UNIVERSIDADE FEDERAL DE JUIZ DE FORA
CAMPUS GOVERNADOR VALADARES
GRADUAÇÃO EM DIREITO

Izabella Alves Jorge Bittencourt

Transferência Internacional de dados: análise dos serviços de armazenamento em nuvem da Google

Governador Valadares
2022

Izabella Alves Jorge Bittencourt

Transferência Internacional de dados: análise dos serviços de armazenamento em nuvem da Google

Trabalho de conclusão de curso apresentado ao curso de Direito da Universidade Federal de Juiz de Fora - *campus* Governador Valadares, como requisito parcial à obtenção do grau de Bacharel em Direito, sob orientação do Prof. Dr. Pablo Georges Cícero Fraga Leurquin

Governador Valadares

2022

Izabella Alves Jorge Bittencourt

Transferência Internacional de dados: análise dos serviços de armazenamento em nuvem da Google

Trabalho de conclusão de curso apresentado ao curso de Direito da Universidade Federal de Juiz de Fora - *campus* Governador Valadares, como requisito parcial à obtenção do grau de Bacharel em Direito.

Aprovado em ____ de _____ de ____.

BANCA EXAMINADORA

_____

Prof. Dr. Pablo Georges Cícero Fraga Leurquin - Orientador
Universidade Federal de Juiz de Fora - Campus GV

_____

Prof. Dr. Lucas Costa dos Anjos
Autoridade Nacional de Proteção de Dados

_____

Profª. Drª. Luciana Tasse Ferreira
Universidade Federal de Juiz de Fora - Campus GV

AGRADECIMENTOS

Gostaria de agradecer aos meus pais e minha família por sempre estarem presentes em todos os momentos importantes em minha vida. O apoio de vocês foi essencial para eu chegar até aqui. Vocês são incríveis!

Um agradecimento a todos os professores que nos acompanharam nestes cinco anos, seja na sala de aula no meio físico, seja seja na sala de aula virtual, em especial ao professor Lucas Anjos, por todas as valiosas contribuições em minha vida acadêmica e profissional. Agradeço também ao meu orientador Pablo Leurquin por todo o apoio e confiança, tanto nas reuniões de Iniciação Científica, quanto na elaboração deste trabalho. Muito obrigada!

Minha eterna gratidão a todos os meus amigos que se fizeram presente em toda a jornada, que a todos os momentos estiveram do meu lado, tornando os dias mais leves.

Por fim, serei extremamente agradecida à Universidade Federal de Juiz de Fora - campus Governador Valadares, por me permitir vivenciar o que uma Universidade Pública pode oferecer. Todos os projetos de pesquisa, grupo de estudos, iniciação científica, treinamento profissional e estágios foram essenciais para minha formação.

Meus sinceros agradecimentos a todos que participaram junto comigo nesta caminhada!

“Muitos anos se passaram desde aquela morna noite no Sul, mas as perguntas mais antigas voltaram rugindo, querendo vingança. A realidade digital está tomando conta e redefinindo tudo que é familiar, antes mesmo de termos tido a chance de ponderar e decidir sobre a situação. Nós celebramos o mundo conectado por causa das muitas maneiras pelas quais ele enriquece nossas capacidades e perspectivas, mas ele gerou novos grandes territórios de ansiedade, perigo e violência conforme o senso de um futuro previsível se esvai por entre nossos dedos. .” - Shoshana Zuboff[1]

[1]ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Rio de Janeiro: Intrínseca, 2021. p. 17. Acesso em: 19/02/22.

RESUMO

O trabalho que se apresenta tem por temática a análise da aplicação da Lei Geral de Proteção de Dados brasileira nos serviços de armazenamento em nuvem oferecidos pela empresa Google. Em razão da intensificação da globalização e dos avanços tecnológicos experimentados na nova sociedade da informação, serviços como o de armazenamento em nuvem puderam ser ofertados por empresas com sede e *data centers* localizados fora do território nacional, caracterizados por ser um serviço com transferência internacional de dados. No entanto, a fim de assegurar a privacidade do indivíduo e dos seus dados, usuários desses serviços, os Estados têm buscado determinar os parâmetros mínimos para a transferência internacional de dados para essas empresas, como a utilização de cláusulas contratuais padrão. A hipótese apresentada é de que apenas a consolidação legislativa que garanta a privacidade dos indivíduos não será suficiente para exaurir todos os problemas advindos com essa atividade, restando clara a necessária estruturação e atuação da Autoridade Nacional de Proteção de Dados.

Palavras-chave: Transferência Internacional de Dados; Computação em nuvem; Lei Geral de Proteção de Dados; Autoridade Nacional de Proteção de Dados; Google.

ABSTRACT

The present work has as its theme the analysis of the application of the Brazilian General Data Protection Law in cloud storage services offered by the company Google. Due to the intensification of globalization and the technological advances experienced in the new information society, services such as cloud storage could be offered by companies with headquarters and data centers located outside the national territory, characterized by being a service with international data transfer. However, in order to ensure the privacy of individuals and their data, users of these services, States have sought to determine the minimum parameters for the international transfer of data to these companies, such as the use of standard contractual clauses. The hypothesis presented is that only legislative consolidation that guarantees the privacy of individuals will not be enough to exhaust all the problems arising from this activity, leaving clear the necessary structuring and performance of the National Data Protection Authority.

Keywords: International Data Transfer; Cloud computing; General Data Protection Law; National Data Protection Authority; Google.

LISTA DE ABREVIATURAS E SIGLAS

LGPD	Lei Geral de Proteção de Dados
GDPR	General Data Protection Regulation
ANPD	Autoridade Nacional de Proteção de Dados
SCCs	Standard Contractual Clauses

SUMÁRIO

INTRODUÇÃO

Nas últimas décadas, houve intensificação da globalização, potencializada pela difusão e uso de novas tecnologias de informação e comunicação. Hoje vivem-se inegáveis transformações sociais, econômicas e culturais, decorrentes dos avanços tecnológicos. A sociedade sempre passou por períodos em que houve alteração na sua forma de organização, sendo cada era marcada por um elemento central para o seu desenvolvimento. Segundo Bruno Bioni[2], a sociedade atual está organizada de maneira que a informação é elemento nuclear para o desenvolvimento da economia, substituindo recursos que antes estruturavam as sociedades agrícola, industrial e pós-industrial.

As revoluções industriais, de acordo com Castells[3], trouxeram um caráter vanguardista das novas tecnologias industriais para a sociedade. A partir do final do século XX, em decorrência do processo de intensificação da globalização, vive-se um processo de transformação tecnológica, no qual a informação passou a ser gerada, armazenada, recuperada, processada e transmitida de maneira veloz, de forma nunca observada antes na história. A nova onda tecnológica criou mecanismos capazes de transmitir informações em quantidade e velocidade jamais inimagináveis, como por exemplo a tecnologia do *big data.*

O *big data* é um mecanismo de análise e interpretação de grandes volumes de dados, de grande variedade e de maneira altamente veloz. Segundo o autor Danilo Doneda[4] o processamento de informações de forma distribuída e o desenvolvimento de tecnologias como o *big data*, de certa forma democratizaram a arquitetura dos dos bancos de dados, fragmentando o tratamento de dados pessoais.

Informações são estruturadas a partir de dados. Estes, por sua vez, são fatos brutos que quando processados, categorizados e organizados, se convertem em algo que daí se extrai a informação, como pontuado pelo autor Bruno Bioni[5]. Com o avanço da internet, houve a possibilidade de um fluxo nacional e internacional de dados, cada vez com mais intensidade. A tecnologia da computação em nuvem permitiu o armazenamento, o acesso e o tratamento

---

[2]BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. Acesso em: 03/12/21.

[3]CASTELLS, Manuel. A sociedade em rede: a era da informação. Vol. 1. 10ª. ed. São Paulo: Paz e Terra, 2009. (A era da Informação: Economia, Sociedade e Cultura). Acesso em: 03/12/21.

[4] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados.São Paulo : Thomson Reuters Brasil, 2020. p.36. Acesso em: 29/01/22.

[5] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. Acesso em: 03/12/21.

de grandes volumes de dados a partir de um poder computacional. Ao mesmo tempo, com o avanço da economia da informação atrelado ao desenvolvimento das tecnologias de informação e comunicação, surgiram vários serviços ligados a essa "cadeia" de dados.

Os modelos de negócio, portanto, se reinventaram. Há um cenário global de forte dispersão econômica, principalmente com grandes empresas transnacionais de tecnologia de oferta de serviços em nuvem e internet que gera a alta importância dos dados no seu fluxo global.

Castells[6] ainda entende que a sociedade da informação decorre da situação descrita, uma vez que ela possui uma economia global e que funciona em rede, ou seja, de uma maneira flexível, dinâmica, na qual há interação de todos esses atores, como Estados, empresas e pessoas. A partir disso, o autor entende que todo o sistema de fluxo internacional de dados possui essa característica de estar em rede.

As condições de tratamento de dados, para seu fluxo transnacional, se tornam elemento central para o desenvolvimento de um país. Por isso, é importante a adoção de medidas e mecanismos regulatórios de abrangência extraterritoriais para a garantia efetiva de direitos fundamentais do cidadão.

A nova legislação brasileira de proteção de dados pessoais (Lei n. 13.709/2018) se insere no mencionado contexto. Ela dispõe de um capítulo específico sobre mecanismos de tutela dos direitos dos cidadãos brasileiros em face da transferência internacional de dados. No entanto, por ser uma norma recente, é importante refletir sobre a sua aplicação nas ofertas de serviços de computação em nuvem, hoje muito usado pelos usuários, principalmente do Google.

Nos últimos anos, houve a acentuação das relações e vínculos entre os países, principalmente de oferta de serviços e produtos, advindos com a ascensão e difusão da Internet. Por esse meio, vários serviços foram possibilitados, dentre eles está o armazenamento em nuvem (*cloud computing)*, por meio do qual um servidor de aplicação oferece ao usuário o serviço de armazenamento de dados em seus servidores (*data centers)*. Essa tecnologia permite que o usuário acesse a qualquer momento, sem que precise armazenar esses dados em algum dispositivo físico (como computadores, celulares e HDs), basta apenas

[6] CASTELLS, Manuel. A sociedade em rede: a era da informação. Vol. 1. 10ª. ed. São Paulo: Paz e Terra, 2009. (A era da Informação: Economia, Sociedade e Cultura). Acesso em: 08/12/21.

acessar a aplicação. Estima-se que há 4.407 *data centers location* (disponíveis para locação e compartilhamento), em 122 países diferentes[7].

