UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

Fernanda Ratzkowski

AS NORMAS CORPORATIVAS GLOBAIS COMO MECANISMO DE COMPROVAÇÃO DE GARANTIAS NAS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS: O MODELO BRITÂNICO E SUAS POSSÍVEIS APLICAÇÕES A UM MODELO BRASILEIRO

Porto Alegre
2023

FERNANDA RATZKOWSKI

AS NORMAS CORPORATIVAS GLOBAIS COMO MECANISMO DE COMPROVAÇÃO DE GARANTIAS NAS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS: O MODELO BRITÂNICO E SUAS POSSÍVEIS APLICAÇÕES A UM MODELO BRASILEIRO

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Fabiano Menke.

Porto Alegre

2023

Fernanda Ratzkowski

AS NORMAS CORPORATIVAS GLOBAIS COMO MECANISMO DE COMPROVAÇÃO DE GARANTIAS NAS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS: O MODELO BRITÂNICO E SUAS POSSÍVEIS APLICAÇÕES A UM MODELO BRASILEIRO

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Direito da Universidade Federal do Rio Grande do Sul.

Porto Alegre, _____de _____ de 2023.

BANCA EXAMINADORA

_____
Prof. Dr. Fabiano Menke (Orientador)

_____

_____

Ao meu pai, Eli Ratzkowski,
Pelo amor que ultrapassa
barreiras.

AGRADECIMENTOS

A entrega do presente trabalho representa o final de um ciclo que vou lembrar com muito carinho.

Mais do que nunca, hoje é dia de lembrar e agradecer ao meu pai, Eli. Ele, que insistiu para que eu completasse a semana de vestibular da UFRGS quando eu estava considerando desistir na metade (e só por isso estou aqui), que me buscou tantas noites na Faculdade, que me ouvia interessado falar horas a fio sobre alguns temas do Direito que, olhando em retrospecto, talvez não fossem tão interessantes. Inclusive, me ouviu falar sobre este trabalho antes de virar texto, quando não passava de alguns esquemas mentais criados durante idas à Faculdade ou ao estágio.

Meu pai é o meu exemplo de força, bondade, dedicação, coragem e profissionalismo. Foi nele e na minha mãe, Marcia, que encontrei inspiração quando o caminho parecia tortuoso. Encerrar esse ciclo sem a presença física do meu melhor amigo e maior companheiro é, com certeza, muito estranho.

Nos dias difíceis, tenho lembrado das palavras escritas por Guimarães Rosa, no Grande Sertão: Veredas: “O que Deus quer é ver a gente aprendendo a ser capaz de ficar alegre a mais, no meio da alegria, e inda mais alegre ainda no meio da tristeza! Só assim de repente, na horinha em que se quer, de propósito — por coragem”. Por isso, hoje, ainda que em meio a tristeza e a saudade, comemoro alegre essa conquista sabendo que, de outro lugar, meu querido pai Eli comemora e vibra comigo, como sempre foi.

Aproveito, também, para agradecer imensamente à minha mãe, Marcia. Minha mãe tem um olhar sensível, e percebe detalhes em tudo e em todos, coisas que, normalmente, passam despercebidas por mim. Minha mãe me ensina a olhar com mais cuidado e empatia para o mundo todos os dias. Acho incrível que, ao mesmo tempo em que ela é sensível, é a pessoa mais forte e resiliente que eu conheço. Ela não mede esforços para me ver feliz e, hoje, eu agradeço por tudo até aqui. Que sigamos juntas, vivendo todas as dores e delícias da vida.

Ao meu irmão Marcelo. Mesmo ele morando longe, sinto que estamos cada dia mais amigos e mais unidos. Sinto saudades todos os dias.

À minha vó, Ida, que acredita em mim quando nem eu mesma acredito. Que me dá forças e incentivo para seguir vivendo em busca de realizar os meus sonhos.

Aos meus avós, Oscar, Maria e Manoel, que apesar de não estarem presentes neste plano, me acompanham em todos os momentos da vida.

À Kim, minha fiel escudeira, sempre ao meu lado.

Aos meus amigos, colegas de faculdade, e de estágio, que dividiram comigo as alegrias e os estresses da vida universitária.

Aos meus chefes de estágio, que contribuíram enormemente para o meu desenvolvimento profissional e pessoal.

Ao meu orientador, Professor Fabiano Menke, cujas aulas, desde os semestres iniciais do curso, despertaram em mim o interesse no Direito Civil, área que tanto gosto. Agradeço, também, por ter aceitado me orientar neste trabalho, e por toda a dedicação e compreensão como orientador.

RESUMO

Este trabalho busca analisar como as normas corporativas globais aprovadas pelo ICO podem contribuir para um futuro modelo brasileiro de normas corporativas globais. O primeiro capítulo do trabalho trata das transferências internacionais de dados pessoais sob as óticas do GDPR do Reino Unido e da LGPD. Nesse sentido, ambas as legislações disponibilizam mecanismos que oferecem e comprovam garantias de cumprimento de princípios e direitos para viabilizar as transferências. Dentre esses mecanismos, estão as normas corporativas globais, tratadas no segundo capítulo do trabalho. Estas normas permitem que dados pessoais sejam transferidos internacionalmente dentro de um grupo corporativo. Enquanto o Reino Unido possui um procedimento de aprovação das normas corporativas globais já consolidado, a regulamentação do tema no Brasil está pendente. Desse modo, a análise das práticas adotadas pelo Reino Unido pode se revelar uma valiosa inspiração para o Brasil na regulamentação e consolidação dos seus instrumentos.

Palavras-chave: Proteção de Dados Pessoais; Transferência Internacional de Dados; Normas Corporativas Globais; Reino Unido; Brasil.

ABSTRACT

This study aims to analyze how the ICO approved binding corporate rules may contribute to a future Brazilian model of binding corporate rules. The first chapter of the study deals with international transfers of personal data from the standpoint of the UK GDPR and the LGPD. In this regard, both legislations provide mechanisms that guarantee the compliance with certain principles and rights to make the transfers feasible. Among these mechanisms are the Binding Corporate Rules, discussed in the second chapter of this study. These Rules allow personal data to be transferred internationally within a corporate group. While the United Kingdom has a well-established procedure for approval of the binding corporate rules, Brazil's regulation of the subject is pending. Thus, the analysis of the practices adopted by the United Kingdom may prove to be a valuable inspiration for Brazil in the regulation and strengthening of its instruments.

Keywords: Personal data protection; Transfers of personal data; Binding corporate rules; United Kingdom; Brazil.

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

ANPD	Autoridade Nacional de Proteção de Dados
Art.	Artigo
CDC	Código de Defesa do Consumidor
EC	Emenda Constitucional
EDPB	European Data Protection Board
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
ITS	Instituto de Tecnologia & Sociedade do Rio
LGPD	Lei Geral de Proteção de Dados
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
SAC	Serviço de Atendimento ao Consumidor
Senacon	Secretaria Nacional do Consumidor
SGT13	Subgrupo de Trabalho Número 13
USD	Dólar Americano

SUMÁRIO

1 INTRODUÇÃO

Em 2006, o matemático britânico Clive Humby afirmou que os “dados são o novo petróleo”[1]. Desde então, a frase foi amplamente difundida, especialmente após a publicação do artigo intitulado *The World's Most Valuable Resource Is No Longer Oil, but Data*, pelo jornal britânico *The Economist*, em maio de 2017[2]. O artigo comparou o significativo crescimento econômico de empresas que dispõem de grandes quantidades de dados pessoais – ilustradas por Alphabet, Amazon, Apple, Facebook e Microsoft – com o crescimento vivenciado por gigantes do petróleo, como a Standard Oil, no século passado[3].

Desde então, a frase “dados são o novo petróleo” tornou-se uma espécie de mantra para as grandes companhias. E, independentemente de possíveis discussões acerca da preponderância econômica dos ativos digitais sobre as fontes tradicionais de riqueza, é inegável a relevância dos dados pessoais no cenário atual.

Isso porque, nas últimas décadas, vivenciamos a digitalização de diversas áreas do cotidiano – como, por exemplo, o trabalho, os relacionamentos, a educação e as transações financeiras. Nesse sentido, como o cadastramento dos dados dos indivíduos é requisito para a constituição dos seus sujeitos digitais, a disponibilização dos dados pessoais tornou-se imprescindível para a utilização de uma série de serviços[4].

Além disso, como relembra Christopher Kuner[5], a proteção de dados não diz respeito a uma questão existente somente no ambiente online, pois, atualmente, praticamente todas as atividades econômicas e sociais envolvem o tratamento de dados pessoais[6]. Também, a temática da proteção de dados não se relaciona a uma

---

[1] Data Isn't The New Oil — Time Is. **Forbes**, Nova York, 15 de julho de 2021. Disponível em: https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/?sh=1db09c1f35bb. Acesso em: 22 fev. 2023.

[2] The world's most valuable resource is no longer oil, but data. **The Economist**, Londres, 06 de maio de 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 22 fev. 2023.

[3] *Ibidem*

[4] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2020, p. RB-23.1. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/195107452/v2/page/RB-23.1. Acesso em: 22 fev. 2023.

[5] KUNER, Christopher. The global data privacy power struggle. **Oxford Univesity Press's (OUPblog)**, 28 jan. 2013. Disponível em: https://blog.oup.com/2013/01/global-data-privacy-power-struggle/. Acesso em: 16 mar. 2023.

[6] *Ibidem*

questão meramente econômica, mas a questões sociais e de desenvolvimento[7]. Como exemplo, o autor cita a iniciativa conhecida como *Global Pulse*, da Organização das Nações Unidas, que utiliza a análise de dados para compreender o estado global de saúde e as crises socioeconômicas[8].

Destarte, com a coleta de dados tornando-se cada vez mais intensa, surgiu o fenômeno conhecido como Big Data[9]. O Big Data pode ser definido como conjuntos de dados cujo tamanho ou tipo está acima do que os bancos de dados relacionais tradicionais conseguem capturar, gerenciar e tratar em baixa latência[10]. O Big Data tem como característica um grande volume, uma alta velocidade e uma ampla variedade de dados[11]. Isso se dá pelo fato de que as fontes dos dados estão cada vez mais dinâmicas, impulsionadas pela Inteligência Artificial, pelos dispositivos móveis, pelas mídias sociais e pela Internet das Coisas[12]. Nesse sentido, conforme sintetizado em relatório elaborado pelo Instituto de Tecnologia & Sociedade do Rio – ITS:

> Todas as ações e comunicações em plataformas digitais, como com telefones celulares, computadores ou mesmo transações de cartão de crédito e, mais recentemente, declarações de imposto de renda, ou ações que, em algum momento, são digitalizadas e assim transformadas em dados, como as câmeras de segurança associadas com software de reconhecimento facial ou de padrões, são passíveis de serem armazenadas, processadas, copiadas e distribuídas quase instantaneamente (...)[13]

Em resumo, os dados correspondem a informações e, quando tratados de forma organizada e adequada, fornecem elementos valiosos para as empresas. Por isso, podemos dizer que os dados são, hoje, um insumo fundamental na produção econômica moderna. Contudo, apesar da coleta, tratamento e utilização dos dados proporcionar uma série de benefícios – dentre eles, por exemplo, a redução nos custos de técnicas de sequenciamento genético por meio de melhoria nas ferramentas de bioinformática, ou a alimentação dos softwares dos veículos autônomos – eles geram,

---

[7] KUNER, Christopher. The global data privacy power struggle. **Oxford Univesity Press's (OUPBlog)**, 28 jan. 2013. Disponível em: https://blog.oup.com/2013/01/global-data-privacy-power-struggle/. Acesso em: 16 mar. 2023.
[8] *Ibidem*
[9] INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Big Data no projeto Sul Global: Relatório sobre estudos de caso**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2016, p. 9. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf. Acesso em: 22 fev. 2023.
[10] BIG DATA ANALYTICS. In: INTERNATIONAL Business Machines Corporation (IBM). New York: IBM, 2023. Disponível em: https://www.ibm.com/analytics/big-data-analytics. Acesso em 22 fev. 2023.
[11] *Ibidem*
[12] *Ibidem*
[13] INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO, *op. cit.*

também, riscos à privacidade dos indivíduos, podendo ocasionar problemas como fraudes e crimes cibernéticos quando utilizados de maneira imprópria.

E, vale dizer, os problemas ocasionados pelo uso inadequado dos dados pessoais não são sempre tangíveis, já que, por vezes, o indivíduo pode sofrer discriminações sem saber que esta se originou de dados disponíveis no ambiente eletrônico, como postagens em redes sociais, por exemplo. Com efeito, o crescimento da relevância do tratamento de dados pessoais se reflete na grande quantidade de países que vêm promulgando leis de proteção de dados[14]. De fato, é primordial que o direito atue de modo a evitar e mitigar os potenciais riscos aos quais o cidadão está exposto, a partir da estruturação de bases normativas de proteção de dados pessoais.

Com esse intuito, a União Europeia promulgou, em outubro de 1995, a Diretiva 95/46/EC[15] – conhecida como Diretiva de Proteção de Dados Pessoais – a fim de regular o tratamento de dados pessoais dentro do território europeu. Todavia, como era necessário que cada Estado-membro internalizasse a Diretiva em sua legislação, os países europeus acabaram apresentando diferentes níveis de garantia à proteção dos dados pessoais[16], com a aplicabilidade direta da Diretiva ocorrendo apenas em via de exceção[17]. Em abril de 2016, aprovou-se o Regulamento Geral de Proteção de Dados Pessoais da União Europeia ("GDPR"), que revogou a Diretiva, justamente com o intuito de uniformizar os níveis de proteção de dados na União Europeia[18].

Já no Brasil, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados ("LGPD"), primeira base normativa do país especificamente voltada à proteção de dados, foi sancionada em agosto de 2018. A LGPD foi resultado de um processo iniciado em 2010 por consulta pública realizada pelo Ministério da Justiça e, após, pela propositura do Projeto de Lei nº 5.276/2016, anexado ao Projeto de Lei nº 4.060/2012, na Câmara

---

[14] KUNER, Christopher. The global data privacy power struggle. **Oxford Univesity Press's (OUPBlog)**, 28 jan. 2013. Disponível em: https://blog.oup.com/2013/01/global-data-privacy-power-struggle/. Acesso em: 16 mar. 2023.

[15] UNIÃO EUROPEIA. **Diretiva 95/46/CE** do Parlamento Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 23 fev. 2023.

[16] UEHARA, Luiz Fernando e TAVARES FILHO, Paulo César. Transferência Internacional de Dados Pessoais: Uma Análise Crítica entre o Regulamento Geral de Proteção de Dados Pessoais da União Europeia (RGPD) e a Lei Brasileira de Proteção de Dados Pessoais (LGPD). **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 2, p. 7, 2019.

[17] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.1. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.1. Acesso em: 10 mar. 2023.

[18] UEHARA, *op. cit.*

dos Deputados que, posteriormente, transformou-se no Projeto de Lei da Câmara n° 53, de 2018, no Senado Federal[19]. A LGPD também alterou a Lei nº 12.965/2016, o Marco Civil da Internet[20-21].

A LGPD é bastante semelhante ao GDPR no contexto, na estrutura e na racionalidade final, qual seja, a proteção dos direitos e liberdades fundamentais das pessoas físicas[22]. De fato, a LGPD foi bastante influenciada pela Diretiva de Proteção de Dados Pessoais[23], e pelo GDPR[24]. O próprio parecer da Comissão Especial da Câmara dos Deputados, instituído para analisar o Projeto de Lei nº 4060/2012, estabeleceu que "grande fonte de inspiração para os projetos advém do arcabouço europeu", em especial a Convenção do Conselho da Europa[25] nº 108[26], de 1981, ou "Convenção para a Proteção de Indivíduos com Respeito ao Processamento

[19] UEHARA, Luiz Fernando e TAVARES FILHO, Paulo César. Transferência Internacional de Dados Pessoais: Uma Análise Crítica entre o Regulamento Geral de Proteção de Dados Pessoais da União Europeia (RGPD) e a Lei Brasileira de Proteção de Dados Pessoais (LGPD). **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 2, p. 7, 2019.

[20] *Ibidem*

[21] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 mar. 2023.

