Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 31.07.2022
Aprovado em: 11.09.2022

Revista de Direito, Governança e Novas Tecnologias

GOVERNANÇA E REGULAÇÃO DO FLUXO DE DADOS PESSOAIS: OBSERVANDO OS CASOS SCHREMS (TJUE)

PERSONAL DATA FLOW GOVERNANCE AND REGULATION: OBSERVING THE SCHREMS CASES (CJEU)

Ariel Augusto Lira Moura[1]

Leonel Severo Rocha[2]

Resumo: O presente artigo tem como grande tema o estudo da regulação e governança do fluxo de dados pessoais a partir da análise dos casos Schrems I e II, julgados pelo Tribunal de Justiça da União Europeia em 2015 e 2020, respectivamente. Após a análise dos casos, avança-se para observação do papel de diversos atores, público e privados, na governança e regulação sobre proteção de dados pessoais. A metodologia utilizada é a pragmático-sistêmica, aliada à técnica de pesquisa bibliográfica e documental. A partir da observação das novas conformações organizacionais e regulatórias da sociedade atual, conclui-se que o papel da autorregulação privada, ressaltado a partir do caso Schrems II, mostra-se essencial. A centralidade nas decisões de adequação deve ser relativizada ou ao menos complementada para que a proteção de dados se estruture por meio de outras formas (híbridas) de regulação (autorregulação regulada) e governança (em rede).

Palavras-chave: Teoria dos Sistemas; Casos Schrems; fluxo de dados pessoais; governança; regulação.

Abstract: This article's general theme is the study of regulation and governance of personal data flow from the analysis of the Schrems I and II cases, judged by the Court of Justice of the European Union in 2015 and 2020, respectively. After analyzing these cases, it observes the role of different (public and private) actors in the governance and regulation of personal data protection. The methodology is the pragmatic-systemic, with bibliographic and documental research techniques. Considering the new organizational and regulatory conformations of digital society, it concludes that the role of private self-regulation, highlighted in the Schrems II case, proves to be essential. The centrality in adequacy decisions must be relativized or at least complemented so that data protection structures through other (hybrid) forms of regulation (regulated self-regulation) and governance (network).

Keywords: System Theory; The Schrems Cases; data flow; governance; regulation;

[1] Mestrando em Direito Público pela Universidade do Vale do Rio dos Sinos (UNISINOS). Bolsista PROEX/CAPES, vinculado ao Grupo de Pesquisa Teoria do Direito (CNPq). Tem experiência na área de Direito, com ênfase em Teoria do Direito, Filosofia do Direito e Direito Constitucional, atuando principalmente nos seguintes temas: Teoria dos Sistemas Sociais; Constitucionalismo Social; Direito e Governança Digital; Privacidade e Proteção de Dados. Endereço para acessar o CV Lattes: http://lattes.cnpq.br/9370431630574637. ORCID: https://orcid.org/0000-0002-1341-7740. E-mail: ari.moura06@gmail.com ou aliram@edu.unisinos.br
[2] Doutor pela École des Hautes études en Sciences Sociales (Ehess), com estudos de pós-doutorado em Sociologia do Direito pela Università degli Studi di Lecce na Itália. Professor titular da Universidade do Vale do Rio dos Sinos (mestrado e doutorado) e do Programa de Pós-Graduação em Direito (PPGD) da Universidade Regional Integrada do Alto Uruguai (URI). Bolsista de Produtividade em Pesquisa do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) – Nível 1D. Tem experiência na área de Direito, com ênfase em Teoria Geral do Direito, trabalhando principalmente os seguintes temas: Teoria dos Sistemas Sociais, Constitucionalismo, Democracia e Teoria do Direito. Endereço para acessar o CV Lattes: http://lattes.cnpq.br/3283434447576859. ORCID: https://orcid.org/0000-0002-6971-1412. E-mail: leonel@unisinos.br

1 INTRODUÇÃO

O presente artigo tem como grande tema a regulação e governança do fluxo de dados, o qual se inscreve no processo de "digitalização" dos processos sociais (econômicos, políticos, jurídicos). Nesse sentido, a União Europeia mostra-se como um *locus* privilegiado para observação da temática, seja pela prominência de seu mercado interno para a economia global, seja pela sua proeminência regulatória no que diz respeito a proteção de dados.

Por essa razão, optou-se por centrar a análise de dois casos emblemáticos sobre a transferência internacionais julgados pelo Tribunal de Justiça da União Europeia, os denominados casos Schrems (I e II). Por mais que a discussão gire em torno do embate do regime regulatório europeu com o dos EUA, o impacto a nível mundial é latente, porquanto discutem-se questões centrais sobre a governança e regulação da proteção de dados. A metodologia pragmático-sistêmica (AUTOR, 2013), aliada à técnica de pesquisa bibliográfica e documental.

Nesse sentido, no primeiro tópico, após uma rápida introdução aos mecanismos jurídicos do Tribunal de Justiça, analise-se os casos Schrems I e II, julgados pelo Tribunal de Justiça da União Europeia em 2015 e 2020, respectivamente. Observa-se, dessa forma, as mudanças nos processos político-jurídicos entre União Europeia e os EUA no que concerne a transferência internacional de dados após as invalidações dos dois grandes acordos internacionais que foram invalidados pelo Tribunal, o Safe Harbour, no primeiro caso, e o Privacy Shield, no segundo.

No segundo tópico, a partir do instrumental teórico da Teoria dos Sistemas, os casos Schrems são redimensionados, inscrevendo-os em um paradigma global da governança e regulação do fluxo de dados. Conclui-se que a centralidade nas decisões de adequação (Schrems I) ainda mostram uma vinculação à centralização dos processos político-jurídicos no Estado. Com o conceito de governança (em "oposição" à governo) quer-se ressaltar, justamente, que a proteção de dados dimensões movimenta novas formas de organização da sociedade atual. Como pode se indicar pelo julgamento do caso Schrems II, a autorregulação das organizações privadas tem um papel fundamental neste âmbito. Assim, fala-se em novas formas ("híbridas") de regulação (autorregulação regulada) e governança (em rede) que não podem ser explicadas apenas pela distinção público/privada.

2 SCHREMS I (C-362/14)

O caso C-362/14 do TJUE ("Schrems I") diz respeito ao pedido de decisão prejudicial pelo Supremo Tribunal de Justiça da Irlanda (*Hight Court Ireland*) no processo de Maximillian Schrems contra *Data Protection Comissioner* (DPC).[1] O questionamento feito, constante no 36º parágrafo do acórdão, diz respeito à competência de investigação de autoridades nacionais de dados para verificar se determinado país possui uma proteção adequada para fins de transferência internacional mesmo que a Comissão já tenha estabelecido que sim por meio de uma decisão de adequação. No caso em questão, Maximillian Schrems fez uma requisição em 25 de junho de 2013 à autoridade de dados irlandesa (DPC) para que ela barrasse a transferência de seus dados do Facebook Ireland ao

[1] Em acordo com o artigo 267 do Tratado sobre o Funcionamento da União Europeia (2007), o Tribunal de Justiça é competente para decidir, a título prejudicial, sobre a interpretação dos Tratados da União Europeia (a), assim como sobre a validade e interpretação de atos das instituições, órgãos e mecanismos da União (b). Trata-se de uma via não contenciosa (consultiva) – obrigatória para os tribunais nacionais de última instância, e facultativa para os demais – por meio da qual se busca a uniformização da interpretação e aplicação do direito europeu. O referido instituto é historicamente responsável pela construção jurisprudencial do direito europeu a partir da consolidação de "princípios centrais" em grandes acórdãos do Tribunal de Justiça Europeu. Contudo, apesar de ser a grande expressão institucional da "supranacionalidade", característica do processo de integração europeu, deve-se ressaltar que não há hierarquia entre os tribunais estatais e o Tribunal de Justiça Europeu, mas sim verificam-se jurisdições com competências distintas (nacional e comunitária). Nesse sentido, a questão prejudicial mostra-se como um instrumento de "cooperação horizontal" entre as jurisdições.