Percebe-se que muitas empresas que oferecem esse serviço, como a Google, não são sediadas no Brasil. Além disso, os seus servidores, que armazenam esses dados, também não estão localizados no território nacional. Eles estão muitas vezes em países diferentes daqueles onde a empresa está sediada, gerando conflitos de jurisdição e de regras de transferência internacional de dados. Além disso, pode-se verificar que a privacidade dos usuários ao utilizar esses serviços está em risco, uma vez que há inúmeros casos de vazamento de dados e de transferência de dados a terceiros não autorizados, por exemplo[8].

Com a vigência da Lei Geral de Proteção de Dados (Lei n. 13.708/2018) que disciplina o tratamento dos dados pessoais no Brasil e o GDPR (*General Data Protection Regulation - Regulamento Geral de Proteção de Dados),* na União Europeia, fica evidente a busca pela efetivação dos direitos relativos à proteção dos dados pessoais e privacidade do usuário. Essas legislações trazem a ideia de que a localização física do dado não deve diminuir as garantias e a proteção pretendida. Ademais, deve-se garantir que as limitações para a transferência internacional de dados, não sejam um impeditivo para coibir o avanço da economia digital globalizada, que se pauta na descentralização da informação.

A escolha da Google, para este trabalho, não é acidental. Segundo Shoshana Zuboff[9], a empresa é pioneira do capitalismo de vigilância[10], lançando, sem precedentes, em uma operação de mercado nos espaços não mapeados da internet, enfrentando poucos

---

[7] Disponível em: < https://www.datacentermap.com/>. Acesso em: 10/12/21.

[8] O caso mais emblemático de vazamento de dados ocorreu com o Facebook, quando bilhões de usuários tiveram seus dados compartilhados, sem o seu consentimento, com a empresa de marketing britânica Cambridge Analytica para serem utilizadas na campanha eleitoral americana em 2016, em prol do candidato Donald Trump. O caso aconteceu em 2016, mas veio à tona apenas em 2018. No entanto, há diversos casos de vazamentos de dados no mundo. No ano de 2013, a Adobe sofreu um ataque que divulgou o vazamento de mais de 38 milhões de dados de usuários da empresa, contendo nomes de usuários, senhas e números de cartões de crédito. No Brasil, o banco Inter, pioneiro em contas digitais no país, também teve dados de correntistas vazados em 2018. A ação realizada por hackers, tinha o objetivo de extorquir o banco. Disponível em: <https://www.valuehost.com.br/blog/vazamento-de-dados/>. Acesso em: 15/12/21.

[9] ZUBOFF, Shoshana. A era do capitalismo de vigilância. Rio de Janeiro: Intrínseca, 2021. p. 21. Acesso em: 10/02/22.

[10] Segundo Shoshana Zuboff, o capitalismo de vigilância é um novo tipo de mercado, onde as empresas reivindicam unilateralmente a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. A dinâmica competitiva desse capitalismo tende a adquirir fontes mais preditivas de excedentes comportamentais, que tem como objetivo automatizar a experiência humana por meio de modificação de comportamento. Além disso, esse capitalismo de vigilância se alimenta de todos os aspectos da experiência humana e se torna o modelo padrão para a maioria das empresas. A explicação para o seu triunfo se encontra no fato dele ser sem precedentes na história da humanidade, uma vez que é direcionado a uma nova lógica de acumulação, com os próprios mecanismos operacionais imperativos, rompendo com as normas e práticas que definem o capitalismo.

impedimentos legais ou concorrenciais. Beneficiada por diversos eventos históricos, a empresa apropriou-se de capacidades emergentes do capitalismo de vigilância. Esse modelo, com seus mecanismos e imperativos econômicos, se tornaram padrão para as empresas que se baseiam na internet para explorar e oferecer seus serviços - como é o caso da Google, que usa desses mecanismos para atingir seu valor de mercado.

Outros dois motivos também foram essenciais para a escolha da empresa. Em primeiro lugar, Scott Galloway afirma que "o Google é o deus do homem moderno", pelo fato de ser fonte do conhecimento para a maioria das pessoas no dia a dia - se tornando uma instituição com um patamar inegável de confiança e credibilidade. O outro motivo, dessa vez econômico, é destacado pelo fato de que, dentre as cinco maiores empresas de tecnologia do mundo, está a Google, subsidiária da Alphabet que, em 2016, obteve um lucro de 20 milhões de dólares, aumentando em 23% o seu faturamento e reduzindo em 11% o curso para seus anunciantes[11].

O objetivo deste trabalho é analisar as hipóteses de transferência internacional que justifiquem o tratamento de dados na realização da transferência dos dados nos serviços de armazenamento em nuvem da Google. Também busca-se identificar os mecanismos que podem ser utilizados para verificar a implementação da LGPD no âmbito de contratos internacionais de serviços de armazenamento em nuvem da Google, bem como, a previsão de regras para responsabilização dos provedores no caso de vazamentos ou riscos aos dados pessoais tratados dos titulares que contrataram os serviços.

Na primeira seção será avaliado como é disposto o serviço de armazenamento em nuvem da Google (Google Drive) e as estruturas legais apresentadas pela empresa para justificar a transferência internacional de dados.

Na segunda seção, será avaliado qual o tratamento jurídico para a transferência internacional de dados, a necessidade de harmonização de normas no cenário internacional e os mecanismos trazidos pela GDPR para o tratamento de dados de europeus em outros países ou organizações. Além disso, também serão abordados os julgamentos Schrems I e II, o qual invalidou a transferência internacional de dados de cidadãos europeus para o Facebook Inc, localizado na Califórnia.

[11] GALLOWAY, Scott. **Os quatro:** apple, amazon, facebook e google - o segredo dos gigantes da tecnologia. Rio de Janeiro. Alta Books, 2019. p. 7. Acesso em: 15/02/22.

A terceira seção, por sua vez, traz as análises das hipóteses de transferência pela Lei Geral de Proteção de Dados em um cenário brasileiro, assim como a verificação dos serviços do Google Drive à luz dos fundamentos e princípios abordados pela legislação.

2 SERVIÇOS DE ARMAZENAMENTO EM NUVEM DA GOOGLE: GOOGLE DRIVE

2.1. ASPECTOS GERAIS DO SERVIÇO DE ARMAZENAMENTO EM NUVEM

Com a evolução da tecnologia, surgiu a oferta de diversos serviços de aplicação da internet. Dentre eles está o de computação em nuvem, que, segundo os autores Eliseu C. Branco Jr., Javam C. Machado e Jose Maria Monteiro[12], é conceituada como:

> "Um modelo de computação em que dados, arquivos e aplicações residem em servidores físicos ou virtuais, acessíveis por meio de uma rede em qualquer dispositivo compatível (fixo ou móvel), e que podem ser acessados a qualquer hora, de qualquer lugar, sem a necessidade de instalação ou configuração de programas específicos."

Com esse novo modelo de serviço, várias empresas gigantes da tecnologia passaram a ofertar tais serviços, como a Google e a Amazon.

Fundada em 1998, no Vale do Silício nos EUA, a Google[13], empresa multinacional de serviços online e software, é considerada uma das cinco maiores empresas mais valiosas do mundo[14]. O modelo de negócio da empresa envolve, principalmente, a oferta do uso dos serviços de busca online, mas também de diversos serviços e produtos como os serviços de e-mail e armazenamento em nuvem, por exemplo[15]. Para definição do escopo deste trabalho, apenas serão analisados os serviços de armazenamento em nuvem, denominado *Google Drive* pela empresa.

A Google oferece o serviço de armazenamento em nuvem, no qual as pessoas podem armazenar, compartilhar e acessar arquivos e pastas em qualquer dispositivo, tendo apenas

---

[12] BRANCO Jr., Eliseu C.; MACHADO, Javam C.; MONTEIRO, José Maria. Estratégias para Proteção da Privacidade de Dados Armazenados na Nuvem. **Tópicos em Gerenciamento de Dados e Informações, Curitiba:** 1ª edição, p. 46-74, 2014**.** Disponível em: <https://www.inf.ufpr.br/sbbd-sbsc2014/sbbd/proceedings/artigos/pdfs/14.pdf>. Acesso em: 13/01/22.

[13] Atualmente, a Google é uma subsidiária da Alphabet, formada em 2015, ao lado da Google Ventures, do Google X e do Google Capital.

[14] Segundo a Forbes, em 2020, as cinco marcas mais valiosas do mundo continuam sendo Apple, Google, Microsoft, Facebook e Amazon. Disponível em: <https://forbes.com.br/listas/2020/07/as-marcas-mais-valiosas-do-mundo-em-2020/>. Acesso em: 13/01/22.

[15] Disponível em: <https://pt.wikipedia.org/wiki/Google>. Acesso em: 12/01/22.

acesso à internet[16], denominado *Google Drive.* No contexto das definições do Marco Civil da Internet (Lei nº 12.965/2014), a Google se caracteriza como uma aplicação de internet[17], que diferentemente de um site, o usuário apenas utiliza e capta informações, nas aplicações, o usuário insere informações que serão processadas.

A utilização dos serviços do Google se dá por meio de aceite de um Termo de Serviço [18]. Os Termos de Uso (ou Termos de Uso e Condições de Serviços) são, na verdade, um contrato entre a empresa prestadora do serviço e o consumidor (usuário). É por meio deste instrumento que são estabelecidas as normas de utilização da plataforma pelo usuário e são delineados os limites de responsabilidades do prestador de serviço[19], além de serem informados, de maneira clara e completa a descrição da atividade desenvolvida[20], delimitação de obrigações e responsabilidades de cada parte.

