TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS DA UNIÃO EUROPEIA E A EVOLUÇÃO DO DIREITO À PRIVACIDADE – UM ESTUDO BASEADO NOS CASOS SCHREMS I E II

INTERNATIONAL TRANSFERS OF PERSONAL DATA FROM THE EUROPEAN UNION AND THE EVOLUTION OF THE RIGHT TO PRIVACY – A STUDY BASED ON THE SCHREMS I AND II CASES

DESC
DIREITO, ECONOMIA & SOCIEDADE CONTEMPORÂNEA

TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS DA UNIÃO EUROPEIA E A EVOLUÇÃO DO DIREITO À PRIVACIDADE – UM ESTUDO BASEADO NOS CASOS SCHREMS I E II

INTERNATIONAL TRANSFERS OF PERSONAL DATA FROM THE EUROPEAN UNION AND THE EVOLUTION OF THE RIGHT TO PRIVACY – A STUDY BASED ON THE SCHREMS I AND II CASES

GUILHERME MEIRELLES PIRES FERREIRA
FACAMP – Faculdades de Campinas
https://wwws.cnpq.br/cvlattesweb/PKG_MENU.menu?f_cod=9FD16DE437700736E9F42A4B309BCCB4#

"Ninguém ignora tudo. Ninguém sabe tudo. Todos nós sabemos alguma coisa. Todos nós ignoramos algumacoisa. Por isso aprendemos sempre."
– Paulo Freire

RESUMO

O presente artigo tem como objetivo abordar a evolução dos Direitos voltados à privacidade e proteção de dados na União Europeia, especificamente no tocante às transferências de dados virtuais. Para que tal objetivo fosse atingido, foram utilizados os estudos dos casos Schrems I e II, além de analisarmos a evolução legislativa europeia em conjunto com os eventos históricos que foram responsáveis por moldar o atual padrão de privacidade e proteção de dados pessoais. Desse modo, o artigo pretende demonstrar a efetiva mudança que se espalha pela EU desde o final do Sec. XX em relação à privacidade e proteção de dados pessoais e a relação dos casos Schrems I e II com a evolução dos direitos acima referidos, além de argumentar a favor da adoção do modelo de obtenção de decisões de adequação por países que desejam realizar transações de dados tendo a EU como parte, e por fim reconhecer a posição de vanguarda obtida pela União Europeia no assunto, de modo a tornar firme sua posição de influenciadora mundial frente à legislações de privacidade e proteção de dados, que cada vez mais terão de se adequar aos parâmetros utilizados pela EU.

Palavras-chave: Direito Europeu, União Europeia, Direito à privacidade, Proteção de dados, Transferências de dados internacionais, Schrems I e II.

ABSTRACT

This paper aims to address the evolution of Rights towards data privacy in the European Union, specifically regarding virtual data transfers. To achieve this objective, the study of the Schrems I and II cases was used, in addition to analyzing the European legislative evolution, together with the historical events that were responsible for shaping the current standard of privacy and protection of personal data. In this way, the work aims to demonstrate the effective change that has spread

across the EU since the end of the 20th century in relation to privacy and protection of personal data and the relationship of the Schrems I and II cases with this evolution of the aforementioned rights, in addition to arguing in favor of adopting the model for obtaining adequacy decisions by countries that wish to carry out data transactions with the EU as a part, and finally to recognize the vanguard position obtained by the European Union in the matter, in order to assert its position as a global influencer in the face of privacy and data protection laws, which will increasingly have to adapt to the parameters used by the EU.

Keywords: European law, European Union, Right to privacy, Data protection, International data transfers, Schrems I and II.

INTRODUÇÃO

As transferências internacionais de dados pessoais se apresentam como um fenômeno mundial que cresce cada dia mais, impulsionadas pela verdadeira revolução digital que o mundo presencia regularmente a partir do final do sec. XX. As transferências de dados pessoais pelo meio digital se tornam, nesse contexto, essenciais ao desenvolvimento econômico mundial, e, portanto, utilizadas em escala cada vez maior, o que leva ao grande problema: Como conciliar a proteção do direito à privacidade frente às transferências internacionais de dados?

Tal problema não está somente no campo das ideias – temos escândalos, tal como os relatados por Edward Snowden, que são concretos. Países sem legislação definida quanto à privacidade espiona os dados que entram em seus domínios sem que os donos sejam devidamente avisados. Os casos Schrems, os quais serão objetos desse trabalho, são mais um exemplo de como as grandes corporações e demais países tem de se atentar ao respeito à privacidade de dados, sob o risco desse direito ser ferido de morte – e uma verdadeira rede de espionagem ser montada, sem que os donos desses dados tenham sequer o mínimo conhecimento.

Em virtude das informações até aqui apresentadas, sendo que estas demonstram com clareza a importância de se estudar a evolução do direito à privacidade na União Europeia à luz das transferências internacionais a partir da mesma, o presente estudo busca, através de dois estudos de caso, enfrentar a seguinte problemática: De que maneira o TJUE interpretou as exigências para as transferências internacionais de dados a partir dos casos Scherms I e II? Dessa forma, o objetivo geral passa a ser a identificação de qual é a abordagem do direito europeu para a privacidade e proteção dos dados pessoais nos períodos pré e pós julgamentos Schrems I e II.

Para que aja êxito na dissertação do objetivo geral, o presente estudo busca demonstrar como se deu e dá a transferência internacional de dados a partir da EU, tal qual com seus fundamentos históricos que embasem esse acontecimento, além ainda de demonstrar a importância da evolução do direito à privacidade no contexto digital para o avanço das diretrizes consideradas seguras e que possibilitem que os países transfiram dados de maneira transparente, segura e com respeito à privacidade pessoal.

Para o efetivo desenvolvimento dos objetivos supracitados em um corpo consistente de análise e argumentação, adota-se como processo metodológico uma abordagem indutiva, com apresentação de análise qualitativa e quantitativa, com base em um estudo com fontes documentais, através de livros, artigos e relatórios além ainda de fontes documentais legais, mediante leis federais, tratados internacionais, regulamentos e qualquer outro documento legal que se fizer necessário ao decorrer da pesquisa. Sem a pretensão de estabelecer um discurso conclusivo sobre as questões pesquisadas, busca-se meramente analisar os conceitos e metodologias adotados pelo direito europeu, contribuindo com novas reflexões e perspectivas de estudo.

Para alcançar o seu objetivo final, esse trabalho encontra-se organizado em 4 capítulos. No capítulo 1, serão apresentados os conceitos básicos das transferências internacionais de dados e a evolução do direito à privacidade na União Europeia, bem como quais são os marcos históricos fundamentais para tal acontecimento. No capítulo dois, um estudo do caso Schrems I e os seus reflexos no panorama europeu e mundial. Já no capítulo 3, mais um estudo de caso, agora do julgamento conhecido como Schrems II, assim como seus reflexos no panorama europeu e mundial. No capítulo quatro, buscaremos lançar luz sobre o instrumento chamado decisões de adequação, estes cada vez mais buscados a partir da era pós Schrems I e II. E. por fim, serão apresentadas as considerações finais.

1. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS NO CONTEXTO DA GLOBALIZAÇÃO E A EVOLUÇÃO DO DIREITO À PRIVACIDADE

1.1 MARCOS HISTÓRICOS FUNDAMENTAIS: O SURGIMENTO DAS TRANSFERÊNCIAS DE DADOS NO CAMPO INTERNACIONAL E AS PREOCUPAÇÕES COM A PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O direito à privacidade em si não é ideia recente, tendo sido notado pela primeira vez através da Declaração Universal dos Direitos Humanos, especificamente contida no chamado 12º direito fundamental, no caso, o Direito à Privacidade[1].

Entretanto, a evolução da sociedade acaba por transformar o direito à privacidade natural, também no direito à privacidade digital. Explicamos: conforme evoluem as formas de transações internacionais, graças ao advento da internet, torna-se cada vez mais necessário que haja certo controle sobre como são tratados os dados pessoais fornecidos pelas pessoas para que se concluam as transações. Registros de vendas de dados de empresas a outras, captação desses dados pelas máquinas estatais de espionagem, entre outros exemplos de violações ao direito à privacidade se tornam cada vez mais comuns, assim como a decorrente necessidade de medidas concretas para a prevenção do vazamento e compartilhamento ilegal de tais dados pessoais. Justificadas, como se percebe, as preocupações com a segurança das transferências de dados no âmbito internacional. Importante, entretanto, diferenciar os conceitos de direito à privacidade e direito à proteção de dados pessoais: O direito à privacidade, como já mencionado acima, se origina do 12º direito fundamental da Declaração Universal dos Direitos Humanos, e nesse contexto de dados, diz respeito a não ser possível usar um dado pessoal que está sob sigilo, a menos que exista consentimento do indivíduo. Já o direito à proteção dos dados pessoais, segundo Karin Klempp[2], diz respeito a uma derivação da doutrina da inviolabilidade da vida privada, da intimidade, da honra e da imagem do indivíduo, visto que estes aspectos dizem respeito à personalidade e à auto determinação do próprio individuo, e ele próprio determina o que faz parte de sua intimidade, respeitados os direitos da autodeterminação informativa, que diz respeito ao indivíduo ter direito de tomar decisões sobre a forma que seus dados pessoais serão utilizados e de se comportar dessa mesma forma.

