PANORAMA EUA

VOL. 4, Nº 6, AGOSTO DE 2018

OPEU
OBSERVATÓRIO POLÍTICO DOS ESTADOS UNIDOS

INCT INEU
INSTITUTO NACIONAL DE CIÊNCIA E TECNOLOGIA PARA ESTUDOS SOBRE OS ESTADOS UNIDOS
NATIONAL INSTITUTE OF SCIENCE AND TECHNOLOGY FOR STUDIES ON THE UNITED STATES

PANORAMA EUA
OBSERVATÓRIO POLÍTICO DOS ESTADOS UNIDOS
INSTITUTO NACIONAL DE CIÊNCIA E TECNOLOGIA
PARA ESTUDOS SOBRE OS ESTADOS UNIDOS – INCT-INEU

ISSN 2317-7977

VOL. 4, Nº 6, AGOSTO DE 2018

CORPO EDITORIAL
EDITOR: Sebastião Velasco e Cruz
SUPERVISÃO: Geraldo Zahran

http://www.opeu.org.br

NAFTA 2.0: CLOUD COMPUTING E TRANSFERÊNCIA DE DADOS EM DESTAQUE NAS NEGOCIAÇÕES COMERCIAIS

Por Neusa Maria P. Bojikian[1]

Com base no discurso de que nenhum dos regimes internacionais vigentes contempla adequadamente definições e instrumentos de combate às práticas comerciais desleais, em maio de 2017, a Administração Trump notificou formalmente o Congresso a intenção de renegociar o North American Free Trade Agreement (NAFTA), constituído no início da década de 1990. Cumprido o prazo (90 dias) aberto às eventuais consultas, as negociações foram iniciadas em agosto de 2017 e programadas para terminar até o primeiro quadrimestre de 2018. Entretanto, as partes ainda não conseguiram chegar efetivamente a um acordo. Entre os aspectos e detalhes práticos mais difíceis do atual processo de negociação do NAFTA, figuram aqueles relativos à transferência de dados ou informações pessoais (termos aqui considerados intercambiáveis) armazenados nas plataformas digitais. De que ordem são essas dificuldades? Quais as preferências de cada uma das partes?

Comércio internacional traduz-se cada vez mais em transações de dados

A computação em nuvem – *cloud computing*–, que envolve fundamentalmente a maximização da capacidade de armazenamento e de cálculo de servidores compartilhados por meio da *internet,* deu um impulso bastante importante ao conceitode que os serviços poderiam ser acessados remotamente, de qualquer lugar do mundo e a qualquer momento. Com isso, o comércio internacional tornou-se mais relacionado a transações transfronteiriças de dados.

Identificar com precisão o valor do comércio internacional envolvendo transação de dados é difícil até mesmo em países membros da OCDE, que tradicionalmente requer que seus membros mantenham diversas séries estatísticas. Nos Estados Unidos, nem mesmo agências específicas de comércio, como a Escritório do Economista Chefe do Departamento de Comércio (OCE-DOC) e a Agência de Análises Estatísticas (BEA), podem fornecer tais índices. O que o BEA produz são estimativas sobre o comércio internacional de serviços dos setores de tecnologia da informação e comunicação (TIC) e dos "potencialmente" viabilizados com TIC – aqueles serviços que podem ser negociados remotamente através da *internet*(PICTE).

Com base em tais estimativas, o OCE-DOC emitiu em janeiro de 2018 um relatório mostrando que, em 2016, os serviços categorizados como PICTE responderam por 54% de todas as exportações de serviços dos Estados Unidos e 48% de todas as importações também de serviços do país. Os serviços PICTE exportados ao Canadá somaram 52% do total das exportações de serviços dos Estados Unidos, que por sua vez importaram US$ 13.9 bi desse tipo de serviço daquele país – o que corresponde a 46% do total de serviços importados pelos Estados Unidos do Canadá. E para o México, os Estados Unidos exportaram US$ 8.8 bi desse tipo de serviço, equivalente a 27% de todas as exportações americanas de serviços. Por outro lado, os Estados Unidos importaram US$ 4.8 bi em serviços PICTE do México, correspondente a 19% do total de serviços importados do México. Ainda conforme o relatório da OCE-DOC, no período entre 2006-2016, as exportações americanas dessa categoria de serviços seguiram crescendo em média 4% para o Canadá e 5.5% para o México.