Os serviços do Google Drive são condicionados ao aceite dos termos de serviço. Em um tópico desse documento, intitulado "Licença", a Google determina que o quem detém os direitos de propriedade intelectual sobre o conteúdo é o próprio usuário. Entretanto, a empresa precisa da permissão do usuário para que o Google "hospeda, reproduza, distribua, comunique e use seu conteúdo, por exemplo, para salvá-lo nos nossos sistemas e torná-lo acessível em qualquer lugar".

Subsidiariamente, alguns dos serviços do Google precisam que usuários aceitem os termos adicionais específicos do serviço[21], como é o caso do Google Drive. Os termos adicionais do Google Drive[22] determinam que, com o serviço, o usuário pode fazer o upload, armazenar, enviar e receber conteúdo. No entanto, esse documento apenas traz disposições

---

[16]GOOGLE. **Armazenamento em nuvem para uso pessoal ou profissional.** Disponível em: <https://www.google.com/intl/pt-BR_ALL/drive/>. Acesso em: 11/02/22.

[17]Art. 5º Para os efeitos desta Lei, considera-se:
VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;

[18]GOOGLE. **Termos de serviço**. Disponível em: <https://policies.google.com/terms>. Acesso em: 11/02/22.

[19]BONANI, Rafael. **Termos de uso o que são e para o que servem**, 2020. Disponível em: <https://www.bonani.adv.br/termos-de-uso-o-que-sao-e-para-que-servem>. Acesso em: 04/02/22.

[20] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade.

[21]GOOGLE. **Termos de serviço específicos.** Disponível em:< https://policies.google.com/terms/service-specific>. Acesso em: 11/02/22.

[22]GOOGLE. **Termos de serviço do Google Drive.** Disponível em: <https://www.google.com/drive/terms-of-service/>. Acesso em: 11/02/22.

sobre o conteúdo dos arquivos e políticas do programa, que analisa o conteúdo para saber se é ilegal ou viola as Políticas do Programa[23].

Além dos Termos de Uso, que dizem sobre os serviços, também há a Política de Privacidade[24], onde dispõe as informações relativas à privacidade e proteção de dados dos usuários[25]. É por meio deste documento que a empresa deverá demonstrar conformidade com os princípios e obrigações estabelecidas na Lei Geral de Proteção de Dados.

Um dos tópicos trazidos na Política de Privacidade da Google é sobre a transferência de dados. Segundo o disposto, a Google mantém servidores em todo o mundo e as informações podem ser processadas em servidores fora do país de moradia do usuário, isto é, um usuário do Brasil pode ter seus dados tratados fora da jurisdição brasileira. É destacado pela empresa que algumas leis de proteção de dados podem oferecer maiores proteções que outras, mas que a Google aplica as mesmas pretensões da política e cumprem com os marcos legais independentemente da localização dos dados.

Os arquivos compartilhados pelo usuário à plataforma da empresa são armazenados pela Google em *data centers* próprios, localizados em diversas localidades do planeta. Como há um tratamento de dados pessoais, a Google é obrigada a observar a LGPD em todos os requisitos, tratamento, princípios, direitos e aplicação de medidas de segurança aos dados - assunto que será abordado no tópico 4.2.

2.2. ESTRUTURAS LEGAIS PARA TRANSFERÊNCIA DE DADOS DA GOOGLE

A partir de 10 de fevereiro de 2022, a Google atualizou as estruturas legais para transferência de dados. São três as possibilidades trazidas: Decisões de adequação, Cláusulas contratuais padrão e Estruturas de Escudo de Privacidade UE-EUA e Suíça-EUA.

As Decisões de Adequação são um mecanismo de transferência de dados da União Europeia para países não pertencentes ao Espaço Econômico Europeu que são considerados

[23] GOOGLE. **Políticas do programa contra abuso e como elas são aplicadas.** Disponível em: <https://support.google.com/docs/answer/148505>. Acesso em: 11/02/22.
[24] GOOGLE. **Política de Privacidade**. Disponível em: <https://policies.google.com/privacy?hl=en&gl=US#inforetaining>. Acesso em: 11/02/22.
[25] Para este trabalho, será utilizada a versão disponível datada de 10 de fevereiro de 2022.

adequados pela Comissão Europeia. São apresentadas decisões de adequação da Comissão Europeia[26], do Reino Unido[27] e da Suíça[28].

Por sua vez, as cláusulas contratuais padrão (SCCs) apresentadas são compromissos entre as partes que podem ser utilizados como base para transferência de dados da UE para países terceiros, com salvaguardas necessárias para a proteção dos dados. São apresentadas três tipos SCCs aprovadas pela Comissão Europeia em 2004[29], 2010[30] e em 2021[31].

De acordo com a certificação do Privacy Shield (Escudo de Proteção da Privacidade)[32] , a Google informa que obedecem às estruturas estabelecidas para a coleta, uso e retenção de informações pessoais em países membros da União Europeia, do Reino Unido e da Suíça. Entretanto, desde julho de 2020 a empresa não conta mais com o Privacy Shield para transferir dados do Espaço Comum Europeu.

Diante das estruturas apresentadas, nota-se que todas dizem respeito a mecanismos de transferências estabelecidos pelo GDPR, exemplificadas no tópico a seguir.

3 TRATAMENTO JURÍDICO DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

[26]COMISSÃO EUROPEIA. **Adequacy decisions.** Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 13/02/22,

[27]ICO. **International transfers after the UK exit from the EU Implementation Period**. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#adequacy>. Acesso em: 13/02/22.

[28]FEDERAL DATA PROTECTION AND INFORMATION COMMISSIONER **Transborder data flow.** Disponível em: <https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html>. Acesso em: 13/12/22.

[29]OFFICIAL JOURNAL OF THE EUROPEAN UNION.**COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.** Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915>. Acesso em: 13/02/22.

[30]OFFICIAL JOURNAL OF THE EUROPEAN UNION. **COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. Disponível em:** < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0087>. Acesso em: 13/02/22.

[31]OFFICIAL JOURNAL OF THE EUROPEAN UNION. **COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on 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: 13/02.22.

[32]PRIVACY SHIELD FRAMEWORK. Disponível em: <https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active>. Acesso em: 13/02/22.

Com o desenvolvimento de tecnologias capazes de transmitirem informações de maneira rápida, principalmente com a internet, percebeu-se que uma efetiva proteção de dados pessoais dependeria de uma harmonização normativa internacional de coerência da matéria. Dessa maneira, obtêm-se duas perspectivas sobre o debate de fluxo internacional de dados entre fronteiras.

A primeira delas é de que as regras condicionantes à transferência internacional de dados pessoais podem se tornar possíveis barreiras para a liberalização das transações e do comércio internacional, aumentando o custo dos negócios entre fronteiras e impor restrições à livre circulação de informação entre países. A segunda delas é de que a necessidade de regular essa atividade é uma justificativa para a proteção dos direitos à privacidade e aos dados pessoais de quem terá seus dados tratados em outros países[33]. Portanto, observar a harmonização normativa internacional é importante para delimitar o tratamento entre fronteiras e avaliar as implicações dentro de cada ordenamento jurídico.

Observando essas perspectivas, o desafio se encontra em estabelecer um ponto de equilíbrio entre elas. Com isso, houveram iniciativas pioneiras, como a da Organização para Cooperação e Desenvolvimento Econômico (OCDE), para estabelecer padrões internacionais comuns que possibilitasse a atividade comercial entre países do globo.

Em 1980 foi aprovado as Diretrizes da OCDE sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais[34]. O guia dispõe que os países membros devem adotar as disposições razoáveis e adequadas para garantir a continuidade e segurança dos fluxos transfronteiriços dos dados, devendo ser observado os princípios da diretriz de limitação de coleta, qualidade dos dados, definição da finalidade, limitação de utilização, *backup* de segurança, abertura, participação do indivíduo e responsabilização.

A elaboração de padrões internacionais possui o objetivo de evitar lacunas na proteção de dados, uma vez que a falta de harmonização e a falta de legislação podem criar riscos para o tratamento de dados pessoais, bem como facilitar os fluxos de dados entre fronteiras, principalmente com o crescente uso de banco de dados disponibilizados globalmente na internet. Além disso, a consolidação de diretrizes garante que, independentemente do

---

[33]MARQUES, Fernanda Mascarenhas. Cláusulas-padrão contratuais como autorizadoras para a Transferência Internacional de Dados: alternativas em casos de ausência de decisão de adequação. **Revista do Advogado: Lei Geral de Proteção de Dados**, São Paulo, nº 144, nov/2019. P. 192. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em 08/02/22.

[34]OCDE **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais.** 2002. Disponível em: < https://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 14/02/22.

território do tratamento de dados, será assegurado o mesmo nível de proteção aos dados pessoais e à privacidade, evitando paraísos de tratamentos de dados. Dessa maneira, a consolidação em matéria de proteção de dados em diversas normas e em ordenamentos jurídicos internacionais abriu portas para que outras diretrizes viessem a ser desenvolvidas.

3.1 NORMAS DA UNIÃO EUROPEIA SOBRE TRANSFERÊNCIA INTERNACIONAL DE DADOS

O direito da União Europeia possui grande importância jurídica no cenário legislativo sobre privacidade e proteção de dados em razão do seu pioneirismo em legislação de determinadas matérias, da preocupação com o mercado comum europeu e com a promoção de direitos fundamentais.

Um desses marcos foi a Diretiva 95/46/CE[35], de 24 de outubro de 1995, que constitui um dos primeiros textos de referência, direcionada a proteger os direitos e as liberdades das pessoas no que diz respeito ao tratamento individual, por meio da adoção dos dados fundamentais que conferem a licitude ao tratamento e dos princípios relativos à qualidade dos dados.

Essa diretiva europeia estabeleceu um entendimento único sobre a transferência de dados a partir de terceiros a ser obedecida pelos países-membros da União Europeia.

Em vigor desde 25 de maio de 2018, o *General Data Protection Regulation* (GPDR) é um regulamento que oferece uma estrutura de proteção de dados aos cidadãos europeus, com maiores obrigações para as organizações. Ela é uma legislação aplicável a qualquer organização que ofereça bens ou serviços à União Europeia ou que monitore o comportamento de indivíduos dentro desse espaço.