Como nos informa Danilo Doneda,

> Fora da esfera estatal a utilização da informação era limitada, basicamente por um motivo estrutural: a desproporção de meios dos organismos privados em relação ao Estado. Tal atividade não era atraente para os privados pelos seus altos custos, tanto para o tratamento dos dados quanto da própria dificuldade para sua coleta. Esta predominância do uso estatal de informações pessoais durou até que fossem desenvolvidas tecnologias que facilitassem sua coleta e processamento para organismos particulares, não somente baixando os custos como também oferecendo uma nova e extensa gama de possibilidades de utilização destas informações, o que aconteceu com o desenvolvimento das tecnologias de informação, em especial com o avanço da informática das últimas décadas. Desta forma, a importância da informação aumenta à medida que a tecnologia passa a fornecer meios para transformá-la em uma utilidade, a um custo razoável.[3]

Mas afinal, por que a preocupação quanto à privacidade se estende ao contexto das transferências de dados internacionais e nacionais? O que se pode fazer com dados?

Segundo um estudo feito pela FORBES em 2018, a cada dia, 2,5 quintilhões de bytes de dados são criados. Entretanto, curiosamente, apenas 0,5% dos dados gerados são, de fato, analisados, o que nos traz incerteza sobre o armazenamento dos

1 https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos: "Artigo 12. Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques"

2 "Privacidade e Proteção de Dados Pessoais" de FACAMP, disponivel em https://vimeo.com/428978695

3 Doneda,Danilo – Da privacidade a proteção de dados pessoais – Pag 8 file:///C:/Users/guimp/Downloads/da-privacidade-a-proteao-de-dados-pessoais-livro_compress%20(1).pdf

dados que geramos, ora, se não vão ser utilizados, por que devem ser armazenados?[4]

Para responder essa questão, devemos explicar o conceito de "big data", cujo responsável por popularizar o termo foi John Mashey, em um artigo publicado em 1998[5]. Esse termo descreve o grande volume de dados (estruturados e não estruturados) que inunda uma empresa no dia a dia. Mas não é a quantidade de dados que é importante. É o que as organizações fazem com os dados que importa. ("Contabilidade digital e Colaborativa: modelo de eficiência - PRIMAVERA BSS") Big data pode ser analisada para insights que levam a melhores decisões e movimentos estratégicos de negócios[6].

Atualmente, quaisquer empresas que possuem um site, rede social, ou utilizam um servidor para fazer operações de forma online já fazem um armazenamento ou processamento de dados virtuais, e, portanto, o "big data". Tais dados são, anonimamente, uma mina de ouro para empresas conseguirem exercer melhor as funções de marketing e mapeamento do seu desempenho e, cada vez mais, potencializar os seus lucros.

Com a análise e processamento dos dados adquiridos, as empresas conseguem tomar as melhores decisões, ou seja, quanto mais dados você tiver, mais clara é a análise de mercado e, com isso, decisões são tomadas com mais respaldo e de forma mais assertiva, evitando a ocorrência de erros futuros. Não só isso, os dados também ajudam a melhorar os processos, diminuindo custos e tempo, visto que as conclusões tomadas utilizando os dados como base, são quase como uma matéria exata, e podem ser formuladas por meio de inteligência artificial e "machine learning", que é um ramo da inteligência artificial baseado na ideia de que sistemas podem aprender com dados, identificar padrões e tomar decisões com o mínimo de intervenção humana[7], o que é extremamente mais rápido, barato, (pois não é necessário uma equipe de pessoas especializadas para fazer esse estudo), e igualmente eficaz. Ademais, torna-se fácil analisar os concorrentes, ajudando a executar estratégias muito mais certeiras para o aumento das vendas. Além disso, mais importante do que se preocupar com a concorrência, os dados ajudam a entender melhor o perfil dos clientes que utilizam os produtos ou que pagam pelo serviço oferecido pela empresa, e, com campanhas de marketing direcionadas, buscar indivíduos que possuem uma chance maior de se tornarem consumidores e, assim, aumentar vendas, sempre tendo um retorno sobre o investimento muito maior.

Mas o advento da era virtual foi claramente um marco importante para o aumento da discussão acerca do tema, visto que trouxe consigo o surgimento dos sistemas de transferências de dados através das redes virtuais. Com a facilidade do armazenamento e rapidez no transporte de informações, o crescimento do debate tomou proporções mundiais, visto que as transferências de dados se tornaram costumeiramente internacionais, o que nos traz discussões sobre como as tornar de fato seguras, de modo a respeitar o direito à privacidade acima de tudo. Tendo o acima exposto em mente, nos cabe mostrar, então, a evolução através do tempo das transferências de dados e suas legislações, primeiramente através da exposição de marcos históricos e datas importantes que colaboraram para criar o atual padrão de privacidade.

As primeiras leis sobre dados pessoais dentro do continente europeu são da década de 70. Nessa época, em todo o globo, devido ao grande progresso tecnológico da indústria e da computação, a rápida transferência e processamento de dados e possibilidade de acúmulo de muitas informações, se dava início a era virtual. Em paralelo com esse avanço, as primeiras preocupações com dados pessoais começaram a surgir.

O Estado de Hessen, na Alemanha, no ano de 1970, com o objetivo de acompanhar esse novo mercado, iniciou a discussão sobre a criação de normas necessárias para a regulação da privacidade e promulgou a primeira lei sobre esse assunto. Tal apontamento durou longos anos de debate no cenário jurídico nacional, até que no final do ano de 1977 os frutos

4 https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#1374f9e360ba

5 https://static.usenix.org/event/usenix99/invited_talks/mashey.pdf|

6 https://inteligencia.rockcontent.com/big-data/

7 https://www.sas.com/pt_br/insights/analytics/machine-learning.html

foram colhidos com a criação de uma legislação Nacional de Proteção de Dados da Alemanha, trazendo padrões necessários para a segurança dos dados pessoais e a necessidade do consentimento do usuário para o processamento de seus dados.

Outros países da Europa acompanharam a febre e legislaram sobre a privacidade e a proteção de dados. A Suécia, em 1973, criou a "datalegen" (Lei 289 de 11 de maio) que legislava sobre a necessidade de uma autorização da Autoridade Sueca de Proteção de Dados para os registros de informações online, a ilegalidade do furto de dados e a possibilidade de indenização, caso o indivíduo sofra danos com o uso indevido de seus dados. A França, em 06 de janeiro de 1978 criou as Leis 78 e 77 relativas ao tratamento de dados, arquivos e liberdades. Em 08 de julho de 1978, a Dinamarca, trouxe proteções também para as pessoas jurídicas com as Leis 243 e 244. Além dessas normas criadas, os países Espanha e Portugal possuem regras constitucionais sobre a proteção de dados, a Espanha, no artigo 18, § 1º de sua constituição, estabelece normas contra invasões cibernéticas e em Portugal, a constituição no artigo 35º prescreve regras para "utilização da informática" e uma série de requisitos para que os dados sejam utilizados, transferidos e processados da forma correta.

Após grande movimentação legislativa pela Europa, já em 1979, a maioria dos países do continente haviam incorporado como direitos fundamentais em suas legislações as normas de proteção de dados e privacidade. A década de 80 também trouxe acontecimentos importantes para o atual padrão de proteção de dados.

Em 1980 a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) emitiu As Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, que representam

> Um consenso internacional sobre a orientação geral a respeito da coleta e do gerenciamento da informação pessoal. "Os princípios determinados nas Diretrizes sobre a Privacidade são caracterizados pela clareza e flexibilidade de aplicação e pela formulação, suficientemente ampla para possibilitar a adaptação às mudanças tecnológicas." ("Síntese Diretrizes da OCDE para a Proteção da Privacidade e ... - OECD") Esses princípios abrangem todos os meios utilizados para o processamento automatizado de dados referentes a indivíduos (do computador local à rede de complexas ramificações nacionais e internacionais), todos os tipos de processamento de dados pessoais (da administração do pessoal ao levantamento de perfis de consumidores) e todas as categorias de dados (da circulação de dados ao seu conteúdo, dos mais comuns ao mais sensíveis). Os princípios aplicam-se a ambos os níveis nacional e internacional. Ao longo dos anos, foram postos em aplicação em grande número de instrumentos de regulamentação nacionais ou de auto-regulamentação, e ainda são amplamente utilizados em ambos os setores público e privado .[8]

No ano de 1981, o Conselho da Europa, com o intuito de unificar e desenvolver melhor as normas para o tratamento automatizado de dados pessoais, adotou a Convenção 108, que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, foi o primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. "Visa garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal"[9]. O Protocolo que altera a Convenção visa alargar o seu âmbito de aplicação, aumentar o nível de proteção de dados e melhorar a sua eficácia.

Em 1983 ocorreu uma decisão pelo Tribunal Constitucional Federal alemão que reconheceu o direito fundamental à autodeterminação informativa.

> O processo dizia respeito a várias queixas constitucionais apresentadas por cidadãos, contestando diretamente a Lei do Censo Federal de 1983. A lei previa uma coleta abrangente de dados que, além de uma contagem da população, incluía informações pessoais como nome, endereço, filiação religiosa, etc., bem como informações sobre a formação educacional dos sujeitos do censo, ocupação profissional e situação de moradia.

Na decisão, ficou clara a preocupação com o usuário aos quais as informações pertencem, e a importância de ele estar ciente a cada movimentação que seja feita com os seus dados, ou seja, se os indivíduos não puderem, com certeza

8 http://www.oecd.org/sti/ieconomy/15590254.pdf

9 https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf

suficiente, determinar que tipo de informação pessoal é conhecida em seu ambiente, e se for difícil determinar que tipo de informação os potenciais parceiros de comunicação têm acesso, isso pode prejudicar seriamente a liberdade de exercer autodeterminação. No contexto do moderno processamento de dados, o livre desenvolvimento da personalidade de alguém exige, portanto, que o indivíduo seja protegido contra a coleta, armazenamento, uso e compartilhamento ilimitados de dados pessoais[10].

