Conflitos entre ordens públicas no espaço cibernético

Uma abordagem cosmopolita em resposta à sobreposição regulatória da internet

FILIPE ROCHA MARTINS SOARES
GUSTAVO FERREIRA RIBEIRO

Resumo: As peculiaridades do espaço cibernético criam entraves ao exercício do poder estatal, como o acesso a informações conectadas a mais de uma jurisdição. Entre as medidas adotadas pelos Estados para garantir esse acesso, figura a projeção de efeitos extraterritoriais de suas normas relativas à internet. Originam-se aí potenciais conflitos entre ordens públicas (acesso a dados *versus* privacidade), que impactam o funcionamento da rede mundial de computadores. A profusão e o embate entre regulações (*overregulation*), até o momento, não foram adequadamente equacionados pelos Estados. Como a resolução do problema depende do reconhecimento da impossibilidade de se dissociar a internet de seu caráter transnacional, é necessária uma abordagem cosmopolita. Por meio dela, a conjugação de critérios pessoais e territoriais para a determinação do *domicílio dos dados cibernéticos* oferece uma via de reflexão. Embora ainda em desenvolvimento, o domicílio dos dados passa a ser indicativo de que ordem pública deve prevalecer na hipótese de sobreposição regulatória.

Palavras-chave: Internet. Excesso de regulação. Extraterritorialidade. Domicílio dos dados.

1. Introdução

Recebido em 24/4/17
Aprovado em 9/5/17

Embora seja uma esfera na qual se desenvolvem interações aptas a gerar diversos efeitos jurídicos, o espaço cibernético não é condicionado unicamente pelas leis que se aplicam ao comportamento no âmbito

físico, de maior tangibilidade. A título de exemplo: torna-se possível limitar, numa velocidade até há pouco inimaginável, a capacidade estatal de acessar o conteúdo de informações – seja pela dispersão do armazenamento de dados em diferentes jurisdições, seja pelo emprego de ferramentas de criptografia.

Os Estados reagem a esse fenômeno por meio da regulação. Ao fazê-lo, buscam reverter o processo de perda do monopólio da capacidade de estabelecer os cânones pelos quais se pautará o espaço cibernético. No entanto, não é raro que imponham barreiras ao desenvolvimento tecnológico e comercial propiciado pela internet.

A extrapolação dos limites territoriais das próprias leis é uma das formas como esses entraves se concretizam. Redigidas sob o impulso de garantir a aplicação da lei local sobre eventos transnacionais, normas de caráter extraterritorial ocasionam conflitos regulatórios. Caracteriza-se, então, o excesso de regulação (*overregulation*)[1], que tem o potencial de desvirtuar a estrutura e o funcionamento da internet. Ao imporem regras inexoráveis com o fim de garantir o acesso às informações, corre-se o risco de as regulações transformarem uma rede global em múltiplas redes fragmentadas[2].

Tome-se o exemplo do Brasil, onde o principal estatuto que disciplina o tema é o Marco Civil da Internet (MCI) (Lei nº 12.965/2014). Em seu artigo 11, o MCI estabelece que:

> 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

[1] Os termos *overregulation*, "excesso de regulação" ou "sobrerregulação" têm sentido econômico e são transpostos e explicados no contexto transnacional. Por exemplo, imagine-se que cada país, na condição de ator racional (DUNOFF; TRACHTMAN, 1999), almeja obter para si o benefício de acesso integral aos dados cibernéticos – por razões de defesa nacional, segurança pública ou por interesses econômicos –, prevendo que o prejuízo sistêmico seria diluído entre todos os demais atores. A atitude, contudo, seria replicada à medida que os demais países passassem a enfrentar dificuldades para acessar dados cibernéticos e proteger as informações de seus cidadãos. No mesmo sentido, Guzman (2001, p. 906-908). Encontram-se ainda, na literatura (KOHL, 2015, p. 54), comparações entre essa sucessão de acontecimentos que ocorrem relativamente ao domínio cibernético com a lógica da tragédia dos comuns (HARDIN, 1968). No entanto, considera-se que, apesar da semelhança entre os acontecimentos, sobretudo se considerados os potenciais efeitos danosos, o problema descrito neste artigo não reflete com precisão o fenômeno da tragédia dos comuns. O elemento da "rivalidade" do bem a se esgotar não é percebido com relação aos dados cibernéticos; ao contrário, é possível a sua replicação em caráter infinito. A comparação com a tragédia dos comuns, todavia, é útil para expor como comportamentos egoísticos podem afetar gravemente recursos transnacionais.

[2] No final desse processo, caso não se reverta a tendência, cada país terá uma versão própria da internet, com diferentes serviços, sites e plataformas disponíveis a seus cidadãos. As limitações à produção e difusão de conhecimentos, e as perdas econômicas decorrentes das dificuldades impostas à atuação global das empresas prestadoras de serviços na internet seriam as mais evidentes manifestações deste retrocesso. Nesse sentido: Daskal (2015, p. 333) e Wu (2006, p. 287).

> 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.
>
> § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 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 (BRASIL, 2014).

A norma brasileira foi redigida de modo a fazer com que as regras locais incidam sobre a maior quantidade possível de fenômenos com algum tipo de contato com o território nacional. Caso não sejam atendidas solicitações de autoridades locais para o acesso aos referidos dados, proíbe-se o funcionamento de determinados serviços, impõem-se multas a empresas que não conseguem adequar-se às normas locais e estrangeiras simultaneamente ou criam-se limitações aos fluxos de dados. O legislador, no entanto, negligenciou a hipótese de tal vínculo ser frágil, limitado ou mais diretamente conectado a uma norma estrangeira, conforme se exporá adiante.

Essa opção não é exclusiva do Direito brasileiro. Paira, sobre o domínio cibernético, uma tensão permanente que decorre da intenção de regular um fenômeno global sob perspectivas exclusivamente locais[3]. O problema manifesta-se por meio de normas ou decisões, como se mencionou, nas quais se almeja simultaneamente (i) forçar a aplicação de normas locais sobre outros Estados e (ii) rechaçar a incidência de leis estrangeiras localmente. Assim, tem-se observado a projeção extraterritorial de regras nacionais que visam a garantir o acesso estatal a dados alojados na nuvem cibernética[4] cumulada com a imposição das proteções à privacidade asseguradas pelos respectivos ordenamentos.

---

[3] Os Estados Unidos impõem severas restrições ao compartilhamento de dados armazenados em servidores de informática situados naquele país. Rússia, China e Irã aprovaram, entre 2014 e 2016, leis que obrigam prestadores de serviços de internet a armazenarem dados cibernéticos em seus respectivos territórios. A União Europeia somente autoriza a transferência de dados de cidadãos dos países integrantes do bloco para países que assegurem "adequado nível de proteção" ou que demonstrem "garantias suficientes de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respectivos direitos" (UNIÃO EUROPEIA, 1995).

[4] O instituto estatal de padrões e tecnologia dos Estados Unidos (*National Institute of Standards and Technology – NIST*) formulou uma definição de "computação na nuvem" amplamente aceita pela doutrina: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (MELL; GRANCE, 2011).

Ao tentar impor as próprias regras à comunidade internacional, Estados ignoram que os demais talvez estejam a fazer o mesmo movimento. Ao mesmo tempo, ao se portarem de maneira intransigente quanto à aplicação de suas leis de privacidade, os Estados repelem ambições de outros países de acessarem dados em seu território. Interessa-lhes, portanto, projetar a própria ordem pública para além de suas fronteiras, mas não em mão dupla: obstrui-se que outros países o façam sobre seus respectivos territórios.

O exclusivo recurso ao critério territorial para a determinação do direito aplicável parece, então, inadequado às interações ocorridas no domínio cibernético. As normas de proteção à privacidade não se estenderiam a uma jurisdição estrangeira, a não ser que houvesse a aquiescência do outro Estado soberano para isso[5]. Além disso, a pretensão de acesso é neutralizada tanto pela inexistência de capacidade executória das normas locais em território estrangeiro quanto pelas leis de proteção do país onde os dados estiverem armazenados.

