ARTIGOS ACEITOS PARA PUBLICAÇÃO
DIREITO DIGITAL E SETOR PÚBLICO - 2020.2

ITS RIO

Pós-Graduação em Direito Digital

CEPED UERJ ITS

CONTEXTO BRASILEIRO PÓS-SCHREMS I E II: INFLUÊNCIAS DE LIMITAÇÕES GEOGRÁFICAS NO FLUXO TRANSNACIONAL DE DADOS PESSOAIS E ASPECTOS PRÁTICOS

Isabella de Castro Satiro Aragão

Contexto brasileiro pós-Schrems I e II: influências de limitações geográficas no fluxo transnacional de dados pessoais e aspectos práticos

Isabella de Castro Satiro Aragão[1]

1. Introdução

Transferências internacionais fazem parte de nosso dia-a-dia: seja através do uso de um sistema de nuvem hospedado em outro país, de compras realizadas em plataforma de *e-commerce* estrangeira ou do armazenamento de dados em *datacenter* de país terceiro, nossas relações estão carregadas de tratamentos de informações de maneira descentralizada e onipresente, em todos os pontos do mundo, ao mesmo tempo.

Entretanto, o contexto histórico atual demonstra que distinções culturais jurídicas sobre privacidade e proteção de dados entre ordenamentos de nações globais geram complexidades nessas trocas transfronteiriças, trazendo à tona uma gama de consequências que devem ser encaradas com urgência, para possibilitar o desenvolvimento pleno de todas as relações sociais, políticas e econômicas derivadas dessas transferências internacionais de informações.

As nuances e repercussões de barreiras à transferência internacional de dados pessoais entre territórios possuem influências internacionais no fluxo transnacional de informações. O presente trabalho se destina a analisar como as limitações geográficas trazidas nas decisões dos casos Schrems I e II impactaram não apenas os territórios diretamente envolvidos nos casos, mas também todas as nações do globo terrestre, dando foco aos efeitos sentidos (ou a serem sentidos) no Brasil, sob os aspectos de privacidade e proteção de dados pessoais.

2. Transferência internacional e relação com a privacidade na Europa e EUA

Em um contexto digital cada vez mais globalizado[2], fortemente influenciado pelas relações tecnológicas (ou mesmo físicas) que conectam pontos distantes do globo terrestre, se

[1] Artigo científico apresentado como trabalho acadêmico, como parte das exigências para aprovação referente ao 2º semestre de 2020 no Curso de Extensão em Direito Digital, ITS/UERJ.
Disciplinas relacionadas: LGPD, Direito Internacional e Jurisdição na Internet e Tópicos Avançados de Direito Digital.

[2] McKinsey Global Institute. *Digital Globalization: The New Era of Global Flows*. March 2016. Relatório disponível em PDF em: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows#. Acesso em 20/11/2020.
"Cross-border data flows are the hallmarks of 21st-century globalization. Not only do they transmit valuable streams of information and ideas in their own right, but they also enable other flows of goods, services, finance, and people. Virtually every type of cross-border transaction now has a digital component. Container ships still move products to markets around the world, but now customers order them on digital platforms, track their movement using RFID codes, and pay for them via digital transactions. Massive online platforms such as Alibaba,

faz essencial a existência de mecanismos que permitam atividades transfronteiriças e o fluxo internacional de informações, para viabilizar o dia-a-dia das operações de instituições e o desenvolvimento econômico das nações.

Com relação, especificamente, à transferência de dados pessoais, a Organização para a Cooperação e Desenvolvimento Econômico ("OCDE") define "*fluxos transfronteiriços de dados pessoais*" como a movimentação de dados pessoais através de fronteiras nacionais, em sua versão revisada de 2013 das "*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*", presentes no relatório "*The OECD Privacy Framework*"[3].

No contexto europeu, o Regulamento Geral sobre a Proteção de Dados 2016/679 (*General Data Protection Regulation* – "GDPR")[4] se trata de um importante instrumento regulamentador do direito europeu sobre privacidade e proteção de dados pessoais, contando com previsões específicas sobre o fluxo transfronteiriço dessas informações, que influenciam diversas outras nações.

O *Recital 101* do GDPR determina os princípios gerais para transferências internacionais de dados, dispondo que, em qualquer caso, as transferências para países terceiros e organizações internacionais só podem ser realizadas se cumprirem plenamente as previsões do referido Regulamento, de modo a garantir que o nível de proteção de dados pessoais não seja enfraquecido.

As transferências de dados pessoais para países terceiros e organizações internacionais são reguladas pelos artigos 44 a 50 do GDPR, e apenas podem ocorrer em determinadas situações previstas em lei. No escopo do presente trabalho, cumpre destacar as hipóteses abaixo listadas:

> (i) com base numa "**decisão de adequação**"[5] pela Comissão Europeia ("Comissão"), que estabeleça que um país terceiro, território, setor(es)

Amazon, eBay, and Facebook link businesses and customers anywhere in the world. By reducing the cost of transactions and allowing digital goods, services, and capital to change hands instantly, digitization is creating a more hyperconnected, hyperspeed era of global flows."

