal para transferências internacionais de dados.

4. DISCUSSÕES E CONTROVÉRSIAS ATUAIS

Em paralelo à discussão do anteprojeto da LGPD Penal, há também dois pontos relevantes para a temática das transferências internacionais no Brasil: ***(i)*** a possível ratificação da Convenção Budapeste e ***(ii)*** o julgamento Ação Direta de Constitucionalidade 51 (ADC 51).

4.1. A Convenção de Budapeste

A Convenção de Budapeste sobre Crimes Cibernéticos é um tratado internacional de direito penal e processual firmado no âmbito do Conselho da Europa. Com o objetivo de facilitar a cooperação internacional para o combate ao crime ciber-

nético, a Convenção prioriza "uma política de criminal comum com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço". Em dezembro de 2019, o Brasil foi convidado a aderir à Convenção[58]. Eventual adesão poderia proporcionar acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de tornar a cooperação jurídica internacional voltada à perseguição penal dos crimes cibernéticos mais efetiva.

Sob o regime estabelecido com a Convenção de Budapeste abrem-se novas formas de transferência internacional de dados para fins de investigações criminais por meio de cooperação jurídica internacional. A expectativa é que eventual adesão à convenção poderia garantir mais agilidade na transferência de provas relacionadas a crimes cibernéticos, assim como de provas eletrônicas. A complexidade que advém desse sistema está nas garantias e salvaguardas. Dentro dos sistemas de adequação mencionados acima, há uma garantia de proteção "equivalente". A Convenção não impõe a mesma regra.

Outro ponto relevante a ser mencionado é que nos sistemas previstos no anteprojeto, a transferência é regulada de um ponto de vista unilateral. Ou seja, o país só consegue regular de maneira definitiva um lado da equação, qual seja os requisitos para sair dados pessoais do país (abrir as comportas). Já a requisição do dado depende pelo menos em parte do ordenamento jurídico do outro país. No caso de mecanismos internacionais de cooperação jurídica como a Convenção de Budapeste, há uma regulação para tanto os requisitos de saída de ambos os lados - saída e requisição.[59]

4.2. ADC 51 e o Acesso a Dados no Exterior

Em 2017, foi interposta no Supremo Tribunal Federal, a Ação Direta de Constitucionalidade nº 51[60], ajuizada pela Federação das Associações das Empresas de Tecnologia da Informação ("ASSESPRO Nacional"). O objeto da ação busca a declaração da constitucionalidade do Decreto 3.810/2001[61], tratado bilateral de cooperação internacional entre o Brasil e o Estados Unidos em matéria penal (*"Mutual Legal Assistance Treaty", "*MLAT").

A ASSESPRO Nacional sustenta que as requisições de dados armazenados nos EUA devem ser requeridas por meio do MLAT.[62] Do outro lado há certas autoridades públicas brasileiras que sustentam que o mecanismo presente no MLAT não satisfaz as necessidades do processo penal, haja vista o tempo de demora (em média pelo menos 18 meses) para a resposta.

Em outras palavras, a discussão diz respeito à seguinte situação: no curso de uma investigação criminal, as autoridades brasileiras desejam ter acesso a um determinado dado. O dado em questão estaria sendo armazenado no exterior, usualmente em algum serviço de nuvem norte-americano.[63] De acordo com a legislação desse país, a entrega de dados, particularmente de conteúdo de comunicações, não é permitida de maneira direta e depende de autorização, usualmente pela via de procedimento presente em MLAT.[64] O pano de fundo para a ação é justamente esse contexto. De um lado há a exigência do MLAT para

realizar requisições de dados no exterior, do outro, tem-se recorrido à requisição direta frente às empresas estrangeiras sem o uso de instrumento de cooperação jurídica internacional.

Segundo dados do Departamento de Recuperação e Cooperação Jurídica Internacional (DRCI), os Estados Unidos são o 3º país mais demandado de pedidos de cooperação do Brasil. **Dentre os pedidos 97% são fundamentados no MLAT e 77,5% deixaram de ser atendidos**[65]. As razões para o não atendimento variam, mas destaca que de acordo com o Ministério da Justiça 59% das negativas são por questões jurídicas, não práticas.[66] Isso pode significar que a diferença entre o direito interno brasileiro e americano pode representar limitação para a cooperação internacional nesse caso.

De todo modo, como apresentado no relatório *Internet & Jurisdiction and ECLAC Regional Status Report 2020*[67], o Brasil não é o único país da região a apontar a baixa eficiência procedimental de acordos bilaterais de cooperação mútua.