Facebook Inc., nos EUA – operação padrão que consta em todos os contratos firmados por qualquer cidadão europeu junto a esta organização. (AUTOR, 2015).

Contudo, mediante a decisão de adequação 2000/520 da Comissão Europeia, validara-se o acordo Safe Harbour entre a União Europeia (via Comissão) e os EUA (via Departamento de Comércio), de forma que nenhuma garantia adicional seria necessária às organizações participantes do programa para essas transferências de dados. Nesse sistema, o Departamento de Comércio norte-americano mantinha uma lista atualizada anualmente das organizações (auto)certificadas. O monitoramento, por sua vez, era, em sua maioria, de responsabilidade da *Federal Trade Commission* (FTC), pois, ao entender as certificações como "promessas" ao consumidor, o descumprimento dos princípios Safe Harbour caracteriza-se como prática injusta e enganosa (*unfair and deceptive practices*), nos termos da secção 5 do *Free Trade Commission Act*. Diante desse cenário, a queixa de Schrems foi arquivada pelo DPC, o que levou o reclamante a buscar a via judicial. Quando o caso se apresenta diante do Supremo Tribunal de Justiça da Irlanda, este órgão submete o referido questionamento ("questão prejudicial") ao Tribunal de Justiça europeu. (AUTOR, 2000a).

Explica-se que a decisão de adequação é a base legal por meio da qual a Comissão Europeia assegura que um país terceiro possui "[...] um nível de proteção adequado [...] em virtude da sua legislação interna ou dos seus compromissos internacionais [...]", conforme prevê o artigo 25(6) da Diretiva 95/46/CE do Parlamento Europeu e do Conselho. (AUTOR, 1995). Porém, o argumento levantado por Max Schrems em sua queixa é de que o vazamento dos arquivos da Agência Nacional de Segurança norte-americana (NSA) por Edward Snowden, ao revelar o projeto de vigilância massiva do governo americano ("PRISM"), colocava em xeque a proteção dos dados transferidos pra os EUA sob o regime Safe Harbour. (AUTOR; AUTOR, 2013).

Conforme reconheceu o Supremo Tribunal de Justiça da Irlanda, apesar da justificativa do programa norte-americano ser a de que ele serve a finalidades indispensáveis ao interesse público (segurança nacional), as revelações de Snowden mostraram os excessos cometidos pelas agências de segurança norte-americanas, além do uso de "procedimentos secretos". (AUTOR, 2015). Assim sendo, a corte irlandesa afirmou que a Decisão 2000/520/CE desrespeitava os artigos 7.º ("Respeito pela vida privada e familiar"), 8º

("Proteção de dados pessoais") e 47º ("Direito à ação e a um tribunal imparcial") da Carta de Direitos Fundamentais Europeia (2000b) e o entendimento jurisprudencial firmado pelo Tribunal de Justiça da União Europeia (2014) no caso *Digital Rights Ireland* (C-293/12 e C-594/12).[2]

Dessa forma, levando-se em consideração a mudança do panorama político-jurídico desde a decisão de adequação de 2000, o Supremo Tribunal de Justiça irlandês questionou se as autoridades nacionais de dados "[...] pode[m] e/ou deve[m] proceder à sua própria investigação sobre a matéria". O Tribunal de Justiça da União Europeia, por sua vez, respondeu que as autoridades nacionais de controle podem investigar as queixas sobre a não adequação do nível de proteção de um país terceiro para fins de transferência internacional (artigo 8.º, n. 3, da Carta e artigo 28.º da Diretiva 95/46), mesmo que elas não tenham poderes para invalidar as decisões da Comissão. Por mais que a decisão de adequação deva ser seguida obrigatoriamente pelos Estados-membros e seus órgãos (artigo 288.º, quarto parágrafo, TFUE), isso não pode suprimir o direito dos titulares a requererem a proteção diante de autoridades nacionais – e, muito menos, seu direito de ação. (AUTOR, 2015).

Assim, entendeu-se que não se pode impedir a investigação dessas agências, pois isto reduziria ilegalmente sua competência, prejudicando uma função substancial para proteção dos dados pessoais – os poderes de fiscalização das agências nacionais. Invalidou-se, à vista disso, o artigo 3.º, nº 1, da Decisão 2000/520 da Comissão. É que, apesar desta disposição reconhecer o poder de suspensão da transferência de dados pelas agências nacionais, em contrapartida, ela excluiu a possibilidade dessas agências tomarem outras medidas para assegurarem o respeito ao artigo 25 da Diretiva 95/46 (princípios da transferência internacional de dados), privando-as dos poderes previsto no artigo 28 do mesmo diploma (independência e funções das autoridades nacionais). (AUTOR, 2015).

Em relação ao regramento do Safe Harbour, constata-se, inicialmente, que o sistema de (auto)certificação realizado no Departamento de Comércio dos EUA diz respeito apenas às

[2] No caso, invalidou-se a Diretiva 2006/24/CE relativa à conservação de dados gerados de redes públicas de comunicação/serviços de comunicações eletrônicas publicamente disponíveis, formulada após ataques terroristas em Madrid e Londres, diante da lesão sistemática em regulamentações nacionais europeias que buscavam internalizar a referida diretiva, principalmente nas matérias sobre a retenção e processamento de dados para investigação criminal.

organizações americanas, e não às autoridades públicas estadunidenses. Adicionalmente, o quarto parágrafo do anexo I da Decisão 2000/520 previa a limitação da aplicabilidade dos princípios Safe Harbour por "[...] requisitos de segurança nacional, interesse público ou cumprimento da lei [...]", bem como por "[...] legislação, regulamento governamental ou jurisprudência que criam obrigações contraditórias ou autorizações explícitas [...]" às organizações. (AUTOR, 2000a). Contudo, a própria Comissão, nos pontos 2 e 3.2 da Comunicação COM(2013) 846 e 7.1, 7.2 e 8 da Comunicação COM(2013) 847, concluiu que as autoridades americanas podiam interceptar e tratar os dados transferidos "[...] para além do que era estritamente necessário e proporcionado à proteção da segurança nacional". Ainda, não se dispunha de instrumentos administrativos e/ou judiciais disponíveis para os titulares ("remédios legais para os indivíduos"), de modo que a autorização generalizada de acesso a comunicações individuais, constante nas regulações norte-americanas, desrespeitava, dentre outros diplomas, o artigo 47 da Carta de Direitos Fundamentais europeia. (AUTOR, 2015).