[3] OCDE. *OECD Privacy Guidelines*. 2013. Disponível em: https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm. Acesso em 20/11/2020.

[4] UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados – *General Data Protection Regulation*).

[5] European Commission. *Adequacy decisions – How the EU determines if a non-EU country has an adequate level of data protection*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em 20 de novembro de 2020.

> ou organização internacional garante um nível adequado de proteção de dados pessoais;
> (ii) se o controlador ou operador oferecer salvaguardas apropriadas, tais como: **cláusulas contratuais padrão** adotadas pela Comissão ou por uma autoridade supervisora (e autorizadas pela Comissão).

Os Estados Unidos da América (EUA) não possuem uma legislação nacional de proteção de dados, contando apenas com legislações estaduais ou setoriais esparsas e alguns projetos de lei sobre o tema. Desta forma, verifica-se que, de maneira geral, enquanto os EUA tendem a intervir de forma "reativa" com relação à privacidade, apenas quando um problema específico é identificado, a União Europeia desenvolveu um conceito paternalista e "preventivo" de privacidade, consolidado como um direito subjetivo, gerando a obrigatoriedade do Estado de proteger os dados de seus cidadãos[6].

Considerando essas distinções, para viabilizar as transferências internacionais de dados pessoais entre a União Europeia e os EUA, numa tentativa de garantir o tratamento seguro dessas informações e alinhar os interesses de todos os envolvidos, foram criados dois acordos: o *Safe Harbor* e o *Privacy Shield*. Entretanto, como veremos a seguir, ambos não se sustentaram, em face da forte complexidade trazida pelas diferentes culturas jurídicas de privacidade e proteção de dados pessoais dos EUA e União Europeia.

3. Casos Schrems I e II: fragilidade dos "escudos" de adequação

A Diretiva 95/46/CE[7], de 24 de Outubro de 1995, revogada pelo GDPR, constituía o texto de referência, a nível europeu, em matéria de proteção de dados. Em seu artigo 25 (6), sobre a transferência de dados pessoais para países terceiros, estabeleceu-se que a Comissão Europeia poderia constatar que um país terceiro assegura um nível de proteção de dados

[6] VERONESE, Alexandre. *Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil.* In: MENDES, Laura Schertel; et. al. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 306-307.
"Uma parte da literatura indicará que existem duas culturas jurídicas nos dois lados do Atlântico Norte. (...) O conceito norte-americano de privacidade teria sido uma continuada evolução em prol do fortalecimento da proteção dos cidadãos contra a interveniência estatal. (...) Em síntese, o direito constitucional e o direito público dos Estados Unidos da América seriam pouco intervenientes no contexto geral nesse tema, ao contrário do que ocorria na União Europeia. (...) Nos países europeus a situação era bem diversa e a intervenção estatal na proteção dos dados pessoais era efetivada pela atuação estatal em relação aos particulares. Tal proteção foi alçada ao patamar de obrigação dos Estados perante os cidadãos, no decorrer de décadas de evolução na cultura jurídica daqueles países."
[7] UNIÃO EUROPEIA. *Diretiva (UE) 95/46/CE do Parlamento Europeu e do Conselho*, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

pessoais adequado em virtude de sua legislação interna ou de seus compromissos internacionais, com o intuito de proteção do direito à vida privada e das liberdades e direitos fundamentais das pessoas.

Com base nessa disposição, e levando em consideração as diferenças culturais jurídicas de proteção de dados pessoais entre União Europeia e EUA, a Decisão 2000/50/EC[8], de 26 de julho de 2000, aprovou os princípios do acordo *Safe Harbor* a serem adotados pelas organizações dos EUA, a fim de limitar as incertezas em relação ao impacto do "padrão de adequação" exigido pela União Europeia e garantir a proteção dos dados pessoais dos cidadãos europeus nas relações comerciais e demais transações internacionais entre os dois territórios.

Contudo, diante da divulgação de informações sobre a interceptação de dados pessoais – inclusive de cidadãos europeus – pelo programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), denominado PRISM, reveladas por Edward Snowden em 2013, as salvaguardas do *Safe Harbor* passaram a ser consideradas insuficientes para a finalidade de "porto seguro" pretendida[9].

Neste sentido, diante do nível inadequado de proteção de dados pessoais apurado, a Decisão do Caso C-362/14 em Outubro de 2015, proferida pelo Tribunal de Justiça da União Europeia ("CJEU") em resposta a ação apresentada por Maximillian Schrems, **invalidou a Decisão 2000/520, derrubando o acordo *Safe Harbor* entre a União Europeia e os EUA[10]**.