Assim, não será resolvido com arrimo no parâmetro territorial o embate entre o interesse de acesso a dados que causem efeitos sobre determinado território e as normas limitadoras do país onde tais informações se encontrem alojadas. É preciso que se busquem soluções cosmopolitas, por meio das quais se avaliem os vínculos e as repercussões dos dados sobre cada país afetado; pode-se indagar, por exemplo, sobre o verdadeiro "domicílio" da informação cobiçada pelo poder público.

[5] "The first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention" (COUR PERMANENTE DE JUSTICE INTERNATIONALE, 1927).

Na primeira parte deste artigo, apresentar-se-ão as razões pelas quais se acredita em que a internet apresenta novos desafios ao Direito; por isso, eventual solução ao impasse apresentado deve fundar-se nessa constatação. Em seguida, analisar-se-á mais detidamente a norma introduzida no ordenamento jurídico brasileiro pelo artigo 11 do MCI e suas consequências. Ao final, defender-se-á uma solução que garanta a integridade da internet, com base no "domicílio" da informação.

2. Por que a internet é diferente?

Conflitos regulatórios são uma realidade bastante antiga; normalmente, decorrem das diferenças de interesses e de alinhamento de incentivos entre as nações quando confrontadas com problemas transnacionais. O compartilhamento de um curso de água, por exemplo, pode levar a um embate. Normas de um país mais tolerante com o despejo de resíduos no manancial podem colidir com as de outro, cujo direito é intransigente quanto à poluição, e que sofre os efeitos das ações desencadeadas no território lindeiro.

Quando se pensa na regulação do acesso a dados bancários em transações internacionais, em essência, o problema é similar ao descrito acima: os interesses de proteção às informações de alguns países colidem com os anseios de acesso aos dados de outros. As soluções adotadas são diversas, a depender do nível da relação entre o país que detém o dado e aquele interessado em obtê-lo. Uma possível solução envolve a cooperação internacional nessa matéria.

Logo, indaga-se: como os Estados se comportam quando se deparam com problema semelhante relativamente à esfera cibernética? Por que, em vez de recorrerem a modelos cooperativos, amparados pelo Direito

Internacional, alguns países almejam, nesse caso, promover a projeção extraterritorial de suas ordens públicas?

A resposta reside exatamente nas peculiaridades que diferenciam os dados cibernéticos. Antes de apresentá-las, entretanto, convém rememorar um importante debate travado à época da popularização inicial da internet, que traz implicações significativas para a regulação de tais peculiaridades.

Simultaneamente à disseminação da rede mundial de computadores, surgiu, na década de 1990, um movimento acadêmico que buscava explicar o novo fenômeno sob uma perspectiva jurídica. Passou-se a utilizar, nos Estados Unidos, termos como *cyberlaw* e *law of cyberspace*.

Easterbrook (1996) provocou alvoroço entre os teóricos dessa nascente disciplina ao afirmar que a criação de um *direito cibernético* seria tão inócua quanto a de um "*direito do cavalo*"[6]. A analogia proposta pelo autor representa o fato de que, sob sua óptica, a internet não teria abalado suficientemente os pressupostos jurídicos a ponto de ser necessária a criação de uma nova disciplina para estudá-la. Nesse sentido, aspectos teóricos atinentes a matérias como obrigações, propriedade, dano ou jurisdição seriam igualmente aplicáveis ao domínio cibernético e à criação e comércio de cavalos.

Lessig (1999) foi de encontro à provocação de Easterbrook com argumentos que, desde então, têm sustentado o desenvolvimento de um *direito cibernético*. No mundo físico, quatro mecanismos regulariam as condutas humanas: as leis, as regras sociais, o mercado e a "arquitetura". Esta representaria a disposição das coisas tal como se encontram. A passagem de um rio, o posicionamento de uma rodovia ou a localização de um prédio impõem balizas ao comportamento humano que geram consequências jurídicas: o rio pode dividir duas cidades; a rodovia, conectá-las; e o local onde se instala um prédio pode ser fator determinante da proeminência de uma instituição pública que nele se instale[7].

A "arquitetura" do espaço cibernético é o elemento que faria da criação humana algo diferenciado. Afinal, trata-se de todo um universo, com potenciais efeitos no âmbito físico, estruturado por linhas de código desenvolvidas para dar forma a essa realidade. A maleabilidade dos códigos e a possibilidade de adaptá-los aos interesses de desenvolvedores tornam o espaço cibernético efetivamente peculiar. O fato de essa inovação ocorrer numa área em que os fluxos de dados são extremamente velozes e a matéria-prima básica é imaterial gera uma série de

[6] O autor empregou a expressão *law of the horse*.

[7] Lessig utiliza como exemplo a Corte Constitucional alemã, situada em Karlsruhe, o que limita a influência dos poderes estabelecidos em Berlim sobre a mais alta Corte daquele país.

repercussões jurídicas que lhe são características e que não se observariam no mundo físico.

Em suma, para Lessig:

> O código, ou os softwares e hardwares que fazem do espaço cibernético o que ele é, constitui um conjunto de restrições sobre o comportamento. A substância destas restrições varia – o espaço cibernético não é um lugar apenas. Mas o que distingue as restrições arquitetônicas de outras é a forma como elas são vivenciadas. Assim como em relação às restrições da arquitetura no espaço real […] elas são vivenciadas como condições para o acesso a áreas do espaço cibernético. Tais condições, entretanto, são diferentes. Em alguns locais, é necessário inserir uma senha antes de se obter acesso; em outros, é possível acessar com ou sem identificação. Em alguns locais, as transações realizadas deixam vestígios que possibilitam a identificação dos envolvidos; em outros locais, este vínculo só existe se houver consenso expresso. Em alguns locais, é possível empregar um idioma que apenas o receptor entenderá (por meio da criptografia); em outros, a criptografia não é uma opção. O código determina estas características; elas são escolhidas pelos programadores; elas restringem algum comportamento (por exemplo, vigilância técnica) ao possibilitarem outro (criptografia). Elas incorporam certos valores, ou impossibilitam a concretização de outros. Neste sentido, estas características do espaço cibernético também regulam, tanto quanto a arquitetura no espaço real (1999, p. 508-509, tradução nossa)[8].

Em vista dos objetivos deste artigo, que se propõe a versar sobre o embate regulatório transnacional decorrente de sua delimitação pelos Estados, uma primeira implicação jurídica das constatações acima decorre da forma como o código determina a dinâmica dos fluxos de dados. Em face da velocidade e da facilidade com que as informações podem transitar pela infraestrutura da internet[9], esta arquitetura é es-

[8] No original: "The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave. The substance of these constraints varies — cyberspace is not one place. But what distinguishes the architectural constraints from other constraints is how they are experienced. As with the constraints of architecture in real space […] they are experienced as conditions on one's access to areas of cyberspace. The conditions, however, are different. In some places, one must enter a password before one gains access; in other places, one can enter whether identified or not. In some places, the transactions that one engages in produce traces, or 'mouse droppings', that link the transactions back to the individual; in other places, this link is achieved only if the individual consents. In some places, one can elect to speak a language that only the recipient can understand (through encryption); in other places, encryption is not an option. Code sets these features; they are features selected by code writers; they constrain some behavior (for example, electronic eavesdropping) by making other behavior possible (encryption). They embed certain values, or they make the realization of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates."

[9] A denominação "dados cibernéticos" aplica-se a códigos informáticos aptos a transmitir determinadas informações. Como tal, sua manifestação física se dá na forma de ondas eletromagnéticas, que se deslocam à velocidade da luz.

truturada de modo que os dados trafeguem pelas rotas menos congestionadas. Isso possibilita maior estabilidade e celeridade à rede; ao mesmo tempo, faz que o fluxo de dados não ocorra, necessariamente, sob um padrão retilíneo.