Essa legislação elevou a consciência sobre privacidade e proteção de dados no mundo todo, influenciando a adoção de regulamentos em outros países do globo, como o Brasil.

Assim como a Diretiva 95/46/CE em seu artigo 25, o GDPR em seu art. 45 (1)[36], utiliza a técnica legislativa de negar, como solução padrão, a transferência internacional de

---

[35]UNIÃO EUROPEIA. **Diretiva 95/46/CE.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>. Acesso em: 13/02/22.

[36] "1. A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.".

dados pessoais da União Europeia para países terceiros, a menos que esse país possua nível adequado de proteção de dados. De acordo com o art. 46 (2) do GDPR, há exceções para que a transferência ocorra sem a adequação, abordadas no tópico a seguir.

3.2 MECANISMOS DE TRANSFERÊNCIA INTERNACIONAL DE DADOS DO GDPR

O GDPR (Regulamento nº 2016/679), em seu capítulo 5 intitulado "Transferências de dados pessoais para países terceiros ou organizações internacionais", disciplina sobre a transferência de dados pessoais de cidadãos europeus para outros países fora do Espaço Comum Europeu. Para que seja realizada essa transferência, a legislação impõe algumas condições.

Só poderá ocorrer quando houver decisão de adequação pela Comissão Europeia (art. 45, GDPR), no qual onde poderá haver fluxo de dados para países considerados adequados, ou quando a transferência apresentar algumas salvaguardas, sendo elas, conforme o art. 46 do GPDR:

> (i) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
> (ii) Regras vinculativas aplicáveis às empresas em conformidade com o art. 47º do GPDR;
> (iii) Cláusulas-tipo de proteção de dados adotadas pela Comissão, de acordo com o procedimento de exame exemplificado pelo art. 93º, 2;
> (iv) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controle, aprovadas pela Comissão e conforme o procedimento do art. 93º, 2;
> (v) Um Código de conduta, aprovados nos termos do art. 40º, seguidos de compromissos vinculativos; e
> (vi) Procedimento de certificação, aprovados nos termos do art. 42º, também acompanhados de compromissos vinculativos.

3.2.1. Nível de Proteção Adequado e os Casos Schrems vs. Data Protection Commissioner

Sobre o primeiro mecanismo de transferência internacional, a Comissão Europeia tem o poder de determinar, com base no art. 45, se um país fora da União Europeia oferece um nível adequado de proteção de dados. Essa decisão envolve uma proposta da Comissão Europeia, um parecer do Conselho Europeu de Proteção de Dados, uma aprovação dos representantes dos países da UE e a adoção da decisão pela Comissão Europeia. Essa decisão

possui efeito de que os dados pessoais possam fluir livremente da União Europeia para países terceiros sem que haja qualquer outra salvaguarda, isto é, a transferência será equiparada às transmissões de dados entre os países do espaço Schengen.

Os critérios analisados para o reconhecimento de países adequados pela Comissão Europeia, de acordo com Fernanda Mascarenhas Marques[37], recaem sobre três eixos principais: direito doméstico, requisitos necessários para a autoridade supervisora e compromissos internacionais. Os requisitos do direito doméstico avalia o Estado de Direito, respeito aos direitos humanos e liberdades individuais, a legislação relevante (geral e setorial) e sua respectiva implementação, as regras de proteção de dados pessoais, regras profissionais e medidas de segurança, regras de transferência subsequente de dados para outros países ou organizações internacionais, jurisprudências, direito dos titulares dos dados e remédios judiciais e administrativos disponíveis aos titulares, cujo dados estão sendo transferidos.

Em segundo lugar, os requisitos aplicáveis à autoridade supervisora, incidem sobre a preocupação da aplicação das regras e com a fiscalização da conformidade do tratamento. A requisição que há é uma autoridade de proteção de dados independente, com poder de investigação e intervenção. No caso do Brasil, a Autoridade Nacional de Proteção de Dados está vinculada à presidência da República, assim, não possui autonomia suficiente para a fiscalização da LGPD no âmbito nacional, ponto que será abordado nos próximos capítulos.

Por fim, os compromissos internacionais incluem as obrigações advindas de convenções ou instrumentos juridicamente vinculativos, assim como participações em sistemas multilaterais ou regionais, em especial quando se tratar de proteção de dados.

Já são considerados países adequados pela União Europeia: Andorra, Argentina, Canadá, Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido e Uruguai[38]. O Brasil não é um dos países contemplados na lista de países reconhecidos pela União Europeia. No entanto, esse cenário deve sofrer mudanças com a consolidação das atividades da Autoridade Nacional de Proteção de Dados no âmbito da aplicação da LGPD em território nacional.

---

[37] MARQUES, Fernanda Mascarenhas. Cláusulas-padrão contratuais como autorizadoras para a Transferência Internacional de Dados: alternativas em casos de ausência de decisão de adequação. **Revista do Advogado: Lei Geral de Proteção de Dados**, São Paulo, nº 144, nov/2019. P. 192. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>. Acesso em: 08/02/22,

[38] COMISSÃO EUROPEIA. **Adequacy decisions.** Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em 11/02/22.

A transferência de dados entre a União Europeia e os Estados Unidos da América possui particularidades, pois há acordos específicos para legitimar essa transferência, que nos últimos anos, tiveram uma importância significativa para os mecanismos de transferência internacional de dados.

Até o ano de 2015, vigorou para a transferência internacional de dados entre a União Europeia e os EUA o *Safe Harbor Agreement*[39]. Esse acordo possuía um conjunto de princípios fundamentais que regiam a troca de dados entre a União Europeia e os Estados Unidos, que eram:

> (i) Aviso: titular dos dados deveria ser informado de que os dados foram coletados e como seriam utilizados;
> (ii) Escolha: titular deveria ser capaz de escolher cancelar o uso dos dados ou permitir encaminhar os dados para terceiros;
> (iii) Transferência progressiva: a transferência dos dados para um terceiro só poderia acontecer se ele atender aos princípios de proteção de dados exigidos;
> (iv) Segurança: os dados deveriam ser protegidos contra perda e roubo;
> (v) Integridade dos dados: os dados devem ser relevantes e confiáveis para atender ao propósito da coleta;
> (vi) Acesso: o titular deveria ser capaz de acessar, corrigir e excluir todas as informações mantidas sobre ele; e
> (vii) Aplicação: devia existir meios eficazes de aplicação das regras contidas no acordo.

As denúncias de Snowden,em 2013, sobre as ações de espionagem por parte governamental dos Estados Unidos, pela NSA (*National Security Agency*)[40], deixou claro que as empresas certificadas pelo acordo permitiam que as autoridades americanas acessassem os dados de cidadãos europeus. Com a repercussão mundial, a discussão sobre a proteção internacional de dados pessoais veio à tona quando o ativista austríaco Maximilian Schrems (conhecido como Max) apresentou uma reclamação judicial perante à autoridade irlandesa (*Data Protection Commissioner*) direcionada para que a empresa Facebook deixasse de transferir dados pessoais para os EUA, visto que com as revelações de Snowden, o *Safe*

---

[39] OFFICIAL JOURNAL OF THE EUROPEAN UNION. **2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.).** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520>. Acesso em: 14/02/22.

[40] G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA**, 2013. Disponível em: < https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 05/01/22.

Harbor Agreement não apresentava proteção suficiente para os dados pessoais e privacidade contra a vigilância americana.

A Suprema Corte Irlandesa rejeitou a queixa, utilizando uma decisão de 26 de julho de 2000, em que a Comissão considerou que os Estados Unidos possuíam um nível de proteção adequado[41]. Posteriormente o caso foi levado à Corte de Justiça da União Europeia, sendo decidido em 2015, que o *Safe Harbor* era inválido e não apresentava proteção suficiente aos dados dos cidadãos europeus. O caso ficou conhecido como "Schrems I"[42].

O Tribunal de Justiça da União Europeia considerou que a existência de uma decisão da Comissão de constatar um país terceiro adequado, não pode eliminar ou reduzir os poderes de que dispõe as autoridades nacionais de supervisão quanto à proteção de dados dos cidadãos europeus. Assim, cabe às autoridades examinar, com total independência, se a transferência dos dados de uma pessoa para um país terceiro cumpre os requisitos estabelecidos pela diretiva[43].

Dessa maneira, a Comunicação da Comissão Europeia ao Parlamento Europeu e ao Conselho[44] estabeleceu, em 2015, que o *Safe Harbour Agreement* não apresentava proteção suficiente para os dados pessoais dos europeus contra a vigilância americana.

A decisão invalidou a transferência de dados entre UE-EUA. No entanto, o bloco europeu ainda precisava de uma nova base jurídica que autorizasse a transferência de dados para os EUA. Ela foi definida em 2016, estabelecendo o chamado *Privacy Shield*[45]. Trata-se de estrutura adequada para a proteção dos dados pessoais que garante, ao mesmo tempo, um forte conjunto de requisitos e salvaguardas de proteção de dados entre o bloco e os EUA.

Ainda que os EUA não fossem considerados um país de nível adequado de proteção de dados perante à Comissão Europeia, por meio do *Privacy Shield*, mais de cinco mil

---

[41] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **O Tribunal de Justiça declara inválida a Decisão de Execução 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA**. Luxemburgo, 16 de julho de 2020. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf>. Acesso em: 14/02/22.

[42] UNIÃO EUROPEIA. **EU proposal for provisions on Cross-border data flows and protection of personal data and privacy.** Disponível em: <https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf> . Acesso em: 14/02/22.

[43]Na época à decisão, ainda encontrava-se vigente na União Europeia a Diretiva 95/46/CE.

[44]COMISSÃO EUROPEIA. **COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems)**. 2015. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52015DC0566>. Acesso em: 14/02/22.

[45]PRIVACY SHIELD FRAMEWORK. Disponível em: <https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active>. Acesso em: 14/02/22.

empresas norte-americanas poderiam aderir ao acordo e se valer da transferência internacional de dados, para viabilizar produtos e serviços dentro do solo europeu.