[22] MONTEIRO, Renato. GDPR matchup: Brazil's General Data Protection Law. **IAPP**, Portsmouth, 18 de outubro de 2018. Disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Acesso em: 25 de fev. 2023.

[23] UNIÃO EUROPEIA. **Diretiva 95/46/CE** do Parlamento Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 23 fev. 2023.

[24] PRADO CHAVES, Luis Fernado. Da Transferência Internacional de Dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice**. LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, p. RL-1.10. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

[25] O Conselho da Europa, localizado em Estrasburgo é a maior e mais antiga intergovernamental da Europa, fundada em 1949. O Conselho da Europa protege e promove três valores fundamentais: os direitos humanos, a democracia e o Estado de direito. Atualmente, o Conselho da Europa possui 46 Estados membros. Ele conta todos os países europeus entre seus membros, assim como países das periferias do continente, como a Turquia ou o Azerbaijão. (COUNCIL OF EUROPE. In: EUROPE´S Human Rights Watchdog. União Europeia: Europe´s Human Rights Watchdog, 2023. Disponível em https://www.europewatchdog.info/en/council-of-europe/. Acesso em: 24 mar. 2023).

[26] UNIÃO EUROPEIA. Council of Europe. **Convention 108 + Convention for the protection of individuals with regard to the processing of personal data**. Jun. 2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 Acesso em 24.03.2023

Automático de Dados Pessoais"; a Diretiva de Proteção de Dados Pessoais; e, ainda, a Diretiva 2002/58/EC[27], que trata da privacidade em comunicações eletrônicas[28].

Deve-se mencionar, ainda, que o avanço da tecnologia digital, juntamente da intensificação do processo de globalização, ampliou a conectividade global de modo que as empresas e indivíduos passaram a compartilhar informações com o mundo todo[29]. E, atualmente, a sobrevivência da economia global demanda cada dia mais dos fluxos contínuos de dados[30].

Assim, diversos comportamentos usuais dos indivíduos, como a comunicação por mensagens, o compartilhamento de fotos em redes sociais, ou a utilização de serviços de entrega podem acarretar transferências internacionais de dados pessoais[31]. É dizer: no contexto atual, qualquer tipo de comunicação de informações pode configurar uma transferência internacional de dados, em razão do fluxo de dados contínuo e instantâneo[32]. Até mesmo empresas brasileiras que oferecem serviços apenas a clientes localizados no Brasil estão sujeitas a realizarem transferências internacionais de dados, caso utilizem tecnologia de infraestrutura externa[33].

Esse fluxo internacional de informações provoca alguns desafios envolvendo privacidade e proteção de dados, pois a circulação contínua e constante de dados gera maior chance de ocorrência de incidentes envolvendo a questões de segurança. Portanto, resta clara a necessidade de regular-se a proteção de dados também em âmbito internacional. Nesse sentido, ambos o GDPR e a LGPD possuem parte relevante de seus textos normativos tratando das transferências internacionais de dados pessoais.

---

[27] UNIÃO EUROPEIA. **Directiva 2002/58/CE** do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), de 12 junho de 2002. Disponível em: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_pt.pdf. Acesso em: 01 mar. 2023.

[28] BRASIL. **Projeto de Lei nº 4.060, de 2012** (Apenso PLs nos 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename. Acesso em: 25 fev. 2023.

[29] MUNDO EDUCAÇÃO. As redes de comunicação no mundo globalizado. Mundo Educação, São Paulo, 2019. Disponível em: https://mundoeducacao.uol.com.br/geografia/as-redes-comunicacao-no-mundo-globalizado.htm. Acesso em: 27 mar. 2023.

[30] LEONARDI, Marcel. Transferência internacional de dados pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 309. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

[31] *Ibidem*

[32] *Ibidem*

[33] *Ibidem*

O GDPR traz as disposições sobre transferências internacionais de dados pessoais em seu capítulo V, entre os arts. 44 e 50[34]; já a LGPD trata do tema, também em seu capítulo V, entre os arts. 33 a 36[35]. Os dois regulamentos estabelecem a necessidade de decisão de adequação para a livre transferência de dados para outros países. E, em caso de falta de adequação, os regulamentos expõem os instrumentos legais adequados. Inspirado pelo GDPR, o legislador brasileiro listou, no art. 33, II, da LGPD, mecanismos para "oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos"[36]. Dentre estes mecanismos, estão as normas corporativas globais.

As normas corporativas globais tratam de um conjunto de regras legalmente vinculantes, ou legalmente executáveis, que viabilizam as transferências internacionais de dados[37]. Basicamente, essas normas constituem um código de conduta aplicável às transferências de dados pessoais que ocorrem no âmbito interno dos grupos corporativos, com o intuito de facilitar as transferências e promover um nível satisfatório de proteção de dados[38].

---

[34] UNIÃO EUROPEIA**. Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Chapter 5. Disponível em: https://gdpr-info.eu/chapter-5/. Acesso em: 25 fev. 2023.

[35] BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 fev. 2023.

[36] **Art. 33 da Lei Geral de Proteção de Dados.** A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional (BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 26 fev. 2023).

[37] PROUST, Olivier e BARTOLI, Emmanuelle. **Binding Corporate Rules: a global solution for international data transfers**. Oxford: International Data Privacy Law, 2011, p. 2.

[38] *Ibidem*

No Brasil, muito embora a LGPD tenha estabelecido os mecanismos a serem utilizados para garantir os níveis adequados de segurança nas transferências internacionais de dados, este tema está pendente de regulamentação. O tema da transferência internacional de dados pessoais foi abrangido item 9 da agenda regulatória bianual 2021-2022 da Autoridade Nacional de Proteção de Dados ("ANPD")[39], tendo sido realizada tomada de subsídios entre maio e junho de 2022, na qual se recebeu 63 contribuições[40]. Por isso, até o momento, o Brasil não possui requisitos a serem preenchidos ou um modelo de normas corporativas globais a serem seguidas.

O Reino Unido, por sua vez, está mais avançado nesse tópico. À época que o GDPR entrou em vigor, em 25 de maio de 2018[41], o Reino Unido – que saiu da União Europeia em 31 de janeiro de 2020, com a ocorrência do *Brexit*[42] – ainda era parte do bloco e, portanto, passou a seguir o regulamento como os demais Estados-membros. Assim, após o *Brexit*, as disposições do GDPR foram incorporadas diretamente na lei do Reino Unido como o "UK GDPR", ou GDPR do Reino Unido[43]. A nova Lei segue basicamente as mesmas regras de proteção de dados que o GDPR, adaptando-o para o seu sistema legal[44]. Na prática, a nova norma é considerada "praticamente idêntica"[45], não havendo mudanças significativas nos princípios fundamentais de proteção de dados, direitos e obrigações[46].

A União Europeia havia estabelecido procedimento a ser seguido pelos grupos corporativos para a obtenção da aprovação das normas corporativas globais. Cabe às empresas, portanto, buscar a autoridade competente em seu país para aprovar as normas corporativas globais e, após, a autoridade competente deve comunicar seu

---

[39] BRASIL. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 24 mar. 2023.

[40] BRASIL. Autoridade Nacional de Proteção de Dados. **Tomada de Subsídios sobre Transferência Internacional.** Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional. Acesso em: 10 mar. 2023.

[41] UNIÃO EUROPEIA. Comissão Europeia. **Data protection**. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. Acesso em: 28 mar. 2023.

[42] REINO UNIDO. UK Parliament. **Artificial intelligence and data protection**. Disponível em: https://commonslibrary.parliament.uk/research-briefings/cbp-7960/. Acesso em: 28 mar. 2023.

[43] REINO UNIDO. Information Commissioner's Office. **Overview of Data Protection and the EU**. Disponível em: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/. Acesso em: 27 mar. 2023.

[44] How do the UK's GDPR and EU's GDPR regulation compare? **GDPR EU**, 2023. Disponível em: https://www.gdpreu.org/differences-between-the-uk-and-eu-gdpr-regulations/Acesso em: 26 fev. 2023.

[45] I*bidem*

[46] REINO UNIDO. Information Commissioner's Office, *op. cit*.

projeto de decisão ao Conselho Europeu de Proteção de Dados, que emite seu parecer[47].

Já no Reino Unido, foi estabelecido o *Information Commissioner's Office* ("ICO"), órgão independente, como o responsável por defender os direitos de informação no interesse público, promovendo a transparência dos órgãos públicos e a privacidade dos dados para os indivíduos[48]. Segundo o ICO, a criação de normas corporativas globais para o fornecimento de salvaguardas nos casos de transferências internacionais de dados foi desenvolvida pela legislação da União Europeia e continua fazendo parte da legislação britânica sob o GDPR do Reino Unido[49]. As normas são aprovadas pelo próprio ICO[50].

Nesse sentido, o ICO definiu procedimento facilitado para que os titulares de normas corporativas globais na União Europeia tornassem-se titulares das normas corporativas globais também no Reino Unido[51]. Utilizando-se deste protocolo, mais de 20 grupos corporativos passaram a valer-se de normas corporativas globais no Reino Unido[52]. Depois junho de 2021, mais de 10 grupos empresariais já tiveram suas normas corporativas globais aprovadas pelo ICO sob o GDPR do Reino Unido[53].

Assim, considerando os avanços realizados pelo Reino Unido no âmbito da proteção de dados pessoais, bem como a relevância do ICO como órgão atuante na regulamentação do GDPR do Reino Unido, o presente trabalho busca responder o seguinte problema de pesquisa: de que forma as normas corporativas globais

---

[47] **Binding Corporate Rules (BCR)**. In: EUROPEAN Commission. União Europeia: European Commission, 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#:~:text=Approval%20of%20binding%20corporate%20rules,-Companies%20must%20submit&text=The%20competent%20authority%20communicates%20its,authority%20will%20approve%20the%20BCRs. Acesso em: 26 fev. 2023.

[48] REINO UNIDO. Information Commissioner's Office. **Information Commissioner's Office**. Disponível em: https://www.gov.uk/government/organisations/information-commissioner-s-office. Acesso em: 25 fev. 2023.

[49] REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/. Acesso em: 22 fev. 2023.

[50] *Ibidem*

[51] REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules: BCR Approvals**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/bcr-approvals/. Acesso em: 27 mar. 2023.

[52] REINO UNIDO. Information Commissioner's Office. **List of BCR holders approved pursuant to paragraph 9, part 3, schedule 21 to the DPA 2018**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/bcr-approvals/list-of-bcr-holders-approved-pursuant-to-paragraph-9-part-3-schedule-21-to-the-dpa-2018/. Acesso em: 27 mar. 2023.

[53] REINO UNIDO. **Information Commissioner's Office. List of BCRs approved under UK GDPR**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/bcr-approvals/bcrs-approved-under-uk-gdpr/. Acesso em: 27 mar. 2023.

aprovadas pelo ICO, bem como o seu consolidado procedimento de aprovação, podem contribuir para um futuro modelo brasileiro de normas corporativas globais?

Destarte, o objetivo principal do presente trabalho é investigar as principais contribuições do procedimento de aprovação das normas corporativas globais no Reino Unido, avaliando se as diretrizes presentes nas normas corporativas globais britânicas podem ser adaptadas às demandas específicas do contexto brasileiro. Já os objetivos específicos são: (i.) definir o conceito de transferência internacional de dados pessoais, buscando compreender a forma como este instituto é tratado no GDPR, com especial atenção ao GDPR do Reino Unido, e na LGPD; (ii.) traçar um breve panorama sobre a evolução das bases normativas envolvendo proteção de dados, tanto na União Europeia quanto no Brasil; e (iii.) explicar as normas corporativas globais, relatando como o ICO vem regulamentando o tema. Para tanto, utilizar-se-á o método de pesquisa dedutivo[54], por meio de análise da doutrina pertinente à proteção de dados pessoais tanto no contexto brasileiro quanto europeu, com destaque para a temática das normas corporativas globais.

Por fim, o trabalho será dividido em duas partes. A primeira cuidará das transferências internacionais de dados pessoais de um modo amplo. Para tanto, buscar-se-á conceituar este mecanismo. Além disso, por meio de um breve panorama da evolução das legislações de proteção de dados nos contextos europeu e brasileiro, verificar-se-á de que forma os dois sistemas normativos tratam a transferência internacional de dados pessoais, especialmente no que tange às bases legais e os mecanismos de salvaguardas.

Após, será tratado o instrumento das normas corporativas globais. Além de defini-las, o trabalho abordará de que forma esse mecanismo tem sido regulado pelo ICO. Para tanto, tratar-se-á das normas corporativas globais para controladores de dados pessoais e das normas corporativas globais voltadas aos operadores de dados pessoais. Após, será analisado o instrumento de normas corporativas globais da multinacional Amgen, aprovado pelo ICO pertencente à multinacional. Ao fim,

[54] Em linhas gerais, este método se aproveita de princípios verdadeiros e inquestionáveis para alcançar soluções de forma puramente formal, por meio de operações lógicas. Destarte, a dedução consiste em um tipo de argumentação que busca tornar explícitas verdades particulares contidas em verdades universais. (GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008, p. 9 e CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia cientifica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007, p. 46).

averiguar-se-á de que forma o modelo britânico das normas corporativas globais pode contribuir para um futuro modelo brasileiro.

2 AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

Manuel Castells escreveu, em 1999, que, no último quarto do século XX, surgiu uma nova economia, a qual o sociólogo intitulou “informacional, global e em rede”[55]. Primeiramente, esta economia é informacional porque a competitividade e a produtividade dos agentes são definidas pela capacidade de gerenciamento, processamento e aplicação, de maneira eficiente, da informação baseada em conhecimentos[56]. Ela é global porque assim são organizados os seus componentes, como trabalho, matéria-prima e capital, bem como as suas atividades produtivas, seu consumo e sua circulação[57]. Ainda, é uma economia em rede pois sua produtividade e sua concorrência se dão por meio de uma rede global de interação das redes empresariais[58].

Vale dizer, o que condicionou o crescimento dessa nova economia foi, justamente, a chamada “revolução da tecnologia da informação”[59]. Isto é, ainda que a informação sempre tenha sido um elemento essencial para o crescimento econômico, foi no final do último século que um novo paradigma tecnológico – caracterizado pelo surgimento de novas tecnologias – permitiu que a informação se transformasse no próprio produto da economia[60].

Assim, inaugurou-se o modelo econômico conhecido como “economia digital”[61], viabilizado, primordialmente, pela desregulamentação dos mercados e pelo surgimento de novas tecnologias da informação[62]. Nesse sentido, os fluxos digitais – antes praticamente inexistentes – passaram a impactar o crescimento do PIB mais do que o tradicional comércio de bens[63].

---

[55] CASTELLS, Manuel. **A sociedade em rede**. 6. Ed. São Paulo: Paz e Terra, 1999, p. 119.
[56] *Ibidem*
[57] *Ibidem*
[58] *Ibidem*
[59] *Ibidem*
[60] *Ibidem*
[61] RODRIGUES, Cristina Barbosa; SANTOS, Jessica Mequilaine Correia dos; GAMBA, João Roberto Gorini. Dados pessoais na economia digital: análise dos impactos da proteção de dados no uso de *Big Data* pelo GAFA. **Revista DIGE - Direito Internacional e Globalização Econômica (PUC-SP)**, v. 8, n. 8, p. 183, 2021. Disponível em: https://revistas.pucsp.br/index.php/DIGE/article/view/58318/40073. Acesso em: 20 fev. 2023.
[62] CASTELLS, *op. cit.*, p. 138.
[63] MANYIKA, James et al. Digital globalization: The new era of global flows. **McKinsey Global Institute**, 24 fev. 2016. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows. Acesso em: 20 fev. 2023.

A economia digital permite o fluxo de informações e ideias, e, por conseguinte, os fluxos de dados possibilitam o movimento de bens, serviços, finanças e pessoas[64]. Com efeito, praticamente todos os tipos de transações transfronteiriças apresentam, atualmente, um componente digital[65].

Segundo a pesquisa anual *The Transatlantic Economy 2022: Annual Survey of Jobs, Trade and Investment between the United States and Europe*, elaborada por Daniel S. Hamilton e Joseph Quinlan[66], entre 2020 e 2023, as empresas devem gastar USD 6,8 trilhões em transformação digital[67]. Além disso, projetou-se que, em 2022, 65% do PIB mundial seria digitalizado[68].