Cumpre notar que, em razão da Decisão da Comissão 2010/87/EU[11], a utilização de modelo de cláusula contratual padrão (*Standard Contractual Clause* – SCC) disponibilizada no Anexo da Decisão, aprovada pela Comissão Europeia e considerada como salvaguarda suficiente para a proteção da privacidade e direitos e liberdades fundamentais de indivíduos, passou a ser uma opção viável para transferências internacionais de dados entre controladores europeus e operadores estadunidenses.

---

[8] UNIÃO EUROPEIA. Comissão das Comunidades Europeias. *Decisão da Comissão 2000/520/CE*, de 26 de Julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de *Safe Harbor* e pelas respectivas questões mais frequentes (FAQ) emitidas pelo *Department of Commerce* dos Estados Unidos da América.

[9] VENTRE, Giovanna; MORAES, Thiago Guimarães. *A saga de Schrems e os programas de conformidade à proteção de dados no Brasil*. JOTA, 09 de outubro de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/saga-schrems-programas-conformidade-protecao-dados-09102020. Acesso em 21/11/2020.

[10] UNIÃO EUROPEIA. Tribunal de Justiça. *Acórdão (Grande Seção) de 6 de outubro de 2015*: Maximillian Schrems contra *Data Protection Commissioner* (processo C-362-14). Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=452958. Acesso em 21/11/2020.

[11] UNIÃO EUROPEIA. Comissão Europeia. *Decisão da Comissão 2010/87/EU,* de 5 de fevereiro de 2010, sobre cláusulas contratuais padrão para a transferência de dados pessoais para operadores estabelecidos em países terceiros, à luz da Diretiva 95/46/EC do Parlamento Europeu e do Conselho.

Entretanto, Maximillian Schrems reformulou sua ação, para questionar também a validade dessas cláusulas contratuais padrão em face das finalidades de tratamento de dados pessoais para programas de monitoramento, considerando o potencial acesso do governo estadunidense aos dados pessoais de cidadãos europeus, a qual foi levada a novo julgamento, sob o nome popular de "Schrems II" (caso C-311/18).

Ao mesmo tempo, visando substituir o *Safe Harbor*, em 12 de julho de 2016, a Comissão Europeia emitiu a Decisão de Execução (UE) 2016/1250[12], que aprovou oficialmente um novo acordo transatlântico entre a União Europeia e os EUA, de adoção voluntária por parte de interessados, adotando uma estrutura de "decisão de adequação" para transferências internacionais de dados pessoais para organizações estadunidenses mais robusta[13]: o *Privacy Shield*.

A Diretiva 95/46 foi revogada e substituída pelo GDPR, que passou a valer a partir de Maio de 2018; entretanto, os problemas relacionados à transferência internacional de dados entre a União Europeia e os EUA não pararam por aí.

Note-se que, apesar de o caso Schrems II não fazer remissão específica ao *Privacy Shield*, seus efeitos respaldaram no referido instrumento na análise da CJEU. Três razões podem explicar essa conexão: (i) o texto do *Privacy Shield* faz menção a cláusulas contratuais padrão como um possível instrumento de transferência de dados pessoais; (ii) as previsões de salvaguardas e limitações trazidas no acordo não definem mecanismos específicos para a validade das transferências internacionais (abrindo margem para o uso das SCCs); e (iii) a Corte Suprema da Irlanda encaminhou diretamente o caso Schrems II para a CJEU, questionando, principalmente, sobre a relevância da determinação de adequação da Comissão Europeia sobre o *Privacy Shield* para a questão do caso em comento[14].

Como resultado, a recente decisão da CJEU, proferida em 16 de julho de 2020[15], dentre suas variadas conclusões, determinou que **a Decisão 2016/1250 seria considerada inválida e, consequentemente, o *Privacy Shield***, sob o argumento de que, diante da aplicação da GDPR

---

[12] UNIÃO EUROPEIA. Comissão Europeia. *Decisão de Execução (UE) 2016/1250*, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo *Privacy Shield* UE-EUA, com fundamento na Diretiva 95/46/CE.

[13] A título de aprofundamento nas diferenças entre os instrumentos: BCLP. *A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor"*. 17 de julho de 2016. Disponível em: https://www.bclplaw.com/en-US/insights/a-side-by-side-comparison-of-privacy-shield-and-the-safe-habor.html. Acesso em 21/11/2020.

[14] FENNESSY, Caitlin. *The Privacy Shield review and its potential to impact Schrems II*. IAPP, 5 de novembro de 2019. Disponível em: https://iapp.org/news/a/the-privacy-shield-review-and-its-potential-to-impact-schrems-ii/. Acesso em 21/11/2020.

[15] UNIÃO EUROPEIA. Tribunal de Justiça. *Acórdão (Grande Sessão) de 16 de julho de 2020*: *Data Protection Commissioner* contra Facebook Ireland Ltd e Maximillian Schrems (processo C-311/18). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311&qid=1606742479317. Acesso em 21/11/2020.