Adicionalmente, há as transações de dados que não necessariamente envolvem pagamentos. Conforme apontado no referido relatório, subsidiárias de empresas americanas instaladas no Canadá e no México contam

[1] Pesquisadora do INCT-INEU. Doutora e mestre em Relações Internacionais pelo PPGRI-Unesp-Unicamp-PUC-SP. Autora do livro Acordos comerciais internacionais: o Brasil nas negociações do setor de serviços financeiros (2009, Unesp) e Coorganizadora do livro Negociações econômicas internacionais: abordagens, atores e perspectivas desde o Brasil (2011, Unesp). A autora gostaria de agradecer a Sebastião Velasco pela atenta leitura e pertinentes sugestões feitas sobre o texto.

com fluxos de dados tanto para realizar operações comerciais, bem como para outros fins.

A questão é que todas essas transações dependem sobretudo de regulamentações favoráveis à transferência de dados entre diferentes países.

As nuvens – grandes computadores de propriedade de empresas privadas – estão sendo acessadas por autoridades governamentais

Os dados enviados para as chamadas nuvens são armazenados em servidores – *hardware*– de propriedade de empresas privadas como Apple, Amazon, Google. O envio de dados dos clientes e/ou usuários para as nuvens significa que eles podem se tornar imediatamente acessíveis a qualquer computador das respectivas empresas fornecedores dos serviços de armazenamento. Ocorre que as autoridades governamentais podem exigir acesso a esses dados.

As atividades de vigilância dos Estados Unidos, feitas com a colaboração de empresas privadas, há muito têm sido denunciadas. Em 2006, o Electronic Frontier Foundation (EFF) – grupo de cidadãos americanos que monitoram e questionam projetos de lei que, de acordo com seus critérios, violam liberdades civis no contexto da contemporaneidade digital – ajuizou ação contra a AT&T, alegando que a empresa ajudara a Agência Nacional de Segurança (ANS) a invadir a privacidade de seus clientes.

Documentos desvelados por um ex-funcionário da AT&T e analisados por especialistas independentes revelaram que se usara um equipamento, instalado em 2003, capaz de monitorar grande quantidade de mensagens eletrônicas, chamadas telefônicas via *internet*e outros fluxos de dados digitais. O equipamento também é capaz de selecionar mensagens identificáveis por: palavras-chaves, protocolos de *internet*, endereços eletrônicos, países de origem.

Em 2013, o PRISM, controverso programa de vigilância usado pela ANS, foi exposto por Edward Snowden, prestador de serviços que havia sido contratado pela agência. Desvelou-se que o sistema permite que a ANS acesse comunicações privadas de usuários, podendo monitorar celulares, dados de cartão de crédito, navegadores de *internet*, diretamente dos servidores da Microsoft, Yahoo, Google, Facebook e de outras empresas de TIC.

Diante dos fatos, muitos cidadãos, grupos de interesses, inclusos ativistas em defesadas liberdades civis, principalmente no âmbito dos países europeus, ficaram alarmados com os acordos comerciais internacionais contendo a cláusula irrestrita de transferência de dados. O embaraço surge porque as autoridades americanas possuem amplos poderes conferidos por leis domésticas que lhes permitem acessar os dados pessoais de cidadãos estrangeiros em nome da segurança nacional, independente de quaisquer que sejam os termos e condições estabelecidos em acordos comerciais. No seguimento do USA Patriot Act (Lei Patriótica), decreto presidencial emitido logo após o 11 de Setembro para favorecer os esforços contra o terrorismo, as atividades de vigilância dos Estados Unidos foram ampliadas de forma excepcional. Depois de várias prorrogações da Lei Patriótica, o Congresso aprovou, em 2015, o Freedom Act.

Alinhados com a Lei Patriótica e sua provisão relativa ao aperfeiçoamento do serviço de inteligência, que altera a National Security Act of 1947 (Lei de Segurança Nacional), outros estatutos legais do país também foram alterados. Em julho de 2008, aprovou-se uma emenda – Seção 702 – à Foreign Intelligence Surveillance Act of 1978, "estabelecendo procedimento para autorizar certas aquisições de inteligência estrangeira e para outros propósitos". Com base na Seção 702, o Procurador-Geral dos Estados Unidos pode requerer isenção de responsabilidade de empresas do setor de TIC no programa de vigilância, sem mandado, se o governo sigilosamente certificar à Corte que a vigilância: (1) não ocorreu; (2) ocorreu legalmente; ou (3) foi autorizada pelo presidente. Adicionalmente, a norma autoriza a ANS a espionar cidadãos estrangeiros localizados fora dos Estados Unidos, usando infraestrutura e ferramentas tecnológicas privadas disponíveis. Note-se que a ANS já possuía permissão pa-

ra acessar cabos de comunicação localizados fora do país e cabos que ligam um país estrangeiro a outro que passam pelo território americano. Com a Seção 702, legitimou-se o uso desses cabos sem precisar sair do território, facilitando e barateando as operações e a solicitação de dados digitais diretamente de empresas privadas.