Assim, em um mundo com cada vez menos fronteiras comerciais – e com uma economia cada vez mais digitalizada – os fluxos de dados transfronteiriços acabam por ocupar um lugar de destaque[69]. Resta claro, portanto, que, na nova economia digital, o fluxo de dados entre fronteiras é essencial para que as empresas realizem as suas operações. Todavia, não podemos esquecer que o aumento da quantidade de dados pessoais nos ambientes digitais, bem como a sua circulação por diferentes websites, servidores e até mesmo países, coloca em risco os titulares de dados pessoais. Daí a importância de que essas transferências sejam viabilizadas e amparadas pelas legislações de proteção de dados.

Portanto, para que se possa adentrar a pesquisa e investigar as possíveis contribuições das normas corporativas globais britânicas para um futuro modelo brasileiro, necessário, primeiramente, que conceituemos as transferências internacionais de dados pessoais. A partir disso, pretende-se investigar os instrumentos regulatórios desenvolvidos até o momento para garantir uma eficaz proteção de dados nos fluxos transnacionais, principalmente no que tange ao Brasil e

---

[64] MANYIKA, James et al. Digital globalization: The new era of global flows. **McKinsey Global Institute**, 24 fev. 2016. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows. Acesso em: 20 fev. 2023.

[65] *Ibidem*

[66] Hamilton, Daniel S., and Quinlan, Joseph P. **The Transatlantic Economy 2022: Annual Survey of Jobs, Trade and Investment between the United States and Europe**. Washington, DC: Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network, 2022. Disponível em: https://transatlanticrelations.org/wp-content/uploads/2022/03/TE2022_report_HR.pdf. Acesso em: 20 mar. 2023.

[67] *Ibidem*, p. 44.

[68] *Ibidem*

[69] **Mecanismos de Transferência Internacional de Dados. Cláusulas-Padrão Contratuais e Regras Corporativas Vinculantes**. São Paulo: Opice Blum, Bruno e Vainzof Advogados Associados, mar. 2022, p. 4. Disponível em: https://opiceblum.com.br/wp-content/uploads/2022/02/white_paper_transferencia_internacional_de_dados_v.final_.pdf. Acesso em: 20 fev. 2023.

à Europa – com ênfase nos desdobramentos ocorridos no Reino Unido. Após apresentadas as principais intersecções entre os dois arcabouços regulatórios, abordar-se-á as garantias necessárias à transferência internacional de dados pessoais em ambas as legislações para que, no segundo capítulo deste trabalho, tratemos das normas corporativas globais.

2.1 O que são Transferências Internacionais de Dados Pessoais

O legislador brasileiro se ateve a conceituar uma transferência internacional de dados pessoais como a "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro" (art. 5º, XV)[70]. O GDPR do Reino Unido traz, em seu texto, definição igualmente vaga, limitando-se a estabelecer, no art. 44, que qualquer transferência de dados pessoais tratados, ou destinados a tratamento após transferidos para país terceiro ou organização internacional, poderá ocorrer somente se observadas as disposições do Regulamento[71].

Assim, ausentes maiores referências sobre o conceito, necessário que recorramos a entendimentos doutrinários e jurisprudenciais. Em outubro de 2020 foi lançado pela Fundação Getúlio Vargas um "Guia de Proteção de Dados Pessoais sobre Transferência Internacional", cujo objetivo é o fornecimento de informações sobre o gerenciamento de atividades e operações de tratamento de dados[72].

De acordo com o Guia, a transferência internacional de dados implica no uso compartilhado de dados[73]. Por isso, quando agentes localizados em países distintos têm como objetivo o "uso compartilhado de informações de pessoas naturais

---

[70] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023.

[71] **Artigo 44 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 44. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined" (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/44. Acesso em: 01 mar. 2023).

[72] **Guia de Proteção de Dados Pessoais: Transferência Internacional**. São Paulo: FGV, out .2020, p. 4. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Acesso em: 01 mar. 2023.

[73] *Ibidem*

identificadas ou identificáveis para a consecução de determinadas finalidades", resta caracterizada a transferência internacional de dados[74].

Também, a ICO disponibiliza, em seu website, um guia para o GDPR do Reino Unido[75]. Segundo o Órgão, para ser configurada a transferência internacional de dados, as informações devem ser repassadas para um controlador ou operador distinto e legalmente independente daquele enviando os dados[76]. Ou seja: a transferência dos dados pode ser feita para qualquer agente independente do seu remetente, podendo, inclusive, tratar-se de empresa do mesmo grupo corporativo[77].

Como exemplos de atividades que configuram a transferência internacional de dados, temos: (i.) uma troca de e-mails entre um indivíduo no Brasil e outro na África do Sul, nos quais circulam currículos contendo dados pessoais de candidatos a vagas de emprego[78]; (ii.) uma ligação telefônica entre funcionário de empresa estrangeira e seu supervisor, na qual o funcionário informa dados de clientes brasileiros (que adquirem produtos da empresa por meio da internet) ao supervisor que, por sua vez, armazena os dados no sistema de empresa estrangeira[79]; (iii.) o compartilhamento das bases de dados de Recursos Humanos entre empresas do mesmo grupo, localizadas em países diferentes[80]; (iv.) o armazenamento de dados em data centers com localização física em outros territórios[81]; (v.) a terceirização de um serviço de atendimento ao consumidor ("SAC") por meio da contratação de empresa localizada em outro país[82]; (vi.) e a contratação de provedores estrangeiros de computador em serviço de nuvem e de e-mail[83].

---

[74] *Ibidem*

[75] REINO UNIDO. Information Commissioner's Office. **Guide to the UK General Data Protection Regulation (UK GDPR)**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/. Acesso em: 01 mar. 2023.

[76] REINO UNIDO. Information Comissioner's Office. **International transfers**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/. Acesso em: 01 mar. 2023.

[77] *Ibidem*

[78] **Guia de Proteção de Dados Pessoais: Transferência Internacional**. São Paulo: FGV, out .2020, p. 15. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Acesso em: 01 mar. 2023

[79] *Ibidem*

[80] PRADO CHAVES, Luis Fernado. Da Transferência Internacional de Dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice**. LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, p. RL-1.10. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

[81] *Ibidem*

[82] *Ibidem*

[83] *Ibidem*

Por outro lado, importante que diferenciemos a transferência internacional do mero transporte de dados[84]. Isto é, há casos em que, embora os dados sejam transportados entre provedores de internet localizados em diferentes países, não se configura a transferência internacional de dados pessoais, uma vez que não há uso compartilhado desses dados, mas o mero tráfego de dados em alta velocidade[85].

Outro exemplo de caso não considerado transferência internacional de dados pessoais é o de um executivo de multinacional que, ao realizar viagem internacional, acessa, em outro país, seu computador contendo dados dos clientes[86]. Isso porque a simples visualização dos dados em território distinto daquele onde foram coletados não caracteriza uma transferência, uma vez que não há uso compartilhado dos dados entre dois agentes, estando um localizado em lugar distinto. Se, contudo, esses dados forem repassados a terceiro por meio do sistema, será caracterizada a transferência[87].

No mesmo sentido decidiu o Tribunal de Justiça Europeu no Tribunal de Justiça Europeu no Processo C-101/01, caso *Bodil Lindqvist vs. Åklagarkammaren i Jönköping*[88]. A controvérsia tratava do conceito da transferência internacional de dados envolvendo o acesso a páginas de internet hospedadas em país fora da Europa[89]. Ressalta-se, apesar de o julgamento do caso ter ocorrido antes de a Diretiva de Proteção de Dados Pessoais ser revogada pelo GDPR, não foram realizadas mudanças no Regulamento capazes de alterar os entendimentos do julgado[90].

Na ocasião, o Tribunal estabeleceu que os dados pessoais oriundos da União Europeia, carregados por um indivíduo em website, e visualizados em outro país, não configuram transferência internacional de dados[91]. Nesse sentido, os dados não foram transferidos entre essas duas pessoas, mas sim mediante a utilização da

---

[84] **Guia de Proteção de Dados Pessoais: Transferência Internacional**. São Paulo: FGV, out .2020, p. 14. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Acesso em: 01 mar. 2023

[85] *Ibidem*

[86] *Ibidem*, p. 15.

[87] *Ibidem,* p. 15.

[88] PRADO CHAVES, Luis Fernado. Da Transferência Internacional de Dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice**. LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, p. RL-1.10. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

[89] *Ibidem*

[90] *Ibidem*

[91] OPINION OF ADVOCATE GENERAL. **Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping**. TIZZANO: InfoCuria Jurisprudência, 19 September 2002. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=47672&doclang=EN

infraestrutura de informática do fornecedor de serviços de hospedagem onde a página está armazenada[92].

Portanto, caso o Tribunal interpretasse o art. 25 da Diretiva de Proteção de Dados Pessoais[93] de modo que sempre que carregados dados pessoais em um website, seria configurada a transferência internacional de dados a todos os países que dispõem dos meios técnicos necessários para acessar o website[94]. Assim, os Estados da União Europeia precisariam impedir o carregamento de dados pessoais na internet sempre que um país terceiro possuidor dos meios de visualizar o dado não obtivesse o nível adequado de proteção de dados, nos moldes do art. 25, 4, da Diretiva de Proteção de Dados Pessoais, correspondente ao art. 45 do GDPR[95].

É dizer: com base na jurisprudência europeia, o mero acesso à aplicação de internet não constitui transferência internacional de dados[96]. Caso fosse considerada, banalizar-se-ia o conceito, definindo como regime jurídico geral um regime que, na verdade, é especial[97].

Vale dizer, ainda, que se a transferência de dados é feita entre dois indivíduos contratados pelo mesmo empregador, ou de um contratante para um contratado – estando o destinatário dos dados em território distinto do remetente – não resta

---

92 PRADO CHAVES, *op. cit.*

92 *Ibidem*

93 **Artigo 25 da Directiva 95/46/CE do Parlamento Europeu e do Conselho.** Artigo 25º 1. Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objecto de tratamento, ou que se destinem a ser objecto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adoptadas nos termos das outras disposições da presente directiva, o país terceiro em questão assegurar um nível de protecção adequado. 2. A adequação do nível de protecção oferecido por um país terceiro será apreciada em função de todas os circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país. 3. Os Estados-membros e a Comissão informar-se-ão mutuamente dos casos em que considerem que um país terceiro não assegura um nível de protecção adequado na acepção do nº 2 (UNIÃO EUROPEIA. **Diretiva 95/46/CE** do Parlamento Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 23 fev. 2023).

94 PRADO CHAVES, Luis Fernado. Da Transferência Internacional de Dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice**. LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, p. RL-1.10. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

95 *Ibidem*

96 *Ibidem*

97 *Ibidem*

configurada a transferência internacional de dados, uma vez que ambas as pessoas são subordinadas a uma mesma pessoa jurídica[98].

Em suma, podemos definir a transferência internacional de dados pessoais como um envio de informações relacionadas a pessoa natural, identificada ou identificável (art. 5º, I)[99] realizado entre dois agentes legalmente independentes, localizados em territórios distintos, com o objetivo de utilizar tais informações de modo compartilhado. Como sabemos, cada dia mais, cresce a quantidade de tais transferências, tendo em vista a globalização da economia e a descentralização da internet. Para que seja assegurada a proteção dos dados pessoais ao longo desse processo, foram e estão sendo criadas diversas ferramentas regulatórias e acordos internacionais estabelecendo regras para as transferências internacionais de dados pessoais, visando a proteção dos direitos dos titulares de dados pessoais em diferentes jurisdições.

2.1.1 Controladores e Operadores

Tanto a LGPD – em seu art. 5º, VI e VII[100] – quanto o GDPR do Reino Unido – em seu art. 4º (7) e (8)[101] – definem os agentes de tratamento de dados pessoais: controlador e operador. Segundo o art. 4º (7), do GDPR do Reino Unido, um controlador é uma pessoa física ou jurídica, autoridade pública, agência ou outro órgão que, sozinho ou em conjunto com outros, determina as finalidades e os meios do tratamento de dados pessoais[102]. Essa definição vai ao encontro do determinado no art. 5º, VI, da LGPD, que conceitua o controlador como “pessoa natural ou jurídica,

---

[98] REINO UNIDO. Information Commissioner´s Office. **International transfers**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/. Acesso em: 02 mar. 2023.

[99] **Artigo 5º, I, da Lei Geral de Proteção de Dados.** Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; (...) (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023).

[100] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023.

[101] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/4. Acesso em: 23 fev. 2023.

[102] **Artigo 4º (7) do General Data Protection Regulation – UK.** Tradução nossa, do original: “Article 4. For the purposes of this Regulation: (...) (7) ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (...) (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/4. Acesso em: 01 mar. 2023).

de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"[103].

O operador, por sua vez, é definido no art. 4º (8), do GDPR do Reino Unido, como a pessoa natural ou jurídica, autoridade pública, agência ou outro órgão que trata os dados pessoais em nome do controlador[104]. Assim também a LGPD caracteriza o conceito, como "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VI)[105].

Destarte, quem decide "por que" e "como" os dados pessoais devem ser tratados, atua como controlador dos dados. O operador, por sua vez, trata os dados em nome dessa empresa. Normalmente, ele atua como um terceiro, externo ao controlador[106]. Todavia, em grupos de empresas, é possível que uma empresa do grupo seja a controladora e outra empresa, do mesmo grupo, seja a operadora[107]. Além disso, deve-se ressaltar que há situações em que uma entidade atue como controladora, enquanto, em outras, atua como operadora[108]. Inclusive, a mesma entidade pode atuar como ambos os agentes simultaneamente[109].

Como exemplo, pode-se citar uma empresa de telecomunicações que contrata serviço terceirizado para fazer a folha de pagamento dos seus funcionários. A empresa de telecomunicações é responsável por informar à empresa da folha de pagamento as informações sobre os seus funcionários e sobre os salários, para que o pagamento seja realizado. Por outro lado, a empresa de folha de pagamentos fornece um software e armazena os dados pessoais dos funcionários. Portanto,

---

[103] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023.

[104] **Artigo 4º (8) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 4. For the purposes of this Regulation: (...) (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (...) (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/4. Acesso em: 01 mar. 2023).

[105] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023.

[106] **What is a data controller or a data processor?** In: EUROPEAN Commission. União Europeia: European Commission, 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en. Acesso em: 20 fev. 2023.

[107] *Ibidem*

[108] **What is a data controller or a data processor?** In: EUROPEAN Commission. União Europeia: European Commission, 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en. Acesso em: 20 fev. 2023.

[109] *Ibidem*

enquanto a empresa de telecomunicações é a controladora dos dados pessoais, a empresa de folha de pagamentos é a operadora[110].

O GDPR do Reino Unido lista, nos arts. 24 e 25, como obrigações do controlador: (i.) a implementação de medidas técnicas e organizacionais para garantir e demonstrar que o tratamento de dados ocorre em concordância com o regulamento; (ii.) a implementação de medidas técnicas e organizacionais projetadas para possibilitar o respeito aos princípios de proteção de dados, como a pseudonimização dos dados; (iii.) a implementação de medidas técnicas e organizacionais para garantir que somente os dados pessoais necessários para cada finalidade específica do tratamento sejam processados; (iv.) a implementação de políticas apropriadas de proteção de dados pelo responsável pelo tratamento e (v.) a adesão aos códigos de conduta aprovados ou aos mecanismos de certificação aprovados[111-112]. Além disso, todos os controladores – e, sempre que aplicável, os representantes dos controladores – deverão manter um registro das atividades de processamento sob sua

---

[110] *Ibidem*

[111] **Artigo 24 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 24. Responsibility of the controller 1.Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2.Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3.Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller˜ (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/24. Acesso em: 01 mar. 2023).

[112] **Artigo 25 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 25. Data protection by design and by default. 1.Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. 2.The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. 3.An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article" (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/25. Acesso em: 23 fev. 2023).

responsabilidade, conforme o art. 30 do GDPR do Reino Unido[113]. No mais, constitui dever do controlador a notificação, de forma célere, de incidentes de violação de dados pessoais ao ICO e aos titulares de dados pessoais, bem como a elaboração de relatórios de impacto à proteção de dados pessoais, nos termos do art. 35 da mesma Lei[114].