No ano de 1995, com a tecnologia da informação chegando próxima ao nível "moderno" conhecido atualmente, o Conselho da União Europeia e o Parlamento Europeu promulgou a Diretiva 95/46, com o intuito de criar um padrão mínimo de proteção de dados e controlar a quase incontrolável quantidade de dados e informações transferidos a cada segundo em toda União Europeia. Tal Diretiva foi responsável por proteger os direitos e as liberdades das pessoas no que diz respeito ao tratamento de dados pessoais, através da adoção dos critérios essenciais que conferem licitude ao tratamento e dos princípios relativos à qualidade dos dados. Importante frisar que a Diretiva ordenava que cada país europeu tivesse um órgão específico para que as regras da Diretiva ficassem harmônicas e em conformidade com as respectivas legislações individuais[11].

A partir dos anos 2000, surgiram algumas ferramentas criadas para a proteção dos dados, como o Safe Harbour, o Privacy Shield e mais tarde, o GDPR europeu, os quais nos debruçaremos mais a frente, neste trabalho[12].

Finda a exposição das datas e marcos históricos fundamentais no âmbito das transferências de dados internacionais, o que se percebe, portanto, é uma crescente preocupação com a segurança das mesmas, o que se realiza através das resoluções e legislações, de modo a tornar cada vez mais seguras tais transferências, visto que são essenciais para o funcionamento do mercado como conhecemos hoje, de expansão e atuação global e com cadeias de consumo que passam por domínios digitais de vários países diferentes em uma mesma compra. Premente, então, os motivos pelos quais a preocupação com a sua segurança são tantos, e a tendência torna-se de mais marcos regulatórios, graças ao advento da globalização do consumo digital.

Como trataremos nos capítulos 2 e 3 desse trabalho, os grandes escândalos de vazamento e tratamento incorretos dos dados pessoais acabam sendo responsáveis, na esfera global e continental, por moldar as legislações que buscam se adaptar aos desafios trazidos pela era da globalização dos dados pessoais. Torna-se importante, dessa maneira, prestar-se a devida atenção aos casos Schrems I e II e as inovações e conclusões que dele podem ser aduzidas, já que são *leading cases* responsáveis por moldar a maneira como a União Europeia trata das questões de transferências de dados pessoais.

1.2 PANORAMA EUROPEU DAS REGULAMENTAÇÕES E SUA EVOLUÇÃO

Após a breve exposição previa sobre os marcos históricos fundamentais no tocante à evolução da legislação de proteção de dados, cabe agora discorrer brevemente sobre o panorama europeu das regulamentações de dados, visto que são a região considerada na vanguarda quanto às legislações e programas de *compliance* de dados, tanto é que de lá saíram os dois casos nos quais esse artigo se propõe a estudar.

Não só isso, mas o estudo do panorama europeu também serve de base para que seja compreendido a importância desse tema no debate atual do *compliance* de dados, seja ele privado ou no meio estatal, e que não é pouco, e nem deve ser menosprezado – entendendo como funciona o panorama legal europeu, se entende uma boa parte de como evolui o próprio paradigma mundial da proteção de dados, visto que a legislação europeia moldou, de fato, as maneiras como as demais

10 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html
11 https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=LEGISSUM:l14012
12 Os capítulos nos quais se pode encontrar as menções são, respectivamente, o 1.2, 2 e 3

legislações internacionais se portam em relação a adequações das transferências de dados para níveis mínimos aceitos pelos países da EU. É o que ressalta Danilo Doneda:

> Na União Europeia, a Diretiva 46/ 95/ CE estabeleceu uma disciplina única sobre a transferência de dados a países terceiros (malgrado as variações regionais) a ser obedecida pelos países-membros da União Europeia, no que foi seguida e complementada pelo GDPR, de espectro amplo o suficiente para influenciar o regime internacional de transferência de dados pessoais. Nesse particular, a normativa europeia possui um âmbito geográfico no direito comunitário, regido pela normativa que prevê a proteção de dados pessoais e seu fluxo interno como matérias de competência do direito comunitário desde o momento que tal necessidade foi sentida pela União Europeia. O estabelecimento de um nível mínimo de proteção aos dados pessoais, presente em todo o espaço da UE foi o pressuposto necessário para possibilitar um livre fluxo desses dados dentro de suas fronteiras. A normativa europeia também acaba tendo uma marcante influência internacional. Entre os motivos para tanto, um é que o crescente fluxo internacional de dados pessoais gera uma demanda por padrões normativos que o legitimem, e as normas europeias são certamente o modelo mais desenvolvido nesse sentido. Outro motivo é a existência de uma cláusula de vedação da transferência de dados para países fora do espaço comunitário que não apresentem nível "adequado" de tutela[13].

Dito isto, não custa também relembrar que a Europa foi pioneira em reconhecer a importância da segurança virtual dos dados pessoais e a regulá-los. Antes mesmo dessa discussão, a cultura de valorização do princípio da privacidade já era debatida e legalizada desde a década de 1950, quando a Convenção Europeia dos Direitos do Homem promulgou um conglomerado de Direitos chamado "Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais". O artigo 8º, §1º desta convenção, prescreve: "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência"[14]. Tal artigo foi um dos primeiros dispositivos que trouxe a preocupação com a privacidade como sendo um direito básico do ser humano. Essa lei reflete a cultura que estaria surgindo em toda União E uropeia e ganhando forças para que fosse espalhada por todo o globo, conforme já demonstrado anteriormente neste trabalho.

Mas afinal, como evoluiu o panorama europeu a partir da Convenção Europeia dos Direitos dos Homens e seu artigo 8º? A resposta, embora forçoso admitir que exposta de maneira breve, é bastante linear quanto à evolução da legislação: No ano de 1973, a Assembleia Consultiva do Conselho Europeu solicitou ao Comitê de Ministros a adoção de recomendações que relacionassem o então novo fenômeno das novas técnicas de coleta de informações com o artigo 8 ° que anteriormente mencionamos. Era então publicada, no mesmo ano, uma resolução que incentivava os países europeus a adotarem princípios mínimos na matéria, com vistas a uma futura convenção para aprofundar as linhas comuns em seu direito interno. Segundo Danilo Doneda, "Efetivamente, as leis editadas por países como Suécia, Alemanha (República Federal da Alemanha, à época) e França, apresentavam certa conformidade com essa resolução[15]." Já nessa época, se percebe, o Conselho da Europa passa a cogitar tratar da matéria de proteção de dados com uma convenção, que se tornaria o primeiro passo para um sistema integrado europeu de proteção aos dados pessoais, o que acontece quase 8 (oito) anos depois.

Afinal, é no ano de 1981 que se encontra redigida e aprovada a Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais -108/ 1981. Segundo Doneda:

> Essa Convenção incita os estados-membros do Conselho da Europa e demais signatários da Convenção a adotar normas específicas para o tratamento de dados pessoais, consonantes aos seus próprios parâmetros de proteção. Ela também adota um prisma universalista, pois não foi estruturada como uma convenção puramente "europeia", tendo sido aberta para adesões também de países não membros do Conselho da Europa–ratificaram a Convenção 108 inclusive países latino-americanos, como Argentina, México e Uruguai. A importância fundamental da Convenção 108 advém de que o Conselho da Europa entende a proteção de dados como um tema de direitos humanos.

13 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3 – 3.3

14 https://www.echr.coe.int/documents/convention_por.pdf).

15 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3 – 3.2

O que se percebe, então, é o esforço europeu para oferecer parâmetros que pudessem ser adotados e integrados por todos os países membros em suas legislações internas, no estilo característico de uniformidade legislativa europeu, que segue evoluindo com o surgimento de mais características e demandas do direito digital. É a partir desses esforços que a ideia de um modelo comum na Europa ganhou força, especialmente depois do acordo TRIPS de 1994, que "bloqueou algumas tentativas de estabelecer (e legitimar) a utilização de dados pessoais como uma mercadoria passível de ser comercializada, ao reconhecer a possibilidade dos estados signatários de estabelecerem suas próprias disciplinas sobre a matéria, sem estarem sujeitos às suas sanções[16]." E afinal, em 1995 surge o documento que veio efetivamente padronizar a proteção de dados pessoais no espaço da União Europeia: a Diretiva 95/ 46/ CE, do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

A diretiva 95/46/CE, que é a legislação nas quais ambos os casos que trataremos nos capítulos 2 e 3 foram julgados, foi, até o advento da GDPR, a fonte de parâmetros pelos quais as legislações internas de cada País membro da União Europeia deveriam adequar as suas proteções quanto às transferências de dados. É ela que, muito mais ambiciosa do que a convenção de Strausborg que anteriormente mencionamos, começa a definir, de maneira muito bem detalhada, os limites que tornam possíveis e impossíveis as transferências de dados, e de fato obriga as legislações internas a aprovar normas internas de acordo com o seu conteúdo, o que implica o reconhecimento do direito fundamental da privacidade e da proteção do mesmo quando se trata de transferências de dados no âmbito nacional e internacional. Nas palavras de Danilo Doneda, mais uma vez:

> Na União Europeia, a Diretiva 46/ 95/ CE estabeleceu uma disciplina única sobre a transferência de dados a países terceiros (malgrado as variações regionais) a ser obedecida pelos países-membros da União Europeia, no que foi seguida e complementada pelo GDPR, de espectro amplo o suficiente para influenciar o regime internacional de transferência de dados pessoais. Nesse particular, a normativa europeia possui um âmbito geográfico no direito comunitário, regido pela normativa que prevê a proteção de dados pessoais e seu fluxo interno como matérias de competência do direito comunitário desde o momento que tal necessidade foi sentida pela União Europeia. O estabelecimento de um nível mínimo de proteção aos dados pessoais, presente em todo o espaço da UE foi o pressuposto necessário para possibilitar um livre fluxo desses dados dentro de suas fronteiras. A normativa europeia também acaba tendo uma marcante influência internacional. Entre os motivos para tanto, um é que o crescente fluxo internacional de dados pessoais gera uma demanda por padrões normativos que o legitimem, e as normas europeias são certamente o modelo mais desenvolvido nesse sentido. Outro motivo é a existência de uma cláusula de vedação da transferência de dados para países fora do espaço comunitário que não apresentem nível "adequado" de tutela[17].