Após o julgamento do caso Schrems I, o Facebook Ireland passou a justificar a transferência de dados para a empresa localizada nos EUA com base em cláusulas-padrão (*Standards Contractual Clauses* - SCCs). Entretanto, mais uma vez, Max Schrems questionou judicialmente o mecanismo sob a ótica da proteção de dados pessoais no fluxo internacional de dados e a sua devida efetividade. O novo caso, denominado "Schrems II", novamente questionava a corte irlandesa de que a decisão sobre o uso das cláusulas-padrão não justificaria a transferência de dados para os EUA, tendo em vista que os programas de vigilância dos EUA interferiram no direito fundamental à privacidade. O ativista austríaco questionava a transferência de dados pessoais do Facebook Ireland para o Facebook Inc., localizado nos EUA.

Após ser levado novamente para o Tribunal de Justiça da União Europeia, a Corte decidiu de que as práticas americanas de vigilância representavam violação aos direitos fundamentais, em especial à privacidade, anulando efetivamente o *Privacy Shield*. dOs controladores de dados da UE tiveram de assumir a responsabilidade da transferência internacional dos dados para o território norte-americano.

A decisão[46], emitida em julho de 2020, estabeleceu que o *Privacy Shield* não garante o mesmo nível de proteção aos dados estabelecidos pelo GPDR, visto que não se verifica o exercício de direitos dos titulares e muito menos limita a vigilância das autoridades americanas, ainda que pelas SCCs. Além disso, a Corte decidiu que a validade das cláusulas-padrão contratuais dependem de o controlador averiguar, na prática, o cumprimento das obrigações impostas, sendo imputada a ele a responsabilidade de suspender a transferência ou rescindir o contrato se as obrigações não puderem ou não forem cumpridas[47]. Assim, as autoridades de supervisão devem verificar as transferências e são obrigadas a

[46]PARLAMENTO EUROPEU. **The CJEU judgment in the Schrems II case**. 2020**.** disponível em: <https://curia.europa.eu/juris/document/document.jsf;jsessionid=B04EBCBEF9C1F1CD0B6AF53B1E85A69B?text=&docid=228677&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1464439>. Acesso em: 12/02/22.

[47] O *European Data Protection Board* (EDPB), para guiar controladores e operadores, criou um documento com orientações relativas à transferência internacional de dados com o intuito de mais segurança jurídica para o tratamento de dados. Tal documento inclui orientações práticas, como o mapeamento de fluxo global de dados e adoção de medidas, por exemplo. Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file2/dk_sa_standard_contractual_clauses_january_2020_en.pdf>. Acesso em: 15/02.22.

proibir as transferências quando constarem que os titulares dos dados não recebem proteção essencialmente equivalente.

A decisão europeia estabeleceu que os controladores passam a ser parcialmente responsáveis pela análise e adequação das cláusulas padrão (SCCs), como a possibilidade de inclusão de cláusulas suplementares para contratos de transferência em países com nível de proteção desconforme ao padrão europeu, quando as cláusulas-padrão não forem suficientes, por exemplo. Tal decisão, portanto, impõe àquele que exporta os dados e ao destinatário dos dados a obrigação de verificar, em primeiro lugar, o nível de proteção observado no país, além de a decisão exigir que o destinatário informe o exportador de dados de qualquer incapacidade de cumprir as cláusulas-padrão de proteção de dados. Dessa maneira, caso verifique a incapacidade de cumprimento das cláusulas, o exportador de dados é obrigado a suspender a transferência de dados e/ou rescindir o contrato.

Para salvar as transferências de dados baseadas em SCCs, as empresas precisam compensar as lacunas na proteção com "salvaguardas adicionais". Entretanto, levanta-se a discussão acerca de se as cláusulas-padrão consistiram ou não em mecanismos totalmente capazes de garantirem a segurança do tratamento dos dados em uma determinada transferência internacional.

Ainda que a decisão do caso seja aplicada apenas para a transferência de dados entre a União Europeia e os EUA, levanta-se a discussão acerca de quais medidas podem ser tomadas para que a transferência de dados continue, mesmo em países que não apresentam o patamar mínimo de adequação com o GDPR e, por fim, quais seriam os grandes impactos econômicos das decisões tomadas caso seja inviabilizado a transferência.

3.2.2. Cláusulas Contratuais Padrão

No Direito da União Europeia, de acordo com o GDPR, as cláusulas contratuais padrão (SCCs) garantem salvaguardas adequadas para proteção de dados, sendo utilizadas com base na transferência de dados da UE para países terceiros. Em 2021[48], a Comissão Europeia emitiu novos modelos de cláusulas contratuais padrão[49] para garantir a transferência

[48]COMISSÃO EUROPEIA. **European Commission adopts new tools for safe exchanges of personal data.** 2020. **Disponível em:** <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847>. Acesso em: 14/02/22.

[49] Os novos modelos substituíram os três conjuntos de cláusulas-padrão adotados sob a Diretiva 95/46, no qual duas se aplicavam para controlador-controlador e outra na relação entre controlador-processador.

de dados de controladores[50] ou processadores[51] sujeitos ao GDPR e para aqueles estabelecidos fora do bloco. A partir da data de 27 de dezembro de 2022, os controladores e processadores deverão utilizar as novas cláusulas-padrão para validarem as transferências internacionais de dados[52].

Foram definidos quatro modelos de cláusulas-padrão contratuais: de controlador para controlador, de controlador para processador, de processador para processador e de processador para controlador. De maneira geral, as cláusulas estabelecem garantias apropriadas e eficazes para a proteção de dados aos titulares sob a ótica da aplicação do GPDR, contendo:

> (i) a descrição das transferências;
> (ii) as salvaguardas necessárias como limitação de propósito, transparência, precisão e minimização de dados, limitação do armazenamento, segurança no processamento, restrição ao uso de dados sensíveis e transferências posteriores;
> (iii) o uso de subprocessadores, onde os agentes deverão obter autorização prévia específica para tal tratamento;
> (iv) os direitos dos titulares de dados, onde os agentes de tratamento deverão lidar com quaisquer consultas e solicitações relacionadas ao processamento dos dados pessoais e fornecer informações acessíveis e inteligível, utilizando-se de linguagem clara e simples;
> (v) a reparação, onde o importador de dados deve informar aos titulares de maneira clara e transparente, pelo aviso individual ou site, um meio capaz de tratar as reclamações dos titulares de dados;
> (vi) as responsabilidades;
> (vii) as autoridades supervisoras, nas quais deverão sempre indicar qual autoridade supervisora será competente para garantir a conformidade do tratamento;
> (viii) as leis e práticas locais que afetam o cumprimento das cláusulas;

---

[50] No art. 4º, item 7, do GDPR, o *controller* (em português, controlador) é o agente "responsável pelo tratamento", sendo "a pessoa singular ou colectiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais". Ao responsável de tratamento de dados pessoais é imputado diversas responsabilidades previstas no ordenamento, como: licitude, lealdade e transparência no tratamento de dados (art. 5º, 1, a), registro das atividades de tratamento (art. 30, 1), cooperação com autoridade de controle (art. 31), segurança da informação (art. 32), notificação de incidente de violação de dados, tanto à autoridade de controle quanto aos titulares (art. 33 e art. 34), realização de avaliação de impacto sobre a proteção de dados (art. 35 e art. 36), designação de um DPO, quando necessário (art. 37) e observância das regras para transferência internacional de dados (art. 44 a 50).

[51] O *processor* (em portugês, processadores) são, de acordo com o art. 4º, item 8 do GDPR, subcontratantes, sendo "uma pessoa singular ou colectiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes". O subcontratante, portanto, depende do responsável do tratamento de dados para que possa ser caracterizado em um contexto, devendo agir de forma limitada às delegações que lhe foram atribuídas por este.

[52] COMISSÃO EUROPEIA. **ANNEX to the COMMISSION IMPLEMENTING DECISION on 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.** 2021. Disponível em: <https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf>. Acesso em: 15/02/22.

(ix) as obrigações do importador de dados em caso de acesso por autoridades públicas;
(x) o não cumprimento das cláusulas e rescisão;
(xi) as leis aplicáveis; e
(xii) a escolha do foro e jurisdição.

Geralmente, para o fornecimento de serviços, firma-se um contrato ou vincula-se um termo de adesão para que o contrato se disponha do serviço/bem oferecido. Nesses casos, pode haver a transferência de dados para a execução de um contrato[53]. Dessa maneira, como há um tratamento de dados, é necessário definir os agentes de tratamento a fim de delimitação de responsabilidades, definição de direitos e deveres[54].

Conforme o site oficial da União Europeia, a Comissão Europeia decidiu quais cláusulas contratuais padrão oferecem salvaguarda suficiente para o tema de transferência internacional de dados. Para isso, foi emitido conjunto de cláusulas contratuais-padrão para a transferência de dados de controladores estabelecidos na UE para controladores de dados estabelecidos fora da EU ou do Espaço Econômico Europeu (EEE), e também de dados de controladores na UE para processadores estabelecidos fora da UE ou do EEE[55].

As recomendações da ICO[56], por sua vez, são de que cada organização é livre para incluir as cláusulas-padrão em um contrato mais amplo e adicionar outras cláusulas, desde que estas não se contradigam ou prejudiquem direitos fundamentais dos titulares dos dados[57].

---

[53] A legislação brasileira de proteção de dados tem como base legal, ou seja, hipóteses legais que condicionam a autorização para o tratamento de dados, a execução de contratos (art. 7º, inciso V).

[54] Na LGPD, os agentes de tratamento são o controlador e o operador, definidos no capítulo VI (arts. 37 a 40).

[55] O conjunto de cláusulas para cada situação de agentes de tratamento de dados está disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>.

[56] ICO. **ICO consults on how organizations can continue to protect people's personal data when it's transferred outside of the UK.** 2021. Disponível em: <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/standard-contractual-clauses/>. Acesso em: 18/02/22.