Sobre os operadores, o GDPR do Reino Unido aduz, no art. 28, que: (i.) devem oferecer garantias suficientes para implementar medidas técnicas e organizacionais adequadas; (ii.) estão proibidos de contratar outro operador sem autorização prévia, específica ou geral por escrito do controlador; (iii) devem notificar os controladores sem demora indevida de violação de dados pessoais que venham a tomar conhecimento e; (iv.) têm seus serviços regidos por contrato ou ato jurídico, vinculativo e responsável por estabelecer as características do tratamento, como o objeto, a duração, a natureza, a finalidade, os tipos de dados pessoais, as categorias dos

[113] **Artigo 30 (1) do General Data Protection Regulation – UK.** Tradução nossa, do original: “Article 30. Records of processing activities. 1.Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. (…)” (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/30. Acesso em: 23 fev. 2023).

[114] **Artigo 35 do General Data Protection Regulation – UK.** Tradução nossa, do original: “Article 35. Data protection impact assessment. 1.Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks (…)˜ (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/35. Acesso em: 23 fev. 2023).

titulares de dados e as obrigações e direitos do responsável pelo tratamento[115]. Ademais, conforme o art. 29 do GDPR do Reino Unido, o operador ou outra pessoa ou entidade agindo sob sua autoridade, ou do controlador, não poderá tratar os dados pessoais por outras razões que não determinação legal ou ordens do controlador[116]. Outrossim, conforme o art. 30 (2), cada operador e, quando aplicável, seu representante, deve manter um registro de todas as atividades de tratamento de dados pessoais realizadas em nome do controlador[117].

---

[115] **Artigo 28 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 28. Processor. 1.Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject. 2.The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. 3.Processing by a processor shall be governed by a contract or other legal act under **[F1**domestic law**]**, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a)processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by **[F2**domestic law**]**; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; (b)ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c)takes all measures required pursuant to Article 32; (d)respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; (e)taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f)assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor; (g)at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless **[F3**domestic law**]** requires storage of the personal data; (h)makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. (...)" (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/28. Acesso em: 23 fev. 2023).

[116] **Artigo 29 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 29. Processing under the authority of the controller or processor. The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by **[F1**domestic law**]**" (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/29. Acesso em: 23 fev. 2023).

[117] **Artigo 30 (2) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 30. Records of processing activities. (…) 2.Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (...)" (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/30. Acesso em: 23 fev. 2023).

Ainda, no que tange a ambos os agentes de tratamento de dados pessoais, tem-se que estes devem, de acordo com o GDPR do Reino Unido: (i.) designar, por escrito, representantes no Reino Unido, quando não estiverem localizados no país, nos termos do art. 27[118]; (ii.) cooperar com o ICO sempre que necessário, conforme o art. 31[119]; (iii.) implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, tais como a pseudonimização, a utilização de criptografia, a capacidade de restaurar a disponibilidade e acesso a dados pessoais em caso de incidente físico ou técnico, entre outros, como disposto no art. 32 (1)[120]; (iv.) designar encarregado de dados pessoais e assegurar que este

[118] **Artigo 27 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 27. Representatives of controllers or processors not established in [F1the United Kingdom] 1.Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in **[F2**the United Kingdom**]**. 2.The obligation laid down in paragraph 1 of this Article shall not apply to: (a)processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b)a public authority or body.**F3**3.. . . . . 4.The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, **[F4**the Commissioner**]** and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation. 5.The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves" (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/27. Acesso em: 23 fev. 2023).

[119] **Artigo 31 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 31. Cooperation with [F19the Commissioner] The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with [F20the Commissioner in the performance of the Commissioner's tasks] (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/31. Acesso em: 23 fev. 2023).

[120] **Artigo 32 (1) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 32. Security of processing. 1.Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a)the pseudonymisation and encryption of personal data; (b)the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c)the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d)a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (…) (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/32. Acesso em: 23 fev. 2023).

esteja envolvido nas questões relacionadas à proteção de dados pessoais, conforme os arts. 37 (1)[121] e 38 (1)[122].

Já a LGPD dispõe, dentre as obrigações dos controladores: (i.) a elaboração de relatório de impacto à proteção de dados pessoais, conforme o art. 38[123]; (ii.) a indicação de encarregado pelo tratamento de dados pessoais, nos termos do art. 41[124]; e (iii.) a comunicação à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, segundo o art. 48[125]. No que tange ao operador, é necessário que este realize o tratamento de dados pessoais segundo as instruções dadas pelo controlador, segundo o art. 39[126].

Sobre os dois agentes de tratamento, a Lei brasileira determina que devem manter registro das operações de tratamento de dados pessoais realizadas, conforme o art. 37[127]. Além disso, os agentes que, no âmbito do tratamento de dados pessoais,

---

[121] **Artigo 37 (1) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 37. Designation of the data protection officer. 1. The controller and the processor shall designate a data protection officer in any case where: (a)the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b)the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or **[X1**(c)the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.**]** (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/37. Acesso em: 23 fev. 2023).

[122] **Artigo 38 (1) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 38. Position of the data protection officer. 1.The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/38. Acesso em: 23 fev. 2023).

[123] **Artigo 38 da Lei Geral de Proteção de Dados.** Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023).

[124] **Artigo 41 da Lei Geral de Proteção de Dados.** Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais (...) (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023).

[125] **Artigo 48 da Lei Geral de Proteção de Dados.** Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (...) (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023).

[126] **Artigo 39 da Lei Geral de Proteção de Dados.** Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023).

[127] **Artigo 37 da Lei Geral de Proteção de Dados.** Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023).

causarem dano patrimonial, moral, individual ou coletivo, devem repará-lo, nos termos do art. 42[128], exceto quando: (i.) não realizarem o tratamento de dados pessoais que lhes é atribuído; (ii.) não tiverem violado a legislação de proteção de dados; ou (iii.) o dano for decorrente de culpa exclusiva do titular dos dados ou de terceiro, conforme o art. 43, da LGPD[129]. No mais, os agentes respondem aos danos ocasionados por violação de segurança quando deixarem de adotar medidas de segurança previstas em lei, nos termos do art. 46[130].

Outrossim, os controladores e operadores de dados pessoais podem formular regras de boas práticas e de governança que estabeleçam as condições de organização; o regime de funcionamento; os procedimentos, incluindo reclamações e petições de titulares; as normas de segurança; os padrões técnicos; as obrigações específicas para os diversos envolvidos no tratamento; as ações educativas; os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, conforme o art. 50, da LGPD[131].

Verifica-se que, ainda que ambas as legislações sejam bastante semelhantes, há diferenças que merecem ser, aqui, pontuadas. Primeiramente, tem-se, no art. 28 (3), do GDPR do Reino Unido, que o tratamento de dados pessoais por um operador se dá por meio de contrato ou outro instrumento legal[132]. Enquanto isso, a LGPD dispõe somente que o operador deve realizar o tratamento de acordo com as instruções fornecidas pelo controlador, em seu art. 39[133].

---

[128] **Artigo 42 da Lei Geral de Proteção de Dados.** Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023).

[129] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023.

[130] **Artigo 46 da Lei Geral de Proteção de Dados.** Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (...) (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023).

[131] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mar. 2023.

[132] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/28. Acesso em: 23 fev. 2023.

[133] **Artigo 39 da Lei Geral de Proteção de Dados.** Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023).

Além disso, percebe-se a existência de diferenças no que tange à responsabilização dos agentes de tratamento. Isso porque, de acordo com a LGPD, art. 42, §1º, II[134][135], a responsabilidade entre controlador e operador, principalmente nos casos de controladoria conjunta – que serão explicados posteriormente – é solidária. Em contrapartida, o GDPR não trata especificamente deste assunto, estabelecendo apenas que a responsabilidade do controlador pode ser limitada às medidas que ele tenha tomado em relação ao tratamento dos dados[136]. Por conseguinte, no GDPR, a responsabilidade do controlador não é uma responsabilidade solidária irrestrita[137].

Outro ponto relevante sobre as duas legislações é a figura dos *joint controllers*, ou co-controladores. Conforme o art. 26 do GDPR do Reino Unido, dois ou mais controladores podem determinar, de forma conjunta, as finalidades e os meios para o tratamento de dados pessoais[138]. Nesse caso, as partes devem estabelecer as respectivas responsabilidades pelo cumprimento das obrigações. No entanto, independentemente desses acordos, cada controlador permanece responsável pelo

---

[134] **Artigo 42, §1º, II, da Lei Geral de Proteção de Dados.** Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: (...) II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei (...) (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023).

[135] MIGUEL, Bruno. **Descomplicando os agentes de tratamento com base na LGPD.** Migalhas Trabalhista, São Paulo, 13 out. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalha-trabalhista/356737/descomplicando-os-agentes-de-tratamento-com-base-na-lgpd. Acesso em: 27 mar. 2023.

[136] RAMOS, Pedro Henrique Soares; MONTEIRO, Renato Leite. **A Regulação Europeia de Proteção de Dados e o Impacto na Publicidade Online**. Disponível em: https://baptistaluz.com.br/regulacao-europeia-de-protecao-de-dados-e-o-impacto-na-publicidade-online/. Acesso em 23 mar. 2023.

[137] RAMOS, Pedro Henrique Soares; MONTEIRO, Renato Leite. **A Regulação Europeia de Proteção de Dados e o Impacto na Publicidade Online**. Disponível em: https://baptistaluz.com.br/regulacao-europeia-de-protecao-de-dados-e-o-impacto-na-publicidade-online/. Acesso em 23 mar. 2023.

[138] **Artigo 26 do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 26. Joint controllers. 1.Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by **[F1**domestic law**]**. The arrangement may designate a contact point for data subjects. 2.The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject. 3.Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/26. Acesso em: 23 fev. 2023).

cumprimento de todas as obrigações dos controladores sob a GDPR do Reino Unido[139]. Ainda, as principais deliberações desse arranjo devem ser disponibilizados aos titulares de dados[140]. Assim, os indivíduos podem buscar compensação de co-controladores exatamente como fariam em relação a um único controlador: cada co-controlador será responsável por todo o dano causado pelo tratamento, exceto se provar não ser responsável pelo evento que originou o dano[141].

Ainda que a LGPD não traga o conceito de controladoria conjunta de forma explícita, aduz, em seu art. 42, §1º, II[142], a responsabilidade solidária de mais de um controlador, o que leva a inferir a existência desta figura em nosso sistema normativo. Conforme Guia Orientativo disponibilizado pela Autoridade Nacional de Proteção de Dados ("ANPD")[143], podemos verificar a existência de co-controladoria quando, cumulativamente: (i.) mais de um controlador exercer poder de decisão sobre o tratamento de dados pessoais; (ii.) houver interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento de dados pessoais; e (iii.) dois ou mais controladores tomarem decisões comuns sobre as finalidades e elementos essenciais deste tratamento[144]. No mais, o Guia estabelece que, se adaptarmos a concepção europeia à LGPD, podemos compreender a controladoria conjunta como:

> A determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD[145].

---

[139] REINO UNIDO. Information Commissioner´s Office. **What does it mean if you are joint controllers?** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/. Acesso em: 27 mar. 2023.

[140] REINO UNIDO. Information Commissioner´s Office. **What does it mean if you are joint controllers?** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/. Acesso em: 27 mar. 2023.

[141] *Ibidem*

[142] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 26 mar. 2023.

[143] BRASIL. Autoridade Nacional de Proteção de Dados. **Guia dos Agentes de Tratamento de Dados Pessoais. Brasília: ANPD, 2021**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 27 mar. 2023.

[144] *Ibidem*, p. 13.

[145] *Ibidem*, p. 13.

Segundo Marcel Leonardi, a caracterização do controlador é de suma importância no âmbito das transferências internacionais[146]. Isso porque as transferências internacionais de dados pessoais geram maiores riscos aos direitos e liberdades dos titulares de dados, de modo que, não sendo implementadas medidas técnicas e organizacionais adequadas, os incidentes de segurança podem facilmente ocorrer[147]. Destarte, ao definir como e por que tratar dados pessoais, o controlador deve observar quais mecanismos de transferência internacional são os mais apropriados entre aqueles disponíveis na LGPD, além de avaliar como os operadores contratados realizam o tratamento de dados pessoais fora do país[148].

Em suma, os agentes de tratamento de dados pessoais são responsáveis por garantir a integridade e segurança dos dados pessoais durante o seu tratamento. Assim, no caso de os dados pessoais serem transferidos internacionalmente, os agentes devem respeitar os princípios de proteção de dados e preservar os direitos dos titulares. Dentre tais direitos, destaca-se o da transparência, pois é imprescindível que os agentes forneçam informações claras e precisas aos titulares de dados sobre o tratamento ao qual seus dados são submetidos[149]. Ainda, os agentes de tratamento de dados pessoais devem observar e zelar pelos procedimentos de segurança envolvidos no tratamento das informações transferidas, garantindo que as partes envolvidas atuem em concordância às legislações protetivas e que o fluxo transfronteiriço de dados seja realizado de forma segura.

2.2 A tutela da Transferência Internacional de Dados no GDPR e na LGPD

Para que possamos verificar as principais intersecções, semelhanças e diferenças entre a LGPD e o GDPR do Reino Unido no que tange às transferências internacionais de dados pessoais – e, posteriormente, às normas corporativas globais

---

[146] LEONARDI, Marcel. Transferência internacional de dados pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 301. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

[147] **Guia de Proteção de Dados Pessoais: Transferência Internacional**. São Paulo: FGV, out .2020, p. 13. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Acesso em: 01 mar. 2023.

[148] *Ibidem*, Leonardi, p. 301.

[149] **Guia de Proteção de Dados Pessoais: Transferência Internacional**. São Paulo: FGV, out .2020, p. 13. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Acesso em: 01 mar. 2023.

– importante que tracemos um panorama da evolução das legislações de proteção de dados na Europa e no Brasil.

2.2.1 A evolução da Proteção de Dados no direito europeu

Na Europa, as primeiras tentativas de elaboração de normas de proteção de dados ocorreram na década de 1970, com a Lei de Proteção de Dados Pessoais do Lande de Hesse, *Hessisches Datenschutzgesetz*, na então Alemanha, e a Lei Sueca sobre o Controle de Banco de Dados, em 1970 e 1973, respectivamente[150]. Após, outros países europeus passaram a legislar sobre o tema, como a França, a Dinamarca, a Áustria, a Noruega, Luxemburgo e a Islândia[151].

No ano de 1973, foi solicitado, pela Assembleia Consultiva do Conselho Europeu, ao Comitê de Ministros, que fossem adotadas recomendações relacionando o fenômeno das novas técnicas de coleta de informações com o Art. 8º da Convenção Europeia para a salvaguarda dos Direitos do Homem e das Liberdades Fundamentais, que trata do direito ao respeito pela vida privada e familiar[152][153]. Por isso, em 1973, publicou-se a Resolução 74 (29), sobre a Proteção da Privacidade dos Bancos de Dados Eletrônicos Individuais vis-a-vis no Setor Público, adotada pelo Comitê de Ministros em setembro de 1974[154]. A Resolução recomendou aos países europeus que adotassem princípios mínimos na matéria de proteção de dados, a fim de, futuramente, realizar convenção para aprofundar os pontos comuns em seus direitos internos[155].

A aprovação da Resolução revelou que a abordagem do tema apenas pelo direito interno não era suficiente, tendo em vista a possível transnacionalidade da

---

[150] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.2. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.2. Acesso em: 10 mar. 2023.

[151] *Ibidem*

[152] UNIÃO EUROPEIA. Council of Europe. **Convenção Europeia dos Direitos do Homem**. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf. Acesso em: 20 fev. 2023.

[153] DONEDA, *op. cit.*

[154] UNIÃO EUROPEIA. Council of Europe (Committee of Ministers). **Resolution (74) 29**, on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector, 20 September 1974. Disponível em: https://rm.coe.int/16804d1c51 Acesso em 21.03.2023.

[155] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.2. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.2. Acesso em: 10 mar. 2023.2

coleta e tratamento dos dados pessoais[156]. Por conseguinte, em 1978, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) formou um grupo de especialistas em tráfego transfronteiriço de dados para confeccionar normativa modelo sobre o tema[157]. Deste trabalho, originaram-se as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[158] – Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais –, em 1980, revisitadas em 2013[159]. Apesar de não ser vinculante, o documento se tornou referência no tema, uma vez que é obrigação dos países membros da OCDE a adaptação das suas legislações às Diretrizes[160].