E, importante para este trabalho notar,

> "Uma outra grande preocupação da Diretiva foi sobre o tráfego de informações entre fronteiras: prevê-se o livre fluxo de dados entre as fronteiras dos estados-membros; já o fluxo para outros países é regulado pelo princípio da equivalência, pelo qual é cerceada a transmissão para países que não possuam um nível de proteção de dados pessoais considerado adequado, de acordo com os padrões da diretiva[18]."

Além disso, como veremos nos dois capítulos adiante, a legislação também previa

> "Uma disciplina única sobre a transferência de dados a países terceiros (malgrado as variações regionais) a ser obedecida pelos países-membros da União Europeia, (...) O estabelecimento de um nível mínimo de proteção aos dados pessoais, presente em todo o espaço da UE foi o pressuposto necessário para possibilitar um livre fluxo desses dados dentro de suas fronteiras. A normativa europeia também acaba tendo uma marcante influência internacional. Entre os motivos para tanto, um é que o crescente fluxo internacional de dados pessoais gera uma demanda por padrões normativos que o legitimem, e as normas europeias são certamente o modelo mais desenvolvido nesse sentido. Outro motivo é a existência de uma cláusula de vedação da transferência de dados para

16 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3 – 3.2

17 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3 – 3.2

18 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3 – 3.2

> países fora do espaço comunitário que não apresentem nível "adequado" de tutela[19]."

Ou seja, a Diretiva realmente se preocupava com os parâmetros de segurança dos dados nas transferências, e o resultado veremos adiante.

A diretiva 95/46/CE vale, então, até o ano de 2018, com a chegada do GDPR (General Data Protection Regulation), o Regulamento Europeu geral de proteção de dados, que traz consigo uma uniformidade necessária, visto que, nas palavras de Doneda

> "Até então ele não havia chegado ainda a assumir uma forma "pura" -por minuciosa que tenha sido a normativa anterior, a Diretiva 95/ 46/ CE, a sua aplicabilidade direta ocorria apenas em via de exceção, já que a lei efetivamente aplicada aos casos concretos era a lei nacional, resultado da transposição da diretiva por cada estado--membro[20]."

O que nos leva aos dias de hoje, nos quais o sistema de proteção de dados pessoais nos estados-membros da União Europeia é unificado em torno de um núcleo composto basicamente do Regulamento Geral de Proteção de Dados (GDPR).

2. O CASO SCHREMS I E A SUA IMPORTÂNCIA PARA O DIREITO À PRIVACIDADE

2.1 CASO SCHREMS I – O QUE FOI?

2.2 CONTEXTO E DECISÃO DA HIGH COURT

O caso Schrems I, o qual tomaremos como base em conjunto com a lide decorrente do mesmo, diz respeito ao processo judicial movido por Maximillian Schrems, na época um estudante de Direito, hoje advogado, austríaco, ativista na privacidade de dados, fundador da ONG "Europa Vs Facebook" e promotor da ONG "NOYB" (None of Your Business), sendo interveniente a *Digital Rights Ireland* LTD.[21], no qual, segundo o próprio acordão, foi "apresentado no âmbito de um litígio que opõe M. Schrems ao *Data Protection Commissioner* (...) a propósito da recusa deste último em investigar uma queixa apresentada por M. Schrems pelo facto de a Facebook Ireland Ltd transferir para os Estados Unidos dados pessoais dos seus utilizadores e os conservar em servidores situados neste país" (ACÓRDÃO DE 6. 10. 2015 — PROCESSO C-362/14 SCHREMS). Tal Processo, como se nota, teve início com o questionamento de Schrems frente à política de compartilhamento de dados adotada na Irlanda e União Europeia como um todo, e tem como base a verificação de segurança na transferência de dados para Países terceiros receptores dos mesmos, o que Schrems questionava, segundo o acordão que usamos como base, por ter percebido que "Todas as pessoas que residam no território da União e pretendam utilizar o Facebook são obrigadas, no momento da sua inscrição, a celebrar um contrato com a Facebook Ireland, filial da Facebook Inc., com sede nos Estados Unidos. Os dados pessoais dos utilizadores do Facebook residentes no território da União são, no todo ou em parte, transferidos para servidores pertencentes à Facebook Inc., situados em território dos Estados Unidos, onde são objeto de tratamento" (ACÓRDÃO DE 6. 10. 2015 — PROCESSO C-362/14 SCHREMS).

Ocorre que, segundo as queixas apresentadas pelo autor, tendo por base as revelações de Edward Snowden sobre a

19 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3 – 3.3

20 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3 – 3.1

21 http://curia.europa.eu/juris/document/document.jsf;jsessionid=B18615879E2C19BA5836FCB1C9F0AFB1?text=&docid=169195&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=16740157

política de tratamento de dados utilizada nos EUA[22], o que se colocava em cheque era o nível de proteção realmente oferecido pelo programa e diretrizes adotados pela União Europeia na transferência de dados, na época o programa conhecido como "Safe Harbour/Porto Seguro". O que se desdobra, segundo a sentença, em:

> Schrems apresenta ao Commissioner uma queixa em que lhe pedia, em substância, que exercesse as suas competências estatutárias proibindo a Facebook Ireland de transferir os seus dados pessoais para os Estados Unidos. Alegava que o direito e as práticas em vigor neste país não asseguravam uma proteção suficiente dos dados pessoais conservados no seu território contra as atividades de vigilância aí exercidas pelas autoridades públicas. (ACÓRDÃO DE 6. 10. 2015 — PROCESSO C-362/14 SCHREMS).

Não foi bem recebido, entretanto, pois o Comissário entendeu que:

> "não estava obrigado a investigar os factos denunciados por M. Schrems na sua queixa, (...) arquivou-a por falta de fundamento. Com efeito, considerou que não havia provas de que a Agência de Segurança Nacional americana (NSA) tivesse acedido aos dados pessoais do interessado. Acrescentou que as críticas suscitadas por M. Schrems na sua queixa não podiam ser utilmente invocadas, dado que qualquer questão relativa ao caráter adequado da proteção dos dados pessoais nos Estados Unidos devia ser decidida em conformidade com a Decisão 2000/520 e que, nesta decisão, a Comissão tinha constatado que os Estados Unidos asseguravam um nível de proteção adequado." (ACÓRDÃO DE 6. 10. 2015 — PROCESSO C-362/14 SCHREMS).

O que leva, Schrems, de fato, a interpor recurso para a High Court (Supremo Tribunal de Justiça) da decisão em causa no processo principal a que nos referimos anteriormente. A decisão obtida, então, é a de que

> "(...) segundo esse mesmo órgão jurisdicional, os cidadãos da União não dispõem de nenhum direito efetivo a ser ouvidos. A supervisão das ações dos serviços de informações é feita através de procedimentos secretos e não contraditórios. Após a transferência de dados pessoais para os Estados Unidos, a Agência de Segurança Nacional americana (NSA) e outros órgãos federais, como o Federal Bureau of Investigation (FBI), podem aceder a tais dados no âmbito da vigilância e das interseções indiscriminadas a que procedem em grande escala. A High Court (Supremo Tribunal de Justiça) declarou que o direito irlandês proíbe a transferência de dados pessoais para fora do território nacional, salvo se o país terceiro em questão assegurar um nível adequado de proteção da vida privada bem como dos direitos e liberdades fundamentais. A importância dos direitos ao respeito da vida privada e à inviolabilidade do domicílio, garantidos pela Constituição irlandesa, exige que qualquer ingerência nestes direitos seja proporcionada e respeite os requisitos previstos pela lei. (...). Ora, o acesso massivo e indiscriminado a dados pessoais é, evidentemente, contrário ao princípio da proporcionalidade e aos valores fundamentais protegidos pela Constituição irlandesa" (PROCESSO C-362/14 SCHREMS).

Em suma, a High Court devolve o caso ao tribunal de justiça ao reconhecer o direito de Schrems de questionar, na realidade, a legalidade do regime do Safe Harbour utilizado, e toma a decisão de "submeter ao Tribunal de Justiça as questões prejudiciais seguintes:

> 1) Tendo em conta os artigos 7.°, 8.° e 47.° da Carta [...] e sem prejuízo das disposições do artigo 25.°, n.° 6, da Diretiva 95/46, o [Commissioner] encarregado de aplicar a legislação sobre a proteção de dados pessoais no âmbito da análise de uma queixa segundo a qual o direito e as práticas de um país terceiro (neste caso, os Estados Unidos da América) para o qual são enviados dados pessoais não oferecem proteção adequada, está vinculado em termos absolutos pela constatação em sentido contrário da União, contida na Decisão 2000/520?
>
> 2) Em alternativa, pode e/ou deve proceder à sua própria investigação sobre a matéria, à luz dos últimos desenvolvimentos de facto ocorridos desde a primeira publicação da decisão da Comissão?"