à transferência de dados pessoais para finalidades comerciais, os limites para a proteção de dados pessoais da lei interna dos EUA sobre acesso e uso de dados pessoais de cidadãos europeus por autoridades públicas estadunidenses não satisfaria os requerimentos equivalentes na lei da União Europeia, havendo violação do princípio da proporcionalidade na autorização da realização de vigilância massiva.

Ademais, a decisão estabeleceu que, a não ser que exista uma decisão de adequação válida por parte da Comissão Europeia, a autoridade de proteção de dados competente deve suspender ou proibir a transferência de dados pessoais para um país terceiro que tenha utilizado cláusulas contratuais padrão adotadas pela Comissão se, na visão dessa autoridade e a partir das circunstâncias da transferência, essas cláusulas não possam ser cumpridas pelo país terceiro e a proteção de dados pessoais transferidos não possa ser garantida por outros meios, quando o controlador ou operador não suspenda ou pare de realizar essa transferência.

4. "Rosa dos ventos": movimentações e orientações recentes na Europa

Após ultrapassarem as barreiras de segurança e "escudos" de acordos transatlânticos entre a União Europeia e os EUA, as decisões supra referidas causaram grande polêmica e despertaram grandes inseguranças: como os EUA e outros países terceiros poderiam continuar a realizar transações e transferências internacionais de dados pessoais mútuas com a União Europeia e quais seriam os limites desses compartilhamentos?

Diversas foram as soluções e discussões apresentadas, numa espécie de "rosa dos ventos" de orientações. Inicialmente, é necessário frisar que, logo após o julgamento da Decisão que invalidou o *Privacy Shield*, o Comitê Europeu para a Proteção de Dados (*European Data Protection Board* – "EDPB") publicou um documento em formato de FAQ (*Frequently Asked Questions*) sobre o caso.

O documento afirmou não haver prazo adicional de adaptação para as empresas que realizavam transferências internacionais para os EUA com base no *Privacy Shield*, reforçando que, como a decisão não manteve os efeitos do acordo, quaisquer transações com base no *Privacy Shield* são imediatamente ilegais.

Ademais, o FAQ reforçou a possibilidade de transferência de dados para os EUA por meio das hipóteses de derrogação previstas no artigo 49 do GDPR[16]; e a necessidade de se

[16] **GDPR**. "Artigo 49º - Derrogações para situações específicas. 1. Na falta de uma decisão de adequação nos termos do artigo 45(3), ou de garantias adequadas nos termos do artigo 46, incluindo normas corporativas globais, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só serão efetuadas caso se verifique uma das seguintes condições:

avaliar, caso a caso, a adoção de SCCs e medidas suplementares que garantam um nível adequado de proteção dos dados pessoais transferidos, verificando também, quando necessário, se o grau de proteção estabelecido pelas leis internas de países terceiros é essencialmente equivalente àquele garantido na Área Econômica Europeia.

Em Outubro de 2020, a Autoridade Europeia para a Proteção de Dados (*European Data Protection Supervisor* – "EDPS") publicou um documento estratégico[17] visando garantir e monitorar o cumprimento das instituições, órgãos, empresas e agências europeias com as disposições da Decisão do "Schrems II", endereçando planos de ação de curto a médio prazo, que envolvem o mapeamento, comunicação e cuidados em serviços futuros e novas operações de tratamento de dados; e avaliações de impacto de transferências, comunicação e avaliações conjuntas.

Outrossim, na 41ª Sessão Plenária do EDPB, foram adotadas recomendações sobre medidas complementares aos mecanismos de transferência internacional[18], de modo a assegurar o cumprimento do nível de proteção de dados pessoais estabelecido na Decisão do "Schrems II", bem como as recomendações sobre as Garantias Essenciais Europeias para medidas de vigilância, derivadas das Recomendações 02/2020 do EDPB[19].

---

a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência proposta, após ter sido informado dos possíveis riscos de tais transferências devido à falta de uma decisão de adequação e das garantias adequadas;
b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o controlador ou para a implementação de diligências prévias à formação do contrato, a pedido do titular dos dados;
c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o controlador e outra pessoa natural ou jurídica;
d) A transferência for necessária por importantes razões de interesse público;
e) A transferência for necessária à declaração, ao exercício ou à defesa de direitos em processo judicial;
f) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;
g) A transferência for realizada a partir de um registro que, nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto.".

[17] European Data Protection Supervisor. *Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling*. EDPS, 29 de outubro de 2020. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and-agencies_en. Acesso em 21/11/2020.

[18] European Data Protection Board. *European Data Protection Board – 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II*. EDPB, 11 de novembro de 2020. Disponível em: https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en. Acesso em 22/11/2020.

[19] European Data Protection Board. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*. EDPB, 10 de novembro de 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_pt. Acesso em 21/11/2020.