Também na década de 1980, o Conselho da Europa elaborou a *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 108/1981[161] – Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais –, a qual incentivou os países membros do Conselho da Europa e os signatários da Convenção a tutelar o tema do tratamento de dados pessoais, compreendendo a proteção de dados como um tema ligado aos direitos humanos[162]. Vale dizer que países latino-americanos, dentre eles Argentina, México e Uruguai também ratificaram a Convenção[163]. Depois da Convenção, diversos Estados europeus legislaram sobre o tema pela primeira vez, ou adequaram suas normas já existentes a ela[164].

Alguns anos mais tarde, em 1994, com o Acordo TRIPS – sobre aspectos dos Direitos de Propriedade Intelectual relacionais ao Comércio – ganhou força a ideia de

---

156 DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.2. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.2. Acesso em: 10 mar. 2023.2

156 *Ibidem*

157 *Ibidem*

158 ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. [S.l.], 2013. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acesso em: 28 mar. 2023.

159 *Ibidem*, DONEDA, p. RB-3.2.

160 *Ibidem*, DONEDA, p. RB-3.2.

161 UNIÃO EUROPEIA. Council of Europe. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 28 mar. 2023.

162 *Ibidem*, DONEDA, p. RB-3.2.

163 *Ibidem*, DONEDA, p. RB-3.2.

164 DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.2. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.2. Acesso em: 10 mar. 2023.

um modelo comum de proteção de dados na Europa[165]. O Acordo TRIPS impediu tentativas de estabelecer a utilização de dados pessoais como produto a ser comercializado, uma vez que reconheceu a capacidade dos estados signatários de elaborarem as suas disciplinas próprias sobre a matéria, sem sujeição à sanções[166].

Finalmente, em 1995, foi estruturado o modelo regulatório europeu de proteção de dados sob a Diretiva 95/46/EC, do Parlamento Europeu e do Conselho[167], a Diretiva de Proteção de Dados Pessoais, que, por sua vez, deveria ser transposta para a legislação interna de cada um dos Estados membros da União Europeia[168]. A Diretiva diz respeito à proteção das pessoas no que tange ao tratamento de dados pessoais e à livre circulação dos dados[169].

Vale dizer, diretivas, na União Europeia, são atos legislativos que fixam um objetivo geral para todos os Estados-membros[170]. Assim, cabe a cada Estado-membro a adaptação das diretivas à sua legislação interna[171]. Alguns exemplos de diretivas emitidas na União Europeia são: (i.) a Diretiva 2019/790, do Parlamento Europeu e do Conselho[172], sobre direitos autorais no Mercado Único Digital, aprovada em 2019, cujo objetivo é atualizar as leis de direitos autorais para a era digital[173]; e (ii.) a Diretiva 2018/2001, do Parlamento Europeu e do Conselho[174], sobre energias renováveis, aprovada em 2018 para estabelecer metas de uso de energia nos Estados-membros[175].

---

[165] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.2. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.2. Acesso em: 10 mar. 2023.
[166] *Ibidem*
[167] *Ibidem*
[168] *Ibidem*
[169] *Ibidem*
[170] UNIÃO EUROPEIA. **Tipos de legislação**. Disponível em: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt. Acesso em: 24 mar. 2023.
[171] *Ibidem*
[172] UNIÃO EUROPEIA. **Diretiva 2019/790** do Parlamento Europeu e do Conselho relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE, de 17 de abril de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0790&from=PT. Acesso em: 23 fev. 2023.
[173] *Ibidem*
[174] UNIÃO EUROPEIA. **Diretiva 2018/2001** do Parlamento Europeu e do Conselho relativa à promoção da utilização de energia de fontes renováveis (reformulação), de 11 de abril de 2018. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L2001&from=ES. Acesso em: 23 fev. 2023.
[175] *Ibidem*

Diferentemente da Convenção anterior, a Diretiva impôs aos legisladores a obrigação de aprovar normas de acordo com o seu conteúdo[176]. No mais, tal como a Convenção, a Diretiva fez, em seu texto, alusão aos direitos fundamentais[177], não deixando, todavia, de explicitar o viés econômico da circulação dos dados pessoais, mencionando "a necessidade de proporcionar a livre circulação de "pessoas, mercadorias, serviços e capitais"[178].

Ainda, é importante salientar que a Diretiva estabeleceu a relação do tratamento e da utilização dos dados pessoais com princípios, apresentando estes como norteadores para a defesa dos interesses a serem protegidos[179]. Também a Diretiva se ocupou da remessa de dados para outros países e territórios, regulando-os pelo princípio da equivalência[180]. É dizer: a transferência de dados pessoais para outros locais deveria ocorrer somente quando o destinatário fosse capaz de assegurar um nível de proteção de dados considerado adequado[181].

Em 2002, promulgou-se a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho[182], que buscou regulamentar a proteção de dados pessoais especificamente nos serviços de comunicação eletrônica[183]. A nova Diretiva não inovou o modelo já presente na Diretiva de Proteção de Dados Pessoais, mas obteve êxito ao fornecer ferramentas para adequar suas finalidades à realidade tecnológica da comunicação em rede[184].

---

[176] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.2. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.2. Acesso em: 10 mar. 2023.

[177] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.3. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.3. Acesso em: 10 mar. 2023.

[178] UNIÃO EUROPEIA. **Diretiva 2018/2001** do Parlamento Europeu e do Conselho relativa à promoção da utilização de energia de fontes renováveis (reformulação), de 11 de abril de 2018. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L2001&from=ES. Acesso em: 23 fev. 2023.

[179] *Ibidem*, DONEDA, p. RB-3.3.

[180] *Ibidem*, DONEDA, p. RB-3.3.

[181] *Ibidem*, DONEDA, p. RB-3.3.

[182] UNIÃO EUROPEIA. **Diretiva 2002/58/CE** do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), de 12 junho de 2002. Disponível em: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_pt.pdf. Acesso em: 01 mar. 2023.

[183] *Ibidem*, DONEDA, p. RB-3.3.

[184] *Ibidem*, DONEDA, p. RB-3.3.

Anos mais tarde, a fim de desfragmentar o sistema europeu de proteção de dados, bem como atualizar a disciplina, entrou em vigor o GDPR[185]. O Regulamento foi responsável por trazer uniformidade para a legislação europeia de proteção de dados, uma vez que dispõe de aplicabilidade direta em todos os Estados-membros da União Europeia[186].

Diferentemente das diretivas, os regulamentos são atos legislativos vinculativos[187]. Portanto, eles devem ser aplicados a todos os países da União Europeia de modo uniforme[188]. Em resumo, ao contrário das diretivas – que estabelecem um objetivo a ser alcançado pelos Estados-Membros – os regulamentos estabelecem regras específicas que se aplicam a todos os Estados-Membros da União Europeia. As diretivas oferecem flexibilidade para os Estados-Membros escolherem as melhores maneiras de implementá-las em suas legislações nacionais, enquanto os regulamentos têm aplicação direta e uniforme em toda a União Europeia.

Infere-se, contudo, que a aplicação direta do GDPR não constitui impedimento para a coexistência de legislações nacionais sobre proteção de dados nos países membros da União Europeia[189]. De qualquer sorte, em razão de não serem mais fonte direta à matéria, estas leis nacionais tratam, primordialmente, de fatores operacionais ou lacunas deixadas pelo GDPR[190].

Assim, o GDPR, junto da Diretiva 2016/680 sobre proteção de dados em atividades de investigação criminal e execução penal e da normativa sobre comunicações eletrônicas, a *ePrivacy Regulation*[191] – que está, atualmente, sendo reelaborada, com base na antiga Diretiva 2002/58/CE (atinente à privacidade e às comunicações eletrônicas) – configuram o padrão mínimo a ser seguido pelos países da União Europeia no tocante à proteção de dados[192].

---

[185] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.1. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.1. Acesso em: 10 mar. 2023.

[186] *Ibidem,* DONEDA, p. RB-3.1.

[187] UNIÃO EUROPEIA. **Tipos de legislação**. Disponível em: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt. Acesso em: 24 mar. 2023.

[188] *Ibidem*

[189] *Ibidem,* DONEDA, p. RB-3.1.

[190] *Ibidem,* DONEDA, p. RB-3.1.

[191] **Proposal for an ePrivacy Regulation**. União Europeia: European Commission, 2023. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation. Acesso em: 20 fev. 2023.

[192] DONEDA, *op. cit*, p. RB-3.2.

Por fim, nota-se que as bases normativas europeias repercutem no cenário internacional, que, cada vez mais, requer padrões legislativos para sustentar o crescente fluxo internacional de dados[193]. Isso se dá tanto porque o modelo europeu é o mais desenvolvido na matéria de proteção de dados, quanto porque a legislação impede que os países europeus enviem dados a estados que não demonstrem um nível adequado de proteção de dados[194], salvo com a apresentação de mecanismos de salvaguarda, ou determinações legais, que serão mencionadas posteriormente.

2.2.1.1 O GDPR do Reino Unido

Como se sabe, a formação da União Europeia envolveu mudanças no ordenamento jurídico dos países membros[195]. É dizer: os ordenamentos nacionais foram uniformizados com o intuito de diminuir as divergências entre as legislações nacionais e promover os valores norteadores da União Europeia[196].

O Reino Unido aderiu à Convenção 108 de 1981, sobre a proteção dos indivíduos com relação ao processamento automatizado de dados pessoais[197] e promulgou o seu *Data Protection Act* em 1984, estabelecendo como autoridade de proteção de dados o *Data Protection Registrar*, que posteriormente integrou-se ao ICO[198].

Ressalta-se que o *Data Protection Act* de 1984 dispunha de efeitos limitados, já que tratava apenas de dados armazenados em computadores, e não cuidava da proteção de dados como uma questão de privacidade[199]. Contudo, aos poucos o *Data Protection Registrar* e o Tribunal de Proteção de Dados – também criado por meio da

---

[193] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.13. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.13. Acesso em: 10 mar. 2023.

[194] *Ibidem*

[195] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, p. RB-3.2. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.2. Acesso em: 10 mar. 2023.

[196] *Ibidem*

[197] *Ibidem*

[198] *Ibidem*

[199] What is Freedom of Information & Data Protection? **The Constitution Unit, London**, 2023. Disponível em: https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/what-freedom-information-data-protection#:~:text=The%20development%20of%20Data%20Protection,to%2Ddate%20and%20lawfully%20used. Acesso em: 24 mar. 2023.

Lei – formaram jurisprudência que melhorou os padrões do tratamento de dados pessoais, especialmente por meio da aplicação do princípio geral de justiça como forma de exigir transparência dos usuários de dados e um certo grau de controle por parte dos indivíduos[200].

Após a promulgação da Diretiva de Proteção de Dados Pessoais, foi publicado um novo *Data Protection Act* pelo Reino Unido, em 1998[201]. Esta Lei transpôs de maneira fiel as disposições da Diretiva, mas, como não tratou de certas dificuldades práticas, foi seguida de 17 Instrumentos Estatutários para ser aplicada[202].

Como popularmente sabido, já em 1973, o Reino Unido entrou na União Europeia que, à época Comunidade Econômica Europeia[203]. Todavia, no ano de 2016, o país optou pela saída do bloco econômico por meio de referendo[204]. A retirada foi formalizada em 31 de janeiro de 2020[205]. Como forma de preparar-se para a retirada, o governo britânico adotou, em 2018, a Lei de Retirada, ou o *Withdrawal*, no qual incorporou uma série de leis da União Europeia em sua legislação interna, recepcionando o GDPR em sua totalidade[206].

No mesmo dia em que o GDPR entrou em vigor, em 25 de maio de 2018, o Reino Unido promulgou seu novo *Data Protection Act*, que substituiu o de 1998[207]. Ele foi emendado em 01 de janeiro de 2021 para refletir o status do Reino Unido fora da União Europeia[208]. Também em 01 de janeiro de 2021, o Reino Unido substituiu o GDPR pelo "UK GDPR", o GDPR do Reino Unido[209].

O GDPR do Reino Unido estabelece os princípios, direitos e obrigações para o processamento de dados no país, com base no GDPR – que era aplicado no Reino

---

[200] What is Freedom of Information & Data Protection? **The Constitution Unit, London**, 2023. Disponível em: https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/what-freedom-information-data-protection#:~:text=The%20development%20of%20Data%20Protection,to%2Ddate%20and%20lawfully%20used. Acesso em: 24 mar. 2023.

[201] *Ibidem*

[202] *Ibidem*

[203] Brexit: a saída do Reino Unido da União Europeia. **Brasil Escola**, 2023. Disponível em: https://brasilescola.uol.com.br/historiag/brexit-ou-saida-inglaterra-uniao-europeia.htm. Acesso em: 26 fev. 2023.

[204] *Ibidem*

[205] BREXIT. In: BRITANNICA. Londres: Britannica, 2023. Disponível em: https://www.britannica.com/topic/Brexit. Acesso em: 20 fev. 2023.

[206] How do the UK's GDPR and EU's GDPR regulation compare? **GDPR EU**, 2023. Disponível em: https://www.gdpreu.org/differences-between-the-uk-and-eu-gdpr-regulations/Acesso em: 26 fev. 2023.

[207] REINO UNIDO. Information Commissioner's Office. **About the DPA 2018**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/about-the-dpa-2018/. Acesso em: 23 mar. 2023.

[208] *Ibidem*

[209] *Ibidem*

Unido antes daquela data – contendo algumas mudanças para torná-lo mais eficaz ao contexto britânico[210]. Por sua vez, o *Data Protection Act* de 2018 atua em conjunto do GDPR do Reino Unido, complementando-o, bem como estabelecendo regras para as autoridades responsáveis pela aplicação da Lei[211]. Além disso, o instrumento amplia a proteção de dados a áreas como segurança e defesa nacional, e estabelece as funções e poderes do ICO[212].

Assim, o *Data Protection Act* de 2018 divide-se em partes, cada uma aplicada a diferentes regimes[213]. A segunda partecuida do tratamento geral – ou seja, do GDPR do Reino Unido –; a terceira, do tratamento para aplicação da lei; e a parte quatro, do tratamento por serviços de inteligência[214]. Já as outras partes contêm disposições de aplicação geral[215].

Apesar das alterações normativas, deve-se ressaltar que, em linhas gerais, a legislação do Reino Unido segue bastante semelhante à da União Europeia[216]. Os titulares de dados do Reino Unido possuem todos os direitos sobre seus dados que tinham antes sob o GDPR – incluindo o direito ao esquecimento e o direito de correção de dados já coletados[217].

Dentre as diferenças existentes entre os dois instrumentos regulatórios, tem-se, principalmente: (i.) a idade mínima para o fornecimento do consentimento do uso de dados: enquanto na União Europeia a idade mínima para tal é 16 anos – com certas exceções –, no Reino Unido, é de 13 anos[218]; (ii.) o órgão fiscalizador: o GDPR é governado pelo *European Data Protection Board*, ou Conselho Europeu de Proteção de Dados ("EDPB"), pelas autoridades de privacidade dos Estados membros e, em última instância, pela Comissão Europeia, ao passo que o órgão fiscalizador do GDPR do Reino Unido é o ICO, como já mencionado[219]; (iii.) a tomada de decisão

---

[210] REINO UNIDO. Information Commissioner's Office. **About the DPA 2018**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/about-the-dpa-2018/. Acesso em: 23 mar. 2023.
[211] *Ibidem*
[212] *Ibidem*
[213] *Ibidem*
[214] *Ibidem*
[215] *Ibidem*
[216] How do the UK's GDPR and EU's GDPR regulation compare? **GDPR EU**, 2023. Disponível em: https://www.gdpreu.org/differences-between-the-uk-and-eu-gdpr-regulations/Acesso em: 26 fev. 2023.
[217] *Ibidem*
[218] GDPR vs UK GDPR — what's the difference? **The Infolaw Partner Showcase**, London, 12 July 2022. Disponível em: https://www.infolaw.co.uk/partners/gdpr-vs-uk-gdpr-whats-the-difference/. Acesso em: 20 mar. 2023.
[219] *Ibidem*

automatizada: o GDPR dá aos titulares de dados o direito de rejeitar a tomada de decisão automatizada ou a criação de perfis automatizados, enquanto o GDPR do Reino Unido permite a realização de perfis automatizados nos casos em que há justificativa legítima para tal[220]; (iv.) o tratamento de dados em razão de interesse público: nesses casos, o GDPR do Reino Unido é mais permissivo que o GDPR[221]; e, ainda (v.) o tratamento de dados criminais: para o GDPR, este tratamento precisa atender à certas exigências legais, enquanto, no GDPR do Reino Unido, isto não é necessário[222].