Assim, a título de exemplo, uma mensagem eletrônica enviada de Brasília para um receptor em Caracas poderá trafegar por diversos outros países, apesar de envolver interlocutores situados em países fronteiriços. A consequência jurídica desse fenômeno é a possibilidade de cada um desses locais onde o dado trafega almejar – adotando exclusivamente um critério territorial – o acesso ou o domínio sobre a informação, a despeito da eventual existência de regras de proteção à privacidade tanto no local de origem quanto no destino.

Retome-se a análise da legislação brasileira. Uma interpretação literal do citado artigo 11 do MCI não permitiria concluir ser possível o acesso, por autoridades brasileiras, a um dado que meramente trafega por cabo situado em território nacional. Prevê-se a aplicação da lei brasileira relativamente a operações de "coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações" (BRASIL, 2014).

Entre as ações previstas na norma, *tratamento* é aquela cuja definição aparenta ser a menos intuitiva[10]. O conceito foi, então, delineado pela via regulamentar (Decreto nº 8.771/2016):

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
>
> I – dado pessoal – dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e
>
> II – tratamento de dados pessoais – toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2016)[11].

---

[10] Foi travado, por exemplo, entre a Google e a autoridade francesa de proteção de dados um extenso debate sobre a definição de *tratamento*, ao fim do qual a segunda optou por impor uma multa à primeira por descumprir a lei francesa. Nesse caso, a Google defendia que não promovia o tratamento de dados de cidadãos franceses em território francês; por isso, a empresa estaria sujeita às leis estadunidenses. Logo, o debate ocorreu em torno do conceito. A decisão da *Commission nationale de l'informatique et des libertés* é bastante didática, e está disponível em: <https://www.cnil.fr/sites/default/files/typo/document/D2013-420_Sanction_Google.pdf>. Acesso em: 30 jan. 2017.

[11] É interessante notar a grande semelhança entre o Decreto brasileiro e a lei francesa que trata do tema (Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés): "Article 2 […] Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que

Da mesma forma como o legislador procedeu quanto ao MCI, optou-se no regulamento pela adoção de fórmula ampla que possibilitasse o enquadramento de diversos fenômenos num mesmo conceito. Assim, combinando-se os dois dispositivos (art. 11 do MCI e art. 14, II, do Decreto nº 8.771/2016), não parece disparatada a hipótese de que seria cabível a aplicação da lei brasileira relativamente a um dado cibernético que meramente trafegasse pelo território nacional. Nesse caso, ocorreriam ações como as de *recepção*, *transmissão* ou *distribuição*, previstas no decreto, o que materializaria o fenômeno do *tratamento*. Isso, nos termos do artigo 11 do MCI, imporia a aplicação da lei brasileira.

A situação descrita seria menos problemática se o Brasil estivesse isolado em sua postura. No entanto, a prática é disseminada, especialmente entre países dotados de capacidades técnicas avançadas, os quais são capazes de diferenciar dados produzidos por seus cidadãos daqueles pertencentes a estrangeiros e promovem a filtragem automática dos conteúdos. Não raro, o Estado tem acesso direto às informações, independentemente de controle judicial[12].

Parte da reação à vigilância, promovida sobretudo por potências mundiais, consiste justamente na tentativa de imposição unilateral da própria lei – inclusive com efeitos extraterritoriais. Outra estratégia – no momento em discussão pelo Brasil, mas já efetivada em muitos países – é a aprovação de rigorosas normas de proteção à privacidade, que estabelecem condições limitadoras dos fluxos internacionais de dados. Por fim, discutem-se regras de nacionalização de centros de armazenamento de dados, de modo que as informações de cidadãos de determinado país sejam obrigatoriamente alojadas em terminais situados em seu território. Conforme exposto, em gradações diferentes, Irã, Rússia e China já impuseram normas dessa natureza.

Eis, então, o círculo vicioso: o interesse simultâneo em acesso e proteção é encetado tanto pela necessidade de garantia da segurança pública e defesa nacional quanto pela intenção de repelir aspirações estrangeiras de acesso a informações produzidas ou armazenadas localmente.

---

soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction" (FRANCE, 1978).

[12] A estadunidense *National Security Agency (NSA)* e a britânica *Government Communications Headquarters (GCHQ)* mantêm um programa sob o codinome *Tempora* cuja finalidade é a interceptação de cabos de fibra ótica situados em alto-mar e que transitam pelos territórios dos respectivos países. O programa é desenvolvido à luz das legislações dos respectivos países, que propiciam poderes diferenciados às agências para a interceptação de dados de estrangeiros. Outro exemplo é a nova lei do serviço de inteligência alemão (*Bundesnachrichtendienst – BND*), aprovada em outubro de 2016, que prevê expressamente a possibilidade de interceptação de comunicações de cidadãos estrangeiros que trafeguem pela infraestrutura da internet situada em território alemão.

Iniciam-se, aí, inúmeras regulações nacionais com efeitos extraterritoriais e os conflitos de ordem pública que têm como objeto principal o domínio dos dados. À medida que legislações rechacem o acesso de outros países às informações ou impeçam determinados serviços de serem oferecidos localmente – seja porque não se ajustam às leis de privacidade, seja porque existem imposições de nacionalização de *data centers* –, desvirtua-se o caráter global da internet. Configuram-se, então, os incentivos que conduzem ao processo de formação de múltiplas redes isoladas[13].

Outra decorrência da celeridade dos fluxos, além do embasamento ao interesse de acesso por múltiplas jurisdições que se apoiam exclusivamente em critério territorial, é a possibilidade de um dado produzido em um país ser armazenado em outro[14]. Quando isso ocorre, o conflito entre ordens públicas torna-se ainda mais explícito, porque há também um choque de princípios que justificaria o acesso ou a necessidade de proteção dos dados.

O país onde as informações são produzidas, além de se apoiar no aspecto territorial, socorrer-se-ia dos princípios da personalidade (ativa ou passiva) e da territorialidade objetiva (geração de efeitos) (KULESZA, 2012). Uma vez que os dados dizem respeito a cidadãos daquele país e, por isso, tendem a produzir efeitos em seu território, tanto as proteções à privacidade quanto as pretensões de acesso às informações pelo poder público seriam justificáveis.

Porém, o local onde os dados estão armazenados representa um elemento dotado de maior objetividade; afinal, trata-se de informações fisicamente localizadas em determinado território, sujeitas a um arcabouço jurídico específico. O debate, ainda não superado, passaria pela determinação do *status* jurídico do dado cibernético. Numa analogia com o setor bancário, a questão seria determinar se os dados corresponderiam a informações sobre a movimentação bancária de um indivíduo ou ao conteúdo de uma caixa-forte particular, mantida num banco (DASKAL, 2015). No primeiro caso, uma filial estabelecida no exterior poderia ser obrigada a fornecer as informações ao país interessado[15]; no

[13] Adiante, neste artigo, apresentar-se-ão exemplos que ilustram a problemática descrita, ao se analisarem os impactos da regulação brasileira sobre a internet.

[14] O local de armazenamento de informações normalmente é determinado por questões técnicas (de "arquitetura") aliadas a motivações econômicas, como a existência de facilidades de instalação de *data centers* em determinado país, incentivos tributários e disponibilidade de mão de obra especializada. Até mesmo questões climáticas são consideradas, pois a instalação de *data centers* em locais frios reduz os gastos com refrigeração (FARBER, 2013).

[15] Apesar da analogia, convém raciocinar nos termos do artigo 11 do MCI, que impõe a lei brasileira independentemente da forma como se percebam os dados cibernéticos (BRASIL, 2014).

segundo, o conteúdo do cofre somente poderia ser repassado no bojo de acordos de cooperação.