Tais recomendações serão submetidas a consulta pública e serão aplicáveis imediatamente após a sua publicação. O texto das recomendações traz um passo-a-passo que os exportadores de dados (*data exporters*) devem observar para descobrir se precisam de medidas complementares para transferir dados pessoais para fora da União Europeia, e quais seriam as medidas mais eficazes, a partir de uma lista não exaustiva de exemplos dessas medidas e condições de aplicação.

Entretanto, ao fim e ao cabo, os *data exporters* serão os responsáveis por fazer a avaliação no caso concreto, considerando o contexto da transferência, a lei de países terceiros e o mecanismo para a realização dessa transferência internacional. Essa avaliação deverá ser diligente e documentada, uma vez que as decisões tomadas a partir dessa avaliação gerarão eventuais responsabilidades aos exportadores de dados.

Já na 42ª Sessão Plenária do EDPB, foram apresentados dois novos esboços de cláusulas contratuais padrão[20]: uma para ser utilizada entre controladores e operadores, e outra para transferências de dados fora da União Europeia. Com relação a esse segundo conjunto de cláusulas, as SCCs propostas substituirão as SCCs existentes (baseadas na Diretiva 95/46), pois possuem atualizações na mesma linha dos requerimentos da GDPR e considerando a Decisão do "Schrems II". Junto com o EDPS, a EDPB elaborará um parecer conjunto sobre as duas propostas de SCCs.

Embora a antecipação da elaboração e divulgação dos projetos de SCCs seja fundamental para o bom desenvolvimento das relações internacionais, a presidente do EDPB afirmou que as novas cláusulas para a transferência de dados pessoais a países terceiros não são uma solução global para as transferências de dados pós-Schrems II, frisando a importância de que os exportadores de dados sigam o passo-a-passo de medidas suplementares para garantir nível adequado de proteção dos dados pessoais, equivalente aos padrões europeus.

Finalmente, o jornal *Financial Times* noticiou, recentemente, que a Comissão Europeia esboçou um projeto para uma renovada cooperação entre a União Europeia e os EUA sobre uma variedade de temas, inclusive sob o aspecto de proteção de dados pessoais – devendo abranger a questão da transferência internacional de dados. A proposta visa criar uma

[20] European Data Protection Board. *European Data Protection Board – 42nd Plenary session: Presentation of two new sets of SCCs & EDPB adopts statement on ePrivacy Regulation*. EDPB, 20 de novembro de 2020. Disponível em: https://edpb.europa.eu/news/news/2020/european-data-protection-board-42nd-plenary-session-presentation-two-new-sets-sccs_pt. Acesso em 22/11/2020.

abordagem conjunta para o cumprimento de leis de proteção de dados e combate a ameaças de cibersegurança e espera lançar uma nova agenda transatlântica já em 2021[21].

A partir de todas as orientações supracitadas, é possível notar que a transferência internacional de dados pessoais é um tema naturalmente complexo, com diversas consequências, mas infinitas possibilidades de resolução de seus desafios. Abaixo, veremos como todas as considerações derivadas dos casos Schrems I e II norteiam o rumo brasileiro sob o aspecto de privacidade e proteção de dados pessoais e como a relação do Brasil com a Europa (e com outros países) pode ser impactada.

5. Brasil: LGPD e transferências internacionais

Preliminarmente, cumpre ressaltar que a Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/18 – "LGPD")[22] traz, em seu artigo 5º, incisos I e XV, a definição de dado pessoal como toda "*informação relacionada a uma pessoa natural identificada ou identificável*" e o conceito de transferência internacional de dados, como a "*transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro*".

Sob a influência do GDPR, a LGPD lista, em seu artigo 33, hipóteses legais em que a transferência internacional de dados pessoais é permitida, pincelando requisitos específicos desse compartilhamento transfronteiriço[23].

---

[21] IAPP. *EU offers new alliance with US on data protection*. 30 de novembro de 2020, publicado originalmente no jornal Financial Times. Disponível em: https://iapp.org/news/a/eu-offers-new-alliance-with-us-on-data-protection/. Acesso em 03/12/2020.

[22] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). DOU: publicado em 15/08/2020.

[23] **LGPD**. "Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;
III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
V - quando a autoridade nacional autorizar a transferência;
VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

Ademais, os artigos 34 e 35 da LGPD discorrem sobre algumas condições para se considerar a validade dos mecanismos legais de transferência internacional previstos, que deverão ser observadas pela Autoridade Nacional de Proteção de Dados brasileira ("ANPD), tais como:

a) a **avaliação do nível de proteção de dados do país estrangeiro ou de organismo internacional**, para verificar se há grau adequado (no mesmo sentido das "decisões de adequação" europeias, seguindo um modelo geográfico regulatório[24]); e
b) a **definição do conteúdo de cláusulas-padrão contratuais**, assim como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta.