2.3 DECISÃO E ANÁLISE DO TRIBUNAL DE JUSTICA DA UNIÃO EUROPEIA

Após a decisão da *High Court Irlandesa* em remeter o processo ao tribunal de justiça, a mesma passa a responder aos questionamentos impostos e acima mencionados. O que se constatou, então, foi uma verdadeira incongruência entre as

22 ("Após a transferência de dados pessoais para os Estados Unidos, a NSA e outros órgãos federais, como o *Federal Bureau of Investigation* (FBI), podem aceder a tais dados no âmbito da vigilância e das interseções indiscriminadas a que procedem em grande escala"),

diretrizes adotadas pelo *Safe Harbour* em relação ao nível de proteção de dados que seria exigido pela Legislação irlandesa em relação à transferência dos mesmos para países terceiros (e nesse caso, especificamente os EUA), o que se constata nos trechos abaixo citados:

> "Como se referiu, nomeadamente, nos n.os 71, 73 e 74 do presente acórdão, a adoção pela Comissão de uma decisão nos termos do artigo 25.°, n.° 6, da Diretiva 95/46 exige a constatação, devidamente fundamentada, por parte daquela instituição, de que o país terceiro em causa assegura efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção dos direitos fundamentais substancialmente equivalente ao garantido na ordem jurídica da União, como resulta, nomeadamente, dos número anteriores do presente acórdão. (...)
>
> 97 Ora, há que salientar que a Comissão não indicou, na Decisão 2000/520, que os Estados Unidos da América «asseguram» efetivamente um nível de proteção adequado em virtude da sua legislação interna ou dos seus compromissos internacionais.
>
> 98 Consequentemente, e sem que seja necessário examinar os princípios do "Porto Seguro" quanto ao seu conteúdo, há que concluir que o artigo 1.° daquela decisão viola os requisitos estabelecidos no artigo 25.°, n.° 6, da Diretiva 95/46, lido à luz da Carta, e é, por esta razão, inválido." (...)
>
> 103 Ora, o poder de execução atribuído pelo legislador da União à Comissão no artigo 25. °, n.º 6, da Diretiva 95/46 não confere a esta instituição competência para limitar os poderes das autoridades nacionais de controlo referidos no número anterior do presente acórdão.
>
> 104 Nestas condições, há que concluir que, ao adotar o artigo 3.° da Decisão 2000/520, a Comissão ultrapassou a competência que lhe é atribuída pelo artigo 25.°, n.° 6, da Diretiva 95/46, lido à luz da Carta, e que esse artigo é, por essa razão, inválido.
>
> 105 Uma vez que os artigos 1.° e 3.° da Decisão 2000/520 são indissociáveis dos artigos 2.° e 4.°, bem como dos anexos da mesma, a sua invalidade tem como efeito afetar a validade dessa decisão na sua totalidade.
>
> "106 Atendendo a todas as considerações precedentes, há que concluir que a Decisão 2000/520 é inválida." ("CURIA - Documents - European Court of Justice")

2.4 SENTENÇA

O que concluiu o Tribunal de Justiça da União Europeia (TJUE), em suma, foi a total invalidação da decisão 200/520, e a legalidade do exame da efetiva validade da proteção garantida aos dados em contexto das transferências internacionais, que pode ser suscitado por qualquer cidadão, e garantindo poderes de fiscalização a serem realizados pelas autoridades competentes, de modo a ser comprovada a efetividade, e não apenas alegada. Foi a sentença de morte do modelo de Safe Harbour:

"Pelos fundamentos expostos, o Tribunal de Justiça da União Europeia (TJUE) (Grande chambre) declara:

> 1) O artigo 25.°, n.° 6, da Diretiva 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, conforme alterada pelo Regulamento (CE) n.° 1882/2003 do Parlamento Europeu e do Conselho, de 29 de setembro de 2003, lido à luz dos artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46 relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ), emitidos pelo Department of Commerce dos Estados Unidos da América, através da qual a Comissão Europeia constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controlo de um EstadoMembro, na aceção do artigo 28.° desta diretiva, conforme alterada, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um EstadoMembro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigor neste último não asseguram um nível de proteção adequado.
>
> 2) A Decisão 2000/520 é inválida."

2.5 REFLEXOS DA DECISÃO DA HIGH COURT E O PARADIGMA DAS LEIS DE PRIVACIDADE E PROTEÇÃO DE DADOS APÓS A SENTENÇA

Finda a análise pratica e jurídica sobre o que consiste a decisão conhecida como Schrems I, passamos a discorrer sobre os reflexos dela no sistema jurídico e o panorama que se instalou na União Europeia após mesma. Pelas palavras do Professor Dr. Lokke Moerel:

> Since 2000, European companies could transfer personal data to US companies that adhered to the Safe Harbor Framework and were considered 'safe' for the transfer of data based on the Safe Harbor Decision by the Commission. About 4.000 companies were Safe Harbor certified, among which many providers of cloud services. As a result of the Schrems judgment, these transfers were invalidated as the privacy of European citizens was not considered being adequately protected[23],

Isto demonstra o quanto a decisão impactou de fato o cenário da UE.

Subitamente, as transferências de dados já não eram mais válidas, e a maioria das empresas não se mostraram preparadas para uma mudança brusca em seu sistema. Mas mais do que isso: as próprias noções sobre o que deveriam ser consideradas transferências seguras de dados no plano internacional foram transformadas. A partir dessa decisão, as transferências não mais podiam se dar no plano internacional se o país que recebia os dados pessoais não demonstrasse ter bases para tratamento de dados que fossem consideradas "seguras" e pelo menos no mesmo nível exigido dos países da EU. Citando mais uma vez o mesmo texto do Professor Dr. Lokke Moerel:[24]

> In any event it is by now clear that unbridled data transfers to non-adequate countries is subject to risks and will remain so for quite some time. As a result, we see a clear trend to store data in European clouds and further to encrypt data as much as possible without the cloud provider having access to the data ('bring your own encryption'), to prevent that data can be read when accessed by US or any third country government.,

O cenário de confusão, então, era claro: o próprio sistema mais utilizado para transferências de dados na época não era considerado seguro e as medidas e standards requeridos dentro da União Europeia tiveram que ser mais bem definidos (já que eram eles as bases em que os tribunais consideravam se um país oferecia proteção em nível parecido e adequado) em casos de revisões solicitadas pelos portadores dos dados.

Como se pode ver, os cenários encontrados pelas leis de proteção de dados eram de urgência, já que existia a necessidade de se fixar parâmetros claros pelos quais se pudessem julgar seguras as transferências de dados pessoais e seguros os países que as recebiam, ou elas teriam que ser feitas por instrumentos secundários e com a concordância de que estariam sujeitas a riscos. A soma desses fatores leva, por fim, a Comissão Europeia a entrar em acordo com os Estados Unidos da América em relação a um segundo programa de transferência de dados, o *Privacy Shield* assunto sobre o qual discorreremos no capítulo 3.

3. SCHREMS II

3.1 CASO SCHREMS II – O QUE FOI?

O questionamento se deu devido à eficiência do mecanismo Privacy Shield (decisão 2016/1250), que foi um acordo feito entre os EUA e a União Europeia, visando uma regulamentação de segurança e transferência de dados entre essas duas

23 https://media2.mofo.com/documents/160913-implications-schrems-data-transfers.pdf
24 https://media2.mofo.com/documents/160913-implications-schrems-data-transfers.pdf

potencias mundiais. Nesse acordo, a União Europeia cobra um padrão mínimo de segurança, para que os dados possam ser transferidos para países terceiros.

1. Atrelado ao caso Schrems I, o qual deu o primeiro passo para definir regras para a transferência internacional de dados, o caso Schrems II foi um debate judicial iniciado novamente por um usuário do Facebook, Maximillian Schrems, advogado austríaco, ativista na privacidade de dados, o qual questionou a eficiência do mecanismo intitulado de *Privacy Shield* e o transporte de seus dados pessoais entre o Facebook Ireland e o Facebook Inc, localizado nos Estados Unidos (EUA).

Para Maximillian, o Facebook não estaria respeitando alguns direitos fundamentais de seus usuários, visto que a empresa repassava para a inteligência americana alguns dados que não eram extremamente necessários, incluindo informações sigilosas, claramente burlando o que visava o Privacy Shield e cobrando mecanismos mais adequados para transferência de dados da Europa para os EUA. Uma investigação própria demonstrou que a rede social utilizava ilegalmente os dados que coletava e armazenava. Aproximadamente 50 dados pessoais dos usuários eram coletados, alguns deles de forma questionável, como por exemplo as mensagens apagadas pelos usuários e informações sobre o que os usuários falam sobre uma pessoa, mesmo que essa pessoa não seja usuária da rede social.