2.2.2 A evolução da Proteção de Dados no direito brasileiro

No ordenamento brasileiro, o estabelecimento de uma estrutura normativa unitária ocorreu mais recentemente, com a publicação da LGPD, em 14 de agosto de 2018. Vale dizer, todavia, que temas associados à proteção de dados não são novidade na estrutura normativa do país, que já tratava do tema por meio de questões ligadas à privacidade, ao direito do consumidor e a outras liberdades individuais[223].

Nesse sentido, ainda que o direito à proteção de dados seja, muitas vezes, ligado ao direito à privacidade, ressalta-se que o desenvolvimento da proteção à privacidade – prevista constitucionalmente e mencionada no Código Civil de 2002 – não foi capaz de trazer soluções para os problemas surgidos com o desenvolvimento de novas tecnologias[224]. Isto é: ainda que o direito à privacidade tenha contribuído para a consolidação de valores presentes na proteção de dados, a dinâmica do desenvolvimento da proteção de dados acabou, em grande medida, não dialogando com o direito à privacidade[225].

Destaca-se que, ainda antes de 1988, as legislações estaduais do Rio de Janeiro e de São Paulo abrangiam leis sobre o direito de acesso e retificação de dados pessoais, trazendo elementos como o princípio da finalidade e o consentimento

---

[220] What is UK GDPR: 9 Key Things Businesses Need to Know. **Secure Privacy**, 11 april 2021. Disponível em: https://secureprivacy.ai/blog/what-is-uk-gdpr. Acesso em: 10 mar. 2023.
[221] *Ibidem*
[222] *Ibidem*
[223] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 29. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.
[224] *Ibidem*
[225] *Ibidem*

informado[226]. Tais legislações foram importantes para abrir o caminho do debate sobre o habeas data na elaboração da Constituição de 1988[227]. Conforme o art. 5º, LXXII, da Constituição Federal, será concedido o habeas data sempre que necessário para: (i.) "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público"; e (ii.) "para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" (art. 5º, LXXII)[228].

E não só no instituto do habeas data inovou a Constituição Federal, mas também na consolidação dos direitos à vida privada e intimidade, no art. 5º, X e no segredo das comunicações telefônicas, telegráficas e de dados, no art. 5º, XII[229]. De qualquer forma, a consolidação desses direitos fundamentais não foi capaz de originar um entendimento que identificasse o direito à proteção de dados[230].

Todavia, partir desse momento, o tema foi se tornando mais frequente no debate político[231]. Como exemplo, temos a menção ao caráter de direito fundamental da proteção de dados pessoais na Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, que foi assinada pelo governo brasileiro em novembro de 2003[232].

Vale citar, também, debate surgido no Mercosul quando, no Subgrupo de Trabalho Número 13 ("SGT13"), responsável pelo debate e encaminhamento de propostas sugeridas pelos países-membros em temas referentes ao Comércio Eletrônico, a Argentina apresentou, em 2004, proposta para regulamentação comum sobre proteção de dados pessoais para os países membros do Mercosul[233]. Este debate originou um documento conhecido como "Medidas para a proteção de dados pessoais e sua livre circulação", aprovado em reunião ocorrida em Buenos Aires em

---

[226] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 31. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.
[227] *Ibidem*, p. 31.
[228] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 mar. 2023.
[229] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 32. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.
[230] *Ibidem*
[231] *Ibidem*
[232] *Ibidem*
[233] *Ibidem*, p. 34.

2010[234]. Apesar de o documento ter sido remetido ao Grupo Mercado Comum, não se tornou uma norma efetiva[235]. De qualquer sorte, essas discussões foram responsáveis por iniciar a conversa sobre o tema dentro do governo brasileiro[236].

O primeiro antecedente da LGPD, um texto base para debate público, foi publicado pelo Ministério da Justiça em 2010, tendo recebido 794 contribuições[237]. Após o debate, foi elaborado o texto-base do Anteprojeto de Lei de Proteção de Dados pelo Ministério da Justiça[238]. Entre os anos de 2011 e 2015, o Anteprojeto sofreu diversas revisões e aperfeiçoamentos e, finalmente, em 2015, consolidou-se em uma nova versão, publicada pela Secretaria Nacional do Consumidor (Senacon), do Ministério da Justiça[239]. Esta versão foi novamente submetida a um debate público, que recebeu mais de 1.000 contribuições[240].

Depois do debate, mais uma versão foi consolidada, sendo enviada em 2016 para a Casa Civil da Presidência da República e, posteriormente, para o Congresso Nacional[241]. O texto foi protocolado na Câmara dos Deputados como o Projeto de Lei nº 5.276/2016[242]. Vale dizer que, na época do envio do texto, já haviam surgido outros projetos sobre o tema – dentre eles o Projeto de Lei nº 4.060/2012, na Câmara dos Deputados e o Projeto de Lei 330, de 2013, do Senado[243].

Nesse sentido, criou-se, em 2015, uma Comissão Especial referente ao Projeto de Lei nº 4.060/2012, na Câmara dos Deputados, que teve seu parecer aprovado em maio de 2018[244]. Após, a matéria foi encaminhada para o Senado Federal como Projeto de Lei nº 53/2018, passando a tramitar em conjunto com outros Projetos de Lei já existentes no Senado, quais sejam, o nº 181/2014, o nº 131/2014 e o nº 330/2013[245].

---

234 DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 35. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.
235 *Ibidem*
236 *Ibidem*
237 *Ibidem*
238 *Ibidem*
239 *Ibidem*
240 *Ibidem*
241 *Ibidem*
242 *Ibidem*
243 DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 36. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.
244 *Ibidem*
245 *Ibidem*

Os projetos foram encaminhados à Comissão de Assuntos Econômicos, sob relatoria do senador Ricardo Ferraço[246]. Em junho de 2018, o senador apresentou relatório a favor do Projeto de Lei nº 53/2018 com emendas, manifestando-se, também, pela prejudicialidade dos demais[247]. Tal relatório foi aprovado na Câmara em julho de 2018, sendo o projeto aprovado por unanimidade pelo Plenário do Senado Federal e, finalmente, promulgada, com vetos, em 14 de agosto de 2018[248]. Assim, a LGPD, sancionada em 14 de agosto de 2018, foi responsável por instaurar, no Brasil, um regime geral de proteção de dados que complementou disposições já trazidas pela Lei de Acesso à Informação, do Marco Civil da Internet e do Código de Defesa do Consumidor (˜CDC˜).

Sobre tais legislações, vale mencionar que o CDC, por ter estabelecido princípios de proteção ao consumidor, concentrou um grande volume de demandas relacionadas a dados pessoais – que, muitas vezes, encontram-se dentro de relações de consumo[249]. Inclusive, sugere-se que princípios da proteção de dados possam ser visualizados no CDC[250]. Nesse sentido, o art. 43 do CDC, que trata dos bancos de dados de proteção de crédito, levou à edição da Lei nº 12.414/2011, a Lei do Cadastro Positivo[251]. Ressalta-se que a Lei do Cadastro Positivo constitui a primeira legislação brasileira com conceitos comuns à proteção de dados, como, por exemplo, os dados sensíveis e os princípios da finalidade, da transparência e da minimização[252].

No mesmo período, foi promulgada a Lei nº 12.527/2011, Lei de Acesso à Informação[253]. Essa Lei regula o acesso à informação, define o conceito de informação pessoal e regulamenta o princípio constitucional da transparência[254]. No

---

[246] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 36. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.
[247] *Ibidem*
[248] *Ibidem*
[249] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 33. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.
[250] *Ibidem*
[251] *Ibidem*
[252] *Ibidem*
[253] BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 26 fev. 2023.
[254] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 34. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.

mais, a Lei, no art. 31, estabelece um regramento para o tratamento de dados pessoais detidos pelo poder público[255-256].

Posteriormente, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, estabeleceu direitos para o usuário da internet – relacionados, inclusive, com o uso dos dados pessoais[257], cuja proteção foi definida como um princípio do uso da internet, no inciso III, art. 3º, da Lei[258-259].

A inspiração do legislador brasileiro no modelo europeu de proteção de dados – e, no caso, britânico – pode ser vista, primordialmente, nas seguintes intersecções entre as normas: (i.) a exigência de base legal para o tratamento de dados, conforme

---

[255] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 34. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.

[256] **Artigo 31 da Lei nº 12.527, de 18 de novembro de 2011.** O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III - ao cumprimento de ordem judicial; IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante. § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal (BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 26 fev. 2023).

[257] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 34. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.

[258] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 mar. 2023.

[259] **Artigo 3º, III, da Lei nº 12.965 de 23 de abril de 2014**. Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) III - proteção dos dados pessoais, na forma da lei; (...)

os arts. 6º (1), do GDPR do Reino Unido[260], e 7º da LGPD[261]; (ii.) a existência de princípios gerais, dispostos nos arts. 5º (1), do GDPR do Reino Unido[262] e 6º da

[260] **Artigo 6º do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 6. Lawfulness of processing. 1.Processing shall be lawful only if and to the extent that at least one of the following applies: (a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b)processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c)processing is necessary for compliance with a legal obligation to which the controller is subject; (d)processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (…)" (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/6. Acesso em: 23 fev. 2023).

[261] **Artigo 7º da Lei Geral de Proteção de Dados.** Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (...)" (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023).

[262] **Artigo 5º (1) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 5. Principles relating to processing of personal data. 1.Personal data shall be:(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d)accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e)kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f)processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality') (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/5. Acesso em: 23 fev. 2023).

LGPD[263]; (iii.) o regime diferenciado para o tratamento de dados sensíveis, conforme os arts. 9º, do GDPR do Reino Unido[264] e 11 da LGPD[265]; (iv.) a definição de uma autoridade para aplicação da lei, nos termos dos arts. 51 do GDPR do Reino Unido[266]

---

[263] **Artigo 6º da Lei Geral de Proteção de Dados.** Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023).

[264] **Artigo 9º do General Data Protection Regulation – UK.** Tradução nossa, do original: “Article 9. Processing of special categories of personal data. 1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited (…) (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/51. Acesso em: 23 fev. 2023).

[265] **Artigo 11 da Lei Geral de Proteção de Dados.** Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023).

[266] **Artigo 51 do General Data Protection Regulation – UK.** Tradução nossa, do original: “Article 51. Monitoring the application of this Regulation. 1.**[F3**The Commissioner is**]** responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/51. Acesso em: 23 fev. 2023).

e 55-A da LGPD[267]; (v.) a edição de regras distintas para o operador e o controlador, conforme o capítulo IV do GDPR do Reino Unido[268] e capítulo VI da LGPD[269]; e (vi.) a possibilidade portabilidade dos dados, nos termos dos arts. 20 (1) do GDPR do Reino Unido[270] e 18, V, da LGPD[271].

No entanto, diferentemente da legislação europeia, a legislação brasileira ainda apresenta diversas lacunas de regulamentação. A Lei nº 13.853/2019 foi responsável por alterar a LGPD, criando a ANPD[272]. Nesse sentido, dentre as competências da ANPD, dispostas no art. 55-J, da LGPD, está a edição de regulamentos e procedimentos sobre proteção de dados pessoais, no inciso XIII[273].

---

[267] **Artigo 55-A da Lei Geral de Proteção de Dados.** Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023).

[268] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/chapter/IV. Acesso em: 23 fev. 2023.

[269] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.

[270] **Artigo 20 (1) do General Data Protection Regulation – UK.** Tradução nossa, do original: Article 20. **Right to data portability.** 1.The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, Where: (a)the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b)the processing is carried out by automated means (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/20. Acesso em: 23 fev. 2023).

[271] **Artigo 18, V, da Lei Geral de Proteção de Dados**. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (...) (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.

[272] BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 26 fev. 2023).

[273] **Artigo 55-J da Lei Geral de Proteção de Dados.** Art. 55-J. Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza

Para regular temas referentes à proteção de dados, a ANPD publicou, até o momento, duas agendas regulatórias – uma para o biênio 2021-2022[274], e outra para o biênio 2023-2024[275]. Até o momento, algumas resoluções já foram publicadas, são elas: (i.) A Resolução CD/ANPD, de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD[276]; (ii.) A Resolução CD/ANPD, de janeiro de 2022, que aprova o Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte[277]; (iii.) A Resolução CD/ANPD, de janeiro de 2023, que institui o Comitê de Governança Digital

---

internacional ou transnacional; X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; XII - elaborar relatórios de gestão anuais acerca de suas atividades; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023)

[274] BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 3 mar. 2023.

[275] BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 35, de 04 de novembro de 2022**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Acesso em: 3 mar. 2023.

[276] BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº1/2021**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021. Acesso em: 3 mar. 2023.

[277] BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº2/202**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 3 mar. 2023.

da ANPD[278]; e (iv.) A Resolução CD/ANPD, de fevereiro de 2023, que aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas[279].

O tema da transferência internacional de dados – qual seja, a regulamentação dos Arts. 33 a 35, da LGPD – constou na Fase 2 da Agenda Regulatória da ANPD para o biênio 2021-2022[280]. Os itens da Fase 2 eram aqueles cujo início do processo ocorreria em até 1 ano e 6 meses da publicação, que foi feita em janeiro de 2021[281]. De fato, em maio de 2022, foi aberta tomada de subsídios sobre transferências internacionais de dados pessoais[282]. A tomada de subsídios ficou aberta para contribuições até o final de junho de 2022, totalizando 63 contribuições[283]. O objetivo da ANPD foi justamente o recebimento de opiniões de diferentes agentes econômicos, titulares de dados pessoais e todos aqueles afetados pela regulação da transferência internacional de dados pessoais[284]. Até o momento, não houve atualizações. Na Agenda Regulatória para o biênio 2023-2024, o tema está alocado na Fase 1, que diz respeito aos itens cujo processo regulatório iniciou na vigência da Agenda para 2021-2022[285].

Em síntese, a legislação de proteção de dados, na Europa, teve seu início oficial em 1995, com a Diretiva de Proteção de Dados Pessoais, que foi substituída, em 2018, pelo GDPR. No Brasil, por sua vez, as normas de proteção de dados foram criadas mais recentemente, sendo a LGPD aprovada em 2018. Desse modo, enquanto a legislação de proteção de dados na Europa tem uma história longa e é conhecida por sua rigidez e severidade, a norma brasileira ainda está em consolidação.

---

[278] BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº3/2023**. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-3-de-25-de-janeiro-de-2023-460124477. Acesso em: 3 mar. 2023.

[279] BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº4/2023**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 3 mar. 2023.

[280] BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 3 mar. 2023.

[281] *Ibidem*

[282] BRASIL. Autoridade Nacional de Proteção de Dados. **Tomada de Subsídios sobre Transferência Internacional**. Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional. Acesso em: 10 mar. 2023.

[283] *Ibidem*

[284] *Ibidem*

[285] BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 35, de 04 de novembro de 2022**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Acesso em: 3 mar. 2023.

2.3 A tutela jurídica da Transferência Internacional de Dados – GDPR do Reino Unido e LGPD

A LGPD e a legislação do Reino Unido tratam das transferências internacionais de dados pessoais. Na LGPD, as regras estão dispostas no capítulo V, entre os arts. 33 e 36[286]. Já na legislação do Reino Unido, estão primeiramente dispostas no *Data Protection Act* de 2018, responsável por adaptar o GDPR ao Reino Unido[287].

No *Data Protection Act* as disposições sobre transferência internacional de dados pessoais estão organizadas nas três partes previamente mencionadas – a segunda parte, que complementa as regras do GDPR do Reino Unido; a terceira parte, que trata das regras relacionadas à aplicação de lei; e a quarta parte, que cuida das regras atinentes aos serviços de inteligência.