O Tribunal de Justiça da União Europeia, então, invalidou por completo a Decisão 2000/520 da Comissão Europeia, reconhecendo que este instrumento não poderia garantir um nível de adequação "essencialmente equivalente" ao do regime europeu – não se quer que a regulação do país terceiro seja idêntica à europeia, mas sim que se garanta um "alto nível de proteção de dados pessoais", como especificado pelo relatório do caso formulado pelo Grupo de Trabalho do Artigo 29 (*Working Party 29*). (AUTOR, 2017). A partir desta decisão, o Supremo Tribunal de Justiça irlandês anulou a decisão da autoridade de dados irlandesa (DPC) de arquivamento da investigação por falta de fundamento jurídico. Uma nova investigação foi iniciada nesse órgão, oportunidade na qual Schrems pode reformular sua reclamação. Considerando a invalidação do Safe Harbour, Schrems passa a questionar qual a base legal autorizava o Facebook Ireland a transferir os dados de titulares europeus para os EUA. A resposta foi a de que a transferência de dados entre Facebook Ireland e o Facebook Inc. ocorria por meio de um acordo entre eles, exatamente para este fim, desde 20 de novembro de 2015. (AUTOR, 2020).

O referido acordo estava em conformidade com as denominadas cláusulas contratuais padrão (SCC – *Standard Contractual Clauses*), as quais representam uma das bases legais alternativas para transferências à países terceiros aos quais não se assegura um

nível adequado de proteção, como previsto no artigo 26(2) da Diretiva 95/46/CE e regulamentado na decisão 2010/87 da Comissão. (AUTOR, 2010). Ademais, uma outra forma de apresentar "garantias suficientes", amplamente usada após a invalidação do Safe Harbour, foi por meio das denominadas *Binding Corporate Rules* (BCRs), códigos de conduta e regramentos vinculantes internos para grupos de empresas.

3 SCHREMS II (C-311/18)

A autoridade de dados irlandesa (DPC), ao iniciar sua investigação sobre a proteção de dados nos EUA, entendeu que a problemática é dependente da análise sobre a validade da decisão da comissão sobre as SCCs (2010/87/CE). (AUTOR, 2020). Nesse sentido, essa autoridade submeteu a questão ao Supremo Tribunal de Justiça da Irlanda e requereu que este órgão iniciasse o pedido de questão prejudicial ao Tribunal de Justiça europeu, na forma do artigo 267 do Tratado sobre o Funcionamento da União Europeia. (UNIÃO EUROPEIA, 2020). Ocorre que, durante esses procedimentos, um novo acordo para transferência de dados entre a União Europeia e os Estados Unidos foi firmado, o *Privacy Shield*. A validade do acordo e o asseguramento de um nível de proteção adequado foi, ainda, confirmado pela nova Decisão de Execução do Comitê (2016/1250). (AUTOR, 2016b).

Dentre as 11 perguntas feitas pelo Supremo Tribunal de Justiça da Irlanda, está a pergunta sobre a aplicabilidade do novo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (*GDPR – General Data Protection Regulation*) que revoga a antiga Diretiva 95/46/CE. (AUTOR, 2016a). Nesse sentido, o Tribunal de Justiça Europeu, em sede preliminar, confirma que a GDPR guiará a resposta aos questionamentos, dado que o Comissário irlandês ainda não havia tomado uma decisão em relação à (nova) queixa de Schrems quando esse regramento entrou em vigor (25 de maio de 2018). (AUTOR, 2020). Ademais, o contexto do caso é também marcado pelo caso Cambridge Analytica.[3]

[3] Em 17 de março de 2018 uma matéria do The Guardian revela a colheita de dados de 50 milhões – apurados em mais de 87 milhões, posteriormente – de perfis do Facebook pela empresa Cambridge Analytica após uma investigação da Channel 4 News. Em 24 de julho de 2019 a FTC (Federal Trade Commision) publica a condenação de $5 (cinco) bilhões de dólares do Facebook em relação a este vazamento de dados. A mineração e análise desses dados e sua projeção para o processo eleitoral norte-americano, no qual Donald Trump foi eleito presidente dos Estados Unidos da América, apresenta-se como um dos casos mais

Também em relação ao direito aplicável, decidiu-se que o processamento de dados pelas autoridades norte-americanas entra no escopo da GDPR. Contrariamente ao entendimento do Advogado Geral Saugmandsgaard Øe (AUTOR, 2019), o Tribunal de Justiça não diferenciou entre o "processamento em si", com intuitos comerciais pelo Facebook, e o tratamento subsequente das agências americanas para fim de segurança nacional, argumentando que o artigo 45(2)(a) da GDPR, ao tratar das decisões de adequação, coloca como um elemento importante a ser levado em consideração o tratamento empregado para fins de segurança pública no país terceiro.

Nessa sequência, em resposta à segunda, terceira e sexta questões, decidiu-se que o nível de proteção adequado ("essencialmente equivalente") exigido para as decisões de adequação também se aplicam às cláusulas-tipo contratuais (artigo 46 da GDPR). Dessa forma, afirma-se que a avaliação do "nível de adequação" deve levar em consideração tanto as estipulações contratuais como os "[...] elementos pertinentes do sistema jurídico [do] país terceiro, nomeadamente os enunciados no artigo 45.º, n.º 2, do referido regulamento [GDPR]", no caso de eventual acesso aos dados pelas autoridades públicas deste país. (AUTOR, 2020).

Contudo, esse juízo de adequação deve ser feito pelos exportadores e importadores, ou seja, ao responsável pelo tratamento e ao destinatário da transferência, e não pela comissão. Deve-se verificar se a legislação doméstica do país terceiro lhes permite cumprir "na prática" as estipulações contratuais e, ainda, sobre a possibilidade de garantir "medidas suplementares". Caso a resposta seja negativa, deve-se suspender ou cessar as transferências, retornando e excluindo os dados já transferidos, e notificar o titular dos dados. E se, mesmo assim, pretende-se continuar com a transferência, deve-se notificar a autoridade de controle competente. Entende a Corte que as autoridades de controle são a responsáveis subsidiárias, e, logo, devem tomar as medidas necessárias (suspender ou proibir) para proteção do titular, no caso de não existir uma decisão de adequação da Comissão, por força do artigo 58.º, n.º 2, alíneas f) e j) do GDPR. (AUTOR, 2020).

emblemáticos acerca dos impactos políticos e jurídicos das novas dinâmicas sociais no interior da internet e da centralidade da proteção de dados para sociedade digital. (THE GUARDIAN, ([2022]); FTC, 2019).

A previsão sobre aquele procedimento encontra-se na cláusula 4(g), 5(a) e anexo II(c) da decisão da comissão sobre as SCCs (2010/87/CE). (AUTOR, 2010). Por mais que se reconheça que os instrumentos contratuais não vinculem as autoridades norte-americanas, o Tribunal de Justiça Europeu decidiu pela validade dessa decisão, já que existem mecanismos suficientes para proteção dos titulares de dados. Também à luz dos artigos 7.º ("respeito à vida privada"), 8.º ("proteção de dados pessoais") e 47.º ("proteção judicial efetiva") da Carta de Direitos Fundamentais, passa-se a avaliar a decisão do Privacy Shield. Nesse sentido, a Grande Secção do Tribunal, diferentemente do Caso Schrems I, ampliou o escopo de observação para considerar a ordem jurídica dos EUA que embasavam as práticas das agências de inteligência norte-americanas. (AUTOR, 2020).