É importante notar que a saída para a controvérsia posta deve contemplar os procedimentos acordados de direito internacional para garantir a sua operacionalidade de forma mais eficaz. Em referência direta ao Anteprojeto da LGPD Penal, em seu art. 55, inciso II, que dispõe sobre a cooperação internacional no domínio da proteção de dados pessoais, prevê tanto a relevância de prestar assistência mútua em matéria de aplicação da legislação de proteção de dados pessoais, como de manter a reserva das garantias adequadas para a proteção de dados pessoais e dos outros direitos e liberdades fundamentais.

Assim, o que está em jogo parece ser mais do que o reconhecimento da constitucionalidade do Decreto que incorpora o MLAT ao Direito pátrio. Logo percebe-se que a decisão na ADC nº 51 pode consolidar uma discussão como se dá na governança do acesso de dados no exterior no que tange às investigações criminais.

Conforme manifestação do ITS Rio em Audiência Pública da ADC nº 51[68], não se pode ignorar o elemento da interoperabilidade. O termo frequentemente utilizado na literatura de tecnologia da informação, pode ser aplicado sob a ótica de que as leis precisam se adequar a interoperabilidade do ciberespaço. Em matéria de Internet e Jurisdição, força-se o olhar para interoperabilidade de leis e a criação de ambiente de cooperação internacional.

O que o anteprojeto da LGPD Penal permite é estabelecer um marco para que o Brasil possa se adequar aos padrões de proteção de dados internacionais facilitando um fluxo seguro e legal de dados para segurança pública e persecução penal. Novamente, como mencionado acima, não substitui de todo a necessidade de cooperação jurídica internacional em matéria penal, mas permite um quadro de proteção, tanto dos direitos de cidadãos brasileiros (ou de estrangeiros que estão cobertos pela lei) no que tange a saída de dados para tratamento no exterior, quanto nos instrumentos possíveis internos para poder requerer dados do exterior para tratamento no país.

CONCLUSÃO

O texto do anteprojeto, lido como uma proposta de lei geral, logra, em grande parte, compatibilizar a disciplina de importantes conceitos e institutos difundidos na experiência internacional com a realidade brasileira. Citamos, a título de exemplo, a robusta base principiológica que regerá esse "microssistema legislativo de tratamento de dados para fins de segurança pública e de investigação criminal"[69] e as consistentes regras concernentes à segurança e o sigilo dos dados (art. 36 e seguintes).

Alguns outros pontos, todavia, merecem maior reflexão e deverão passar por aperfeiçoamentos no que tange a necessidade de especificações e detalhamento e inclusive da atuação de autoridade de supervisão.

No que diz respeito especificamente às regras sobre transferência internacional de dados, que são o objeto desta análise, o anteprojeto se mostra bastante consistente e alinhado aos melhores modelos internacionais, notadamente o europeu, o que tende a contribuir para a integração do Brasil nos fluxos internacionais de dados.

Ainda assim, aponta-se a importância de colher aprendizados também com as dificuldades encontradas pelo modelo europeu durante o processo das decisões de adequação. Não se pode esquecer que o Reino Unido foi o primeiro e - até o presente momento - único país a obter uma decisão de adequação no que concerne a Diretiva 680/2016. Essa dificuldade pode levar que se recorra às garantias de adequação e as derrogações. As últimas são principalmente idealizadas para circunstâncias excepcionais e que sujeitam os titulares a riscos

No decorrer da maturação do debate do Anteprojeto de Lei, implementar um sistema robusto e eficaz destinado à persecução da segurança pública pode ser importante para garantir uma adequada proteção de dados. Deve-se lembrar que as iniciativas voltadas a maior agilidade nos fluxos internacionais de dados para fins de segurança pública e persecução penal, devem considerar que soluções unilaterais que não se enquadram numa lógica internacional bilateral de transferências de dados podem ter um efeito contrário do desejado. Em vez de facilitar o acesso, além de desproteger os cidadãos brasileiros - por incentivar práticas unilaterais, que não necessariamente detém as mesmas garantias de direitos, também podem deixar o Brasil de fora dos principais meios de transferência possíveis.

Há aqui interesses em jogo de dois lados, tanto o de buscar mais acesso a dados com transferências internacionais para resolver os desafios da segurança pública e da persecução criminal, como o de proteger os direitos dos cidadãos brasileiros de acessos indevidos. Esses interesses são melhor atendidos através de procedimentos de transferência internacional bem estruturados e que permitam mecanismos de cooperação e interoperabilidade de sistemas.