[57] A saída do Reino Unido do bloco da União Europeia possui impacto em diversos setores, principalmente quanto à regulação de proteção de dados. Percebe-se que a autoridade britânica,, continuará a seguir não só com os padrões de privacidade aplicados pelo GDPR, mas também com os SCCs adotados, além de disponibilizar para os controladores e operadores modelos de cláusulas-padrão. Vale ressaltar que com a saída da UE, o GDPR não será mais aplicado ao Reino Unido. Entretanto, se operar dentro do RU, a operação precisará ser cumprido pela lei nacional de proteção de dados. Na prática, com a intenção britânica de incorporar o GDPR na lei de proteção de dados após o período de transição, haverá poucas mudanças no que tange aos princípios, direitos e obrigações essenciais de proteção de dados já regulamentados pela Comissão Europeia. Além disso, o GDPR continuará a ser aplicado quando empresas ou organizações do RU oferecerem bens ou serviços a cidadãos europeus ou monitorar comportamentos desses cidadãos. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/>. Acesso em: 18/02/22.

4 A LGPD E AS HIPÓTESES DE TRANSFERÊNCIA INTERNACIONAL DE DADOS DO ART. 33

Os legisladores, ao elaborarem a Lei Geral de Proteção de Dados (Lei n. 13.709/18), criaram um capítulo específico para tratar sobre o tema da transferência internacional de dados. Esse capítulo possui semelhanças quanto a matéria tratada no GDPR, já que ambos possuem como regra geral a proibição da transferência para países terceiros ou organismos e organizações internacionais, estabelecendo algumas hipóteses para legitimar essa transferência.

Anteriormente à legislação específica, o Marco Civil da Internet (Lei n. 12.965/14) tratou sobre os direitos dos usuários na transferência internacional de dados. O texto legislativo dispõe que o Marco Civil é aplicável sobre qualquer ato relacionado à transferência internacional de dados, em situações que pelo menos um ato se materialize ou produza efeitos no Brasil. Ainda que pioneira, o Marco Civil da Internet possui um conteúdo ainda incipiente em relação à matéria de proteção de dados e, especificamente, sobre transferência internacional de dados.

Como observado no modelo europeu de proteção de dados, tratado no capítulo anterior, buscava efetivar um padrão internacional de proteção de dados pessoais, principalmente com a colocação de mecanismos de avaliação pelas autoridades nacionais em face de países terceiros e/ou organizações internacionais. Nesse ponto, é importante destacar a importância que a Autoridade Nacional de Proteção de Dados (ANPD) brasileira possui não só para a manutenção da economia digital, mas também para a continuidade de efetivação dos direitos à privacidade e proteção de dados.

O art. 33 da LGPD, entre os incisos I a IX, indica as hipóteses autorizativas sobre a transferência internacional de dados[58]. Dentre esses mecanismos, estão: nível de proteção

[58] LGPD. "Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;
III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

adequado; cláusulas contratuais específicas; cláusulas-padrão contratuais; normas corporativas globais; selos, certificados e códigos de conduta; cooperação jurídica internacional; proteção da vida ou incolumidade física; autorização pela ANPD; acordo de cooperação internacional; execução de política pública; consentimento e outras hipóteses como obrigação legal ou regulatória, execução de contrato e exercício regular de direito.

Na atual legislação brasileira, conforme o art. 33, II, da LGPD, uma das hipóteses para permitir e validar a transferência é quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos dos titulares e do regime de proteção de dados. Essas garantias podem ser na forma de: cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais e selos, certificados e códigos de conduta regularmente emitidos.

Por sua vez, o art. 35[59] da LGPD determina que a definição do conteúdo de cláusulas-padrão contratuais, entre outros, será realizada pela ANPD, sendo necessária uma regulamentação pelo órgão. Em 2021, a ANPD, criada em 2020, publicou a agenda regulatória do órgão para o biênio 2021-2022 por meio da Portaria nº 11 de 27 de janeiro de 2021[60]. Na previsão, a regulamentação da matéria de transferência internacional de dados para os artigos 33 ao 35 da LGPD, tem a prioridade da fase 2, isto é, a iniciativa do processo regulatório acontecerá em até 1 ano e 6 meses da publicação da portaria.

Este trabalho não tem como fim exaurir todas as possibilidades trazidas pelo art. 33, mas apenas aquelas em que as decisões incidem sobre os mecanismos de transferência de dados em armazenamento em nuvem. De maneira aprofundada, apenas serão analisadas as

---

IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
V - quando a autoridade nacional autorizar a transferência;
VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
IX - quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

[59]Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

[60]BRASIL. **PORTARIA Nº 11, DE 27 DE JANEIRO DE 2021.** Torna pública a agenda regulatória para o biênio 2021-2022. Diário Oficial da União, Brasília, DF. 28 jan. 2021. Seção 1, pt. 3. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em: 03/02/22.

hipóteses de: nível de proteção adequado e as cláusulas contratuais específicas, cláusulas contratuais padrão e normas corporativas globais.

Para a análise das possibilidades de transferência de dados, cabe salientar que não há relação de hierarquia entre os mecanismos de transferência, visto que ele será escolhido de acordo com a finalidade e o contexto da transferência e da natureza dos dados pessoais, devendo ser necessário avaliar cada caso concreto para definir o mais adequado.

4.1 NÍVEL DE PROTEÇÃO ADEQUADO

Segundo o inciso I do art. 33, a transferência internacional de dados é permitida para países ou organismos internacionais que proporcionem grau de proteção adequado aos dados pessoais previstos na LGPD.

A avaliação quanto ao nível de proteção adequado será feito pela ANPD, a qual levará em consideração[61]: as normas gerais e setoriais em vigor no país ou organismo internacional, a natureza dos dados, a observância de princípios gerais de proteção de dados e direitos dos titulares, a adoção de medidas de segurança, a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados e a outras circunstâncias específicas que forem relevantes para a transferência.

Assim, conforme dito por Marcel Leonardi[62]:

> "Uma vez declarada a adequação do nível de proteção de determinado país ou organismo internacional, os controladores poderão transferir dados pessoais livremente para tal território, sem a necessidade de anuência da ANPD ou dos titulares".

Levando em consideração a influência do GDPR sobre a legislação brasileira, Marcel Leonardi ainda considera importante a avaliação não só do texto da lei, mas também de meios

[61]Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
II - a natureza dos dados;
III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
IV - a adoção de medidas de segurança previstas em regulamento;
V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
VI - outras circunstâncias específicas relativas à transferência.

[62]LEONARDI, Marcel. Transferência Internacional de dados pessoais. DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR. Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de proteção de dados pessoais.** 1ª ed. Rio de Janeiro: Forense, 2021. p. 535-553. Acesso em: 10/02/22.

para assegurar a proteção - como a existência conjunta de uma Autoridade de Proteção de Dados Pessoais capaz de dar efetividade à tutela dos direitos dos titulares.

Conforme abordado no tópico 3.2, sobre as regras aplicáveis às autoridades supervisoras, impõe-se que ela seja independente e com poder de investigação e intervenção. Espera-se que a experiência europeia siga como norte para a atuação da ANPD no cenário brasileiro.

4.2 CLÁUSULAS CONTRATUAIS PADRÃO

As cláusulas contratuais padrão possuem grande importância na matéria de transferência internacional de dados, visto que há uma busca por padronização do modelo de cláusulas contratuais que devem ser observadas pelos Estados e pelas instituições. Tal mecanismo busca assegurar que os princípios, direitos e garantias decorrentes das leis de proteção de dados sejam pactuados em toda a cadeia de valor do negócio, deixando claras as regras e patamares mínimos a serem observados na prestação do serviço, isto é, no contrato entre as partes.

As cláusulas-padrão constituem um mecanismo de adoção voluntária. A autora Fernanda Marques[63] afirma que uma vez feita a escolha, não é possível que as partes realizem modificações ou variações das cláusulas conforme as especificidades do negócio. Essa hipótese, ao mesmo tempo que viabiliza a transferência internacional de dados, enrijece, por outro lado, a liberdade das partes sobre as escolhas das cláusulas que governarão a relação dos agentes de tratamento.

No que tange aos mecanismos de transferência internacional de dados elencados pela empresa Google em suas políticas e termos de uso, ainda que ela não informe nenhum mecanismo específico para a LGPD, considera-se o mecanismo mais adequado para justificar a transferência das Cláusulas Contratuais Padrão, mesmo que sejam do modelo da União Europeia. Essa utilização, inclusive, pode ser vista como uma Política de Boas Práticas,

[63] AQUINO, Theófilo Miguel de. MARQUES, Fernanda Mascarenhas. O regime de transferência internacional de dados da LGPD: delineando as opções regulatórias em jogo. DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR. Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de proteção de dados pessoais.** 1ª ed. Rio de Janeiro: Forense, 2021.p. 554-587. Acesso em: 15/02/22.

enquanto a Autoridade Nacional de Proteção de Dados ainda não emite um posicionamento ou um conjunto de cláusulas adequadas para justificar a transferência[64].

4.2 PRINCÍPIO DA TRANSPARÊNCIA NA LOCALIZAÇÃO DOS DADOS PESSOAIS

Na relação de tratamento de dados entre usuário e a Google, o usuário se classifica como titular, pessoa natural a quem se referem os dados pessoais que são objetos de tratamento (art. 5º, V, LGPD) e a Google como Controladora de dados, pessoa jurídica de direito privado a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, LGPD).

Percebe-se que a LGPD determina que o tratamento de dados somente poderá ocorrer quando possuir uma base legal, conforme disposto no art. 7º. Na relação de consumo entre o usuário e a Google, a base legal trazida pelo inciso V, Execução de Contrato, é a mais adequada para justificar o tratamento. Ela é utilizada quando os dados pessoais são necessários para a execução de obrigações contratualmente firmadas, em que o titular seja parte do instrumento.

Os mecanismos de transferência internacional de dados trazidos pelo art. 33 são, portanto, formas suplementares às bases legais para tratamento de dados. Isto é, além de obedecerem todos os requisitos trazidos pela LGPD, como a utilização de uma base legal que justifique o tratamento, deverão ser utilizados algum mecanismo do art. 33 que legitime a transferência desses dados para outros países.