Nesse sentido, observou-se dois instrumentos normativos destinados a regulação das atividades de vigilância das agências de inteligência norte-americanas. A primeira, a *Executive Order* (EO) 12333, assinada pelo Presidente Ronald Reagan (4/12/1981) e atualizada pelo Presidente George Bush (30/07/2008), é a "autoridade fundacional" pela qual a NSA (*National Security Agency*) coleta, retem e analisa os "sinais de inteligência estrangeiros". Sua aplicação principal é, então, "[...] a coleção de comunicações de estrangeiros que ocorrem totalmente fora dos Estados Unidos".[4] (AUTOR, 1981, tradução nossa). Ela é aplicada nos casos não compreendidos pela Seção 702 do Foreign Intelligence Surveillance Act of 1978 (FISA).

A referida Seção 702 do FISA, por sua vez, é a base legal dos dois grandes programas de vigilância revelados por Snowden, o UPSTREAM e o PRISM (nesse tempo renomeado de DOWNSTREAM). O primeiro é a coleta de informação diretamente pelo *backbone* da internet, como, a exemplo, o plug que se conecta aos cabos submarinos, interceptando as informações transferidas de um continente a outro ou, com a ajuda de parceiros, como a AT&T, coletando informações diretamente de outros cabos de fibra ótica. O segundo é a coleta de informações de companhias como o Facebook e o Google, que são obrigados a reterem informações de alvos (dados) marcados (e não marcados, para uma segunda análise da NSA), mas proibidos de informarem essas ações aos usuários. (AUTOR, [2022]).

[4] "[...] the collection of communications by foreign persons that occur wholly outside the United States".

Assim, entendeu o Tribunal de Justiça que esses programas são uma ingerência com relação aos direitos fundamentais previstos nos artigos 7 e 8 da Carta de Direitos Fundamentais. Explica-se que apesar desses direitos não serem absolutos, as restrições devem ser previstas em lei e respeitarem o conteúdo essencial desses direitos, quer dizer, as restrições devem ocorrer na "estrita medida do mínimo necessário", devendo as regras e o âmbito da regulação serem claros, precisos e dispondo de garantias suficientes para proteção dos dados pessoais contra o risco de abusos (artigo 52 da Carta). (AUTOR, 2020).

Outrossim, salienta-se que "o mecanismo de supervisão da ingerência da segurança nacional", o mediador independente (*Ombudsperson*) do Privacy Shield (Anexo III), uma das principais mudanças de compromisso com relação ao antigo acordo Safe Harbour, não pode ser comparado à um tribunal, na acepção do artigo 47.º da Carta. (AUTOR, 2016b). Não há garantia de que esta autoridade possua poderes suficientes para decidir de forma que vincule as agências de inteligência norte-americanas. Portanto, conclui-se que o acordo não garante um nível de proteção adequado ("essencialmente equivalente") para proteção dos titulares de dados, exigido pelo artigo 45 da GDPR. (AUTOR, 2020). Por todo o exposto, a Decisão de Adequação do Privacy Shield foi invalidada sem a manutenção de seus efeitos. Declara-se a ilegalidade das transferências sob este regime e, ainda, como veio a reconhecer o *European Data Protection Board* (EDPB), sem um prazo moratório para a implementação da decisão. No mesmo documento, o EDPB também reconhece que o julgamento acerca das cláusulas-tipo contratuais também se aplica para as BCRs, de forma que, no caso de não existir uma decisão de adequação, a avaliação sobre o nível de adequação do país terceiro fica por parte da organização que transfere os dados. (AUTOR, 2020).

No caso dos EUA, ou de qualquer outro país no qual não é garantido o mesmo nível de proteção adotado na União Europeia, as transferências só podem ser feitas por meio da implementação de "medidas suplementares". Seguindo o princípio da *accountability* (artigo 5.2 e 28.3 (h) da GDPR) – que prescreve uma atuação positiva por parte dos controladores e operadores para garantir a efetividade da proteção de dados (e não apenas um *compliance* passivo com as regras) – o EDPB especificou, em uma lista não exaustiva, as medidas técnicas, contratuais e organizacionais necessárias para que essas transferências cumpram com o requisito de uma proteção "essencialmente equivalente" às transferências internas.

(AUTOR, 2020). Ainda, remanescem como bases legais validas para transferências internacionais as "derrogações" do artigo 49 do GDPR, apenas aplicadas para situações específicas e ocasionais (não repetitivas), conforme a diretriz 2/2018 do EDPB. (AUTOR, 2018).

Apesar dos dois julgamentos, M. Schrems, por meio da NOYB, ONG para proteção de dados de qual é líder, protesta que o Facebook não mudou substancialmente suas práticas, e que continuam a realizar as transferências de dados ilegalmente. Por meio do *Transfer Impact Assessment* (TIA) – documento para avaliação de impacto previsto na decisão atualizada das SCCs (4 jun. 2021) para o regime da GDPR – o Facebook estabelece que o regime jurídico dos EUA e da UE para proteção de dados são equivalentes ("*Equivalence Assessment"*), que o risco para os usuários é mínimo ("*Factors Assessment"*) e que ele toma as medidas de segurança necessária para compensar qualquer violação da legislação europeia, como as do artigo 32 da GDPR. (AUTOR, 2021). Do outro lado, alega-se que além de contrariar o entendimento dos julgamentos do Tribunal de Justiça Europeu, as medidas de segurança adotadas não são relevantes diante da Seção 702 do FISA. (AUTOR, 2021).

4 GOVERNANÇA E REGULAÇÃO DO FLUXO DE DADOS PESSOAIS: PARA ALÉM DA DISTINÇÃO PÚBLICO/PRIVADO

O presente tópico destina-se a construir uma observação sobre a regulação e governança do fluxo de dados pessoais. Os conflitos jurídico-políticos entre União Europeia e Estados Unidos da América, analisados sob a luz dos julgamentos dos casos Schrems, são, então, redimensionados por meios dos pressupostos epistemológicos da Teoria dos Sistemas. Nesse seguimento, o primeiro ponto a ser destacado é o fato de que as tomadas de decisões políticas (burocracia) e jurídicas (tribunais) do Estado serem confrontadas com àquelas de outras organizações (públicas, privadas e público-privadas) em diversos âmbitos (sistemas) ao redor do globo. Na Teoria dos Sistemas, esse fato é explicado pelos impulsos da diferenciação funcional dos sistemas de sentido na sociedade "moderna" (pós-1789). (AUTOR, 2007).

É que, apesar da organização estatal ter-se estruturado como núcleo do direito e da política (diferenciação segmentária, *i.e.* territorial), a descrição de Luhmann ressalta a circulação das comunicações em sistemas globais que se diferenciam pela função que

exercem na sociedade – a tomada de decisão politicamente vinculante, no caso do sistema político (AUTOR, 2004); a estabilização das expectativas normativas, no caso do sistema jurídico (AUTOR, 2016); e o asseguramento de provisões futuras em condições de escassez, no caso sistema econômico. (AUTOR, 2017).