Ainda que existam elementos que podem vir a ser ajustados no anteprojeto de LGPD Penal, os mecanismos apresentados são robustos e compatíveis em larga medida com as melhores práticas europeias. Deve, então, servir como ponto de partida de discussões sobre transferências internacionais de dados para fins de segurança pública e persecução criminal.

NOTAS

1. JÚNIOR, Isalino Antonio Giacomet. Cinco anos de Operação Lava Jato. Cooperação em Pauta.

2. Banco Mundial. World Development Report 2021. Disponível em: https://wdr2021.worldbank.org/stories/crossing-borders/.

3. (MCKINSEY GLOBAL INSTITUTE. Globalization in transition: the future of trade and value chains. Janeiro de 2019, p. 25. Disponível em: https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/%20Innovation/Globalization%20in%20transition%20The%20future%20of%20trade%20and%20value%20chains/MGI-Globalization%20in%20transition-The-future-of-trade-and-value-chains-Full-report.ashx).

4. OECD, Internet Economy 2012. Paper 143. *In* GSMA. Cross-Border Data Flows Enable the Digital Economy: An overview. 2017, p. 1.

5. OCDE, International agreements on cross-border data flows and international trade: A statistical analysis. Disponível em: https://www.oecd-ilibrary.org/docserver/b9be6cbf-en.pdf?expires=1625499177&id=id&accname=guest&checksum=3F8C2AABEF523358F6361141877A5AE2.

6. A estruturação legal das transferências internacionais de dados no geral é abordada em profundidade no Relatório do ITS Rio intitulado Transferência de Dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira.

7. Nesse sentido, confere-se a lógica do art. 4, III em consonância com o seu §1º. Veja-se:

"Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...)

III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou (...)

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

8. *General Data Protection Regulation*. Disponível em: https://gdpr-info.eu.

9. Diretiva (EU) 680/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX-%3A32016L0680.

10. No sistema do Reino Unido, por exemplo, ainda que se trate de uma só norma, o *Privacy Ac*t, este também segue a lógica do sistema da União Europeia com especificidades para o tratamento de dados para segurança pública e investigações criminais.

11. SOUZA, Ramon de. Pela primeira vez na história, G7 cita crime cibernético como ameaça global. The Hack. Disponível em: https://thehack.com.br/pela-primeira-vez-na-historia-g7-cita-crime-cibernetico-como-ameaca-global/.

12. https://thehack.com.br/pela-primeira-vez-na-historia-g7-cita-crime-cibernetico-como-ameaca-global/

13. A prática conhecida como *phishing* consiste em uma técnica de engenharia social utilizada para enganar usuários e obter informações confidenciais como nome de usuário, senha e detalhes do cartão de crédito.

14. *Identity theft* significa utilizar o nome e dados pessoais de outra pessoa para obter acesso à cartões de crédito e outros bens, ou mesmo às contas bancárias.

15 ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. *In* Proteção de dados pessoais e investigação criminal /Associação Nacional dos Procuradores da República, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores: Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. – Brasília: ANPR, 2020. p. 26. Disponível em http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf.

16. BITENCOURT, Cezar Roberto. Comentários à Lei de Organização Criminosa: Lei 12.850/2013. São Paulo: Saraiva, 2014. p. 108.

17. STF. HC 73.351, Rel. Min. Ilmar Galvão, Tribunal Pleno do Supremo Tribunal Federal, julgado em 09/05/1996, DJ 19/03/1999.

18. Trecho do voto proferido pelo Ministro Rogério Schietti Cruz, do Superior Tribunal de Justiça, no julgamento do Incidente de Deslocamento de Competência nº 24/DF. Disponível em https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Voto%20Ministro%20Schietti.pdf

19. ARAS, Vladimir. A título de introdução: segurança pública e investigações criminais na era da proteção de dados. *In* Proteção de dados pessoais e investigação criminal /Associação Nacional dos Procuradores da República, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores: Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. – Brasília: ANPR, 2020. p. 26. Disponível em http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf.

20. A Europol é um serviço Europeu de polícia, incumbido do tratamento e intercâmbio de informação criminal. Tem por missão contribuir para a aplicação das leis da União Europeia no âmbito do combate à criminalidade organizada.