A LGPD se aplica independente do país da sede ou do país da localização dos dados tratados[65]. Desde que a operação de tratamento seja realizada em território nacional, a

---

[64] Conforme o art. 52, §1º, IX, a adoção de política de boas práticas e governança será um parâmetro e um critério considerado para a aplicação de sanções pela Autoridade Nacional de Proteção de Dados,

[65] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

atividade de tratamento tem como objetivo a oferta ou fornecimento de bens ou serviços ou tratamento de dados de indivíduos localizados no território nacional e os dados pessoais objeto do tratamento tenham sido coletados no território nacional. Assim, sendo os titulares (usuários) brasileiros e os dados coletados no território brasileiro, incidirá à Google todas as obrigações estabelecidas por este marco normativo.

Uma característica importante da Lei Geral de Proteção de Dados é que ela nasceu como uma lei principiológica[66], ou seja, possui uma base forte de princípios trazidos pelo art. 6º que deverão ser seguidos na interpretação da lei. De acordo com Newton de Lucca[67], ao comentar sobre Ronald Dworkin, há distinção entre princípios, regras e políticas. Dos princípios, em *stricto sensu,* têm origem as orientações gerais, subsequentes das exigências de equidade, de justiça ou de moralidade. Das regras, por sua vez, decorrem consequências jurídicas das próprias condições previstas. Das políticas, princípios em *lato sensu*, desdobram-se os padrões a serem observados como exigência econômica, política ou social desejável. Assim, Newton constrói o raciocínio de que os princípios são todas as normas jurídicas consideradas determinantes de outra ou outras normas que lhe são subordinadas, que a pressupõem, desenvolvendo e especificando posteriormente o preceito em direções específicas.

São dez princípios elencados no art. 6º da LGPD, para além da boa-fé: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Na oferta de serviço de armazenamento em nuvem pela Google, destaca-se dois princípios para serem analisados: o do livre acesso e o da transparência.

O Princípio do Livre Acesso (art. 6º, IV, LGPD) garante aos titulares a consulta facilitada e gratuita sobre a forma e duração do tratamento, assim como a integralidade dos dados pessoais. Esse princípio, em observância ao fundamento da autodeterminação informativa[68], visa que o titular possa ter controle sobre o uso do seus dados por terceiros.

---

[66]GIMENEZ, Gabriel Nantes. **Guia de boas práticas da lei geral de proteção de dados - LGPD**, 2020. Disponível em: <https://www.migalhas.com.br/depeso/328723/guia-de-boas-praticas-da-lei-geral-de-protecao-de-dados---lgpd>. Acesso em: 13/02/22.

[67] LUCCA, Newton de. Marco Civil da Internet. Uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III: Marco civil da internet**. Quartier Latin, 2015, t.1, p.39. Acesso em: 17/02/22.

[68] Autodeterminação informativa é uma expressão para designar o direito dos indivíduos de "decidirem por si próprios, quando e dentro de quais limites seus dados pessoais podem ser utilizados". Esse direito, segundo

O art. 9º[69] é um reforçador desse princípio ao prever que o titular possui direito ao acesso facilitado das informações sobre o tratamento de seus dados pessoais. Esse é um caminho que viabiliza o titular o acompanhamento da utilização de seus dados pessoais junto ao controlador de dados, monitorando o fluxo informacional em que está envolvido, avaliando as informações perante o tratamento de seus dados[70].

Já o Princípio da Transparência (art. 6º, VI, LGPD) é fundamental para que os titulares possuam conhecimento sobre os agentes de tratamento, as características do tratamento, com informações claras, precisas e acessíveis. Esse é um dos pressupostos para que os direitos fundamentais de proteção de dados[71], privacidade e livre desenvolvimento da personalidade sejam alcançados.

A transparência deve ser dada pelos controladores, informando ao titular de dados sempre que possível, ou seja, observando os direitos de propriedade intelectual, as condições, a legalidade, a legitimidade e a segurança do tratamento de dados dos usuários. Além disso, sempre que solicitado[72], deverá o controlador informar, de ofício ou mediante requerimento dos titulares, informações claras, completas e ostensivas aos titulares, sendo, portanto, requisitos legais mínimos.

Uma decisão importante no âmbito da infração do princípio da transparência (na aplicação do GDPR), foi que em 2019 a Autoridade Francesa de Proteção de Dados, *Commission Nationale de L'Informatique Et Des Libertés* (CNIL) multou a empresa Google em 50 milhões de euros por, principalmente, não atender ao princípio da transparência de

---

Danilo Doneda, além de ser fundamento da disciplina de proteção de dados, proporciona ao indivíduo o controle de suas informações.

[69] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
I - finalidade específica do tratamento;
II - forma e duração do tratamento, observados os segredos comercial e industrial;
III - identificação do controlador;
IV - informações de contato do controlador;
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI - responsabilidades dos agentes que realizarão o tratamento; e
VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

[70] MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. *Lei Geral de Proteção de Dados comentada.* São Paulo: Revista dos Tribunais, 2019. p. 149.

[71] Promulgada pelo Congresso Nacional a Emenda Constitucional 115, em 10 de fevereiro de 2022, a Constituição Federal passa a prever expressamente a proteção de dados pessoais como um direito fundamental autônomo. Ou seja, o Brasil passa a reconhecer que a proteção de dados pessoais é um direito inviolável de todo ser humano, sem distinção de qualquer natureza, que não pode ser desrespeitado por nenhuma autoridade ou lei infraconstitucional.

[72] Arts. 9º, 18 e 19 da LGPD

forma suficiente nas informações fornecidas aos usuários, que não são de fácil acesso[73]. Segundo a decisão, as informações relevantes são acessíveis apenas em várias etapas, implicando às vezes em até 5 ou 6 ações, os propósitos são descritos de maneira genérica e vaga. O Comitê ainda avaliou que algumas informações nem sempre são claras, de forma que os usuários não conseguem entender completamente a extensão das operações de processamentos realizadas pelo Google. Tal decisão demonstra que a observância aos princípios deve ser fundamental para a oferta de serviços que usam os dados como ativos econômicos.

No caso do Google Drive, ainda que a Google compartilhe em seu site as localizações dos *data centers* [74], responsáveis pelo armazenamento de dados, o usuário não consegue obter as informações de onde os seus dados estão armazenados, de maneira específica. Ou seja, o usuário, como titular de seus dados, não consegue ter informações precisas sobre o armazenamento de seus dados, ferindo, assim, os princípios da transparência e do livre acesso.

5 CONSIDERAÇÕES FINAIS

Diante das transformações tecnológicas e do avanço da economia, houve o crescimento de ofertas de serviços e produtos que utilizam os dados pessoais como base para o desenvolvimento de seus negócios. Concomitantemente, os Estados se viram obrigados a elaborarem legislações em que imputassem regras a fim de proteger os direitos fundamentais à privacidade e ao livre desenvolvimento de sua personalidade dos titulares dos dados.

Com a inovação dos modelos de negócio, a Google, uma das cinco maiores empresas do mundo, conhecida principalmente pela sua ferramenta de busca, inovou também na oferta de serviços em armazenamento em nuvem - o *Google Drive.* Em razão da tecnologia, os dados são armazenados em diversos locais do mundo, existindo, portanto, um fluxo internacional de dados. Como os dados armazenados estão relacionados a um titular, fica evidente a necessidade de aplicação de mecanismos que assegurem a proteção de dados e a

---

[73] CNIL. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.** 21.01.2019. Disponível em: <https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en>. Acesso em: 18/02/22.

[74] Localização dos data centers da Google, disponível em: <https://www.google.com/intl/pt-br/about/datacenters/locations/>. Acesso em: 15/02/22.

privacidade dos usuários, destacando que a localização dos dados não é um fator que diminua as garantias.

Foram apresentados os mecanismos de transferência utilizados tanto na normativa da União Europeia (GDPR), quanto na atual legislação de proteção de dados brasileira. O Direito comparado se faz necessário, tendo em vista a consolidação de direitos e garantias no solo europeu, bem como o avanço na fiscalização e imputação de sanções para o descumprimento dessas normas. Além disso, pela evolução da globalização e da cadeia internacional de informação e comunicação, decisões em outras jurisdições podem ter impacto na aplicação da legislação no território nacional.

Como objeto do trabalho, foram avaliados os termos de serviço, política de privacidade e outros documentos disponíveis pela Google, na oferta dos serviços do Google Drive. Além disso, também foram observadas a aplicação dos requisitos impostos pela atual Lei Geral de Proteção de Dados para o tratamento de dados de usuários brasileiros, principalmente no que tange à aderência aos princípios norteadores.

Conclui-se, portanto, que a transferência internacional de dados no cumprimento do contrato do Google Drive utiliza-se da hipótese de transferência por meio de cláusulas contratuais padrão, no modelo europeu. Entretanto, ainda que sejam mecanismos válidos de transferência, exige-se a consolidação e fiscalização da Autoridade Nacional de Proteção de Dados para verificar, na prática, o cumprimento de suas obrigações.

Observou-se, ainda, que a falta de transparência quanto à localidade dos dados pessoais no armazenamento em nuvem fere os princípios do livre acesso e da transparência, sendo, portanto, negado ao titular informações relevantes quanto ao tratamento de seus dados pessoais.

REFERÊNCIAS

AQUINO, Theófilo Miguel de. MARQUES, Fernanda Mascarenhas. O regime de transferência internacional de dados da LGPD: delineando as opções regulatórias em jogo. DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR. Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de proteção de dados pessoais.** 1ª ed. Rio de Janeiro: Forense, 2021.p. 554-587.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **The future of privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.** Bruxelas: [s. n.], 2009. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf>.

BIAZATTI, Bruno et al. **Transferência Internacional de Dados no PL 5276/16.** Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2017. Disponível em: http://bit.ly/34YkcbZ.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. Constituição (1988). **Emenda constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm> . Acesso em:

BRASIL. Lei nº13.709, de 14 de agosto de 2018: **Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**. Diário Oficial [da] República Federativa do Brasil, Brasília, DF. Disponível em: <http://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html>.

BRASIL. Lei nº12.965, de 23 de abril de 2014: **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial [da] República Federativa do Brasil**, Brasília, DF. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>.