Por um ângulo complementar, Ladeur (2002) descreve, no decorrer do século XX, as transformações da sociedade-de-organizações (ou "pluralista-de-grupos") e a crescente dependência de conhecimentos técnicos para a regulação e gestão de áreas específicas da sociedade, fato que impulsionou, a exemplo, o surgimento das agências reguladoras, mormente nos EUA, e diversos tipos de parcerias público-privadas, no cenário europeu. Na segunda metade do século XX, consolida-se a forma do "Estado cooperativo" e os modos híbridos de regulação. As teorias de governança (corporativa), originadas no âmbito econômico em 1970, passam a invadir o campo de reflexão da ciência política. Nesse sentido, a governança estatal começa a ser caracterizada de modo mais "negocial" e "heterárquico". Ainda, a teoria do direito, preocupada, tradicionalmente, com a validade (interna) de expectativas normativas, amplia sua atenção para com os efeitos sociais da regulação jurídica, abrindo um maior diálogo para com as ciências sociais (e econômicas). (AUTOR, 2017).

Teubner (1997), inspirado no "direito vivo" de Eugen Ehrlich (1916), repensa o direito regulatório e o pluralismo jurídico no contexto de intensificação do processo de globalização, após a queda do Muro de Berlim (1989). Diante da policontexturalidade social, têm-se que a binaridade do código jurídico (direito/não-direito) é programada (norma jurídica) de distintas formas, a depender do ambiente social com o qual se relaciona. Assim, Teubner (2016) fala em uma dupla fragmentação da sociedade mundial, qual seja, não só dos sistemas funcionais, como também das culturas regionais diante dos múltiplos processos culturais colidentes. Em oposição à Luhmann, que concebia as organizações estatais (tribunal e burocracia) como centrais à reflexão jurídico-política, Teubner concebe a policentralidade dos sistemas e suas múltiplas conexões com normatividades periféricas, dentro (*e.g.* direito das favelas e direitos das minorias) e fora (*e.g.* direito de organizações privadas internacionais e regimes transnacionais privados) do Estado. (AUTOR, 2005).

Nessa continuidade, reconhece-se a fragmentação do direito internacional e a consolidação de diversos *self-contained regimes*. (AUTOR, 2006). Sobre estes, a *lex*

mercatória (AUTOR, 2002), o direito autônomo das práticas comerciais, cuja história remete ao início do período moderno, é o caso central para estudos de diversas outras normatizações próprias de regimes transnacionais, como, a exemplo, a *lex digitalis,* no âmbito do ciberespaço. (AUTOR, 2018). Para além da emancipação do direito econômico da OMC em relação ao direito internacional, e sua posterior constitucionalização (AUTOR, 2016), a *lex mercatória* constrói sua independência com a participação de empresas transnacionais, estas já autorreguladas internamente (*e.g.* códigos de conduta), e a partir de centros decisórios privados, como o *International Chamber of Commerce*, que também resolve conflitos nos quais Estados figuram como parte.

Assim, verifica-se, a partir dos anos 1990, a proliferação de regimes de "governança global", como denomina Zurn (2018), para além das lógicas nacionais e regionais, e dos próprios âmbitos políticos, econômicos e jurídicos, como é o caso da rede global de governança da internet que se formara a partir da ICANN (*Internet Corporation for Assigned Names and Numbers*), uma organização sem fins lucrativos fundada como associação privada vinculada ao direito societário da Califórnia (EUA), a qual é responsável pela manutenção de uma enorme base de dados e da coordenação de inúmeros processos relacionados ao registro de nomes de domínio na internet. (AUTOR; AUTOR, 2020). "Governança", nesse sentido, é o conceito que engloba novas formas de conexão institucional em rede de diversos atores em uma multiplicidade de ordens normativas, sendo a "regulação" uma parte específica da governança "[...] que lida com a direção de eventos e estados de coisas". (AUTOR, 2015. p. 144, tradução nossa).

Diante dessas reflexões, o primeiro ponto a ser observado é sobre o papel de diversos atores, público e privados, na governança e regulação sobre proteção de dados pessoais. Se, no caso Schrems I, verifica-se a centralidade dada pelo mecanismo da decisão de adequação, a partir do caso Schrems II consolida-se o papel das cláusulas-padrão contratuais (*SCCs*) e das normas corporativas vinculantes (*BCRs*). Mas, dizer que esse movimento, angariado pela própria mudança para um robusto princípio da *accontability* a partir da GDPR, vai do público ao privado, é um reducionismo, já que o próprio conceito de policontexturalidade é uma alternativa para se pensar para além das binaridades público/privada, nacional/internacional e direito/não-direito.

Nessa continuidade, a possibilidade de se falar sobre um regime autônomo da proteção de dados pessoais, de uma *lex privacy*, como observa, mostra-se latente. (AUTOR, 2019). Sua formação, na esteira de Teubner, explicar-se-ia como um processo de transformação de (autor)regulações sociais em processos jurídicos por meio do mecanismo do acoplamento estrutural entre sistema jurídico e um âmbito social autônomo. Explica-se. A partir da descrição luhmanniana, observa-se a relação entre sistemas funcionais (autopoiéticos) de modo horizontal – relegando-se a hierarquia apenas como princípio possível para as organizações – por meio de estruturas específicas (*e.g.* constituição como acoplamento estrutural entre sistema jurídico e político). (AUTOR, 2017). A desconstrução dessa hierarquia e sua substituição pela distinção entre centro/periferia decentraliza a politização da produção normativa, ou seja, retira a política do topo da hierarquia da produção de normas e a coloca em um mesmo nível que outros tipos de produção social de normas. (AUTOR, 2002).

Destaca-se que parece ser problemática a identificação de um sistema (autopoiético) de proteção de dados que poderia se acoplar com o sistema jurídico, principalmente, no âmbito da internet, que não pode ser considera um sistema. (AUTOR; AUTOR, 2021). Por outro lado, o reconhecimento de um direito fundamental a proteção de dados e a afirmação de sua regulação autônoma com relação âmbito do mercado (*e.g.* as problemáticas entre proteção de dados e o direito concorrencial) parecem ser um bom indicativo, por mais não seja um padrão que ainda possa ser generalizado para todo o globo. De qualquer forma, isso não deslegitima a observação da forma de governança em rede e o regime híbrido de regulação para o fluxo global de dados.

Para fins didáticos, poder-se-ia "categorizar" a governança e regulação da proteção de dados em "dimensões" para que se visualize a formação em rede dos diversos atores e o entrelaçamento entre regulações público/privadas e técnicas.[5] Em um primeiro plano, estaria a governança a partir dos mecanismos dos Estados e a correspondente centralidade da decisão de adequação como regulação para o fluxo global dos dados, como pode-se verificar pela

[5] A própria dificuldade de se manter uma classificação analítica dessas dimensões e categorias demonstrar a complexidade da governança e regulação da proteção de dados que não pode ser "cooptada" ou "centralizada" em um ponto.

descrição dos casos Schrems. Contudo, as agências reguladoras (autônomas) nos EUA e a rede das autoridades (independentes) de proteção de dados na União Europeia mostram já a descentralização da governança pública tradicional. Ademais, por meio da *Federal Communications Commission* (FCC), a *Federal Trade Commission* (FTC) e o *Office of the Attorney General - State of California*, do lado dos EUA, e o *European Data Protection Supervisor* (*EDPS)*, da União Europeia, participam de uma rede global ("informal") das *Privacy Enforcement Authorities* junto a OCDE (Organização para a Cooperação e Desenvolvimento Econômico). (2013).