Em 2012, sob Administração Obama, e em 2018, sob a Administração Trump, a Seção 702 foi renovada. Com a última aprovação do Congresso, a vigilância doméstica nos Estados Unidos ganha *status* legal por pelo menos mais seis anos, aumentando a possibilidade de tal provisão se tornar parte permanente da lei de 1978. O sistema de freios e contrapesos – de revisão congressional e judicial do aparato de inteligência do presidente – não abriu um esperado espaço para discussão ampla e madura. Tanto no Senado como na Câmara, os atributos da Seção 702 foram engrandecidos.

Os governos e o controle da regulamentação dos dados pessoais: as regulamentações de localização de dados no Canadá e no México

A articulação de atores sociais levou vários governos a adotar requisitos para que determinados dados sobre cidadãos ou residentes de um país sejam coletados, processados e armazenados em servidores localizados fisicamente no respectivo país. No Canadá por exemplo aresistência maior refere-se aos dados, de cidadãos e residentes, relacionados à saúde. Os negociadores canadenses exigem que tais dados sejam armazenados onde estejam seguros e não sejam revelados a terceiros, especialmente a governos estrangeiros. Além disso, em determinadas províncias do país, há normas exigindo que dados pessoais sejam armazenados localmente.

A Colúmbia Britânica tornou-se a primeira província canadense a exigir a localização de dados a partir de 2004. A regulamentação, traduzida em uma emenda à Lei de Liberdade de Informação e Proteção à Privacidade, foi baseada em relatório emitido pelo Comissário de Informação e Privacidade da referida província – Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing. Concluiu-se que havia "possibilidades razoáveis" de que o governo dos Estados Unidos usaria a Lei Patriótica para acessar dados pessoais relativos à saúde de residentes da Colúmbia Britânica, caso tais dados fossem terceirizados a empresas no Canadá ligadas aos Estados Unidos.

Assim, a nova regulamentação válida na tal província exige que os órgãos públicos garantam que todas as informações pessoais sob sua custódia ou sob seu controle sejam armazenadas e acessadas apenas no Canadá, a não ser que se enquadrem em determinadas exceções previstas na lei. Isso se estende a órgãos públicos e seus prestadores de serviços em educação, transporte, assistência médica e judiciário e abrange todos os dados armazenados em computadores, em unidades de *backup* e na nuvem.

John Horgan, que veio a ocupar o cargo de primeiro-ministro da Colúmbia Britânica desde julho de 2017, prometera em sua campanha eleitoral que manteria a regulamentação sobre privacidade e a preservação dos direitos a ela relacionados e resistiria a qualquer proposta em contrário apresentada pela Administração Trump.

Em 2006, a província Nova Escócia seguiu a iniciativa da Colúmbia Britânica, aprovando a Lei de Proteção de Divulgação Internacional de Informações Pessoais, que restringe a transferência de dados pessoais. Espelhando o que já previa a regulamentação da Colúmbia Britânica, a regulamentação da Nova Escócia estabelece que um órgão público, prestador de serviços ou associado deve notificar as autoridades competentes da Nova Escócia caso receba ou tenha dúvidas sobre eventuais solicitações estrangeiras para divulgação de dados pessoais.

Além dessas, outras duas províncias – Quebec e Alberta – também possuem estatutos que estabelecem termos e condições para a transferência de dados. Ou seja, embora não se proíba a transferência de dados para fora do país, há determinadas condicionalidades.
No México, a proteção de dados pessoais é uma garantia constitucionale também objeto de várias leis infraconstitucionais, mas, dife-

rente do Canadá, a transferência de dados, nos âmbitos doméstico e internacional, é amplamente permitida. Além dos casos em que haja a manifestação da vontade pessoal, também são permitidas as transferências nas seguintes situações: (1) previsto em lei ou em tratado do qual o México é parte; (2) necessário para prevenção ou diagnóstico medico; (3) realizada entre empresas pertencentes a um grupo empresarial que partilhar determinados processos ou políticas internas; (4) cumprimento de um contrato de interesse do país celebrado entre a empresa proprietária dos dados e um terceiro; (5) por interesse público da procuradoria ou da administração da justiça; (6) diante de solicitação emitida por um juiz mediante processo judicial.

Manifestações das partes nas negociações

Os negociadores americanos exigem o relaxamento de qualquer restrição relativa à transferência transfronteiriça de dados e, portanto, têm como alvo as regras vigentes nos outros países onde se estabelece que determinados dados pessoais sejam armazenados em computadores localizados dentro de suas fronteiras. Tal exigência já foi apresentada nas negociações do Trans-Pacific Partnership Agreement (TPP), onde representantes dos setores de serviços financeiros, de telecomunicações, de tecnologia da informação, comércio digital em geral (bens e serviços) e outros se mobilizaram junto aos negociadores americanos para garantir a liberalização plena da transferência de dados. Enquanto os negociadores mexicanos não apresentaram um requisito sequer de localização, indicando que tendem a fazer concessões e satisfazer as preferências de seus interlocutores americanos, os negociadores canadenses precisam lidar com algumas reservas internas.