Schrems estava correto em sua indagação, visto que o Facebook coleciona polêmicas que colocam a sua credibilidade com relação à política de dados em "xeque" (vide polêmica da Cambridge Analytica nas eleições presidenciais; vazamento de dados para empresas terceiras de forma ilegal, entre outros.)[25]

Não é de hoje que a política de dados dos EUA é invasiva com os usuários. O país passou por mudanças drásticas após o ocorrido no dia 11 de setembro de 2001, principalmente na questão da segurança nacional, tornando extremamente difícil conseguir trabalhar com políticas de segurança de dados em conjunto com o governo dos EUA, pela forma como lidam com as informações de praticamente todas as redes sociais que funcionam na América do Norte. Exemplo dessa dificuldade é a acusação de que o Facebook não raro auxiliava e fornecia dados pessoais dos usuários para a Agência de Segurança Nacional Americana (NSA), órgão que é famoso por criar programas sigilosos para extração de informações pessoais na internet .[26]

Um desses programas de vigilância se chama "Prism" e foi mencionado durante o processo movido contra o Facebook. É um programa que tem como proposta monitorar comunicações estrangeiras e nacionais consideradas valiosas e que podem servir para proteger os Estados Unidos e seus aliados. Apesar de parecer limitado a estes países, o programa tem abrangência global, supervisionando dados de qualquer pessoa em qualquer parte do mundo. ("O que é PRISM? - Canaltech") Conforme os documentos vazados alegam, o Prism está ligado a servidores de todo o mundo, em especial aos situados nos Estados Unidos e sob a responsabilidade de várias empresas de porte no ramo de tecnologia[27]. ("Socializando Saberes » Blog Archive » O que é PRISM?") ("O que é PRISM? - Canaltech")

3.2 DECISÃO - A DECISÃO DO TRIBUNAL

"O Tribunal de Justiça (Grand Chambre) declarou:

> I) O artigo 2.°, nº 1 e 2, do Regulamento (UE) 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), deve ser interpretado no sentido de que está abrangida pelo âmbito de aplicação deste regulamento uma transferência de dados pessoais efetuada para fins comerciais por um operador económico estabelecido num EstadoMembro para

25 Disponível em: <https://www.techtudo.com.br/listas/2018/12/oito-polemicas-envolvendo-o-facebook-em-2018.ghtml> Acesso em 24/08/2020.

26 Disponível em: <https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?hpid=z1> Acesso em 24/08/2020.

27 Disponível em: <https://canaltech.com.br/espionagem/O-que-e-PRISM/> Acesso em 24/08/2020.

outro operador econômico estabelecido num país terceiro, não obstante o facto de, no decurso ou na sequência dessa transferência, esses dados serem suscetíveis de ser tratados pelas autoridades do país terceiro em causa para efeitos de segurança pública, de defesa e de segurança do Estado.

II) O artigo 46.°, n° 1, e o artigo 46.°, n° 2, alínea c), do Regulamento 2016/679 devem ser interpretados no sentido de que as garantias adequadas, os direitos oponíveis e as medidas jurídicas corretivas eficazes exigidos por estas disposições devem assegurar que os direitos das pessoas cujos dados pessoais são transferidos para um país terceiro com base em cláusulas padrão de proteção de dados beneficiam de um nível de proteção substancialmente equivalente ao garantido na União por este regulamento, lido à luz da Carta. Para este efeito, a avaliação do nível de proteção assegurado no contexto dessa transferência deve, nomeadamente, ter em consideração tanto as estipulações contratuais acordadas entre o responsável pelo tratamento ou o seu subcontratante estabelecidos na União e o destinatário da transferência estabelecido no país terceiro em causa como, no que respeita a um eventual acesso das autoridades públicas desse país terceiro aos dados pessoais assim transferidos, os elementos pertinentes do sistema jurídico deste país terceiro, nomeadamente os enunciados no artigo 45.°, n.° 2, do referido regulamento.

III) O artigo 58.°, n° 2, alíneas f) e j), do Regulamento 2016/679 deve ser interpretado no sentido de que, a menos que exista uma decisão de adequação validamente adotada pela Comissão Europeia, a autoridade de controlo competente está obrigada a suspender ou a proibir uma transferência de dados para um país terceiro, fundada em cláusulas padrão de proteção de dados adotadas pela Comissão, se essa autoridade de controlo considerar, à luz de todas as circunstâncias especificas dessa transferência, que essas cláusulas não são ou não podem ser respeitadas nesse país terceiro e que a proteção dos dados transferidos exigida pelo direito da União, em particular pelos artigos 45.° e 46.° deste regulamento e pela Carta dos Direitos Fundamentais, não pode ser assegurada por outros meios, no caso de o responsável pelo tratamento ou o seu subcontratante estabelecidos na União não ter ele próprio suspendido ou posto termo à transferência.

IV) O exame da Decisão 2010/87/UE da Comissão, de 5 de fevereiro de 2010, relativa a cláusulas contratuais padrão 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, conforme alterada pela Decisão de Execução (UE) 2016/2297 da Comissão, de 16 de dezembro de 2016, à luz dos artigos 7.°, 8.° e 47.° da Carta dos Direitos Fundamentais não revelou nenhum elemento suscetível de afetar a validade desta decisão.

V) A Decisão de Execução (UE) 2016/1250 da Comissão, de 12 de julho de 2016, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UEEUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, é inválida[28]."

3.3 O *PRIVACY SHIELD* GARANTE A SEGURANÇA DOS DADOS?

A Decisão de Adequação do processo que o deferiu foi tomada com base na constatação de um nível adequado de proteção para dados pessoais transferidos da UE para organizações nos EUA ao abrigo do *Privacy Shield*. O Tribunal de Justiça da União Europeia (TJUE) examinou detalhadamente esta "constatação de um nível adequado de proteção", e decidiu que é "impossível concluir" que esse mecanismo pudesse garantir um nível de proteção ao menos equivalente, ao garantido pelo GDPR.

3.4 AS CLÁUSULAS CONTRATUAIS PADRÃO

As cláusulas padrão permanecem válidas à luz dos artigos 7º, 8º e 47º. Neste ponto da decisão, o Tribunal de Justiça da União Europeia (TJUE) levou muitos fatores em consideração, incluindo o fato de que as Cláusulas contratuais padrão (CCP) possuem um mecanismo eficaz que garante que a transferência de dados para um país terceiro seja segura. Além disso, concluiu que a validade dos CCPs depende da existência de mecanismos eficazes que permitirão o nível de proteção exigido pela legislação da UE, e que faça suspender ou proibir a transferência de dados, ao ocorrer a violação das CCP. Ademais,

28 Disponívelem:<http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=PT&part=1&occ=first&mode=lst&pageIndex=0&cid=134%E2%80%A6>Acesso em 24/08/2020.

também abordou a situação em que a aplicação da lei faz um pedido juridicamente vinculativo de divulgação de dados pessoais, mas o importador de dados está proibido por lei de notificar o exportador de dados sobre isso. Nessa situação, o importador de dados está autorizado a não notificar o exportador de dados sobre a solicitação, mas deve informar ao exportador de dados de uma incapacidade de cumprir as CCPs.

O Tribunal de Justiça da União Europeia (TJUE) decidiu que as CCPs continuam a ser uma "proteção apropriada" para as transferências internacionais de dados nos termos do Artigo 46º do GDPR, mas que, ao utilizá-las, uma organização deve verificar "caso a caso" se os dados pessoais que forem transferidos serão adequadamente protegidos no país de destino, de acordo com os requisitos da legislação da União Europeia (EU). O padrão de proteção deve ser "essencialmente equivalente" ao garantido na União Europeia (UE) pelo GDPR.

O Tribunal de Justiça da União Europeia (TJUE) observou, ainda na sua decisão, que a cláusula 6º das CCPs prevê que a sua violação resultará no direito de a vítima exigir uma indenização pelos danos sofridos. Se o exportador de dados estiver ciente de que categorias especiais de dados podem ser transferidas para um país que não oferece proteção adequada, ele deve notificar os titulares dos dados com antecedência ou o mais rápido possível depois. Se o importador de dados receber uma notificação de que as leis do terceiro país foram alteradas de uma maneira que afetaria a capacidade de cumprir as CCPs, ele deverá notificar o exportador de dados[29].

3.5. REFLEXOS DO CASO NOS EUA E NO RESTO DO MUNDO

O acórdão Schrems II é um marco na regulamentação da transferência de dados da UE, e levanta uma série de questões importantes. De acordo com uma pesquisa da IAPP (International Association of Privacy Professionals ou Associação Internacional de Profissionais de Privacidade), 88% das empresas que transferem dados para fora da UE utilizam as CCPs, enquanto 60% utilizavam Privacy Shield. Devido à revogação do Privacy Shield, as empresas que o utilizavam deverão buscar outro tipo de ferramenta segura de transporte de dados, tais como as CCPs. Ademais, extrai-se da decisão que quem já utiliza CCPs também não está isento de realizar uma avaliação individual de cada caso e informar a autoridade de supervisão competente para "checagem de segurança", visto que apenas poderão continuar a utilizar os CCPs, os que forem capazes de oferecer uma garantia de que a lei dos EUA não consiga interferir no nível adequado de proteção, e, caso um exportador de dados da UE-EUA não consiga isso, ele precisará interromper a transferência de dados[30].

No tocante à relação jurídica com os EUA, O Tribunal de Justiça da União Europeia (TJUE) concluiu que a lei americana (Seção 702 FISA -Lei de Vigilância de Inteligência Estrangeira- e EO -Ordem Executiva- 12333) interfere no nível de proteção de dados ideal e agora está claro que o GDPR deixa pouco espaço de manobra e de diálogo para acomodar as normas de países terceiros.

Observamos que simplesmente tentar criar um terceiro acordo que faça pequenas alterações no Privacy Shield não seria aceito e muito menos daria às partes envolvidas a segurança jurídica necessária. Em paralelo a isso, a ideia de burlar a legislação de Segurança Nacional Americana também não parece ser uma boa alternativa. Em vez disso, novas abordagens e novos pensamentos são necessários para que a relação econômica (de 7,1 trilhões de dólares!) entre EU-EUA não seja cortada e tampouco abalada.