Importante frisar que, embora a ANPD tenha sido criada ainda em 2018[25], a Autoridade apenas teve sua estrutura regimental definida e aprovada em agosto de 2020[26] e os indicados para a composição do primeiro Conselho Diretor da ANPD foram muito recentemente nomeados, dando início aos mandatos no dia 06 de novembro de 2020[27].

Devido à sua recente formação, a Autoridade ainda não exerceu nenhum ato de sua competência e, portanto, ainda não há orientações consolidadas no "mapa" de transferência internacional de dados pessoais no Brasil, restando muitas dúvidas sobre a aplicação prática e limitações das previsões legais sobre o tema.

6. "Pontos cardeais": principais impactos de Schrems no Brasil

Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional."

[24] MARQUES, Fernanda Mascarenhas; Aquino, Theófilo Miguel de. *O regime de transferência internacional de dados da LGPD: delineando as opções regulatórias em jogo.* In: MENDES, Laura Schertel; et. al. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 306-307.
"A escolha regulatória contida na redação do art. 33, I, do PL 5.276/2016 e da LGPD aplicada às transferências internacionais de dados reflete o chamado 'modelo geográfico'. (...) Esse modelo é definido como geográfico porque 'concentra os critérios de equivalência e adequação que autorizam a transferência internacional no nível de proteção de cada país, em sua legislação doméstica e compromissos internacionais'".

[25] **LGPD**. "Art. 65. Esta Lei entra em vigor:
I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B".

[26] BRASIL. *Decreto nº 10.474, de 26 de agosto de 2020*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. DOU: publicado em 27/08/2020, edição 165, seção 1, página 6, órgão: Atos do Poder Executivo.

[27] BRASIL. *Decretos de 5 de novembro de 2020*. Casa Civil. DOU: publicado em 06/11/2020, edição 212, seção 2, página 1, órgão: Atos do Poder Executivo.

Considerando o recente trajeto brasileiro em direção à proteção de dados pessoais no país, as decisões dos casos Schrems I e II saltam ainda mais aos olhos, representando influências importantes na rota a ser seguida pelo Brasil – que, em comparação aos EUA, possui uma tradição jurídica sobre privacidade e proteção de dados pessoais mais aproximada da União Europeia, ainda que em processo de desenvolvimento.

Um dos "pontos cardeais" trazidos pelas decisões europeias é sua influência na atuação da recém-formada ANPD em âmbito brasileiro. Levando-se em consideração que a redação da LGPD foi bastante influenciada pelo GDPR[28], não seria de se admirar que as atividades exercidas pela Agência brasileira também olhassem para o exemplo estrangeiro para fundamentar e guiar suas práticas[29].

Neste sentido, observe-se que a LGPD traz elementos muitos similares aos da decisão "Schrems II" – como a responsabilidade do controlador de verificar se as cláusulas-padrão estão sendo cumpridas, com base no princípio da responsabilização[30], e um sistema organizado de definição, aprovação e fiscalização dessas cláusulas –, o que poderia fazer com que a ANPD, em suas validações e autorizações de mecanismos de transferências internacionais, questionasse e buscasse invalidar determinados fluxos transfronteiriços (até mesmo do Brasil para os EUA)[31].

Ainda, as muito aguardadas "decisões de adequação" a serem avaliadas pela ANPD devem seguir os mesmos passos da União Europeia, buscando permitir o bom funcionamento da economia digital atual e um relacionamento saudável com o grupo econômico europeu, a fim de garantir o reconhecimento do nível de adequação do Brasil com relação à proteção de dados pessoais e a continuidade das trocas de dados entre Brasil e União Europeia.

Ao mesmo tempo em que permanece a dúvida sobre como a LGPD se posicionará com relação à legislação de vigilância dos EUA[32], é certo que o país norte-americano é um parceiro

---

[28] GODOY, Bruna M. W. *Privacy Shield EUA x Brasil: é possível?* In: PALHARES, Felipe; et. al. *Temas Atuais de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2020.

[29] URUPÁ, Marcos. *LGPD é a garantia da entrada do Brasil na economia digital*. Teletime, 16 de novembro de 2020. Disponível em: https://teletime.com.br/16/11/2020/lgpd-e-a-garantia-da-entrada-do-brasil-na-economia-digital/. Acesso em 22/11/2020.

[30] **LGPD**. "Artigo 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.".

[31] CABELLA, Daniela M. M. S.; TEÓFILO, Caroline. *Schrems II e LGPD: reflexões acerca dos impactos da decisão da CJEU no cenário brasileiro.* Migalhas, 13 de agosto de 2020. Disponível em: https://migalhas.uol.com.br/depeso/331982/schrems-ii-e-lgpd--reflexoes-acerca-dos-impactos-da-decisao-da-cjeu-no-cenario-brasileiro. Acesso em 03/12/2020.

