Caso de uso do Modo Internet de Interconectividade: Localização de Dados

1 Como a localização obrigatória de dados impacta o Modo Internet de Interconectividade

Este caso de uso analisa o efeito que as políticas governamentais relacionadas à localização de dados podem ter no Modo Internet de Interconectividade. Para entender como essas políticas podem prejudicar os benefícios mais amplos da Internet, como inovação e crescimento socioeconômico, nós os vemos através das lentes das propriedades críticas da Internet.

2.1 O que é localização de dados obrigatória?[1]

A localização de dados obrigatória refere-se às exigências do Estado que controlam o armazenamento e o fluxo de dados para mantê-los em uma jurisdição específica. As leis de localização de dados - às vezes chamadas de "residência de dados" ou "soberania de dados" - normalmente destinam-se a manter dados pessoais ou de transações financeiras no país onde estão sujeitos ao acesso e à regulamentação local. As medidas obrigatórias de localização de dados vão desde a obrigação de localizar fisicamente os dados no país de origem, até restringir ou mesmo proibir sua transferência para outros países. O que significa a localização obrigatória de dados para as propriedades críticas da Internet, e o que aconteceria se mais países impusessem essas restrições?

2.2 Tendências atuais

Nos últimos anos, Índia, Indonésia e Vietnã debateram ou aprovaram leis exigindo que dados pessoais ou comerciais sejam mantidos dentro das fronteiras nacionais e não sejam processados em outros países.[2] Embora a Lei de Proteção de Dados Pessoais de 2019 da Índia tenha descartado medidas para manter todo o processamento de dados pessoais geograficamente localizado na Índia, ela ainda força a localização de um conjunto indefinido de "dados pessoais críticos". A Indonésia tem medidas obrigatórias de localização de dados desde 2012, embora tenham sido um tanto relaxadas em 2019. A Lei de Cibersegurança do Vietnã de 2019 inicialmente exigia que todas as empresas de serviços de Internet não residentes que processassem dados pessoais vietnamitas criassem uma presença física no país, mas esse requisito era abordado de forma mais restrita na legislação secundária.

Mas enquanto alguns países tenham considerado, e pelo menos parcialmente evitado, forçar as empresas a manter dados pessoais e comerciais dentro de suas fronteiras,[3] ainda há "uma tendência emergente de leis de localização de dados mais recentes e abrangentes

[1] [Nota da Tradução: foi mantida a numeração dos títulos constante no documento original]
[2] https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

[3] https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam

com alcance global".[4]

Leis recentes na Rússia e na China proíbem as empresas de enviar dados pessoais de cidadãos para fora do país. Uma lei russa de 2019 impõe multas a empresas e funcionários que não cumpram a lei de localização de dados de 2015 do país (a qual resultou ela mesma no bloqueio do site LinkedIn na Rússia). A Lei de Cibersegurança de 2017 da China exige que os operadores de infraestrutura crítica e operadores de rede armazenem "dados importantes" – pessoais e comerciais – na China, ou concluam uma ampla e rigorosa "avaliação de segurança" para solicitar a capacidade de exportarem os dados. Essas leis resultaram em empresas com cargas e riscos mais elevados, restringindo a disponibilidade de serviços de valor agregado. Muitas empresas abandonaram totalmente esses mercados.

As medidas de localização de dados geralmente focam em dados pessoais ou comerciais, e assim são voltadas principalmente para empresas que os processam, por exemplo, empresas de business-to-consumer, bancos, e plataformas de tecnologia que predominantemente lidam com conteúdo de terceiros. As medidas geralmente não visam os serviços de infraestrutura da Internet que transportam esses dados cujo conteúdo eles não conhecem. No entanto, todas as leis de localização de dados visam reconfigurar a parte mais visível da Internet – a parte onde o conteúdo se prolifera – ao longo de linhas nacionais, e isso restringe a experiência e as escolhas na Internet de todos os seus usuários. Além disso, países que impõem as medidas de localização de dados mais extremas – por exemplo, Rússia e China – tendem também a introduzir medidas para centralizar, controlar e restringir os serviços de infraestrutura da Internet, levando à fragmentação da Internet em todos os níveis.