No debate para tentar achar uma solução para o litigio, duas ações podem ser tomadas, a priori: a primeira delas poderia ser a mudança da localização dos dados, ou seja, as empresas podem decidir por armazenar na UE todos os dados

29 Disponível em: <https://www.lexology.com/library/detail.aspx?g=880f1a89-20b7-4d14-be92-9d8e7e3d7814> Acesso em 24/08/2020.

30 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

pessoais originários de lá, devido à possível falta de uma forma legal de exportá-los. Essa ação seria cara e causaria vários problemas técnicos, e, embora o acórdão TJEU aparentemente não se preocupe com este tipo de dificuldades práticas, é difícil imaginar como empresas e serviços multinacionais poderiam realizar seus negócios se os dados que entram na UE não podem sair dela. A segunda estratégia seria arriscar continuar com os negócios normalmente, levando em consideração que o risco de vigilância da Agência de Segurança Nacional Americana (NSA) é relativamente diferente para os diferentes tipos de dados transferidos. A parte ruim da segunda opção é a penalidade: uma multa que pode chegar a 4% da receita GLOBAL da empresa[31].

A decisão Schrems II traz consequências não só à relação EU-EUA, mas a todo o mundo. Obviamente, em países em que a fiscalização do governo é questionável (como Rússia, China, entre outros), o tratamento tende a ser mais severo, seguindo o mesmo padrão de segurança "equivalente" que demanda a GDPR, caso contrário, a transferência de dados deverá cessar. Porém, deve-se lembrar que a decisão terá efeito em países da própria Europa, que não possuem um padrão de segurança tão rígido. Inúmeras análises independentes, incluindo da própria Agência de Direitos Fundamentais da União Europeia (FRA), documentaram grandes variações no rigor entre as salvaguardas de privacidade contra vigilância conduzida por estados europeus sob autoridades legais nacionais. Até mesmo estados com profundo comprometimento com o Estado de Direito, como o Reino Unido, conduz uma ampla vigilância para fins de segurança nacional, podendo entrar em conflito com os rigorosos padrões do TJEU.

4. SISTEMA DE DECISÃO DE ADEQUAÇÃO PELA COMISSÃO EUROPEIA E A SUA IMPORTÂNCIA NO CENÁRIO PÓS SCHREMS I E II

O cenário das transferências internacionais de dados após os dois casos Schrems torna-se muito mais restrito, como se pode perceber. Os programas do Safe Harbour e Privacy Shield são considerados como ineficazes, e, portanto, não seguros na visão da proteção à privacidade que buscavam tanto a diretiva 46/95/CE quanto a GDPR que se instala depois, o que invalida as transferências realizadas por meio deles. O que resta, então, para os países interessados em realizar as referidas transferências de dados internacionais com países pertencentes á União Europeia , ainda mais tendo em vista que existe uma cláusula de vedação de transferência de dados para países fora da EU que não apresentem nível adequado de tutela. Não somente isto, mas após os casos Schrems não basta apenas as alegações de que os requisitos de privacidade dos dados pessoais são cumpridos para sua liberação – e sim uma verificação adequada que prove as alegações-; e que por fim, qualquer cidadão ou parte interessada pode requerer às Cortes uma avaliação de segurança da privacidade.

Por fim, o que se conclui então é de que o instrumento mais seguro para que sejam facilitadas as transferências de dados seria através das decisões de adequação, as quais vamos explicar adiante.[32]

Já nos ensinava Danilo Doneda: "O GDPR, em seu artigo 45(1), como já o fazia a Diretiva 95/ 46/ CE em seu artigo 25, utiliza a técnica de negar, como solução padrão, a transferência de dados pessoais da União Europeia para países terceiros, a não ser que esse país possua um sistema de proteção de dados pessoais que atenda ao nível requerido de "adequação"[33].

E afinal, do que se tratam as tais decisões de adequação? A resposta é mais simples do que parece: com elas, podem

31 Disponível em: <https://iapp.org/news/a/cjeus-schrems-ii-decision-slated-for-july-16/> Acesso em 30/08/2020.

32 Primeiro, a normativa exige que a proteção dos dados pessoais no país fora da União Europeia seja "adequada" – e não "equivalente" ao padrão europeu, o que indica uma certa maleabilidade. Portanto, existe a necessidade de verificar essa adequação para que a Comissão Europeia a reconheça, nos termos do art. 45 do GDPR.

33 Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados de Danilo Cesar Maganhoto Doneda – Cap 3.3

ser realizadas transferências de dados pessoais para um país terceiro ou uma organização internacional, se a Comissão tiver decidido que o país terceiro, território, um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado, esta transferência não exige autorização específica. (artigo 45.º, n.º 1, RGPD)[34].

Portanto, as decisões de adequação são avaliações feitas para concluir se o País em transferir dados da/para a Europa está apta para cumprir os requisitos de segurança da GDPR). Tais avaliações são feitas pela European Data Protection Board (EDBP), que é o organismo da União Europeia encarregado da aplicação da GDPR desde 25 de maio de 2018.

Após a European Data Protection Board (EDBP) analisar e concluir que o país terceiro possui um nível adequado de proteção, tal decisão reconhece que o sistema desse país é seguro como o sistema dos Estados-Membros da UE. Portanto, é considerado que as transferências de dados do país interessado em transferir dados serão equiparadas às transmissões de dados feitas dentro do território Europeu, o que permitirá conceder um acesso privilegiado e desobstruir diversos canais comerciais presentes no gigantesco mercado da Europa, visto que poderão usufruir, tratar e transferir dados online para dentro e fora da UE.

Essa decisão não é tomada de forma subjetiva, existem alguns critérios que deverão ser observados para que a decisão de adequação possa ser considerada válida. A Comissão Europeia estabelece a necessidade de verificação da presença dos critérios da GDPR e julgar de acordo com os seguintes elementos:

> 1º Conceitos: Devem existir conceitos e/ou princípios básicos em matéria de proteção de dados; 2º Fundamento para o tratamento lícito e leal para fins legítimos: Os dados devem ser tratados de forma lícita, leal e legítima; 3º Princípio da limitação da finalidade: os dados devem ser tratados com uma finalidade específica e, subsequentemente, utilizados apenas na medida em que essa utilização não seja incompatível com a finalidade do tratamento; 4º Princípio da qualidade e proporcionalidade: os dados devem ser exatos e, quando necessário, objeto de atualização, além de deverem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados; 5º Princípio da conservação: regra geral, os dados não devem ser conservados mais tempo do que o necessário; 6º Princípio da segurança e da confidencialidade: qualquer entidade que proceda ao tratamento de dados pessoais deve assegurar que os dados são tratados de modo a garantir a sua segurança; 7º Princípio da transparência: todos os titulares devem ser informados de todos os principais elementos do tratamento dos seus dados pessoais de forma clara, facilmente acessível, concisa, transparente e inteligível; 8º Direito de acesso, retificação, apagamento e oposição: o titular dos dados deve ter o direito de obter confirmação do eventual tratamento dos dados que lhe dizem respeito, bem como de aceder a esses dados, obter sua retificação quando estes estiverem incorretos ou incompletos ou seu apagamento quando seu tratamento deixar de ser necessário ou for ilícito. Podem ainda se opor a tratamento de dados por motivos legítimos imperiosos relacionados com a sua situação particular; 9º Restrições relativas a transferências subsequentes: outras transferências dos dados pessoais por parte do destinatário inicial da transferência de dados original só devem ser permitidas se o destinatário seguinte também estiver sujeito a normas (incluindo normas contratuais) que garantam um nível de proteção adequado e seguir as instruções pertinentes aquando do tratamento de dados em nome do responsável pelo tratamento dos dados; 10º Categorias especiais de dados: Devem existir salvaguardas específicas aplicáveis a categorias especiais de dados (p. ex. dados relativos à saúde, opção sexual, crença religiosa, dentre outros); 11º Comercialização Direta: se os dados forem tratados para efeitos de comercialização direta, o titular deve poder opor-se sem qualquer custo ao tratamento dos dados para essa finalidade, em qualquer momento; 12º: Decisões automatizadas e definição de perfis: as decisões baseadas unicamente no tratamento automatizado (decisões individuais automatizadas), incluindo definição de perfis, que produzem efeitos jurídicos ou afetam significativamente o titular dos dados, só podem ser tomadas nas condições fixadas no quadro normativo do país terceiro; 13º Autoridade de controle competente e independente: Deve existir uma ou mais autoridades de controle independentes, responsáveis pelo seguimento e por assegurar e aplicar a conformidade com as disposições de proteção de dados e privacidade no país terceiro; 14º Responsabilização: o quadro de proteção de dados do país terceiro deve obrigar os responsáveis pelo tratamento dos dados e/ou aqueles que tratam dados pessoais em seu nome a cumprir esse mesmo quadro e conseguir comprovar esse cumprimento; 15º Apoio e ajuda destinada aos titulares de dados no exercício dos seus direitos e mecanismos de reparação adequados: as pessoas singulares devem ter acesso a vias de recurso para

34 Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em: 01 de nov. de 2020

fazer valer os seus direitos rápida e eficazmente, e sem custos proibitivos, bem como assegurar a conformidade[35].