Como previamente mencionado, este trabalho busca investigar as semelhanças e diferenças das hipóteses autorizadoras das transferências internacionais de dados pessoais da legislação brasileira e britânica para, após, adentrarmos os mecanismos de salvaguardas existentes em cada legislação e, finalmente, estudarmos as normas corporativas globais aprovadas pela ICO e suas possíveis contribuições a um modelo brasileiro. Assim, para a execução do trabalho, não será analisado o *Data Protection Act*, uma vez que os princípios, bases legais e mecanismos de salvaguardas utilizados, no Reino Unido, para transferir dados internacionalmente, estão dispostos no GDPR do Reino Unido – de modo que apenas esse instrumento normativo será comparado à LGPD brasileira.

O GDPR do Reino Unido trata das transferências internacionais de dados no capítulo V, entre os arts. 44 e 50[288]. O art. 44 dispõe sobre o princípio geral para as transferências internacionais de dados[289]. Segundo o dispositivo, todas as transferências internacionais de dados pessoais tratados ou que se destinem a tratamento, após a transferência, para países terceiros ou organizações internacionais, ocorrerão somente se observadas as disposições do Regulamento e as condições nele estabelecidas sejam cumpridas pelo responsável pelo tratamento

---

[286] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.
[287] REINO UNIDO. Information Commissioner's Office. **Guide to the UK General Data Protection Regulation (UK GDPR).** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/. Acesso em: 10 mar. 2023.
[288] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/44. Acesso em: 23 fev. 2023.
[289] *Ibidem*

e pelo operador – inclusive no que tange às transferências posteriores a essa primeira transferência[290]. Em suma, o objetivo é garantir que o nível de proteção de dados pessoais estabelecido no Regulamento não seja prejudicado[291].

A LGPD, por sua vez, não traz regra introdutória como o art. 44, do GDPR do Reino Unido. De qualquer sorte, o tema passa a ser tratado a partir do Art. 33, o qual define as hipóteses autorizadoras da transferência internacional de dados[292]. O art. equivalente, no GDPR do Reino Unido, é o 45[293]. O art. 33, da LGPD, determina, como

---

[290] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/44. Acesso em: 23 fev. 2023.

[291] *Ibidem*

[292] **Artigo 33 da Lei Geral de Proteção de Dados.** Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023).

[293] **Artigo 45 do General Data Protection Regulation – UK.** Tradução nossa, do original: Article 45. Transfers on the basis of an adequacy decision. 1.A transfer of personal data to a third country or an international organisation may take place [F1where it is based on adequacy regulations (see section 17A of the 2018 Act)]. Such a transfer shall not require any specific authorisation. 2.When assessing the adequacy of the level of protection [F2for the purposes of sections 17A and 17B of the 2018 Act, the Secretary of State] shall, in particular, take account of the following elements: (a)the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; (b)the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with [F3the Commissioner]; and (c)the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its

primeira hipótese autorizadora da transferência internacional de dados, a existência de nível de proteção de dados considerado adequado[294]. Da mesma forma, o art. 45, do GDPR do Reino Unido, permite as transferências internacionais de dados quando houver declaração de adequação aos níveis de proteção de dados estabelecidos por Lei[295].

O primeiro mecanismo para transferência internacional de dados pessoais em ambas as legislações é, portanto, o nível de proteção de dados pessoais do país terceiro ou da organização internacional receptora dos dados. Segundo o art. 34, da LGPD, "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"[296]: (i.) "as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional"[297]; (ii.) "a natureza dos dados" [298]; (iii.) a "observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos"[299] na Lei; (iv.) "a adoção de medidas de segurança previstas em regulamento" [300]; (v.) "a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais"[301]; e (vi.) "outras circunstâncias específicas relativas à transferência" [302].

No mesmo sentido, o art. 45, do GDPR do Reino Unido, estabelece que, para avaliar a adequação do nível de proteção de dados pessoais, o Secretário de Estado deve levar em conta os seguintes fatores: (i.) o Estado de direito, o respeito aos direitos humanos e às liberdades fundamentais, a legislação pertinente, o acesso das autoridades públicas aos dados pessoais, bem como a implementação de tal legislação, regras de proteção de dados, regras profissionais e medidas de segurança, a jurisprudência, e os direitos efetivos e executórios do titular dos dados e recursos administrativos e judiciais efetivos para as pessoas cujos dados pessoais sejam transferidos; (ii.) a existência e o funcionamento eficaz de uma ou mais autoridades

---

participation in multilateral or regional systems, in particular in relation to the protection of personal data (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/45. Acesso em: 23 fev. 2023).

294 BRASIL*, op. cit.*

295 REINO UNIDO, *op. cit.*

296 BRASIL*, op. cit.*

297 *Ibidem*

298 *Ibidem*

299 *Ibidem*

300 *Ibidem*

301 *Ibidem*

302 *Ibidem*

de supervisão independentes no país terceiro ou a que uma organização internacional esteja sujeita; e (iii.) os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, ou outras obrigações decorrentes de convenções ou instrumentos legalmente vinculantes, bem como a participação em sistemas multilaterais ou regionais sobre proteção de dados pessoais[303].

Desse modo, uma vez que o nível de proteção de um país ou organização internacional tenha sido declarado adequado, os controladores poderão transferir dados pessoais livremente para tal destinatário, sem a necessidade do consentimento de suas autoridades nacionais. Em razão da influência da União Europeia, presume-se que a ANPD considere uma proteção "substancialmente equivalente" para definir o "nível adequado de proteção"[304]. Também o autor Luís Fernando Prado Chaves determina que, considerando a semelhança entre a LGPD e o GDPR, há uma tendência de que a ANPD considere os países sujeitos ao GDPR – bem como os reconhecidos pela Comissão Europeia – adequados à proteção de dados[305]. Nesse sentido, é relevante analisar não apenas o texto da lei, mas os mecanismos para garantir a proteção de dados[306].

2.3.1 Os mecanismos de salvaguardas

Além da hipótese do nível adequado de proteção de dados, ambas as legislações estipulam como bases legais para a transferência internacional de dados mecanismos capazes de oferecer e comprovar garantias do cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados. Isto é, caso o ordenamento jurídico destinatário dos dados não seja considerado adequado perante os critérios da autoridade nacional, é possível que o controlador ofereça e comprove garantias de cumprimento dos princípios da legislação.

O art. 33 da LGPD, coloca como segunda hipótese possibilitadora das transferências internacionais de dados o oferecimento e comprovação das "garantias

---

[303] REINO UNIDO, *op. cit.*

[304] LEONARDI, Marcel. Transferência internacional de dados pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 303. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

[305] PRADO CHAVES, Luís Fernado. Da Transferência Internacional de Dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice**. LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, p. RL-1.10. *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

[306] LEONARDI, *op. cit.*

de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos" na Lei[307]. Esses mecanismos estão dispostos em lista taxativa[308]. São eles: (i.) "cláusulas contratuais específicas para determinada transferência"; (ii.) "cláusulas-padrão contratuais"; (iii.) "normas corporativas globais"; e (iv.) "selos, certificados e códigos de conduta regularmente emitidos"[309].

O art. 46 do GDPR dispõe que, no caso de não haver decisão de adequação, os dados poderão ser transferidos para um país terceiro ou organismo internacional se o controlador ou operador fornecer salvaguardas apropriadas, e desde que sejam disponibilizados, ao titular dos dados, direitos e recursos legais eficazes[310]. O GDPR também elenca, taxativamente, as salvaguardas apropriadas: (i.) instrumento juridicamente vinculativo e executável entre autoridades ou órgãos públicos; (ii.) normas corporativas globais; (iii.) cláusulas-padrão de proteção de dados; (iv.) código de conduta; e (v.) certificados, conforme o art. 46 (2)[311]. No mais, definiu-se que, mediante autorização do ICO, tais salvaguardas podem ser previstas por meio de cláusulas contratuais ou disposições inseridas em acordos administrativos entre autoridades ou órgãos públicos[312]. Ressalta-se, ainda, que conforme os arts. 35, da

---

307 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.

308 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.

309 *Ibidem*

310 **Artigo 46 (2) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 46. Transfers subject to appropriate safeguards (...) 2.The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from [F2the Commissioner], by: (a)a legally binding and enforceable instrument between public authorities or bodies; (b)binding corporate rules in accordance with Article 47; [F3(c)standard data protection clauses specified in regulations made by the Secretary of State under section 17C of the 2018 Act and for the time being in force;] [F4(d)standard data protection clauses specified in a document issued (and not withdrawn) by the Commissioner under section 119A of the 2018 Act and for the time being in force;] (e)an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f)an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights (…) REINO UNIDO. Regulation (EU) 2016/679 of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/46. Acesso em: 23 fev. 2023).

311 *Ibidem*

312 *Ibidem*

LGPD[313], e 46 (2), do GDPR do Reino Unido[314], a avaliação de tais mecanismos, e consequente permissão para a transferência é tarefa das autoridades nacionais.

Portanto, tanto o GDPR do Reino Unido quanto a LGPD buscam garantir a proteção dos dados pessoais transferidos para países com leis e regulamentos de proteção de dados menos abrangentes. Desse modo, além da hipótese do nível adequado de proteção de dados, ambas as legislações estabelecem que as transferências internacionais de dados pessoais devem ser baseadas em mecanismos que garantam o cumprimento dos princípios, dos direitos dos titulares e do regime de proteção de dados. Vale dizer, há, ainda, outras hipóteses autorizadoras das transferências internacionais de dados pessoais em ambas as legislações, as quais serão abordadas no próximo subcapítulo.

2.3.2 Outras hipóteses

Além disso, outras situações que permitem a transferência internacional de dados, para a LGPD, são, conforme o art. 33: (i.) a cooperação jurídica internacional; (ii.) a proteção da vida ou da incolumidade física; (iii.) a autorização ANPD; (iv.) a cooperação internacional; (v.) a execução de política pública ou a atribuição legal do serviço público; (vi.) o consentimento específico e destacado, com informação prévia sobre o caráter internacional da operação; (vii.) o cumprimento de obrigação legal ou regulatória, por parte do controlador; (viii.) a execução de contrato; e (ix.) o exercício de direitos em âmbito judicial, administrativo ou arbitral[315].

Conforme o art. 49 (1) do GDPR do Reino Unido, não sendo o nível de proteção de dados considerado adequado, e tampouco dispondo de salvaguardas apropriadas, as hipóteses autorizadoras da transferência internacional de dados são: (i.) o consentimento do titular de dados; (ii.) a execução de contrato; (iii.) as razões de interesse público; (iv.) a defesa legal; (v.) a proteção de interesses vitais; e (vi.) o

---

[313] **Artigo 35 da Lei Geral de Proteção de Dados.** 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 (...) (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023).

[314] REINO UNIDO, *op. cit.*

[315] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.

fornecimento de informações ao público, estando aberta à consulta do público em geral ou a qualquer pessoa capaz de provar interesse legítimo[316].

Para o GDPR do Reino Unido, estas transferências devem respeitar algumas condições dispostas no art. 49 (1), tais como: (i.) a não ocorrência de forma repetitiva; (ii.) o tratamento de um número limitado de titulares de dados; (iii.) a imprescindibilidade para efeitos dos interesses legítimos do responsável pelo tratamento, desde que tais interesses não se sobreponham aos direitos e liberdades dos titulares de dados; (iv.) a análise e avaliação das circunstâncias nas quais ocorrem a transferência internacional de dados, pelo responsável pelo tratamento de dados, com apresentação de garantias adequadas para a proteção de dados; (v.) a comunicação ao ICO; e (vi.) o fornecimento de informações sobre a transferência ao titular de dados pessoais pelo responsável pela transferência[317].

No mais, o art. 50 do GDPR aduz que o ICO tomará medidas para: (i.) desenvolver mecanismos de cooperação internacional a fim de facilitar a aplicação efetiva da legislação para a proteção de dados pessoais; (ii.) prestar assistência mútua

---

[316] **Artigo 49 (1) do General Data Protection Regulation – UK.** Tradução nossa, do original: "Article 49. Derogations for specific situations. 1.In the absence of [F1adequacy regulations under section 17A of the 2018 Act], or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a)the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b)the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c)the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d)the transfer is necessary for important reasons of public interest; (e)the transfer is necessary for the establishment, exercise or defence of legal claims; (f)the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (g)the transfer is made from a register which according to **[F2**domestic law**]** is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by **[F2**domestic law**]** for consultation are fulfilled in the particular case. Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform **[F3**the Commissioner**]** of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/49. Acesso em: 23 fev. 2023).

[317] *Ibidem*

internacional na aplicação da legislação para a proteção de dados pessoais; (iii.) engajar as partes em discussões e atividades destinadas a promover a cooperação internacional na aplicação da legislação para a proteção de dados pessoais; e (iv.) promover o intercâmbio e a elaboração de documentação a respeito da legislação e da prática na proteção de dados pessoais[318]. Vale dizer, o art. 48, que no GDPR europeu trata das transferências ou divulgações de dados pessoais não autorizadas pelo direito da União Europeia, foi revogado pelo Reino Unido. Além disso, o art. 47, que trata especificamente das normas corporativas globais, será tratado no próximo capítulo.

Em suma, podemos observar que, de um modo geral, a LGPD estabeleceu disposições bastante semelhantes ao GDPR no que tange às transferências internacionais de dados pessoais[319]. Dentre algumas diferenças entre as legislações estão, contudo: (i.) a autorização específica, no GDPR, para realizar transferências mediante registro acordando sobre o oferecimento de informações ao público, encontrando-se aberto à consulta do público em geral ou de pessoa com interesse legítimo, no art. 49 (1) (g) do GDPR do Reino Unido[320] (ii.) as vedações às transferências internacionais de dados pessoais que não forem amparadas por decisão de adequação ou mecanismos de salvaguardas (ou seja, fundamentadas nas hipóteses do art. 49, do GDPR do Reino Unido) que forem repetidas diversas vezes ou dispuserem de um grande número de titulares de dados envolvidos, nos termos do art. 49 do GDPR do Reino Unido[321]; e (iii.) a autorização pela autoridade nacional

---

[318] **Artigo 50 do General Data Protection Regulation – UK.** Tradução nossa, do original: “Article 50. International cooperation for the protection of personal data. In relation to third countries and international organisations, [F1the Commissioner] shall take appropriate steps to: (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (c)engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/50. Acesso em: 23 fev. 2023).

[319] **Guia de Proteção de Dados Pessoais: Transferência Internacional**. São Paulo: FGV, out .2020, p. 20. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Acesso em: 01 mar. 2023

[320] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/49. Acesso em: 23 fev. 2023.

[321] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/49. Acesso em: 23 fev. 2023.

como uma hipótese autorizadora da transferência internacional de dados, no art. 33, V, da LGPD[322].

Em síntese, tal como no GDPR, a LGPD prevê que as transferências internacionais de dados sejam permitidas baseando-se no grau de proteção adequado, sendo, a segunda modalidade, os mecanismos de salvaguardas, ou garantias de cumprimento. Ademais, ambas as legislações trazem situações excepcionais, nas quais é possível a transferência internacional de dados ainda que não haja decisão de adequação ou mecanismos de cumprimento de garantias.

Excluindo-se diferenças pontuais, é possível observarmos que a Lei brasileira foi amplamente influenciada pela Lei europeia. Considerando-se a influência europeia, esperado que o legislador brasileiro se utilizasse do GDPR como fonte de inspiração. De fato, a LGPD pode usufruir da evolução legislativa da União Europeia para incorporar seus elementos[323].

3 AS NORMAS CORPORATIVAS GLOBAIS

Conforme retratado no capítulo anterior, as normas corporativas globais constituem um dos mecanismos utilizados para oferecer e comprovar garantias do cumprimento dos princípios, dos direitos dos titulares e do regime de proteção de dados previstos em lei quando realizadas transferências internacionais de dados pessoais. Este mecanismo consiste em códigos de conduta que estabelecem as políticas internas aplicáveis às transferências de dados pessoais no âmbito interno das empresas[324], grupos corporativos, e grupos de empresas envolvidos em atividade econômica conjunta, como franquias, *joint ventures* ou parcerias profissionais[325].

---

[322] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.

[323] VERONESE, Alexandre. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 718. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

[324] PROUST, Olivier; BARTOLI, Emmanuelle. Binding Corporate Rules: a global solution for international data transfers. **International Data Privacy Law**, London, p. 2, November 25, 2011. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/12/International_Data_Privacy_Law-2011-Proust.pdf. Acesso em: 20 mar. 2023.