É possível vislumbrar uma situação ainda mais icônica sobre o embate de ordens públicas, na qual um dado cibernético é produzido num país, armazenado em outro e produz efeitos no território de uma terceira nação. Na ausência de um critério estabelecido para a resolução do conflito, os três tentarão aplicar as próprias leis. Acrescente-se a isso outra peculiaridade dos dados cibernéticos: sua divisibilidade.

A distribuição das informações na nuvem não precisa submeter-se à lógica espacial do mundo físico: a rápida movimentação de dados é o que torna ubíqua a nuvem cibernética. Logo – por razões seja de economia, seja de eficiência na distribuição de conteúdo –, a "arquitetura" do código permite que os dados sejam fracionados ou duplicados em servidores distintos. Novamente, eclodem problemas relativos à determinação da jurisdição e do direito aplicável, agravados pelos aspectos técnicos que impedem a exata aferição da relevância jurídica de cada fração de um dado cibernético para a determinação da lei que incidirá sobre uma relação jurídica específica.

Por fim, convém apontar outras duas peculiaridades, que novamente decorrem da facilidade de movimentação dos fluxos cibernéticos. A primeira: é tecnicamente possível o acesso remoto a dados alojados na nuvem cibernética – o que é um pressuposto elementar a essa forma de distribuição de informações. Assim, é possível compelir um prestador de serviços na internet a extrair prontamente um dado de um local e apresentá-lo em outro. No âmbito físico, ao contrário, o acesso a um bem tangível por autoridades públicas de um país não seria possível sem a aquiescência do outro Estado ou sem a ocorrência de uma afronta explícita à sua soberania. A segunda peculiaridade decorre da lógica empregada pelo setor privado para a escolha do local de armazenamento das informações. Como essa determinação é pautada por aspectos técnicos e econômicos, é fácil perceber que não se trata de categorias estanques; ou seja, alterando-se as circunstâncias, uma empresa pode facilmente mover os dados de um local para outro. A cada nova mudança, diferentes pretensões estatais de acesso ou proteção às informações surgirão.

Em síntese, a velocidade com que os dados cibernéticos transitam, a possibilidade de se deslocarem através de múltiplos territórios e a facilidade com que podem ser movidos, replicados ou fragmentados criam repercussões jurídicas diferenciadas, se comparados aos regimes aplicáveis a bens tangíveis. No entanto, algumas das soluções encontradas são insatisfatórias justamente porque se valem destas peculiaridades para buscar pontos de contato entre o dado e o território de determinado

país. Nesse processo, não raro se cometem arbitrariedades. Ao invés disso, o diferencial de rapidez e mobilidade dos dados deveria fomentar regimes que respeitem o caráter global dos fluxos, adotando-se soluções que busquem uma determinação mais adequada da sede das relações jurídicas.

3. Consequências da projeção extraterritorial da ordem pública sobre a internet

Como já se afirmou, decorre de comportamentos egoísticos o problema com que se depara a internet relativamente à determinação da jurisdição competente e do direito aplicável sobre relações jurídicas específicas. Convém analisar, isoladamente, as consequências dessas posturas.

O referencial de análise será o Marco Civil da Internet, mas é evidente que as outras legislações com iguais pretensões de geração de efeitos extraterritoriais têm o condão de provocar embates regulatórios com o potencial de deturpar todo o funcionamento da internet, no longo prazo.

A primeira importante consequência incide sobre o público alvo da norma: em essência, aqueles que, de alguma forma, têm relação com operações ocorridas em território brasileiro. Ao propor que "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" (BRASIL, 2014) relativamente a operações ocorridas em território nacional, um objetivo declarado do estatuto é o de assegurar a privacidade das pessoas nele situadas.

Tais operações materializar-se-iam com a "coleta, armazenamento, guarda e tratamento" de dados cibernéticos. Conforme exposto no item anterior, é possível que um dado seja coletado num país e armazenado em outro, ou produzido pelo nacional de um país e armazenado no território de outro Estado. Ao mesmo tempo, a definição de *tratamento* prevê uma série de ações, mas o ponto a se destacar é que parte delas poderá ocorrer em território nacional e outra no exterior. Em suma, as hipóteses de "coleta, armazenamento, guarda e tratamento" de dados cibernéticos podem envolver simultaneamente diversos territórios e, portanto, podem estar sujeitas a múltiplas tentativas de imposição das próprias normas.

Note-se, então, que sob a perspectiva de proteção à privacidade, o direito nacional é inócuo fora dos limites territoriais do Brasil nas situações em que os dados são armazenados no exterior[16]. Acresce a isso o fato de que, diante de tal hipótese, a única consequência que uma norma brasileira poderia gerar sobre o direito estrangeiro seria uma reação proporcional, repelindo a aplicação da lei do Brasil e impondo a legislação local. Ainda que não se trate de uma reação deliberada, esse é o resultado sistêmico que deriva das aspirações extraterritoriais: em vez de se buscarem soluções compartilhadas, cada país tenta preservar ou avançar o espaço de sua jurisdição.

A importância do argumento é evidenciar que, ao invés de cumprir o propósito para o qual foi criada, a norma consignada no artigo 11 do MCI é um dos elementos que contribuem para sua própria inutilidade. Por um lado, é óbvio que o direito brasileiro, pelo menos no que toca à determinação da norma cabível, seria aplicável dentro do território nacional. Por outro, a tentativa de projeção extraterritorial

[16] Se armazenados no Brasil, a lei brasileira poderia rechaçar eventuais pretensões de acesso por governos estrangeiros. Na prática, contudo, a maioria dos dados privados de cidadãos brasileiros mantidos por grandes prestadores de serviços de internet está armazenada fora do território nacional.

gera um incentivo à repulsa desse direito e à imposição arbitrária das normas locais. O propósito de proteção à privacidade é esvaziado por normas estrangeiras de acesso a partir do momento que o dado cibernético passe a ter qualquer tipo de contato com territórios de outros países interessados. Assim, o dado que não está armazenado em território nacional ou que transite pela infraestrutura localizada em outros países seria acessível pelas respectivas autoridades, a despeito da norma brasileira.

Em vez de buscarem uma solução cosmopolita, que resolva em definitivo o problema, os Estados passam por um momento no qual optam por se fecharem em torno das próprias regulações. O artigo 11 do MCI é uma expressão desse fenômeno.

O segundo aspecto digno de nota é a impossibilidade de as empresas se ajustarem simultaneamente a normas que preveem mandamentos opostos. Em fevereiro de 2016, no âmbito de uma audiência no Congresso estadunidense sobre "conflitos de normas e suas implicações para solicitações internacionais de dados por órgãos de segurança pública"[17], o presidente da Microsoft (que também é diretor jurídico da empresa), ao tratar especificamente dos conflitos entre o direito brasileiro e o estadunidense, afirmou que:

> Estes conflitos não são especulativos. De fato, as consequências para fornecedores globais e seus empregados nos países que solicitam dados são bastante reais. Isso é ilustrado, ao menos para a Microsoft, por eventos recentes no Brasil. Cortes brasileiras há muito reivindicam autoridade para obrigar empresas de tecnologia estadunidenses a revelar o conteúdo de comunicações de usuários para autoridades brasileiras, mesmo quando os dados estão localizados em outros países. Recentemente, o governo brasileiro impôs uma nova legislação que reafirma este ponto. A Microsoft presentemente armazena estes dados nos Estados Unidos, e a sua divulgação é explicitamente vedada pela Lei de Privacidade de Comunicações Eletrônicas de 1986 ("ECPA"), mesmo quando o dado pertencer a um usuário brasileiro. […] Embora tenhamos explicado este conflito intratável às autoridades no Brasil, até hoje elas têm se recusado a buscar a informação pela via de acordos de cooperação judiciária devido à demora desta solução. Ao invés disso, quando nós nos recusamos a violar a lei estadunidense, o que ocorreria caso obedecêssemos às ordens unilaterais e extraterritoriais das Cortes brasileiras, o governo e as autoridades do Brasil impuseram multas contra nossa subsidiária local e em um caso até mesmo prenderam e processaram criminalmente um empregado local (INTERNATIONAL…, 2016, tradução nossa).[18]

[17] A transcrição da audiência está disponível em: <https://judiciary.house.gov/hearing/international-conflicts-of-law-concerning-cross-border-data-flow-and-law-enforcement-requests/>. Acesso em: 4 fev. 2017.