Em dezembro de 2017, o Diretor de Comércio de Serviços para Assuntos Globais do Canadá afirmou à Comissão Parlamentar de Comércio Internacional do país que a posição canadense nas atuais negociações comerciais deve seguir uma abordagem "equilibrada" entre garantir um fluxo transfronteiriço de dados e proteger as informações mantidas pelo governo ou em um contexto de compras governamentais.

Isso pode ser interpretado como uma disposição dos negociadores canadenses em concordar com o fator de transferência de dados, excepcionando aqueles mais sensíveis e de interesses estratégicos, especificamente dados relativos à saúde de seus nacionais e residentes e à segurança nacional. Além disso, devem ficar fora do escopo do acordo as províncias que já mantêm suas próprias regras sobre localização de dados.

Caso essa condição seja aceita pelos negociadores americanos – o que não deve ser fácil e sem custo para os negociadores canadenses uma vez que qualquer exceção torna-se um precedente contrário às preferências dos negociadores americanos e tende a ser usado pelas contrapartes em futuras negociações – haverá outra questão a ser enfrentada junto aos defensores do controle do Estado sobre a regulamentação dos dados pessoais. Com o procedimento Lista Negativa,acompanhado das regras*Standstill*e *Ratchet*quedevem ser adotados no novo NAFTA, haverá restrições para se promulgar novos regulamentos similares aos existentes nas províncias excepcionadas.

O princípio da Lista Negativa é liberalizar todos os tipos de bens e serviços transacionáveis, inclusive o que vier a surgir no futuro, a menos que haja exceções e ressalvas devidamente listadas pelos respectivos negociadores. No sentido oposto, o princípio da Lista Positiva é liberalizar apenas os bens e serviços listados no momento presente. E enquanto a regra Standstill – 'congelamento' – fixa o *status quo* regulatório, a regra Ratchet – 'catraca' – requer que alterações futuras não afetem negativamente o grau de compromissos assumidos no âmbito do acordo. Na prática, tais regras fazem com que futuras liberalizações – unilaterais ou decorrentes de arranjos comerciais com terceiros países – sejam imediatamente consolidadas e se tornem parte da obrigação junto ao acordo em questão.

Um acordo baseado em tal procedimento e em tais regras subtrai espaço regulatório essencial para se implementar futuras políticas públicas relativas à privacidade e proteção dos dados pessoais. Significa que para rea-

ver tal espaço ou a autonomia antes incontestável, os respectivos signatários teriam que concordar em se reunir novamente para negociar novos termos e novas condições do acordo em questão.

Em síntese

À medida que as atividades econômicas e sociais crescem nas plataformas digitais, ações para proteção de dados e privacidade tornam-se cada vez mais demandadas, sobretudo por mobilizações de atores sociais e suas preocupações locais no contexto das inúmeras negociações comerciais internacionais.

Na outra ponta, os agentes econômicos alegam ser crucial abordar a questão das transferências internacionais de dados com regras específicas, evitando ou removendo as exigências de localização de dados. Em síntese, eles defendem que uma maior harmonização de leis e regimes reduziria grandemente a probabilidade de atrito em relação à transferência de dados e, em última instância, reduziria os custos de transação.

Uma vez mais a questão da harmonização das abordagens regulatórias torna-se um desafio do ponto de vista político e das implicações de ordem prática em cada um dos países signatários de um determinado acordo comercial.

Ao concordarem com regimes que buscam a harmonização de regras, os governos enfrentam o problema de não mais poder implementar as regulamentações refletindo as legitimas preferências dos consumidores ou usuários nacionais. Naturalmente, há visões diferentes sobre riscos, como os relacionados à proteção de dados pessoais e privacidade, assim como há concepções variadas de como as atividades econômicas devem se relacionar com as diferentes partes interessadas. Os acordos comerciais internacionais inviabilizam a produção de padrões normativos diferentes.

Não se trata de comum argumentação relativa às vantagens ou desvantagens econômicas da liberalização. A pressão pela transferência indiscriminada de dados suscita questões fundamentais para a garantia dos direitos individuais e a integridade da democracia.


OPEU
OBSERVATÓRIO POLÍTICO
DOS ESTADOS UNIDOS
INCT
INEU
INSTITUTO NACIONAL DE CIÊNCIA
E TECNOLOGIA PARA ESTUDOS
SOBRE OS ESTADOS UNIDOS
NATIONAL INSTITUTE OF SCIENCE
AND TECHNOLOGY FOR STUDIES
ON THE UNITED STATES