No geral, as políticas de localização de dados existentes ainda são gerenciáveis. Elas se concentram principalmente nos dados em repouso, ou seja, dados que não estão se movendo ativamente de um dispositivo para outro ou de rede para rede, como dados armazenados em um disco rígido, um laptop ou arquivados/armazenados de alguma outra forma. As leis atuais – estendendo-se a extremos diferentes – tendem a confinar esses dados dentro das fronteiras nacionais.

Mas à medida que os estados continuam a se mover agressivamente em direção a aplicações de soberania na Internet, as tendências perceptíveis serão em direção a leis de localização de dados mais rígidas, que exigirão a re-imaginação de parte da arquitetura da Internet. À medida que essa tendência evolui, por exemplo, há uma grande probabilidade de que os países tenham que impor políticas que requeiram um controle mais centralizado sobre as rotas de tráfego.

Se a tendência de localização de dados continuar, isso criará uma rede mais restrita e menos resiliente, adaptada para cumprir as fronteiras nacionais. As empresas terão que restringir suas opções e recursos, e as operadoras de rede podem ser forçadas a usar meios não

[4] https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization/

econômicos e menos resilientes para rotear o tráfego. A segurança cibernética pode ser prejudicada porque as organizações são menos capazes de armazenar dados fora das fronteiras com o objetivo de aumentar a confiabilidade e mitigar uma ampla variedade de riscos, incluindo ataques cibernéticos e desastres nacionais.

Os países que tentam localizar dados à força impedirão a abertura e a acessibilidade da Internet global. Os dados não poderão fluir ininterruptamente com base na eficiência da rede; em vez disso, arranjos especiais precisarão ser estabelecidos para que esses dados permaneçam dentro dos limites de uma jurisdição. O resultado será o aumento das barreiras de entrada, em detrimento de usuários, empresas e governos que busquem acessar a Internet. Em última análise, a localização forçada de dados torna a Internet menos resiliente, menos global, mais cara e menos valiosa.

2.3 Quais propriedades críticas a localização forçada de dados afeta?

Propriedade crítica 1 - Uma infraestrutura aberta e acessível com um protocolo comum

A única condição essencial para uma rede ou nó acessar a Internet é adotar seus protocolos comuns, IP no mínimo. Esse modelo “sem permissão” da barreira técnica mais baixa possível é a base do rápido crescimento e alcance global da Internet. Ele não exige que os operadores de rede operem de maneira compatível com as fronteiras nacionais, pois trocam tráfego de rede para rede.

As leis de localização de dados, como as consideradas na Índia e no Vietnã, normalmente visam o processamento e o uso de categorias específicas de informações pessoais e comerciais no nível de aplicativo da Internet, por exemplo, aplicativos de computação em nuvem. Eles não visam os provedores de infraestrutura da Internet diretamente, exigindo que o tráfego que passa pelas redes esteja em conformidade com as fronteiras nacionais. No entanto, países com soberania de dados ou políticas de localização mais extremas, como China e Rússia, poderiam, em sua maioria, impor políticas que visam restringir os fluxos de dados. Portanto, embora as políticas de localização de dados com foco em dados comerciais e pessoais não criem barreiras diretamente para as redes que ingressam na Internet, ao adotar seus protocolos comuns, elas são um passo nessa direção na camada de aplicação mais visível e podem levar à fragmentação no nível de infraestrutura se a tendência continuar.

Propriedade crítica 3 - Gestão descentralizada e um sistema de roteamento distribuído comum

A Internet é uma “rede de redes”, composta por quase 70.000 redes independentes que usam os mesmos protocolos técnicos e optam por colaborar e se conectar. Cada rede toma decisões independentes sobre como rotear o tráfego para seus vizinhos, com base em suas próprias necessidades, modelo de negócios e requisitos locais. Não há controle ou

coordenação centralizada.