[18] O executivo da Microsoft refere-se ao Marco Civil da Internet no início do depoimento. Quanto às multas, trata-se da seguinte situação: *Justiça multa Microsoft Brasil em R$ 650 mil por não revelar dados de email*. Disponível em: <http://olhardigital.uol.com.br/pro/noticia/justica-multa-microsoft-brasil-em-r-650-mil-por-nao-revelar-dados-de-email/37403>. Acesso em: 4 fev. 2017. Na questão criminal, trata-se de uma investigação que almejava acessar dados do *software* de comunicação Skype, pertencente à Microsoft. No original: "These conflicts are not speculative. In fact, the consequences for global providers and their employees in the countries requesting data are very real. This is illustrated, at least for Microsoft, by recent events in Brazil. The Brazilian courts have long asserted the authority to compel U.S. tech companies to disclose the contents of users' communications to Brazilian law enforcement, even when the data is located in other countries. Recently, the Brazilian Government enacted new legislation that reaffirms this point. Microsoft currently stores this data in the United States, and its disclosure is clearly prohibited by the Electronic Communications Privacy Act of 1986 ("ECPA"), in 18 U.S.C. § 2702(a), even when the data belongs to a Brazilian user. […] Though we have explained this intractable conflict to authorities in Brazil, to date they have refused to seek the information through a Mutual Legal Assistance Treaty (MLAT) due to time sensitivities. Instead, when we have refused to violate U.S. law by complying with unilateral and extraterritorial Brazilian orders, government authorities have levied fines against our local subsidiary and in one case even arrested and criminally charged a local employee."

Perante normas com pretensões extraterritoriais como o MCI, os prestadores de serviços na internet são postos na difícil posição de ter de escolher qual lei violar. As repercussões, como as ocorridas no exemplo citado, são perdas financeiras e até sanções penais.

Outro caso envolvendo a Microsoft encaminhou-se para solução diversa. Em 2013, um magistrado norte-americano emitiu ordem para que a empresa repassasse ao juízo dados de um usuário sobre o qual incidia o interesse de uma investigação criminal. Contudo, parte das informações estavam fisicamente alojadas em servidores na Irlanda; logo, a Microsoft apelou à instância superior com o intuito de não cumprir a ordem no tocante aos dados situados fora dos Estados Unidos.

Uma questão significativa neste caso foi o interesse também demonstrado pelo governo irlandês, que atuou como *amicus curiae* em favor da Microsoft. A Irlanda almejava que suas leis de privacidade e limitação de fluxos de dados fossem respeitadas. No polo contrário, a outra parte (o Departamento de Justiça dos Estados Unidos) pretendia dar efeitos extraterritoriais às suas regras, sob a alegação de que se tratava de uma demanda com interesse e efeitos predominantes em território norte-americano.

Em julho de 2016, o Tribunal de segunda instância concordou com o argumento da Microsoft[19], segundo o qual "o cumprimento do mandado da forma como o governo propõe implicaria uma aplicação extraterritorial da lei sobre armazenamento de comunicações […] e promoveria uma intrusão ilegal na privacidade do cliente da Microsoft" (UNITED STATES, 2016, [n.p.], tradução nossa). Com base nesse argumento, a Corte estatuiu:

> Evidentemente, não podemos ter certeza quanto ao alcance das obrigações que as leis de uma soberania estrangeira – e em particular, aqui, da Irlanda ou da União Europeia – relativas a um prestador de serviços que aloje dados digitais ou de outra forma conduza negócios em seu território. Entretanto temos dificuldade em ignorar esses interesses por completo apenas com base na teoria de que os interesses da soberania estrangeira não são afetados quando um juiz estadunidense emite uma ordem requerendo que um provedor de serviços "colete" dados, possivelmente pertencentes a um cidadão estrangeiro, de servidores no exterior e os "importe" para os Estados Unidos simplesmente porque o prestador de serviços tem uma base de operações no território dos Estados Unidos (UNITED STATES, 2016, [n.p.], tradução nossa).[20]

A Corte entendeu que as normas irlandesas ou da União Europeia não poderiam ser simplesmente ignoradas, o que ocorreria se fossem atribuídos efeitos extraterritoriais à lei estadunidense. Firmou-se a percepção de que a localização da sede da empresa (nos Estados Unidos) e a prestação de serviços ao público norte-americano não poderiam ser os únicos critérios para a determinação da lei aplicável. Havia ainda outra barreira mais contundente: a eficácia da lei irlandesa agregada à impossibilidade de se proverem efeitos extraterritoriais à norma estadunidense.

Grandes corporações atuantes na internet tendem a ajustar-se às normas de todos os paí-

[19] A decisão foi mantida, após recurso do Departamento de Estado ao mesmo Tribunal, em janeiro de 2017.

[20] No original: "Admittedly, we cannot be certain of the scope of the obligations that the laws of a foreign sovereign – and in particular, here, of Ireland or the E.U. – place on a service provider storing digital data or otherwise conducting business within its territory. But we find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to 'collect' from servers located overseas and 'import' into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States".

ses onde estão presentes (SWIRE, 2005). O ajuste, afinal, é menos custoso que potenciais sanções. No entanto, conflitos de normas inconciliáveis terão apenas duas resoluções possíveis caso se mantenham posturas egoístas como a adotada por muitos países, incluindo o Brasil. Uma das partes terá de ceder em sua pretensão (seja a interessada no acesso, seja a que almeja proteger os dados) ou os prestadores de serviços terão de submeter-se a perdas decorrentes de sanções pelo descumprimento de normas. Um aspecto nefasto dessa segunda opção, que pode prevalecer em decorrência da posição brasileira, é o desestímulo a investimentos no país e à inovação como um todo, uma vez que a principal força motriz das novidades trazidas pela internet é o capital privado.

Convém ainda apresentar uma variação da situação analisada acima: a hipótese de os dados serem armazenados em território brasileiro. Nesse caso, as normas de proteção à privacidade produzem os efeitos para os quais foram idealizadas; em tese, passa a ser possível (e defensável) afastar pretensões de acesso por autoridades de outros países.

Ao se imporem restrições severas ao compartilhamento de dados, logram-se dois efeitos. O primeiro é que efetivamente se consegue proteger a privacidade daqueles cujos dados têm contato com o território brasileiro, contra o interesse de acesso por autoridades estrangeiras. O segundo efeito é garantir a exclusividade do acesso aos dados pelo poder público local; possibilitam-se, inclusive, ações de vigilância contra aqueles (nacionais ou estrangeiros) que têm dados armazenados no país[21].

Ambos os efeitos podem motivar regulações de outros países que proíbam ou dificultem a atuação de determinadas empresas em seu território – o que, depois de extenso imbróglio, acabou por ocorrer com relação à Google na China, por exemplo. Assim, tanto uma norma que projete seus efeitos fora do território nacional com o intuito de acessar informações quanto outra que rechace, em absoluto, pretensões de obtenção de dados no próprio território por outros países pode ocasionar efeitos negativos para a evolução da internet. A legislação brasileira promove, simultaneamente, as duas ações – no que não está isolada. A única conclusão possível é que se faz necessário encontrar um equilíbrio entre os dois extremos.