Após as falhas (invalidação) dos acordos firmados entre o Departamento de Comércio norte-americano e a Comissão Europeia, verifica-se o crescimento de importância das cláusulas-tipo contratuais (*SCCs*) e as normas corporativas vinculantes (*BCRs*), mecanismos que podem ser caracterizados como pertencentes à dimensão "privada", mas que, por outro lado, seguem os parâmetros e procedimentos da regulação regional "pública". Leciona-se que essa dimensão autorregulatória da proteção de dados por meio das organizações privadas, como medidas de *compliance*, seguem o princípio da *accountability*, previsto no artigo 5(2) do GDPR. Esse princípio, lido em conformidade com o artigo 32 (segurança do tratamento de dados), consubstancia diversos outros mecanismos (autor)regulatórios, como os códigos de conduta (artigo 40), o relatório de impacto a proteção de dados (artigo 35), uma medida prévia para tratamentos de alto risco a lesão aos direitos dos titulares, e os mecanismos de certificação do nível de proteção de dados pessoais (artigo 42-43). (AUTOR, 2016a).

Destaca-se que a auto certificação do Privacy Shield continua vigente, por mais que não mais autorizativas das transferências internacionais ("por si só") e que o número de empresas participantes tenha caído vertiginosamente. (AUTOR, 2021). Assim como, também, os casos de derrogação do artigo 49 do GDPR, da qual destaca-se o base legal do consentimento (livre, específico, informado e inequívoco, de acordo o artigo 7 e o *recital* 32 da GDPR) do titular de dados. (AUTOR, 2016a). Por fim, há a dimensão técnica da regulação e governança, que, nos casos analisados, é extrema importância para as garantir as "medidas suplementares" necessárias para que as transferências cumpram com o requisito de uma proteção "essencialmente equivalente" no caso de não existir a decisão de adequação. Nesse

ponto, além do especificado pelo *EDPB* (2021), o artigo 32 da *GDPR* se complementam pelos estândares 27000:2018, 27001:2013 e 27002:2013 de segurança da informação da ISO (*International Organization for Standardization*). ([2022]).

Fala-se, nesse sentido, em um modelo de autorregulação regulada, na qual a autorregulação das organizações (e plataformas) segue parâmetros procedimentais estabelecidos na regulação estatal e é fiscalizado de modo descentralizado com a publicização dos próprios mecanismos internos dessas organizações a serem auditados. Nesse sentido, constata-se a figura de certificadores privados – como, a exemplo, no *Cross Border Privacy Rules* (CBPRs, [2022]) da APEC (*Asia-Pasific Economic Cooperation*) – e não apenas centralizados nas agências estatais. O novo compromisso de acordo anunciado recentemente promete fortalecer as salvaguardas jurídicas acerca das atividades de captação dos sinais pelas agências de inteligência norte-americanas, as quais adotarão novos procedimentos para garantir sua supervisão, e estabelecer um mecanismo de reparação que inclui "[...] uma Corte de Revisão independente para proteção de dados que será formada por indivíduos escolhidos de fora do Governo dos EUA".[6] (AUTOR, 2022, tradução nossa).

Caso seja formada uma autêntica autoridade julgadora independente, ela poderá contribuir para a evolução e autonomização desse regime de governança e regulação do fluxo de dados, melhorando, assim, o controle do "vigilantismo" (público/privado) que é a base dos processos político-econômicos hodiernos. (AUTOR, 2019). É que a organização em rede em um âmbito global e as novas formas de controle regulatório que passam a se desenvolver hodiernamente, como se destaca, buscam contornar não só a falta de conhecimento técnico, como também a própria dinâmica do fluxo global de dados. (AUTOR, 2021). Os casos apresentados mostram a insuficiências dos processos político-jurídicos centrados apenas nos estados e órgãos estatais ("decisão de adequação") e a dificuldade de controle da cooptação estatal do fluxo de dados. A ideia de "cultura de dados" consistiria, justamente, em desenvolver uma complexidade regulatória que engloba diversas vias para proteção do direito dos titulares (administrativas, nas agências nacionais e regionais, judiciais, nos Estados e regiões, e diretas, com as organizações e plataformas). Os grupos profissionais, como a IAPP

[6] "[...] an independent Data Protection Review Court that would consist of individuals chosen from outside the U.S. Government".

(*International Association for Privacy Professionals*) e as ONGs, como a NOIB, de Schrems, realizam uma função extremamente necessária a nível global, seja para articulação do conhecimento técnico-regulatório, seja para proteção coletiva dos direitos dos titulares a nível global. (AUTOR, 2020).

Ressalta-se, por fim, que apesar do paradigma regulatório europeu ser entendida por vezes como uma "imposição europeia", a própria GDPR fora construída pela incorporação de diversos elementos desenvolvidos em outras regiões. Ademais, as próprias "decisões de adequação" tem ocorrido de maneira bem mais flexível com relações a "países em desenvolvimento". Talvez o grande problema europeu seja, assim como a vigilância massiva dos EUA, um problema antigo que deve ser reestruturado e não apenas (re)centralizado. O "*pro-integrationist bias*" da União Europeia, por vezes, ainda centraliza a política no âmbito da Comissão, que leva o controle jurídico a sempre ser direcionado ao Tribunal de Justiça. Mas a potencialidade da União Europeia ser o grande modelo organizacional para uma regulação e governa em rede está apenas no fato de que ela já se caracteriza por uma simbiose de dimensões – "semi-hierarquia" jurídica (regional e nacional), a "triangulação" política entre Conselho, Comissão e Parlamento, e uma infraestrutura administrativa "hybrida" de estruturas de governança. (AUTOR, 2019).

5 CONSIDERAÇÕES FINAIS

Os casos Schrems I e II são representativos das diversas transformações da sociedade movida a dados. No primeiro caso, a acordo Safe Harbour entre EUA e União Europeia, realizado sob o regime da Diretiva 95/46/CE, fora invalidado pelo Tribunal de Justiça Europeu em um contexto na qual as acusações de Snowden revelaram a lesão sistemática de direitos fundamentais pela vigilância estatal. Para além do reconhecimento da importância dos poderes fiscalizatórios das autoridades nacionais de dados, esse julgamento começa a destacar uma incompatibilidade das antigas dinâmicas da proteção da "privacidade" desenvolvidas nos anos 2000. Nessa sequência, a invalidação do acordo Privacy Shield, consubstanciado pelo novo Regulamento Geral de Proteção de Dados Europeu, mostra as falhas das negociações

políticas centralizadas nas organizações estatais e abre a observação da governança e regulação da proteção de dados pessoais para além da distinção público/privada.

A partir da observação das novas conformações organizacionais e regulatórias da sociedade atual, o papel da autorregulação privada afirmado no caso Schrems II mostra-se essencial. A centralidade nas decisões de adequação deve ser relativizada ou ao menos complementada para que a proteção de dados se estruture por meio de outras formas ("híbridas") de regulação (autorregulação regulada) e governança (em rede) que já se verificam no interior dos próprios âmbitos estatais e regionais. O Tribunal de Justiça Europeu, por mais que desempenhe um papel central no interior da União Europeia, somente fora acionado seguidamente pelas próprias dificuldades da eficácia dos acordos em cumprir com a proteção adequada dos titulares de dados, o que deveria ter sido realizado se não pelo próprio Facebook, pelas autoridades nacionais independentes. Com a nova promessa de acordo, talvez podemos caminhar a autonomização desse regime de proteção para o fluxo de dados pessoais com novos mecanismos de supervisão e controle sobre as atividades estatais e privadas.