21. Ver Art. 1º do Decreto 10.364/20,

22. Disponível em https://www2.camara.leg.br/legin/int/atoprt_sn/2019/atodopresiden-

te-58133-26-novembro-2019-789470-publicacao-original-159494-cd-presi.html#:~:text=Institui%20Comiss%C3%A3o%20de%20Juristas%20destinada,%22d%22%20da%20Lei%20n.

23. "A Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) teve a oportunidade de usufruir da evolução dos padrões normativos da União Europeia e da evolução havida desde as primeiras leis nacionais de proteção de dados pessoais. Assim, ela pode incorporar elementos que se tornaram desde a Diretiva 95/46/CE e que estão presentes no RGPD." (VERONESE, Alexandre. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. ***In*** Tratado de Proteção Dados Pessoais / coord. Gilmar Ferreira Mendes, Danilo Doneda, Ingo Wolfgang Salert e Otavio Luiz Rodrigues Jr. Rio de Janeiro. Forense, 2021. p. 716.)

24. O anteprojeto traz a seguinte definição para transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organização internacional. (art. 5º, XVI)

25. Ver em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680.

26. Trecho da exposição de motivos do anteprojeto da LGPD Penal.

27. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

28. GDPR, Art. 45. Disponível em: https://gdpr.algolia.com/pt/gdpr-article-45.

29. DOMINGOS, Fernanda Teixeira Souza.SILVA, Melissa Garcia Blagitz de Abreu e Silva. OLIVEIRA, Neide M. Cavalcanti Cardoso de. Transferência internacional de dados pessoais para fins de investigações criminais à luz das Leis de Proteção de Dados Pessoais.. ***In*** Proteção de dados pessoais e investigação criminal / Associação Nacional dos Procuradores da República, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores: Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. – Brasília: ANPR, 2020. p. 26. Disponível em http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf.

30. Deve-se entender que a regra é o fluxo seguro de dados. O que do ponto de vista da Europa e se verá que também do Brasil só se dá nos casos específicos previstos em lei em que os mecanismos garantem a proteção equivalente ou os riscos para os titulares são mínimos.

31. Tradução oficial em português de Portugal.

32. Diretiva (EU) 680/2016, art. 37. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680.

33. GSMA. Cross-Border Data Flows: Realising benefits and removing barriers. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Cross-Border-Data-Flows-Realising-benefits-and-removing-barriers_Sept-2018.pdf

34. Deve-se ter em mente que esse tipo de "localização forçada de dados" não ocorre só no Vietnã. Em diferentes momentos inclusive no Brasil se flertou com a possibilidade de obrigar a localização forçada de dados local. Felizmente, o sistema brasileiro optou por estar em consonância com o padrão internacional e permite fluxos internacionais de dados pessoais (saída e entrada).

35. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2263413.

36. https://www.jota.info/opiniao-e-analise/artigos/stf-deve-reconhecer-acordo-para-acesso-a-dados-no-exterior-13042021

37. NU. CEPAL. Internet & Jurisdiction and ECLAC Regional Status Report 2020. ECLAC, Novembro 2020. p. 99-100 Disponível em: https://www.cepal.org/en/publications/46421-internet-jurisdiction-and-eclac-regional-status-report-2020

38. O Marco Civil da Internet, por exemplo, garante o respeito à legislação brasileira em certas circunstâncias - ainda que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil, ***vide***: art. 11: "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (...)

§2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil."

39. https://repositorio.cepal.org/bitstream/handle/11362/46421/1/S1901092_en.pdf

40. Diretiva 680/2016: "Art. 61. Os acordos internacionais que impliquem a transferência de dados pessoaispara países terceiros ou para organizações internacionais, celebrados pelos Estados-membros antes de 6 de maio de 2016, e que sejam conformes com o direito da União tal como aplicável antes dessa data, continuam a vigorar até serem alterados, substituídos ou revogados."

41. DOMINGOS, Fernanda Teixeira Souza, SILVA, Melissa Garcia Blagitz de Abreu e Silva. OLIVEIRA, Neide M. Cavalcanti Cardoso de. Transferência internacional de dados pessoais para fins de investigações criminais à luz das Leis de Proteção de Dados Pessoais.. *In* Proteção de dados pessoais e investigação criminal / Associação Nacional dos Procuradores da República, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores: Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. – Brasília: ANPR, 2020. p. 26. Disponível em http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf.