Uma alternativa tão prejudicial quanto a proscrição de empresas estrangeiras é a já citada nacionalização compulsória de centros de armazenamento de dados. Tal postura, reitere-se, é motivada principalmente pelo anseio governamental de acessar as informações, sem a necessi-

[21] O exemplo mais emblemático é o programa *PRISM*, da já citada *National Security Agency*, dos Estados Unidos. No âmbito do programa, grandes empresas com *data centers* em território estadunidense são obrigadas a compartilhar dados de seus usuários com a NSA. Sobre o assunto, ver Greenwald e MacAskill (2013).

dade de recorrer à ajuda de outros países, e o de exercer o domínio exclusivo sobre os dados.

A ação de compelir as empresas a armazenarem dados cibernéticos produzidos pelos cidadãos de determinado país dentro dos limites do território nacional inviabiliza a principal vantagem do modelo de distribuição em nuvem: a economia dos custos. Em vez de manterem *data centers* em locais estratégicos[22], as empresas passam a ser obrigadas a construírem novos centros de armazenamento todas as vezes que um país aprovar legislação desta natureza. De imediato, pode-se imaginar que essa determinada jurisdição tenha tecnologia obsoleta ou mais dispendiosa, afetando provedores e usuários de forma generalizada.

Quanto mais países o fizerem, mais se agravarão os efeitos da *overregulation* sobre a internet. À medida que cada país atraísse para si a precedência jurídica sobre determinada fração do espaço cibernético, seu ganho seria facilmente observável, ao passo que os prejuízos aos fluxos de dados seriam diluídos entre os demais países. Se todos procedessem da mesma forma, os fluxos simplesmente se reduziriam significativamente e a internet deixaria de ser uma rede mundial.

4. Prescrição cosmopolita: por uma teoria do "domicílio" dos dados

A economia digital tende a tornar-se tão relevante quanto a comercialização de bens tangíveis. O acesso ampliado à internet mesmo nos mais recônditos locais possibilita a difusão de amplo espectro de novos produtos e serviços. Ademais, é viável para indivíduos antes isolados nesses mesmos rincões desenvolverem soluções tecnológicas e oferecerem-nas simultaneamente a todo o planeta, por meio do modelo de distribuição de conteúdo na nuvem cibernética.

Num cenário no qual se estabelecesse um modelo regulatório verdadeiramente global para a internet, as limitações ao desenvolvimento dessa economia dependeriam apenas de qualificação técnica. Os países mais bem-sucedidos seriam os dotados de capacidade de formação e captação de profissionais aptos a desenvolverem o espaço digital, uma vez que aspectos estruturais seriam regulados de modo a permitir a rápida disseminação de dados. Ter-se-ia uma economia verdadeiramente global, cujos produtos se deslocam à velocidade da luz.

Existem, todavia, três importantes barreiras à disseminação do modelo: o protecionismo, a censura e a citada proeminência do interesse estatal no acesso aos dados cibernéticos, especialmente sob as motivações de garantia da segurança pública e da defesa nacional. O protecionismo tolhe o funcionamento do sistema a partir do momento em que se criam barreiras para os fluxos de dados com o intuito de privilegiar fornecedores de soluções locais[23].

Não raro, os fluxos de dados também são limitados pela censura. Além de mecanismo de controle ideológico, tal prática pode ser uma manifestação dos outros dois fenômenos: pode tratar-se tanto de protecionismo velado quanto da proibição de funcionamento de um serviço cujo responsável não sucumba à imposição de compartilhamento dos dados. O caso

[22] Com base numa lógica determinada por questões tanto de "arquitetura" quanto de economia e praticidade.

[23] Curiosamente, tal prática pode encontrar limites no direito da Organização Mundial do Comércio, envolvendo o Acordo Geral sobre Comércio de Serviços (*GATS*, no acrônimo em inglês). Em caso relevante (*US – Gambling*), o governo do arquipélago caribenho de Antígua e Barbuda acionou os Estados Unidos no órgão de solução de controvérsias da OMC, envolvendo a compatibilidade da proibição de sites estrangeiros de apostas *on-line* pelo governo norte-americano. Sobre o tema, ver Burri (2015) e Meltzer (2013).

mais representativo dessas duas circunstâncias é, novamente, a sucessão de eventos que envolveu a Google e o governo da China[24].

Embora haja mecanismos jurídicos reiteradamente testados e bem estabelecidos para fazer frente ao protecionismo, o mesmo não se pode dizer da censura ou da resolução da dicotomia derivada do embate transnacional entre privacidade e segurança – e dos conflitos de normas que decorrem de ambos. No entanto, à medida que a economia digital avança, e mais países se tornam fornecedores de produtos e serviços *on-line* (e não apenas consumidores), aumentará a importância de se buscar uma saída negociada. O interesse na solução será encetado sobretudo pelas motivações econômicas que se apresentarão perante os novos atores do comércio digital.

Contudo, não se pode negligenciar o fato de que, para alguns governos, a estabilidade institucional e a segurança nacional são elementos considerados prioritários, mesmo se contrapostos à prosperidade econômica. Logo, haverá dificuldades maiores para reverter o ímpeto de alguns países pelo controle exclusivo de dados cibernéticos. Tal fato também precisa ser considerado na busca por uma solução.

Kohl (2015), ao tratar especificamente da jurisdição no espaço cibernético, aponta a evolução em Cortes europeias e estadunidenses, que passaram a adotar, ao longo do tempo, parâmetros mais bem definidos para a aplicação de suas normas. Um teste muito relevante foi apresentado por um tribunal dos Estados Unidos no âmbito do caso *Zippo Manufacturing v. Zippo Dot Com*[25].

O raciocínio proposto pela decisão no caso é o seguinte: considerando-se que conteúdos disponíveis na rede podem, em regra, ser acessados a partir de qualquer lugar, deve-se analisar determinado website ou serviço de internet pelas suas funcionalidades e pelo seu grau de interatividade com o usuário. O objetivo dessa análise é averiguar se, em uma escala decrescente de nível de relacionamento, um serviço foi efetivamente prestado ou contratado; se, no extremo oposto, apenas se postou conteúdo passivamente, o qual podia ser acessado pelos usuários de internet; ou se, em um meio termo, havia algum nível de interatividade. Neste terceiro caso, o teste impõe a avaliação do relacionamento entre as partes e a averiguação da natureza comercial – ou não – desta interação.

Kulesza (2012) cita, ainda, dois casos extraídos da jurisprudência estadunidense que aprimoraram o referencial introduzido pelo caso *Zippo*. Em *Mattel. v. Adventure Apparel*, de 2001, uma corte distrital de Nova York acrescentou o teste dos "efeitos" ao referencial estabelecido no caso Zippo. Não bastaria apenas a interação do usuário com o conteúdo disponível para a atração de uma contenda a determinado foro, mas a efetiva ocorrência de efeitos danosos em seu território. Ademais, em 2006, um Tribunal de segunda instância estadunidense, no âmbito do caso *Peblle Beach Company v. Caddy*, determinou que a jurisdição local somente se estenderia a uma página de internet se esta deliberadamente direcionasse suas atividades aos Estados Unidos.

Nos três casos, notam-se progressos nas tentativas de se estabelecerem critérios objeti-

[24] Ante a recusa da empresa a compartilhar dados solicitados por autoridades daquele país, promoveram-se, a mando de lideranças em Beijing, ataques cibernéticos contra servidores da Google, com o objetivo de se obterem dados pertencentes a dissidentes políticos chineses. A empresa acabou optando por deixar o país. Essa saída possibilitou o crescimento do concorrente local, uma empresa chinesa, que se submete à regulação do governo, e hoje é a principal ferramenta de busca empregada naquele país. Sobre o tema, ver Wu (2006) e Google (2010).

[25] Decisão disponível em: <https://cyber.harvard.edu/metaschool/fisher/domain/dncases/zippo.htm>. Acesso em: 4 fev. 2017.

vos para a determinação da Corte competente para a análise das contendas. No entanto, não se trata de situações em que o conflito de normas era o aspecto mais relevante e tampouco nas quais se discutia o acesso a dados. A problemática também não envolvia interesses relacionados à segurança pública e à defesa nacional.