BRASIL. Portaria nº 11, de 27 de janeiro de 2021**. Torna pública a agenda regulatória para o biênio 2021-2022**. Diário Oficial da União, Brasília, DF. 28 jan. 2021. Seção 1, pt. 3. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em:

BONANI, Rafael. **Termos de uso o que são e para o que servem**, 2020. Disponível em: <https://www.bonani.adv.br/termos-de-uso-o-que-sao-e-para-que-servem>.

BRANCO Jr., Eliseu C.; MACHADO, Javam C.; MONTEIRO, José Maria. Estratégias para Proteção da Privacidade de Dados Armazenados na Nuvem. **Tópicos em Gerenciamento de Dados e Informações, Curitiba:** 1ª edição, p. 46-74, 2014**.** Disponível em: <https://www.inf.ufpr.br/sbbd-sbsc2014/sbbd/proceedings/artigos/pdfs/14.pdf>.

BRANDÃO, Luiza. **FLUXO TRANSNACIONAL DE DADOS:** estruturas, políticas e o Direito nas vertentes da governança. 2020. 129. Mestra em Direito - UFMG, Belo Horizonte. Disponível em: <https://repositorio.ufmg.br/bitstream/1843/33716/1/DissertacaoLuizaB.pdf>.

CASSIOLATO, José Eduardo; LASTRES, Helena M. M. **Celso Furtado e os dilemas da indústria e inovação no Brasil.** *Cadernos do Desenvolvimento*, v. 10, n. 17, Rio de Janeiro: Centro Internacional Celso Furtado de Políticas para o Desenvolvimento, jul./dez. 2015, p. 188-213.

CASTELLS, Manuel. **A sociedade em rede: a era da informação.** Vol. 1. 10ª. ed. São Paulo: Paz e Terra, 2009. (A era da Informação: Economia, Sociedade e Cultura).

CHAVES, Luís Fernando Prado Chaves. Da transferência internacional de dados. **LGPD: Lei Geral de Proteção de Dados Comentada.** Viviane Nóbrega Maldonado; Renato Opice Blum, coordenadores. – São Paulo: Thomson Reuters Brasil, 2019; p. 291-308.

CHURCHES, Genna; ZALNIERIUTE, Monika. A groundhog day in Brussels: Schrems II and international data transfers.

CNIL. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.** 21.01.2019. Disponível em: <https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en>.

COMISSÃO EUROPEIA. **Adequacy decisions.** Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

COMISSÃO EUROPEIA. **COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems)**. 2015. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52015DC0566>. Acesso em:

COMISSÃO EUROPEIA. **European Commission adopts new tools for safe exchanges of personal data.** 2020. **Disponível em: <**https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2847>.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da lei geral de proteção de dados.São Paulo : Thomson Reuters Brasil, 2020.

DONEDA, Danilo. **O que está em jogo com a nova Autoridade Nacional de Proteção de Dados,** 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protecao-de-dados-13082018>.

EDPB. **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.** Disponível em: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf?utm_campaign=newsletter_-_17112020&utm_medium=email&utm_source=RD+Station>.

EUROPA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Dispõe sobre a 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://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT> . Acesso em:

EXPERIAN. **What is the Safe Harbor Agreement?** Disponível em: <https://www.experian.co.uk/business/glossary/safe-harbour-agreement/>.

FEDERAL DATA PROTECTION AND INFORMATION COMMISSIONER **Transborder data flow.** Disponível em: <https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html>.

FENNESSY, Caitlin. **New EU SCCs:** a modernized approach, 2020. Disponível em: <https://iapp.org/news/a/new-eu-standard-contractual-clauses-a-modernized-approach/>.

GALLOWAY, Scott. **Os quatro: apple, amazon, facebook e google - o segredo dos gigantes da tecnologia.** Rio de Janeiro. Alta Books, 2019.

GIMENEZ, Gabriel Nantes. **Guia de boas práticas da lei geral de proteção de dados - LGPD**, 2020. Disponível em: <https://www.migalhas.com.br/depeso/328723/guia-de-boas-praticas-da-lei-geral-de-protecao-de-dados---lgpd>.Acesso em:

GOOGLE. **Política de Privacidade**. Disponível em: <https://policies.google.com/privacy?hl=en&gl=US#inforetaining>.

GOOGLE. **Políticas do programa contra abuso e como elas são aplicadas.** Disponível em: <https://support.google.com/docs/answer/148505>.

GOOGLE. **Termos de serviço**. Disponível em: <https://policies.google.com/terms>.

GOOGLE. **Termos de serviço específicos.** Disponível em: <https://policies.google.com/terms/service-specific>

GOOGLE. **Termos de serviço do Google Drive.** Disponível em: <https://www.google.com/drive/terms-of-service/>

HALLE-SMITH, Claire. **New standard contractual clauses published by the European Commissioned,** 2020. Disponível em: <https://www.wrighthassall.co.uk/knowledge-base/new-standard-contractual-clauses-published-by-the-european-commission>.

ICO. I**CO consults on how organizations can continue to protect people's personal data when it's transferred outside of the UK.** 2021. Disponível em: <https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/standard-contractual-clauses/>. Acesso em:

ICO. **International transfers after the UK exit from the EU Implementation Period**. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#adequacy>.

KURTZ, Lahis; VIEIRA, Victor. **Obtenção transnacional de conteúdo de comunicações telemáticas na América Latina:** relatório de pesquisa. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2020. Disponível em: https://bit.ly/2RkAmaL.

KUNER, Christopher. **The Schrems II judgment of the Court of Justice and the future of data transfer regulation**, 2020. Disponível em: <https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation/>.

LEONARDI, Marcel. **Fundamentos do Direito Digital.** São Paulo: Thomson Reuters Brasil, 2019.

LEONARDI, Marcel. Transferência Internacional de dados pessoais. DONEDA, Danilo; MENDES, Laura Schertel; RODRIGUES JR. Otavio Luiz; SARLET, Ingo Wolfgang. **Tratado de proteção de dados pessoais.** 1ª ed. Rio de Janeiro: Forense, 2021. p. 535-553.

LUCCA, Newton de. Marco Civil da Internet. Uma visão panorâmica dos principais aspectos relativos às suas disposições preliminares. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III: Marco civil da internet.** Quartier Latin, 2015.

MARQUES, Fernanda Mascarenhas. Cláusulas-padrão contratuais como autorizadoras para a Transferência Internacional de Dados: alternativas em casos de ausência de decisão de adequação. **Revista do Advogado: Lei Geral de Proteção de Dados**, São Paulo, nº 144, nov/2019. P. 192. Disponível em: <https://aplicacao.aasp.org.br/aasp/servicos/revista_advogado/paginaveis/144/index.html>.

MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. **Lei Geral de Proteção de Dados comentada.** São Paulo: Revista dos Tribunais, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. 2ª edição. São Paulo: Revista dos Tribunais, 2019.

MACHADO, Diego Carvalho et al. **GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa.** Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2018. Disponível em: <http://bit.ly/2smFX6D>.

MONTEIRO, Renato Leite. **O impacto da regulação geral de proteção de dados da UE em empresas brasileiras:** eficácia extraterritorial e transferência internacional de dados. Baptista

Luz Advogados: São Paulo, 2018. Disponível em: <https://baptistaluz.com.br/o-impacto-da-regulacao-geral-de-protecao-de-dados-da-ue-em-empresa-brasileira/>.

NORTON ROSE FULBRIGHT. **Schrems II landmark ruling:** A detailed analysis, 2020. Disponível em: <https://www.nortonrosefulbright.com/en/knowledge/publications/ad5f304c/schrems-ii-landmark-ruling-a-detailed-analysis>.

OCDE **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais.** 2002. Disponível em: < https://www.oecd.org/sti/ieconomy/15590254.pdf>.

OFFICIAL JOURNAL OF THE EUROPEAN UNION. **2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.).** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32000D0520>. Acesso em:

OFFICIAL JOURNAL OF THE EUROPEAN UNION. **COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on 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>.

OFFICIAL JOURNAL OF THE EUROPEAN UNION.**COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.** Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915>.

OFFICIAL JOURNAL OF THE EUROPEAN UNION. **COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.** Disponível em: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0087>.

OLIVEIRA, Davi Teófilo Nunes et al. **A Internet e suas repercussões sobre a Cooperação Jurídica Internacional:** estudo preliminar sobre o tema no Brasil. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2018. Disponível em: <http://bit.ly/38Dxpt0. 0>.

PARLAMENTO EUROPEU. **The CJEU judgment in the Schrems II case**. 2020**.** disponível em: <https://curia.europa.eu/juris/document/document.jsf;jsessionid=B04EBCBEF9C1F1CD0B6AF53B1E85A69B?text=&docid=228677&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1464439>.Acesso em: .

PERRONE, Christian. **Dados internacionais na encruzilhada e o contexto brasileiro**, 2020. Disponível em: <https://www.jota.info/coberturas-especiais/liberdade-de-expressao/dados-internacionais-na-encruzilhada-e-o-contexto-brasileiro-21072020>.

PRIVACY SHIELD FRAMEWORK. Disponível em: <https://www.privacyshield.gov/participant?id=a2zt000000001L5AAI&status=Active>.

SHAW, Thomas. **A deep dive into the 'Schrems II' case**, 2018. Disponível em: <https://iapp.org/news/a/a-deep-dive-into-the-schrems-ii-case/>.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **O Tribunal de Justiça declara inválida a Decisão de Execução 2016/1250, relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA**. Luxemburgo, 16 de julho de 2020. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf>. Acesso em:

UNIÃO EUROPEIA. **Diretiva 95/46/CE.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>.

UNIÃO EUROPEIA. **EU proposal for provisions on Cross-border data flows and protection of personal data and privacy.** Disponível em: <https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf> . Acesso em:

VIOLA, Mario. **Transferência de dados entre Europa e Brasil:** análise da adequação da Legislação Brasileira. ITS Rio: Rio de Janeiro, 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf.

WEBER, Rolf. **Transborder data transfers: concepts, regulatory approaches and new legislative initiatives.** International Data Privacy Law, 2013. Vol. 3, N. 2. P. 117 - 129.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Rio de Janeiro: Intrínseca, 2021.