42. Ao tratarmos das semelhanças entre as regras sobre transferência internacional de dados da LGPD e as vigentes na Europa, tivemos a oportunidade de tecer as seguintes considerações: **"**isso deve ser interpretado como algo extremamente positivo, especialmente por indicar a possibilidade de que haja, de maneira juridicamente segura, um aumento no fluxo de transferência de dados do Brasil para os países da União Europeia e vice-versa. E mais, essa similitude poderá servir para que o Brasil, que instituiu a LGPD mais recentemente, absorva experiências exitosas da União Europeia no que diz respeito à proteção de dados pessoais, podendo, futuramente, almejar o reconhecimento, por meio de uma decisão de adequação da Comissão da União Europeia, da qualidade do seu sistema jurídico de proteção de dados pessoais, isso a depender, é claro, do formato definitivo da Autoridade Nacional, ainda pendente de decisão pelo Congresso Nacional.**"** (VIOLA, Mario; HERINGER, Leonardo. Um olhar internacional: lei geral de proteção de dados pessoais (LGPD) e o general data protection regulation (GDPR), adequação e transferência internacional de dados. *In* Caderno Especial: Lei Geral de Proteção de Dados. Coord. Carlos Affonso Souza, Eduardo Magrani e Priscilla Silva. 1. ed. – São Paulo: Thomson Reuters Brasil. 2019. p. 238.

43. European Comission. Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection. European Comission. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

44. European Comission. Decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive. Disponível em: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-law-enforcement-directive_en.

45. A necessidade de cooperação nessa área advém justamente porque do ponto de vista comercial a circulação de dados é um fato. Já do ponto de vista da persecução penal, essa mesma circulação depende de fatores institucionais que não necessariamente estão presentes. Esta última pressupõe uma infraestrutura legal que, se não estiver presente, pode impedir o acesso a dados e a possibilidade de realizar as funções estatais necessárias.

46. Deve-se entender que nem todos os países entendem que proteção de dados é em si um direito fundamental. No entanto, há um crescente consenso de que a proteção de dados escuda direitos e é uma tendência emergente de que seja uma dimensão do direito à privacidade.

47. As decisões de adequação para as transferências internacionais baseadas na LGPD cabem à Autoridade Nacional de Proteção de Dados (ANPD). O anteprojeto indica, contudo, que essa competência caberá ao Conselho Nacional de Justiça (CNJ). Para não adentrarmos na controvérsia sobre essa questão e para facilitar a compreensão, empregamos a genérica expressão "autoridade brasileira de proteção de dados".

48. No âmbito europeu, o Tribunal de Justiça da União Europeia já teve a oportunidade de assentar que "É verdade que o termo «adequado» que figura no artigo 25°, n° 6, da Diretiva 95/46 **implica que não se pode exigir que um país terceiro assegure um nível de proteção idêntico ao garantido na ordem jurídica da União.** Porém, como o advogado geral salientou no n° 141 das suas conclusões, a expressão «nível de proteção adequado» deve ser entendida no sentido de que exige que esse país terceiro assegure efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União nos termos da Diretiva 95/46, lida à luz da Carta. Com efeito, na falta de uma exigência desta natureza, o objetivo referido no número anterior do presente acórdão seria ignorado. Além disso, o elevado nível de proteção garantido pela Diretiva 95/46, lida à luz da Carta, poderia ser facilmente contornado através de transferências de dados pessoais da União para países terceiros com vista ao seu tratamento nesses países." (Decisão do Processo C-362/1b bv 4)

49. O art. 54 do anteprojeto remete ao 34 da LGPD:

Art. 54. A transferência de dados pessoais para um país estrangeiro ou para uma organização internacional pode ser efetuada com base em decisão de adequação que determine que aquele país, território ou uma de suas unidades subnacionais, ou a organização internacional destinatária, asseguram nível de proteção adequado.

§1º A transferência de dados pessoais com base em decisão de adequação deve observar o artigo 34 da Lei nº 13.709/2018 e dispensa autorização específica, sem prejuízo dos demais requisitos legais.

50. Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração: I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II - a natureza dos dados; III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; IV - a adoção de medidas de segurança previstas em regulamento; V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI - outras circunstâncias específicas relativas à transferência.

51. GDPR, Artigo 36º. (...) 2. Ao avaliar a adequação do nível de proteção, a Comissão tem particularmente em conta os seguintes elementos:

a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação desta legislação, das regras de proteção de dados, das regras profissionais e das medidas de segurança relativas à proteção de dados, incluindo as regras para transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e meios efetivos de recurso administrativo e judicial para os titulares dos dados cujos dados pessoais sejam objeto de transferência;

b) A existência e o funcionamento efetivo de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e fazer cumprir as regras de proteção de dados e dotadas de poderes sancionatórios adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e por cooperar com as autoridades de controlo dos Estados-Membros; e

c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

52. Disponível em: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362.

53. Leva-se em consideração que a época do julgamento, tratava-se da Diretiva 95/46/EC. União Europeia. Diretiva 95/46/EC, 1995. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046.