[32] Ibidem.

comercial de extrema relevância para o Brasil e, portanto, as relações com esta nação devem ser preservadas para se manter o fluxo de informações e os benefícios mútuos entre os países.

Um eventual acordo transatlântico entre EUA e Brasil seria possível, no futuro, no mesmo sentido da promessa de nova aliança feita pela União Europeia anteriormente mencionada; entretanto, no momento, parece ser mais diplomaticamente apropriado buscar outros mecanismos eficientes de transferência internacional de dados (como cláusulas contratuais específicas, por exemplo).

Ademais, considerando a economia globalizada baseada em dados que necessita de fluxos contínuos de informações, as decisões Schrems I e II e seus desdobramentos são relevantes para garantir modelos flexíveis, mas também seguros para a realização de múltiplas transferências internacional de dados pessoais no dia-a-dia de instituições, órgãos e empresas.

Isso porque a burocratização de fluxos internacionais de dados, sem a apresentação de soluções viáveis para torná-los dinâmicos, pode criar barreiras comerciais e afastar investimentos estrangeiros no Brasil, devido à insegurança jurídica e aos custos (entendidos como tempo, dinheiro e oportunidades) inerentes ao atendimento de exigências exageradas[33].

A atração de investimentos externos e credibilidade internacional também tendem a ser favorecidas através da aproximação do modelo brasileiro com o posicionamento europeu e eventual reconhecimento do grau de adequação de proteção aos dados pessoais da LGPD pela União Europeia, já que essa convergência de entendimentos potencialmente criaria mais chances de entrada do Brasil na OCDE.

Por fim, diante da emergência em saúde pública a nível global causada pelo COVID-19 e do surgimento de diversas tecnologias que requerem a transferência internacional de uma imensa quantidade de dados pessoais para o controle de disseminação da doença, a cooperação internacional por meio da harmonização regulatória e coerência política com relação ao compartilhamento transfronteiriço de informações é essencial para preservar a essência da proteção de dados pessoais e permitir a recuperação econômica dos países no combate à crise sanitária e humanitária trazida pelo COVID-19[34].

7. Conclusão

[33] LEONARDI, Marcel. *Transferência Internacional de Dados Pessoais*. In: MENDES, Laura Schertel; et. al. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021, p. 298.
[34] SOUZA, Carlos Affonso. *Internet & Jurisdiction and ECLAC – Regional Status Report 2020*. United Nations Economic Commission for Latin America and the Caribbean (ECLAC), novembro de 2020. Prefácio. Disponível em: https://www.cepal.org/en/publications/46421-internet-jurisdiction-and-eclac-regional-status-report-2020. Acesso em 03/12/2020.

Diante do "mapa-múndi" de possibilidades de transferências internacionais, desafios regulatórios e operacionais surgem a todo instante, principalmente em razão das diferentes tradições jurídicas e legislativas entre as nações, que podem gerar consequências na privacidade e proteção dos dados pessoais dos cidadãos globais.

Entretanto, independentemente de qual cultura jurídica sobre privacidade seja a mais apropriada, é certo que fatores externos como a realidade socioeconômica, interesses internos e relações políticas externas devem ser consideradas na representação espacial de cada nação sobre transferências internacionais, desde que mantendo a essência dos princípios de proteção de dados pessoais e a eficácia de sua aplicação em fluxos de dados transfronteiriços.

Para manter um relacionamento diplomático com todos os lados envolvidos, é essencial que o Brasil (e, especialmente, a ANPD) faça a sua própria "projeção cartográfica" sobre a transferência internacional de dados pessoais – ou seja, balanceando os níveis de adequação dos países terceiros com quem realiza transações internacionais, caso a caso, ou utilizando os mecanismos apropriados, podendo se inspirar em modelos estrangeiros para a aplicação prática dessas hipóteses, mas abrindo espaço para o desenvolvimento de um modelo nacional, soberano e democrático, que permita a transferência internacional de dados pessoais com segurança jurídica e técnica para todos os envolvidos.

Referências bibliográficas

BRASIL. *Decreto nº 10.474, de 26 de agosto de 2020*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. DOU: publicado em 27/08/2020, edição 165, seção 1, página 6, órgão: Atos do Poder Executivo.

BRASIL. *Decretos de 5 de novembro de 2020*. Casa Civil. DOU: publicado em 06/11/2020, edição 212, seção 2, página 1, órgão: Atos do Poder Executivo.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). DOU: publicado em 15/08/2020.

CABELLA, Daniela M. M. S.; TEÓFILO, Caroline. *Schrems II e LGPD: reflexões acerca dos impactos da decisão da CJEU no cenário brasileiro.* Migalhas, 13 de agosto de 2020. Disponível em: https://migalhas.uol.com.br/depeso/331982/schrems-ii-e-lgpd--reflexoes-acerca-dos-impactos-da-decisao-da-cjeu-no-cenario-brasileiro. Acesso em 03/12/2020.