Confrontados com ameaças dessa natureza, os países geralmente tendem a revestir-se das aspirações egoísticas que motivam as pretensões extraterritoriais. Materializam-nas, como fez o Brasil, pela adoção de vários critérios simultaneamente para a imposição da própria lei. Assim, considera-se o local onde um dado é produzido, armazenado ou processado; vislumbra-se o local onde o dado produz efeitos, por onde transita ou quem foi o responsável por sua produção. Ainda, contemplam-se os locais onde os prestadores de serviços mantêm suas sedes ou filiais e os métodos empregados para distribuir seus conteúdos (que podem ser fragmentados e replicados em diversos *data centers*). Todas essas hipóteses, saliente-se, estão – direta ou indiretamente – previstas no artigo 11 do MCI.

A adoção simultânea dos variados critérios por diversos países ocasiona – como já se explicitou – um excesso de regulações domésticas interpoladas. A solução do imbróglio, portanto, iniciar-se-ia pela definição de um critério em comum ou, alternativamente, pelo estabelecimento de uma hierarquia entre os critérios. A rota a ser traçada dependeria da adoção de uma abordagem cosmopolita perante os conflitos de normas e de jurisdição, como aponta Berman (2005, p. 1.880, tradução nossa).[26]

> Em um mundo altamente interdependente, preocupações com o imperialismo legal podem ser tão significativas quanto preocupações com imperialismo militar, político ou cultural. E enquanto é irrealista (e talvez desinteressante) esperar por harmonização internacional de normas legais, uma abordagem cosmopolita ao menos permitiria aos juízes que avaliassem as múltiplas filiações comunitárias enquanto elaborassem regras de resolução de conflitos de leis como parte de um empreendimento transnacional.

A interdependência, mencionada pelo autor, ampliar-se-ia à medida que mais países se convertessem tanto em fornecedores de produtos e serviços na internet quanto em consumidores. Nesse processo, veriam seus interesses cada vez mais afetados por regulações arbitrárias. Em

[26] No original: "In a highly interdependent world, concerns about legal imperialism may be as significant as concerns about military, political, or cultural imperialism. And while it is unrealistic (and perhaps unappealing) to expect international harmonization of legal norms, a cosmopolitan approach would at least allow judges to evaluate multiple community affiliations while developing choice-of-law rules as part of a joint transnational enterprise."

tal cenário, é possível que se criem incentivos para a cooperação e o abandono do "imperialismo legal". Enquanto tal construção não se realizar pela via dos tratados, seria papel dos tribunais a correta análise dos pontos de contato de determinada lide com a jurisdição e o direito que se pretende impor a ela.

Portanto, seja por meio de acordos internacionais, seja por construção jurisprudencial, uma solução cosmopolita tenderia a reverter os efeitos nefastos de regulações egoístas sobre a internet. A adesão a esse movimento seria iniciada em virtude de interesses econômicos, sobretudo relativos ao acesso a mercados. À medida que os fornecedores de soluções cibernéticas – inicialmente os principais interessados – aderissem à solução, os países dela alijados sentiriam os efeitos do isolamento sobre a capacidade das próprias empresas de fazerem parte de um mercado global. Num cenário no qual se oferecem cada vez mais produtos e serviços exclusivamente na plataforma digital, a persistência na regulação egoísta agravaria as perdas e o isolamento dos países que não aceitassem abdicar parcialmente do acesso a informações.

Resta, enfim, aventar quais seriam as linhas gerais para o desenvolvimento dessa solução.

A primeira observação importante é que a prevalência do critério territorial tem de ser questionada, ou ao menos modulada perante determinadas circunstâncias. É claro que o aspecto territorial é importante, na análise tanto do local onde um dado foi produzido quanto de onde se materializam seus efeitos; mas haverá situações em que os efeitos serão mais relevantes em outra jurisdição, ou em que o local de produção dos dados seja impossível de se determinar ou seja mera casualidade[27].

Daskal (2015), por exemplo, defende a *aterritorialidade* dos dados, em face de todas as suas peculiaridades. Ao contrário dessa autora, não se vislumbra o completo abandono do critério territorial. No entanto, preconiza-se efetivamente que se avaliem os vínculos dos casos concretos submetidos a juízo em face dos ideais e valores das comunidades nas quais os atores se inserem e sobre as quais incidem os efeitos de suas ações. O elemento territorial nem sempre reflete a real inserção de uma situação fática em determinado contexto social.

Portanto, acredita-se que a busca dos vínculos mais fortes de um caso com o Direito de determinado país é um processo factível, potencialmente motivado pelos ganhos econômicos que geraria, e que implicaria, ao final, na determinação do "domicílio" da informação. Assim como o domicílio de uma pessoa física é o lugar onde ela se estabelece com ânimo definitivo, a analogia ora proposta parte de uma determinação do ímpeto dos envolvidos na relação jurídica ocorrida no ambiente digital. Convém investigar quais são os seus objetivos, onde tais indivíduos vislumbrariam que suas ações produziriam efeitos ou até que ponto estariam conscientes da potencial geração de efeitos em dado território. Domicílio, nesse sentido, não guarda correspondência estrita com o local de armazenamento da informação. Muito mais: com um conjunto de fatores que precisam ser desenvolvidos.

Note-se, então, que, apesar de não ser abandonado totalmente, o critério territorial seria, na metodologia proposta, acompanhado de uma análise do ânimo dos atores – o que, em parte, já se aplicou na jurisprudência estadunidense em relações de Direito privado, conforme já se expôs. Em se tratando do acesso estatal a dados ou da incidência de normas de proteção, o referencial teria de ser ampliado, pois não se estaria mais no âmbito de rela-

[27] Em face de tecnologias que permitem ao usuário camuflar sua real localização, aparentando estar em outro local.

ções privadas. Efetivamente, os Estados teriam de abdicar de parcela de sua autoridade em benefício de um sistema global. Desse modo, a determinação do "domicílio" dos dados, ao combinar os critérios pessoal e territorial, e ao atribuir a devida relevância ao ânimo dos envolvidos em uma relação jurídica, seria uma possível resolução para os múltiplos conflitos de normas que caracterizam o espaço cibernético atualmente.

5. Conclusão

A possibilidade de a internet ser definitivamente descaracterizada em decorrência do excesso de regulação se eleva continuamente, à medida que a atual tendência dos países ainda é a de tentar projetar extraterritorialmente suas normas. Em vez de intervirem sobre a rede mundial de computadores para preservar seu caráter global, os Estados se revestem de aspirações egoísticas e regulam-na exclusivamente sob a óptica de interesses locais. E o Brasil não é diferente.

Todavia, à medida que as perdas econômicas se tornarem relevantes a ponto de suplantarem, ao menos em parte, a obstinação pelo acesso a dados cibernéticos motivada pelo imperativo de assegurar a defesa nacional e a segurança pública, buscar-se-ão maneiras de conciliar as duas realidades. A opção por uma saída cosmopolita não inviabiliza os ideais de segurança: apesar de abdicarem de parte de suas pretensões, ainda restaria aos Estados o recurso a mecanismos de cooperação bilateral. Este artigo apenas se insurge contra a aplicação arbitrária da própria lei e sua projeção extraterritorial, e não, obviamente, contra o interesse legítimo do Estado de acessar informações úteis à sua segurança e à de sua população.

Ao se propor uma "teoria do domicílio dos dados", entende-se que esta formulação ainda se encontra em fase incipiente. Utilizou-se este espaço para lançar a ideia, que, adiante, precisará ser desenvolvida.