54. GDPR, Recital 104. Disponível em: https://gdpr-text.com/pt/read/recital-104/.

55. European Data Protection Board. Recommendations 01/2021 on the adequacy referential

under the Law Enforcement Directive. EDPB, fev. 2021. Disponível em: https://dataprotection.gov.sk/uoou/sites/default/files/recommendations_on_the_adequacy_referential_under_the_law_enforcement_directive.pdf.

56. Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015, ECLI:EU:C:2015:650, §§73 and 74 (Schrems I).

57. European Data Protection Board. Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive. Fev., 2021. Disponível em: https://dataprotection.gov.sk/uoou/sites/default/files/recommendations_on_the_adequacy_referential_under_the_law_enforcement_directive.pdf. Acesso em: 05 jul. 2021.

58. Mais informações disponíveis em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica#:~:text=Também%20conhecida%20como%20”Convenção%20de,o%20combate%20ao%20crime%20cibernético.

59. Alguns pontos de cuidado com relação à convenção foram levantados no artigo: Os cuidados com a Convenção de Budapeste. Jota 8 de julho de 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021

60. Mais informações disponíveis em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379.

61. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm.

62. LAUX, Francisco de Mesquita.Direito à prova na internet, o julgamento da ADC 51 pelo STF e o alcance do MLAT. Jota. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/direito-a-prova-na-internet-o-julgamento-da-adc-51-pelo-stf-e-o-alcance-do-mlat-20022020

63. SOUZA, Carlos Affonso de. STF deve reconhecer acordo para acesso a dados no exterior. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/stf-deve-reconhecer-acordo-para-acesso-a-dados-no-exterior-13042021 .

64. Conforme dispõe o *Stored Communications Ac*t. Para mais informações: https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim

65. https://www.conjur.com.br/2018-mar-08/cooperacao-eua-quebra-sigilo-fracassa-77-vezes

66. https://www.conjur.com.br/2018-mar-08/cooperacao-eua-quebra-sigilo-fracassa-77-vezes

67. Economic Commission for Latin America and the Caribbean (ECLAC)/Internet & Jurisdiction Policy Network (I&JPN), Internet & Jurisdiction and ECLAC Regional Status Report 2020 (LC/TS.2020/141), Santiago, 2020. Disponível em: https://www.cepal.org/en/publications/46421-internet-jurisdiction-and-eclac-regional-status-report-202.

68. Mais informações sobre a Audiência Pública: https://www.youtube.com/watch?v=ljmyqU4jf5o.

69. Trecho extraído da exposição de motivos do anteprojeto da LGPD Penal.

SOBRE OS AUTORES

Mario Viola
Doutor em Direito pelo Instituto Universitário Europeu (Florença, Itália), Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro. É atualmente Pesquisador Associado do Centre for Media Pluralism and Media Freedom do Instituto Universitário Europeu e Consultor do Instituto de Tecnologia e Sociedade do Rio de Janeiro para os temas da privacidade e proteção de dados pessoais.

Leonardo Heringer
Advogado, sócio do escritório Borges e Schumacher Advogados.

Celina Carvalho
Pesquisadora na equipe de Direito e Tecnologia no ITS Rio. Advogada e Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-graduanda da Pós-Graduação de Direito Digital do ITS Rio.

Celina Bottino
Mestre em direitos humanos pela Universidade de Harvard. Foi pesquisadora da Human Rights Watch em Nova York. Supervisora da Clínica de Direitos Humanos da FGV Direito-Rio. Foi consultora da Clínica de Direitos Humanos de Harvard e pesquisadora do ISER. Diretora de projetos do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Christian Perrone
Pesquisador Fulbright (Universidade de Georgetown, EUA). Doutorando em Direito Internacional (UERJ); Mestre em Direito Internacional (L.L.M/Universidade de Cambridge, Reino Unido). Ex-Secretário da Comissão Jurídica Interamericana da OEA. Coordenador da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Esse relatório contou com o generoso
apoio financeiro do Reino Unido através
de programa *Digital Access*

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Acesse nossas redes

itsrio.org