Embora haja uma variedade de abordagens à localização de dados, isso significa que as medidas de política se concentrariam nos serviços e na camada de aplicação das decisões de negócios de como processar dados pessoais e comerciais. Como tal, a localização pode exigir que os intermediários da Internet imponham requisitos adicionais à política de roteamento. Dependendo de quão extrema é a política de localização de dados, ela pode impactar como as informações são transmitidas entre as redes, incluindo os objetivos de reduzir a latência, fornecer redundância e replicação para distribuir dados mais perto de seu destino, e outras metas básicas de engenharia de tráfego e otimização de tráfego ameaçadoras. Isso reduziria a autonomia de roteamento das operadoras de rede e sua capacidade de otimizar a conectividade. Em geral, o alinhamento da política de roteamento com os requisitos de diferentes jurisdições cria complexidade e ineficiência desnecessárias, pois o roteamento não atenderia mais aos requisitos técnicos de conectividade, resiliência e fluxo otimizado.

É importante observar que o topologicamente mais próximo (e, portanto, o mais rápido) na rede para colocar os dados pode não estar no mesmo país. Os dados são armazenados onde faz mais sentido - e isso envolve considerações de eficiência e confiabilidade de desempenho, em vez de localização. Mesmo se os dados estiverem localizados em um país, o caminho de transmissão pode cruzar as fronteiras nacionais por motivos de resiliência ou desempenho. As medidas de localização de dados podem direta ou indiretamente forçar os dados da Internet a seguir as fronteiras nacionais em detrimento da eficiência.

Se as tendências atuais continuarem, a localização forçada de dados interferirá no roteamento distribuído autônomo e ágil da Internet, reduzindo a capacidade de colaboração com outras redes e, em última análise, restringindo o alcance global da Internet.

Propriedade crítica 5 - Rede de uso geral

A Internet é uma “rede de uso geral” porque não há limite definido para os usos que sua infraestrutura pode suportar. Uma rede de propósito geral exige que os operadores de serviços de rede executem apenas funções muito básicas: passar pacotes de dados para seu próximo destino sem se preocupar com seu conteúdo.

A localização forçada de dados exigiria limites para os serviços que podem ser oferecidos em países específicos se esses serviços envolverem o envio de dados pessoais ou comerciais através das fronteiras. Embora as leis atuais provavelmente não exijam mudanças diretas por parte dos provedores de rede, esses requisitos podem diminuir com o tempo. Regimes de localização de dados mais severos trariam uma necessidade maior de coordenação entre empresas e governos para determinar quais redes de dados estão transportando, e entre

redes para garantir que fluxos de tráfego especificados sigam as fronteiras nacionais. Quaisquer requisitos adicionais baseados no entendimento de todos os operadores da natureza de dados/conteúdo tornariam a rede mais especializada e menos de uso geral, precisando de funcionalidades adicionais, como inspeção profunda de pacotes, e prescreveriam de forma mais restrita as funções das redes em geral.

A perda de simplicidade e funcionalidade básica nas camadas de trânsito da Internet causada por medidas de localização de dados tornaria as redes mais complexas e menos eficientes, com uma necessidade maior de coordenação. Isso prejudicaria o modelo de inovação da Internet sem permissão e criaria barreiras à entrada de novas operadoras de rede e provedores de infraestrutura de Internet.

3 Conclusão

Embora alguns países do Sul da Ásia tenham recentemente evitado impor leis rígidas de localização de dados, em outras regiões, como a União Europeia, novas medidas para aumentar a "soberania dos dados" estão sendo consideradas.[5] Se a tendência de localização de dados continuar, ela restringirá serviços como a computação em nuvem, que podem ser oferecidos a usuários da Internet em diferentes países, transformando a Internet como muitas pessoas a usam hoje em uma experiência mais nacional. As medidas de localização de dados projetadas para mudar as práticas de negócios também correm o risco de moldar e restringir o fluxo desimpedido de tráfego na infraestrutura da Internet. O impacto das leis de localização de dados forçada acabará por se espalhar pela infraestrutura da Internet e minar as propriedades críticas do Modo Internet de Interconexão.

Esse provável impacto nas propriedades críticas diminuirá o valor da Internet para todos os usuários ao redor do mundo, pois ela não é mais uma rede "ponta a ponta" que oferece às pessoas em todos os lugares a mais ampla gama de oportunidades.

[5] https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html