REFERÊNCIAS

BORA, Alfons. Semantics of ruling: reflective theories in regulation, governance and law. In: PAUL, Regine (et al.). Society, regulation and governance: new modes of shaping social change. Cheltenham; Northampton: Edward Elgar, 2017. p. 15-38.

BORA, Alfons. The Shadow of the Law: Intermediary institutions and the ruling part of governance. In: HARTMANN, Eva; KJAER, Poul. The evolution of intermediary institutions in Europe: from corporatism to governance. Houndmills; Basingstoke; Hampshire; New York: Palgrave MacMillan, 2015. p. 141-157.

CASAROSA, Federica. Transnational collective actions for cross-border data protection violations. Internet Policy Review: Journal on Internet Regulation, v. 9, n. 3, Sep./2020. Disponível em: https://policyreview.info/articles/analysis/transnational-collective-actionscross-border-data-protection-violations. Acesso em: 1 abr. 2022.

CROSS BORDER PRIVACY RULES (CBPRs). About CBPRs. Disponível em: http://cbprs.org/about-cbprs/. Acesso em: 1 abr. 2022.

EHRLICH, Eugen. The sociology of law. Harvard Law Review, Cambridge, v. 36, n. 2, Dec. 1916. p. 130-145. Disponível em: https://bit.ly/3nsrM7v. Acesso em: 1 abr. 2022.

ELETRONIC FRONTIER FOUNDATION (EFF). End 702. Disponível em: https://www.eff.org/pt-br/pages/upstream-prism. Acesso em: 1 abr. 2022.

EUROPEAN UNION. European Parliament. Directorate-General for Parliamentary Research Services. From safe harbour to privacy shield: advances and shortcomings of the new EUUS data transfer rules: in-depth analysis. European Parliament, 2017. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/48f33bb1-e2ca-11e6-ad7c01aa75ed71a1/language-en. Acesso em: 1 abr. 2022.

EUROPEAN UNION. European Data Protection Board (EDPB). Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en. Acesso em: 1 abr. 2022.

EUROPEAN UNION. European Data Protection Board (EDPB). Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020. Disponível em: https://edpb.europa.eu/news/news/2020/europeandata-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_en. Acesso em: 1 abr. 2022.

EUROPEAN UNION. Commission Implementing Decision (EU) 2021/914, 4 June 2021. Standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. Acesso em: 1 abr. 2022.

EUROPEAN UNION. European Data Protection Board (EDPB). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 18 June 2021. Disponível em: https://edpb.europa.eu/system/files/2021-

06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf. Acesso em: 1 abr. 2022.

FEDERAL TRADE COMMISSION (FTC). FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. 24 jul. 2019. Disponível em: https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penaltysweeping-new-privacy-restrictions. Acesso em: 1 abr. 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Information security management. Disponível em: https://www.iso.org/isoiec-27001-informationsecurity.html. Acesso em: 1 abr. 2022.

KJAER, Poul. Three-dimensional conflict of laws in Europe. Zentrum für Europäische Rechtspolitik (ZERP), Universität Bremen, 1 Mar. 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1489939. Acesso em: 1 abr. 2022.

LADEUR, Karl-Heinz. The changing role of the private in public governance: the erosion of hierarchy and the rise of a new administrative law of cooperation: a comparative approach. European University Institute, sep./2002. Disponível em: https://cadmus.eui.eu/handle/1814/187. Acesso em: 1 abr. 2022.

LUHMANN, Niklas. Economía de la Sociedad. Ciudad del México: Herder, 2017.

LUHMANN, Niklas. La política como sistema. Ciudad del México: Universidad Iberoamericana, 2004.

LUHMANN, Niklas. La sociedad de la sociedad. Ciudad del México: Herder, 2007.

LUHMANN, Niklas. O direito da sociedade. São Paulo: Martins fontes, 2016.

MACASKILL, Ewen; DANCE, Gabriel. NSA files: decoded. The Guardian, 1 Nov. 2013. Disponível em: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsafiles-surveillance-revelations-decoded#section/1. Acesso em: 1 abr. 2022.

MEDZINI, Rotem. Governing the shadow of hierarchy: enhanced self-regulation in European data protection codes and certifications. Internet Policy Review: Journal on Internet Regulation, v. 10, n. 3, Sep./2021. Disponível em: https://policyreview.info/articles/analysis/governing-shadow-hierarchy-enhanced-selfregulation-european-data-protection-codes. Acesso em: 1 abr. 2022.

MOURA, Ariel Augusto Lira. “Lex digitalis” e flexibilidade do direito. In: SCHWARTZ, Germano (coord.). Anais Sociology of Law 2018: o direito entre o caos e desconstrução. Canoas: Unilasalle, 2018. p. 88-98.

NOYB. 4th Advent Reading: Facebook fully ignores "Schrems" rulings by Court of Justice. 19 dez. 2021. Disponível em: https://noyb.eu/en/4th-advent-reading-facebook-fully-ignoresschrems-rulings-court-justice. Acesso em: 1 abr. 2022.

NOYB. Deep Dive: how facebook tries to ignore the CJEU - despite two judgments. 19 dez. 2021. Disponível em: https://noyb.eu/en/deep-dive-how-facebook-tries-ignore-cjeu-despitetwo-judgments. Acesso em: 1 abr. 2022.

OCDE (ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO). Action plan for the Global Privacy Enforcement Network (GPEN). 22 Jan. 2013. Disponível em: https://www.privacyenforcement.net/content/action-plan-globalprivacy-enforcement-network-gpen. Acesso em: 1 abr. 2022.

ROCHA, Leonel Severo. Epistemologia do direito: revisitando as três matrizes jurídicas. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD), v. 5, n. 2, jul./dez. 2013, p. 142-145. Disponível em: http://revistas.unisinos.br/index.php/RECHTD/article/view/rechtd.2013.52.06. Acesso em: 1 abr. 2022.

ROCHA, Leonel Severo. Direito e autopoiese. In: STRECK, Lenio Luís; ROCHA, Leonel Severo; ENGELMANN, Wilson (orgs.). Constituição, sistemas sociais e hermenêutica: anuário do programa de pós-graduação em direito da UNISINOS. n.13. Porto Alegre: Livraria do advogado, 2017. p. 123-136.

ROCHA, Leonel Severo; MOURA, Ariel Augusto Lira de. Epistemologia das redes e a governança digital da ICANN: teoria e práxis do direito na cultura das redes. In: ROCHA, Leonel Severo; COSTA, Bernardo Leandro Carvalho (org.). Atualidade da constituição: o constitucionalismo em Luhmann, Febbrajo, Teubner e Vesting. Porto Alegre: Fi, 2020. p. 504-538. Disponível em: https://bit.ly/3cYc7Kh. Acesso em: 1 abr. 2022.

