Ribeiro e Belotti: Medidas de localização de dados

Um tribunal russo aplicou multa de US$ 260 mil ao Google alegando falhas no armazenamento dos dados pessoais coletados na Rússia em bancos de dados localizados no território do país [1]. Outras empresas, como a Meta (antigo Facebook) e o Twitter, também vêm sendo alvo da aplicação de multas e outras restrições na Rússia por, na visão das autoridades, desrespeitarem o regulamento de proteção de dados. Esse é um exemplo dos impactos concretos dos requerimentos de Localização de [illegible]rciais internacionais no contexto da economia digital.

Ainda que a Rússia seja um exemplo emblemático, tal política não é exclusividade desse país e vem crescendo em ritmo acelerado. Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a proibição de fluxo e armazenamento de dados entre países não signatários da organização, no período compreendido entre 2011 e 2021, aumentou cerca de 450% [2].

Apesar dessa relevância, ainda não existe uma definição universal para a LD. Um estudo da OCDE [3] apresenta a seguinte definição: *"um requisito legal ou administrativo obrigatório que estipula direta ou indiretamente que os dados sejam armazenados ou processados, exclusivamente ou não, dentro de uma jurisdição específica"* [4]. Logo, a LD funciona como uma restrição ao fluxo de dados, aumentando o custo de condução do negócio entre países por meio da manutenção da imposição de dados dentro de uma determinada fronteira.

Em um esforço de sistematização, Ferracane dividiu a LD em três tipos [5]. O **primeiro** versa sobre a exigência de os dados não poderem ser transferidos entre fronteiras a não ser que uma cópia seja armazenada nas localidades da jurisdição estatal. Já o **segundo**, para além da necessidade de cópia dos dados, deve-se também realizar o seu processamento localmente. A regulação russa é um exemplo de uma LD de segundo tipo. Já o **terceiro** é o mais restritivo de todos, pois proíbe expressamente o envio dos dados para o exterior, sendo impedidas até mesmo de enviar cópia dos dados para fora de um território delimitado.

2023 - www.conjur.com.br - Todos os direitos reservados.

A regulação russa é um exemplo de uma LD de segundo tipo. A Rússia requer, em seu artigo 18, §5º da lei federal de proteção de dados nº 242-FZ/2014, que os *"operadores dos dados garantam que o registro, sistematização, armazenamento, atualização e recuperação de dados pessoais dos cidadãos da Federação Russa sejam feitos usando centro de dados localizados em sua jurisdição"*.

As jurisdições que aplicam esse tipo de medida argumentam que elas são fundamentais para a soberania digital e a segurança cibernética de seus cidadãos. Quanto à questão de soberania, caso os servidores sejam exclusivamente localizados fora do território, é mais fácil realizar retaliações por meio da paralisação dos serviços, à exemplo do que ocorreu como reação de algumas empresas de tecnologia à invasão russa à Ucrânia. Em relação à preocupação de segurança, servidores estrangeiros dificultam o cumprimento de leis e regulamentos por terem menor capacidade de execução das ordens administrativas e judiciais para, por exemplo, a obtenção de determinadas informações.

Já as jurisdições que advogam pela não-aplicação ou pela redução substancial dessas medidas, tendo os EUA como principal ator, argumentam que elas geralmente constituem barreiras comerciais injustificáveis ao comércio digital, diminuem o caráter livre e global da internet e podem ser usadas para fins autoritários.

É relativamente fácil entender que a necessidade de garantir um servidor para cada jurisdição constitui um grande ônus e uma possível barreira protecionista para as empresas de tecnologia que queiram operar globalmente. As multas, com a aplicada pelo governo russo, também representam uma ameaça em potencial, especialmente quando as regras e os seus processos de aplicação não são claros e transparentes. Sem a preparação adequada, as pequenas e médias empresas ficam praticamente impossibilitadas de operar nesses mercados.

Outra consequência, é o crescente desinteresse nas iniciativas de convergência de regras e de regulamentos para o mundo cibernético, pois simplesmente se decide restringir o fluxo de dados que não sigam as normas domésticas. A aplicação dessas medidas por alguns parceiros comerciais gera, também, um efeito em cadeia de restrições em parceiros que inicialmente não pretendiam adotá-las, conforme eles aplicam regras de reciprocidade. A rede mundial de computadores fica, assim, cada vez menos global, assim como os mercados a ela associados.

Por fim, muitas jurisdições que aplicam tais medidas, especialmente as do tipo 3, possuem práticas de censura, restrições a liberdades individuais e forte controle social. Um exemplo extremo é a própria Coreia do Norte. Como consequência, a LD será mais um instrumento à disposição desses governos autoritários para dar efetividade a suas políticas de violação aos direitos humanos com impactos negativos ao comércio digital internacional.

2023 - www.conjur.com.br - Todos os direitos reservados.

A LD é, portanto, um instrumento que pode ser utilizado para criar um ônus excessivo ao fluxo transnacional de dados. Como consequência, alguns acordos internacionais já vêm tentando regular sua aplicação, mas ainda sem uniformidade e com notáveis divergências de abordagem. Uma possibilidade seria seguir os critérios de proporcionalidade propostos pela OCDE no seu Guidelines on the Protection of Privacy and Transborder Flows of Personal Data de 2013. De todo modo, vai ficando clara a crescente dificuldade de navegar nessa teia fragmentada de regulamentações relacionadas ao acesso dos mercados digitais internacionais.

Por fim, nos restam as reflexões: será que a internet como conhecemos permanecerá a mesma? Qual a regra ou o conjunto de regras a ser criado para regular o mundo digital que ofereça segurança e não represente restrições ou barreiras ao comércio internacional?

---

[1] REUTERS. Russian court fines Google $260,000 for breaching data rules. Disponível em: https://www.reuters.com/technology/russia-fines-google-260000-breaching-data-localisation-rules-tass-2022-06-16/. Acesso em 19 de julho de 2022.

[2] GONZÁLEZ, Javier López; CASALINI, Francisca; PORRAS, Juan. **A Preliminary Mapping of Data Localisation Measures.** OECD Trade Policy Paper, nº 262. Disponível em: https://www.oecd-ilibrary.org/trade/a-preliminary-mapping-of-data-localisation-measures_c5ca3fed-en. Acesso em 15 de julho de 2022.

[3] SVANTESSON, D. **Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines.** OECD Digital Economy Papers, Nº. 301, OECD Publishing, Paris. 22/12/2020. Disponível em: http://dx.doi.org/10.1787/7fbaed62-en. Acesso em 11 de julho de 2022.

[4] SVANTESSON, D. **Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines. OECD Digital Economy Papers**, Nº. 301, OECD Publishing, Paris. 22/12/2020. Disponível em: http://dx.doi.org/10.1787/7fbaed62-en. Acesso em 11 de julho de 2022.

[5] FERRACANE, M. Restrictions on cross-border data flows: a taxonomy. ECIPE Working Paper, 2017, p. 2.

2023 - www.conjur.com.br - Todos os direitos reservados.