Sobre os autores

Filipe Rocha Martins Soares é bacharel em Direito pela Universidade Federal do Piauí (UFPI), Teresina, PI, Brasil; mestrando em Direito pelo Centro de Ensino Unificado de Brasília (UniCEUB), Brasília, DF, Brasil.
E-mail: filipe.soares@protonmail.com

Gustavo Ferreira Ribeiro é doutor em Direito pela Maurer School of Law, Indiana University Bloomington, Bloomington, IN, Estados Unidos da América, com bolsa do programa Capes/Fulbright; professor do Centro de Ensino Unificado de Brasília (UniCEUB), Brasília, DF, Brasil.
E-mail: gribeirobr@gmail.com

Título, resumo e palavras-chave em inglês[28]

CONFLICTS AMONG PUBLIC ORDERS IN CYBERSPACE: A COSMOPOLITAN APPROACH IN RESPONSE TO THE OVERREGULATION OF THE INTERNET

ABSTRACT: the particularities of cyberspace create obstacles to the exercise of State power, such as the access to information connected to more than one jurisdiction. The imposition of extraterritorial effects to their laws concerning the internet is among the measures States adopt in order to guarantee such access. At such point, conflicts of public orders arise (data access v. privacy) which affect the operation of a worldwide web. So far, States have not properly solved the profusion and the clash of regulations (*overregulation*). The resolution of such problem depends on the reckoning of the impossibility of dissociating the internet of its transnational nature: a cosmopolitan approach is required. In the latter, the combination of personal and territorial criteria in the determination of the *cyber data domicile* offers a way of thinking. Though incipient, the *cyber data domicile* may become indicative of the public order that should prevail, whilst overregulation occurs.

KEYWORDS: INTERNET. OVERREGULATION. EXTRATERRITORIALITY. DATA DOMICILE.

Como citar este artigo

(ABNT)
SOARES, Filipe Rocha Martins; RIBEIRO, Gustavo Ferreira. Conflitos entre ordens públicas no espaço cibernético: uma abordagem cosmopolita em resposta à sobreposição regulatória da internet. *Revista de Informação Legislativa*: RIL, v. 54, n. 216, p. 45-66, out./dez. 2017. Disponível em: <http://www12.senado.leg.br/ril/edicoes/54/216/ril_v54_n216_p45>.

(APA)
Soares, F. R. M., & Ribeiro, G. F. (2017). Conflitos entre ordens públicas no espaço cibernético: uma abordagem cosmopolita em resposta à sobreposição regulatória da internet. *Revista de Informação Legislativa: RIL*, *54*(216), 45-66. Recuperado de http://www12.senado.leg.br/ril/edicoes/54/216/ril_v54_n216_p45

Referências

BERMAN, Paul Schiff. Choice of law and jurisdiction on the internet: towards a cosmopolitan vision of conflict of laws. *University of Pennsylvania Law Review*, v. 153, n. 1, p. 1819-1882, 2005.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. *Diário Oficial da União*, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 11 maio 2017.

[28] Sem revisão do editor.

_____. Decreto nº 8.771, de 11 de maio de 2016. *Diário Oficial da União – Edição Extra*, 11 maio 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 11 maio 2017.

BURRI, M. The international economic law framework for digital trade. *Zeitschrift für Schweizerisches Recht*, v. 135, n. 2, p. 10–72, 2015.

COUR PERMANENTE DE JUSTICE INTERNATIONALE. *Affaire du "Lotus"*: recueil des arrêts. [S.l.]: Cour Permanente de Justice Internationale, 1927. Disponível em: <http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf>. Acesso em: 11 maio 2017.

DASKAL, Jennifer. The un-territoriality of data. *The Yale Law Journal*, v. 125, n. 2, p. 326-398, 2015.

DUNOFF, Jeffrey; TRACHTMAN, Joel. Economic analysis of international law. *Yale Journal of International Law*, v. 24, n. 1, p. 1-59, 1999. Disponível em: <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1096&context=yjil>. Acesso em: 10 maio 2017.

EASTERBROOK, Frank. Cyberspace and the Law of the Horse. *University of Chicago Legal Forum*, v. 207, p. 207-216, 1996. Disponível em: <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2147&context=journal_articles>. Acesso em: 10 maio 2017.

FARBER, Dan. *Facebook turns on data center at edge of the Arctic Circle* [*on-line*]. 2013. Disponível em: <https://www.cnet.com/news/facebook-turns-on-data-center-at-edge-of-the-arctic-circle/>. Acesso em: 11 maio 2017.

FRANCE. Loi nº 78-17, du 6 janvier 1978. Relative à l'informatique, aux fichiers et aux libertes. *Journal Officiel de la République Française*, 7 janv. 1978. Disponível em: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&dateTexte=20170511>. Acesso em: 11 maio 2017.

GOOGLE. *Enabling trade in the era of information technologies*: breaking down barriers to the free flow of information [*on-line*]. 2010. p. 1-25. Disponível em: <https://static.googleusercontent.com/media/www.google.com/pt-BR//googleblogs/pdfs/trade_free_flow_of_information.pdf>. Acesso em: 10 maio 2017.

GREENWALD, Glenn; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, [S.l.], 7 jun. 2013. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 10 maio 2017.

GUZMAN, Andrew. Choice of law: new foundations. *Berkeley Law Scholarship Repository*, v. 90, n. 883, p. 883-940, 2001. Disponível em: <http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=2691&context=facpubs>. Acesso em: 10 maio 2017.

HARDIN, Garret. The tragedy of the commons. *Science*, v. 162, n. 3859, p. 1243-1248, 1968. Disponível em: <http://science.sciencemag.org/content/162/3859/1243/tab-pdf>. Acesso em: 10 maio 2017.

INTERNATIONAL conflicts of law and their implications for cross border data requests by law enforcement [gravação de som]. [Washington, DC]: House Judiciary Committee, 2016. Hearing before the Committee on the Judiciary House of Representatives. Disponível em: <https://judiciary.house.gov/hearing/international-conflicts-of-law-concerning-cross-border-data-flow-and-law-enforcement-requests/>. Acesso em: 11 maio. 2017.

KOHL, Uta. Jurisdiction in cyberspace. In: TSAGOURIAS, Nicholas; BUCHAN, Russel (Ed.). *Research handbook on international law and cyberspace*. Cheltenham: Edward Elgar Publishing, 2015. p. 30-54.

KULESZA, Joanna. *International internet law*. Abingdon: Routledge, 2012.

LESSIG, Lawrence. The Law of the Horse: what cyberlaw might teach. *Harvard Law Review*, v. 113, n. 2, p. 501-546, 1999. Disponível em: <https://cyber.harvard.edu/works/lessig/finalhls.pdf>. Acesso em: 10 maio 2017.

MELL, P.; GRANCE, T. *The NIST definition of cloud computing*: recommendations of the National Institute of Standards Technology. Gaithersburg, MD: NIST, 2011. Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 11 maio 2017.

MELTZER, Joshua. The internet, cross-border data flows and international trade. *Issues in Technology Innovation*, n. 22, p. 1-21, 2013. Disponível em: <https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf>. Acesso em: 10 maio 2017.

SWIRE, P. Elephants and mice revisited: law and choice of law on the internet. *University of Pennsylvania Law Review*, v. 153, n. 1975, p. 1975-2001, 2005. Disponível em: <https://www.law.upenn.edu/journals/lawreview/articles/volume153/issue6/Swire153U.Pa.L.Rev.1975%282005%29.pdf>. Acesso em: 23 maio 2017.

UNIÃO EUROPEIA. Parlamento Europeu. Directiva 95/46/CE, de 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial das Comunidades Europeias*, 23 nov. 1995. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L:1995:281:TOC>. Acesso em: 11 maio 2017.

UNITED STATES. United States Court of Appeals for the Second Circuit. *In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation*. Nova York, EUA, 14 jul. 2016. Não paginado. Disponível em: <http://law.justia.com/cases/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.html>. Acesso em: 22 maio 2017.

WU, T. The world trade law of censorship and internet filtering. *Chicago Journal of International Law*, v. 7, n. 1, p. 263–287, 2006. Disponível em: <http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1243&context=cjil>. Acesso em: 11 maio 2017.