European Commission. *Adequacy decisions – How the EU determines if a non-EU country has an adequate level of data protection*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em 20 de novembro de 2020.

European Data Protection Board. *European Data Protection Board – 41st Plenary session: EDPB adopts recommendations on supplementary measures following Schrems II*. EDPB, 11 de novembro de 2020. Disponível em: https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en. Acesso em 22/11/2020.

European Data Protection Board. *European Data Protection Board – 42nd Plenary session: Presentation of two new sets of SCCs & EDPB adopts statement on ePrivacy Regulation*. EDPB, 20 de novembro de 2020. Disponível em: https://edpb.europa.eu/news/news/2020/european-data-protection-board-42nd-plenary-session-presentation-two-new-sets-sccs_pt. Acesso em 22/11/2020.

European Data Protection Board. *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*. EDPB, 10 de novembro de 2020. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_pt. Acesso em 21/11/2020.

European Data Protection Supervisor. *Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling*. EDPS, 29 de outubro de 2020. Disponível em: https://edps.europa.eu/data-protection/our-work/publications/papers/strategy-union-institutions-offices-bodies-and-agencies_en. Acesso em 21/11/2020.

FENNESSY, Caitlin. *The Privacy Shield review and its potential to impact Schrems II*. IAPP, 5 de novembro de 2019. Disponível em: https://iapp.org/news/a/the-privacy-shield-review-and-its-potential-to-impact-schrems-ii/. Acesso em 21/11/2020.

IAPP. *EU offers new alliance with US on data protection*. 30 de novembro de 2020, publicado originalmente no jornal Financial Times. Disponível em: https://iapp.org/news/a/eu-offers-new-alliance-with-us-on-data-protection/. Acesso em 03/12/2020.

McKinsey Global Institute. *Digital Globalization: The New Era of Global Flows*. March 2016. Relatório disponível em PDF em: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows#. Acesso em 20/11/2020.

MENDES, Laura Schertel; et. al. *Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

OCDE. *OECD Privacy Guidelines*. 2013. Disponível em: https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm. Acesso em 20/11/2020.

PALHARES, Felipe; et. al. *Temas Atuais de Proteção de Dados*. São Paulo: Thomson Reuters Brasil, 2020.

SOUZA, Carlos Affonso. *Internet & Jurisdiction and ECLAC – Regional Status Report 2020*. United Nations Economic Commission for Latin America and the Caribbean (ECLAC), novembro de 2020. Prefácio. Disponível em: https://www.cepal.org/en/publications/46421-internet-jurisdiction-and-eclac-regional-status-report-2020. Acesso em 03/12/2020.

UNIÃO EUROPEIA. Comissão das Comunidades Europeias. *Decisão da Comissão 2000/520/CE*, de 26 de Julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de *Safe Harbor* e pelas respectivas questões mais frequentes (FAQ) emitidas pelo *Department of Commerce* dos Estados Unidos da América.

UNIÃO EUROPEIA. Comissão Europeia. *Decisão da Comissão 2010/87/EU,* de 5 de fevereiro de 2010, sobre cláusulas contratuais padrão para a transferência de dados pessoais para operadores estabelecidos em países terceiros, à luz da Diretiva 95/46/EC do Parlamento Europeu e do Conselho.

UNIÃO EUROPEIA. Comissão Europeia. *Decisão de Execução (UE) 2016/1250*, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo *Privacy Shield* UE-EUA, com fundamento na Diretiva 95/46/CE.

UNIÃO EUROPEIA. *Diretiva (UE) 95/46/CE do Parlamento Europeu e do Conselho*, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados – *General Data Protection Regulation*).

UNIÃO EUROPEIA. Tribunal de Justiça. *Acórdão (Grande Seção) de 6 de outubro de 2015*: Maximillian Schrems contra *Data Protection Commissioner* (processo C-362-14). Disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=169195&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=452958. Acesso em 21/11/2020.

UNIÃO EUROPEIA. Tribunal de Justiça. *Acórdão (Grande Sessão) de 16 de julho de 2020*: *Data Protection Commissioner* contra Facebook Ireland Ltd e Maximillian Schrems (processo C-311/18). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311&qid=1606742479317. Acesso em 21/11/2020.

URUPÁ, Marcos. *LGPD é a garantia da entrada do Brasil na economia digital*. Teletime, 16 de novembro de 2020. Disponível em: https://teletime.com.br/16/11/2020/lgpd-e-a-garantia-da-entrada-do-brasil-na-economia-digital/. Acesso em 22/11/2020.

VENTRE, Giovanna; MORAES, Thiago Guimarães. *A saga de Schrems e os programas de conformidade à proteção de dados no Brasil*. JOTA, 09 de outubro de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/saga-schrems-programas-conformidade-protecao-dados-09102020. Acesso em 21/11/2020.