Desse modo, e com base nos critérios ilustrados acima, fica visível a dificuldade de se obter uma decisão de adequação favorável dentro da EU, mas também se percebe que é o caminho mais seguro, além do que garante maiores benefícios no longo prazo, em relação às adequações contratuais pontuais (como as Binding Corporate Rules BCR – Art.47 da GDPR que serviriam como base para a liberação da transferência de dados caso o país em questão não tenha uma decisão de adequação (e poucos têm no presente momento). As decisões de adequação de fato resolvem problemas de confiança quanto aos níveis de à privacidade e proteção dos dados pessoais exigidos pela EU (e nesse caso, também do país com o qual ela se relaciona) e é de longa duração.[36]

Acreditamos que esse é o caminho que será seguido por boa parte do mundo que tenha um direito centralizado e que se preocupa com a proteção da privacidade de seus cidadãos, especificamente no tocante do assunto cada vez mais premente que se torna a transferência de dados pessoais na esfera digital. As soluções encontradas pela EU são louváveis em todos os aspectos – seja pela posição de pioneirismo e liderança em relação à evolução da privacidade pessoal e da consequente privacidade pessoal no meio digital, mas também pelas soluções que encontra quando colocada frente às dificuldades de se manter o respeito à privacidade, assim como a introdução da diretiva 95/46/CE, as revisões feitas as legislações e exigências após os modelos de transferências utilizados (Privacy Shield/Safe Harbour) serem considerados inadequados (Schems I e ii), e por ter encontrado uma solução atual (Liberação mediante decisões de adequação), que, mais uma vez, inspira legislações ao redor do mundo de maneira positiva.

35 Disponível em: <https://itsrio.org/wpcontent/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf>. Acesso em: 01 de nov. de 2020.

36 Embora seja revista regularmente pela autoridade competente e possa ser questionada no caso de desconfiança quanto à preservação da privacidade pelos indivíduos pertencentes a EU.

CONCLUSÕES

Finda a exposição do trabalho, o que se percebe é uma clara evolução do que chamamos de direito à privacidade e de como a evolução da sociedade para a era digital transforma esse direito. As preocupações, hoje, se voltam de fato às regulamentações das transferências de dados internacionais, em uma clara evolução de um direito que nasce na Europa, com a Declaração Universal dos Direitos Humanos, e pelas mãos europeias se aperfeiçoa, primeiro pelas mãos da Diretiva 95/46/CE, e depois pelo GDPR. Acreditamos, portanto, e com base em toda a problemática exposta ao longo do trabalho, que as transferências de dados internacionais se tornarão cada vez mais comuns frente às adequações que quase todos os Países irão buscar tomar, baseadas na legislação e exigências Europeias.

E neste contexto torna-se nítido o papel fundamental que os casos Schrems I e II detém nessa evolução do direito à privacidade na União Europeia, visto que a partir deles se tem uma visão importante de que não adianta apenas as alegações de que os sistemas de transferências de dados internacionais são seguros quanto à privacidade – Eles têm de demonstrar de fato serem seguros – e podem ser questionados por qualquer um, e a qualquer momento.

Embora seja cedo para que possamos compreender todas as mudanças que se colocam em marcha a partir dos julgamentos, já que são mesmo recentes, podemos concluir que é a partir das sentenças desses casos aqui explicados que se percebe a profundidade da preocupação quanto à privacidade existente na EU, que manda recados claros – se o País que buscar realizar transferências de dados a partir da EU não fornecer garantias adequadas aos olhos das legislações e comitês, então a política básica é a da não transferência, ou pelo menos da negação da transferência pelos meios mais simples. A União Europeia, pelo visto, continuará sendo a vanguarda mundial em termos de preocupação com a segurança de dados e privacidade pessoal no meio digital – e a maior parte do mundo irá seguir quer queira, quer não queira.

Isto se percebe, por exemplo, nos reflexos inegáveis que o GDPR e a preocupação com a obtenção de uma decisão de adequação causaram na Lei Geral de Proteção de Dados brasileira. O papel do chamado *compliance* de dados também obtém cada vez mais importância nesse contexto, seja ele empresarial ou a serviço dos governos, e com razão – ninguém deveria ser submetido a redes de inteligência ou a movimentos escusos com seus dados pessoais sem que se tenha conhecimento. O direito à privacidade, como reconhece com razão a EU, é inestimável e deve ser resguardado.

Quanto antes o Brasil se adequar, portanto, melhor a todos.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSIS E MENDES. Histórico das leis de proteção de dados e da privacidade na internet. [S. l.], 2020. Disponível em: https://assisemendes.com.br/historico-protecao-de-dados/. Acesso em: 7 fev. 2022.

BRACY, Jedidiah. CJEU's 'Schrems II' decision slated for July 16. [S. l.], 14 maio 2020. Disponível em: https://iapp.org/news/a/cjeus-schrems-ii-decision-slated-for-july-16/. Acesso em: 7 fev. 2022.

CONCIL OF EUROPE (UE). European Court of Human Rights Council of Europe. Convenção Europeia dos Direitos do Homem. [s. l.], 2 out. 2013. Disponível em: Convenção Europeia dos Direitos do Homem. Acesso em: 20 jul. 2022

CORBET , Rob; ROONEY, Colin; MULLOOLY, Olivia; BENSON , Rachel. The Ruling in Schrems II. Irlanda, 24 jul. 2020. Disponível em: https://www.lexology.com/library/detail.aspx?g=880f1a89-20b7-4d14-be92-9d8e7e3d7814. Acesso em: 7 fev. 2022.

DONEDA, Danilo Cesar Maganhoto. Da privacidade a proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. Livro eletrônico: Thomsom Reuters, 2020. ISBN 978-65-5065-030-8.

GELLMAN , Barton; SOLTANI , Ashkan. NSA collects millions of e-mail address books globally. [S. l.], 14 out. 2013. Disponível em: https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?hpid=z1. Acesso em: 7 fev. 2022.

IRLANDA. SUPREMO TRIBUNAL DE JUSTIÇA. ECLI:EU:C:2015:650. Apelante: Maximillian Schrems. Apelado: Data Protection Commissioner. Relator: Digital Rights Ireland Ltd. Irlanda, 17 de julho de 2014.GLOBO. Oito polêmicas envolvendo o Facebook em 2018. [S. l.], 24 dez. 2018. Disponível em: https://www.techtudo.com.br/listas/2018/12/oito-polemicas-envolvendo-o-facebook-em-2018.ghtml. Acesso em: 7 fev. 2022.

IRLANDA. TRIBUNAL SUPERIOR. Jurisprudência 2010/87/UE. Relator: K. Lenaerts. Irlanda, 4 de maio de 2018. Disponivel em: http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=PT&part=1&occ=first&mode=lst&pageIndex=0&cid=134%E2%80%A6

MARR, Bernard ("How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone...")Forbes, 2018. Disponível em: https://www.Bernard Marrforbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=4ce6863260ba. Acesso em: 31 ago. 2020.

NASCIMENTO, Anderson. O que é PRISM?. Canaltech, 2014. Disponível em: https://canaltech.com.br/espionagem/O-que-e-PRISM/. Acesso em: 31 ago. 2020.

OCDE. Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais. OCDE, 2003. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 31 ago. 2020.

ONU. Declaração Universal dos Direitos Humanos. 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 31 jul. 2020.

PARLAMENTO EUROPEU E CONSELHO. Diretiva nº Diretiva 94/46, de 8 de março de 2014. A Diretiva 95/46/CE. Protecção dos dados pessoais, [S. l.], 8 mar. 2014. Disponível em: Protecção dos dados pessoais. Acesso em: 11 jul. 2022.

PARLAMENTO EUROPEU E CONSELHO. Proteção de dados pessoais. In: MACIEJEWSKI, / Mariusz et al. Fichas técnicas sobre a União Europeia. [S. l.], 2022. Disponível em: https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf. Acesso em: 20 ago. 2020.

PARLAMENTO EUROPEU E CONSELHO. Regulamento nº L 119/1, de 7 de fevereiro de 2022. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016: Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 7 fev. 2022.

PARLAMENTO EUROPEU E DO CONSELHO.REGULAMENTO (UE) 2016/679 DO. ("regulamento (ue) 2016/ 679 do parlamento europeu e") Jornal Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 31 ago. 2020.

ROCKCONTENT. "Big Data: entenda o conceito, suas aplicações em diferentes contextos e como impacta as iniciativas de Marketing." Rockcontent, 2021. Disponível em: https://rockcontent.com/br/blog/big-data//. Acesso em: 31 ago. 2021.

SAS. Machine Learning: O que é e qual sua importância?. SAS, 2020. Disponível em: O que é e qual sua importância? Acesso em: 31 ago. 2020.

UE. TRIBUNAL DE JUSTIÇA (UE). Acordão do tribunal de justiça. Infocuria, [s. l.], 12 out. 2015. Disponível em: https://media2.mofo.com/documents/160913-implications-schrems-data-transfers.pdf. Acesso em: 20 jul. 2022.

USA. Abstract of the Federal Constitutional Court's Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES]

VIOLA , Mario. Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira. Instituto de Tecnologia e Sociedade do Rio , Rio de Janeiro, 2019. ("Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS)") ("Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS)") Disponível em: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf. Acesso em: 2 de fev. 2022

VIOLA, Mario. Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira. Relatorio UK, 2019. Disponível em: https://Análise da Adequação da Legislação Brasileiritsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf. Acesso em: 31 ago. 2020.

SOBRE O AUTOR:

Bacharel em Direito pela Facamp em 2020, graduando em Medicina pela SLMandic. Pesquisador do GRIG-Facamp.

DESC
DIREITO, ECONOMIA & SOCIEDADE CONTEMPORÂNEA