ROCHA, Leonel Severo; MOURA, Ariel Augusto Lira. Teoria dos sistemas e constitucionalismo digital. In: ROCHA, Leonel Severo; COSTA, Bernardo Leandro Carvalho (org.). O futuro da Constituição: Constitucionalismo social em Luhmann e Teubner. Porto Alegre: Editora Fi, 2021. Disponível em: https://www.editorafi.org/249constitucionalismo. Acesso em: 1 abr. 2022.

SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva. São Paulo: Thomson Reuters Brasil, 2019.

TEUBNER, Gunther. Breaking frames: economic globalization and the emergence of lex mercatória. European journal of social theory, New York, v. 5, n. 2, abr./jun. 2002, p.199- 217. Disponível em: https://bit.ly/3lAROVE. Acesso em: 1 abr. 2022.

TEUBNER, Gunther. Direito, sistema e policontexturalidade. Unimep: Piracicaba, 2005.

TEUBNER, Gunther. Fragmentos constitucionais: constitucionalismo social na globalização. São Paulo: Saraiva, 2016.

TEUBNER, Gunther. Global Bukowina: legal pluralism in the world society. In: TEUBNER, Gunther (ed.). Global law without a State. Aldershot; Brookfield: Dartmouth, 1997. p. 3-28.

THE GUARDIAN. Cambridge Analytica files. Disponível em: https://www.theguardian.com/news/series/cambridge-analytica-files. Acesso em: 1 jan. 2022;

THORNHILL, Chris. The future of State. In: KJAER, Poul; TEUBNER, Gunther; FEBBRAJO, Alberto (ed.). The financial crisis in constitutional perspective: the dark side of functional differentiation. Oxford; Portland: Hart, 2011. p. 357-395. TRACOL, Xavier. 'Schrems II: the return of the Privacy Shield. Computer Law & Security Review, v. 39, Nov./2020. p. 7. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364920300893#:~:text=The%20Schrems%20II%20judgment%20has,Privacy%20Shield%20remains%20legally%20valid. Acesso em: 1 abr. 2022.

TRACOL, Xavier. Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it. Computer Law & Security Review, v. 30, n. 6, Dec. 2014. p. 736-746. Disponível em:

https://www.sciencedirect.com/science/article/abs/pii/S0267364914001587?via%3Dihub. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, 24 outubro 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046&qid=1642507300888. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Decisão 2000/520 da Comissão Europeia, 26 julho 2000a. Relativa ao nível de protecção assegurado pelos princípios de "porto seguro" [safe harbour privacy principles] e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=CELEX%3A32000D0520. Acesso em: 1 abr. 2022. UNIÃO EUROPEIA. Carta de Direitos Fundamentais da União Europeia. 18 dez. 2000b. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Tratado sobre o Funcionamento da União Europeia, 2007. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=celex%3A12012E%2FTXT. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Decisão 2010/87 da Comissão Europeia, 5 fevereiro 2010. Relativa a cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para subcontratantes estabelecidos em países terceiros nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?qid=1643040965548&uri=CELEX%3A32010D0087. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, 27 abril 2016a. 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). Disponível em: https://eurlex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A32016R0679. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Decisão 2016/1250 da Comissão Europeia, 12 julho 2016b. Relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?qid=1643027909451&uri=CELEX%3A32016D1250#ntr14- L_2016207EN.01000101-E0014. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Pedidos de decisão prejudicial apresentados pela High Court (Irlanda) e pelo Verfassungsgerichtshof. Comunicações eletrónicas — Diretiva 2006/24/CE — Serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações — Conservação de dados gerados ou tratados no contexto da oferta desses serviços — Validade — Artigos 7.°, 8.° e 11.° da Carta dos Direitos Fundamentais da União Europeia. Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e o. Relator: Thomas von Danwitz, 8 abril 2014. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2014%3A238. Acesso em: 1 abr. 2022.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Pedido de decisão prejudicial apresentado pela High Court (Irlanda). Reenvio prejudicial — Dados pessoais — Proteção das pessoas singulares no que diz respeito ao tratamento desses dados — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.°, 8.° e 47.° — Diretiva 95/46/CE — Artigos 25.° e 28.° — Transferência de dados pessoais para países terceiros — Decisão 2000/520/CE — Transferência de dados pessoais para os Estados Unidos — Nível de proteção inadequado — Validade — Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos — Poderes das autoridades nacionais de controlo. Maximillian Schrems contra Data Protection Commissioner. Relator: Thomas von Danwitz, 6 de outubro de 2015. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?qid=1642288054180&uri=CELEX%3A62014CJ0362. Acesso em: 1 jan. 2021.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Processo C-311/18. Conclusões do advogado-geral Saugmandsgaard Øe, 19 dezembro 2019. Disponível em:

https://eurlex.europa.eu/legal-content/PT/TXT/?qid=1643402586985&uri=CELEX%3A62018CC0311. Acesso em: 1 jan. 2021.

UNIÃO EUROPEIA. Tribunal de Justiça (Grande Secção). Pedido de decisão prejudicial apresentado pela High Court (Irlanda). Reenvio prejudicial — Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.o, 8.o e 47.o — Regulamento (UE) 2016/679 — Artigo 2.o, n.o 2 — Âmbito de aplicação — Transferências de dados pessoais para países terceiros para fins comerciais — Artigo 45.o — Decisão de adequação da Comissão — Artigo 46.o — Transferências mediante garantias adequadas — Artigo 58.o — Poderes das autoridades de controlo — Tratamento dos dados transferidos pelas autoridades públicas de um país terceiro para efeitos de segurança nacional — Apreciação do caráter adequado do nível de proteção assegurado no país terceiro — Decisão 2010/87/UE — Cláusulas-tipo de proteção para a transferência de dados pessoais para países terceiros — Garantias adequadas oferecidas pelo responsável pelo tratamento — Validade — Decisão de Execução (UE) 2016/1250 — Adequação da proteção assegurada pelo Escudo de Proteção da Privacidade União Europeia-Estados Unidos — Validade — Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos. Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems. Relator: Thomas von Danwitz, 16 de julho de 2020. Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/?qid=1642447809498&uri=CELEX%3A62018CJ0311. Acesso em: 1 jan. 2021.

UNITED NATIONS. International Law Commission. Report on the work of its fifty-eighth session (1 May to 9 June and 3 July to 11 August 2006). General Assembly Official Records, Sixty-first Session Supplement n. 10 (A/61/10). Disponível em: http://untreaty.un.org/ilc//reports/2006/english/chp12.pdf. Acesso em: 1 abr. 2022.

UNITED STATES (US). NATIONAL SECURITY AGENCY (NSA). Executive Order (EO) 12333, 4 Dec. 1981. Disponível em: https://www.nsa.gov/Signals-Intelligence/EO12333/. Acesso em: 1 abr. 2022. UNITED STATES (US). DEPARTMENT OF COMMERCE (DoC). FAQs – EU-U.S. Privacy Shield Program Update. 31 Mar. 2021. Disponível em:

https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update. Acesso em: 1 abr. 2022.

UNITED STATES. THE WHITE HOUSE. Fact Sheet: United States and European Commission announce Trans-Atlantic Data Privacy Framework. March 25, 2022. Disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheetunited-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/. Acesso em: 1 abr. 2022.

ZUBOFF, Shoshana. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

ZÜRN, Michael. A theory of global governance: authority, legitimacy, and contestation. Oxford: Oxford University Press, 2018.