[325] REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/. Acesso em: 10 mar. 2023.

Estas diretrizes, legalmente vinculantes[326], possibilitam que as empresas multinacionais deixem de implementar mais de um instrumento legal para regulamentar tais transferências. Dessa forma, o procedimento de transferir dados pessoais internacionalmente se torna mais simples e otimizado, uma vez que as normas corporativas globais configuram um instrumento único, capaz de fornecer garantias aos titulares de dados pessoais e um alto nível de proteção à todas as transferências efetuadas dentro do mesmo grupo corporativo, independentemente para qual entidade do grupo o dado for transferido[327].

Com efeito, as normas corporativas globais asseguram que todas as transferências realizadas dentro de um grupo empresarial contêm: (i.) princípios de proteção de dados, como transparência, qualidade dos dados e segurança; (ii.) ferramentas eficazes, como auditoria, treinamentos dos colaboradores e gerenciamento das reclamações; e (iii.) um componente provando que as normas corporativas globais são vinculativas, tanto em âmbito interno quanto externo[328].

Além disso, as normas corporativas globais servem como um padrão interno de proteção de dados dentro de um grupo corporativo, harmonizando as práticas entre as diferentes empresas, independentemente da localização destas ou da cidadania dos funcionários[329]. Isto contribui, inclusive, para mitigar os riscos associados ao tratamento de dados pessoais – especialmente nas entidades localizadas em países que não dispõem de bases normativas sobre a proteção de dados[330]. No mais, estas normas ajudam a promover a confiança dos titulares de dados pessoais no controlador dos dados, já que, muitas vezes, as empresas podem utilizar-se das normas como uma forma de garantir aos clientes, fornecedores e demais terceiros que estão em conformidade com os princípios da proteção de dados pessoais[331].

---

[326] PROUST, *op. cit.*
[327] PROUST, *op. cit.*
[328] **Binding Corporate Rules. The General Data Protection Regulation**. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 23 mar. 2023.
[329] **Binding Corporate Rules. The General Data Protection Regulation**. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 23 mar. 2023.
[330] *Ibidem*
[331] PROUST, Olivier; BARTOLI, Emmanuelle. Binding Corporate Rules: a global solution for international data transfers. **International Data Privacy Law**, London, p. 2, November 25, 2011. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/12/International_Data_Privacy_Law-2011-Proust.pdf. Acesso em: 20 mar. 2023.

Este mecanismo, desenvolvido pela legislação da União Europeia, se manteve na legislação britânica de proteção de dados, sob o art. 47, do GDPR do Reino Unido[332]. Na LGPD, conforme já mencionado, as normas corporativas globais estão dispostas no art. 33, II, c[333].

3.1 O que são Normas Corporativas Globais

A Diretiva de Proteção de Dados Pessoais dispunha, no art. 26 (2), que os Estados-membros da União Europeia poderiam autorizar transferência ou transferências internacionais de dados pessoais a um país que não apresenta nível de proteção de dados adequado desde que o responsável pelo tratamento dos dados pessoais fornecesse garantias suficientes de proteção da vida privada e dos direitos e liberdades fundamentais dos titulares de dados[334]. Em 03 de junho de 2003, o Grupo de Trabalho do Artigo 29 adotou o *Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*[335], um documento que trata da aplicação do art. 26 (2) da Diretiva de Proteção de Dados da União Europeia às Normas Corporativas Globais.

No documento, o Grupo determinou que a avaliação para a concessão de autorização para a transferência internacional de dados, nos termos do art. 26 (2) da

---

[332] REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/. Acesso em: 10 mar. 2023.

[333] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 fev. 2023.

[334] **Artigo 26 (2) da Directiva 95/46/CE do Parlamento Europeu e do Conselho.** Sem prejuízo do nº 1 , um Estado-membro pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um país terceiro que não assegura um nível de protecção adequado na acepção do nº 2 do artigo 25º, desde que o responsável pelo tratamento apresente garantias suficientes de protecção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respectivos direitos; essas garantias podem, designadamente , resultar de cláusulas contratuais adequadas.

Equivalente ao artigo 46 (1), do GDPR do Reino Unido: In the absence of adequacy regulations under section 17A of the 2018 Act**]**, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

[335] UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 7. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

Diretiva de Proteção de Dados Pessoais[336], deve ser feita mediante análise das salvaguardas estabelecidas pelo responsável pelo tratamento dos dados, a fim de que seja garantida proteção adequada aos dados pessoais transferidos[337]. É dizer: sempre que dados forem transferidos para controlador ou operador de dados em um país terceiro, ou em um organismo internacional, necessário que se avalie se os princípios atinentes à proteção de dados são, de fato, respeitados.

Destarte, segundo o Grupo, os princípios de proteção contidos nas normas corporativas globais devem abranger os princípios de proteção da Diretiva de Proteção de Dados Pessoais – e, consequentemente, do GDPR – permitindo que os grupos empresariais constituam política de privacidade verdadeiramente global[338]. Vale mencionar que tais princípios podem significar pouco para empresas e colaboradores que tratam dados fora da União Europeia[339]. Assim, é imprescindível que as solicitações para aprovação das normas corporativas globais contenham descrições minuciosas de informações como o fluxo de dados pessoais, as transferências autorizadas, os destinos dos dados e as finalidades do tratamento, a fim de que se verifique se, o tratamento realizado em países terceiros é compatível com os níveis de proteção de dados pessoais da União Europeia[340].

Além disso, as normas corporativas devem ser, de fato, globais, aplicáveis ao grupo corporativo como um todo, independentemente do local de estabelecimento dos membros ou da nacionalidade das pessoas cujos dados pessoais estão sendo tratados[341]. As terminologias sugeridas pelo Grupo são: “regras corporativas vinculantes para transferências internacionais de dados" ou "regras corporativas legalmente exigíveis para transferências internacionais de dados"[342]. Nesse sentido, tais normas são: (i.) vinculativas ou legalmente exigíveis pois somente dessa forma são consideradas "garantias suficientes"; (ii.) corporativas, pois consistem nas regras em vigor nas empresas multinacionais, geralmente constituídas sob a

---

[336] **Artigo 26 (2) da Directiva 95/46/CE do Parlamento Europeu e do Conselho**, *op. cit.*
[337] UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 8. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.
[338] *Ibidem*
[339] *Ibidem,* p. 14.
[340] *Ibidem,* p. 10.
[341] *Ibidem*
[342] *Ibidem*

responsabilidade da matriz; e (iii.) cuja principal finalidade é a transferência internacional de dados[343].

Vale dizer, a noção de grupo corporativo pode variar de um país para outro e pode corresponder a realidades de negócios muito diferentes[344]. Tais diferenças na estrutura e atividade impactam sobre a aplicabilidade, projeto e escopo das regras corporativas obrigatórias e grupos corporativos devem ter isto em mente ao apresentar suas propostas[345]. Na prática, espera-se que as empresas multinacionais sejam as usuárias mais frequentes desses mecanismos, pois é benéfico para esse tipo de empresas que a regulação das transferências intragrupo em todo o mundo seja feita da mesma forma[346].

No mais, o Grupo destaca que as normas corporativas globais devem ser vinculantes, tanto interna quando externamente[347]. Nesse sentido, o Grupo afirma que, embora a aplicabilidade dos contratos e instrumentos possa ser demonstrada do ponto de vista conceitual, a verificação do efetivo exercício dos direitos dos titulares de dados pessoais no contexto transfronteiriço é uma tarefa mais complexa[348]. Isso porque é necessário avaliar se as entidades participantes das normas corporativas globais são de fato compelidas a cumprir as regras internas[349]. Daí a importância de se investigar se as empresas realizam treinamentos e capacitações voltadas à proteção de dados pessoais, se os colaboradores conhecem as políticas de proteção de dados pessoais e se têm informações sobre o tema facilmente alcançáveis, como, por exemplo, na intranet.

Ademais, o Grupo ressalta que as normas corporativas globais devem prever a realização de auditorias, bem como o dever cooperação com as autoridades de proteção de dados pessoais[350]. Desse modo, há a obrigação inequívoca de que todas

---

343 *Ibidem*
344 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 9. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.
345 *Ibidem*
346 UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 9. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.
347 *Ibidem,* p. 10.
348 *Ibidem,* p. 10.
349 *Ibidem,* p. 10.
350 *Ibidem,* p. 16.

as entidades do grupo corporativo aceitem eventuais auditorias e solicitações realizadas pelas autoridades nacionais[351]. Além disso, é imprescindível que todas as partes das normas corporativas globais cumpram as recomendações da autoridade nacional sobre as normas corporativas globais[352]. Também as normas devem estabelecer o sistema de atendimento das reclamações e solicitações dos titulares de dados pessoais[353].

Outrossim, o Grupo sublinha que o objetivo das normas, de um modo geral, é garantir que as autorizações concedidas para a transferência internacional dos dados pessoais não privarão os titulares de dados pessoais dos direitos detidos por eles caso seus dados não tivessem saído do território europeu[354]. Além disso, as normas devem apresentar disposições sobre a responsabilidade em caso de incidentes envolvendo os dados pessoais[355].

Por fim, é necessário que os grupos corporativos titulares de normas corporativas globais informem aos titulares de dados pessoais sobre a transferência transfronteiriça dos dados[356]. Com efeito, é primordial que se informe, aos titulares, a existência das normas corporativas globais, as obrigações assumidas pelo grupo corporativo e as formas como os titulares de dados pessoais podem verificar o cumprimento das regras[357].

Destarte, as normas corporativas globais são um conjunto de regras e políticas adotadas por um grupo corporativo para regular e amparar as transferências internacionais de dados pessoais entre suas entidades, garantindo um alto nível de proteção de dados pessoais em todas as suas operações. Percebe-se que tais normas configuram um instrumento útil para as empresas multinacionais que desejam implementar um regime uniforme de proteção de dados em todas as suas subsidiárias, independentemente da localização geográfica.

As normas corporativas globais podem, inclusive, gerar benefícios para a imagem das empresas, uma vez que demonstram compromisso com a proteção de

---

[351] *Ibidem,* p. 17.
[352] UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003, p. 17. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.
[353] *Ibidem,* p. 16.
[354] *Ibidem,* p. 18.
[355] *Ibidem,* p. 18.
[356] *Ibidem,* p. 19.
[357] *Ibidem,* p. 19.

dados pessoais e com o cumprimento das leis de proteção de dados aplicáveis. Isso pode, aumentar a confiança dos titulares de dados pessoais no grupo, pois a adoção das normas pode ser percebida como uma medida proativa para antecipar e gerenciar os riscos de privacidade e proteção de dados. Contudo, deve-se ter em mente que a adoção das normas corporativas globais envolve um processo rigoroso de aprovação pela autoridade nacional de proteção de dados, sendo essencial que as empresas estejam preparadas para demonstrar sua conformidade com a legislação de proteção de dados mesmo depois da aprovação das normas.

3.2 Como as Normas Corporativas Globais vêm sendo regulamentadas pelo ICO

No Reino Unido, o ICO é o órgão responsável por aprovar as normas corporativas globais[358]. O Órgão dispõe, em seu website, de um guia para orientar as companhias que buscam essa autorização[359]. O Guia divide suas diretrizes entre as destinadas às normas corporativas globais para controladores e as relativas aos operadores[360].

3.2.1 Normas Corporativas Globais para controladores e para operadores

As normativas europeias reconhecem a existência de normas corporativas globais para controladores e para operadores. As normas corporativas globais para controladores cuidam das transferências internacionais de dados realizadas de controladores estabelecidos na União Europeia para controladores ou operadores, do mesmo grupo empresarial, localizados fora da União Europeia[361]. Já as normas corporativas globais dos operadores tratam dos dados pessoais recebidos por um controlador localizado na União Europeia que não faz parte do grupo empresarial, sendo, os dados, posteriormente tratados por operadores e suboperadores membros do grupo[362].

---

[358] REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679. Acesso em: 23 fev. 2023.
[359] REINO UNIDO. Information Commissioner's Office. **Controller guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/. Acesso em: 10 mar. 2023.
[360] *Ibidem*
[361] **Binding Corporate Rules. The General Data Protection Regulation**. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf, p. 1. Acesso em: 23 mar. 2023
[362] *Ibidem*

Ambos os tipos de normas corporativas globais apresentam um conjunto similar de disposições – as destinadas aos operadores entretanto, têm obrigações adicionais específicas de uma relação controlador-operador[363]. Tais normas incluem deveres de cooperação com o controlador para todos os membros do grupo, suboperadores e funcionários[364]. Também as regras sobre auditoria de proteção de dados são mais detalhadas que o modelo aplicado aos controladores, devendo as avaliações da auditoria serem disponibilizadas ao controlador de dados[365]. Nesse sentido, o GDPR não faz distinção entre as normas destinadas aos controladores e as normas aplicadas aos operadores, mas apenas fornece um conjunto de normas aplicáveis a ambas[366].

O Guia elaborado pelo ICO diferencia as normas corporativas globais para operadores ao determinar que estas têm, como objetivo principal, permitir e proteger as transferências internacionais de dados pessoais entre membros do grupo corporativo do operador[367]. Nesse sentido, o Organismo ressalta que, por vezes, controladores externos do Reino Unido enviam dados para operadores membros do grupo que, apesar de abrangidos pelas normas corporativas globais, não estão localizados no Reino Unido[368]. É dizer: há situações em que controladores externos transferem dados para operadores estabelecidos fora do Reino Unido, e tais dados não passam por qualquer entidade localizada no país[369].

O art. 28 do GDPR do Reino Unido estabelece as regras para o tratamento de dados pessoais por um operador nome de um controlador[370]. O dispositivo prevê a obrigação de celebrar um contrato escrito entre o controlador e o operador que defina as condições para o tratamento de dados pessoais, bem como os direitos e responsabilidades de ambas as partes[371]. Além disso, o art. exige que o operador adote medidas técnicas e organizacionais apropriadas para garantir a segurança e proteção dos dados pessoais que ele processa. Nesse sentido, o ICO sustenta que,

---

363 *Ibidem*, p.6.
364 *Ibidem*
365 *Ibidem*
366 *Ibidem*
367 REINO UNIDO. Information Commissioner's Office. **Processor guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/processor-guidance/. Acesso em: 10 mar. 2023.
368 *Ibidem*
369 *Ibidem*
370 REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/28. Acesso em: 23 fev. 2023.
371 *Ibidem*

embora seu Guia não tenha o intuito de repetir as obrigações gerais para controladores e operadores, é extremamente necessário que tais obrigações sejam levadas em consideração[372].

Ademais, o Órgão enfatiza que não examina acordos contratuais específicos como parte do processo de aprovação das normas corporativas globais para operadores, mas espera que as partes ajam ao encontro destes[373]. Também ressalta que os acordos de tratamento de dados pessoais devem refletir os arranjos das normas corporativas globais em vigor para a transferência dos dados[374].

De modo geral, percebe-se que ambos controladores e operadores devem levar em conta os objetivos principais do capítulo V, do GDPR do Reino Unido, quais sejam: (i.) garantir que as proteções previstas no GDPR do Reino Unido não sejam limitadas; (ii.) assegurar que os titulares de dados pessoais não sofram quaisquer prejuízos; (iii.) proteger os direitos dos titulares de dados pessoais e também dos controladores – no que tange às garantidas fornecidas pelas normas corporativas globais para operadores[375].

3.2.2 Exigências do ICO

As normas corporativas globais do Reino Unido devem cumprir os requisitos do art. 47 do GDPR do Reino Unido, bem como eventuais diretrizes e exigências publicadas pelo ICO[376]. No GDPR do Reino Unido, o art. 47 é o responsável por tratar das normas corporativas globais[377]. A primeira exigência para que as normas sejam aprovadas é que estas sejam juridicamente vinculativas e aplicáveis, sendo cumpridas por todos os membros do grupo empresarial envolvidos na atividade econômica conjunta, incluindo colaboradores[378].

---

372 REINO UNIDO. Information Commissioner's Office. **Processor guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/processor-guidance/. Acesso em: 10 mar. 2023.
373 *Ibidem*
374 *Ibidem*
375 **Binding Corporate Rules. The General Data Protection Regulation**. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 23 mar. 2023
376 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for data Controllers**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/application-for-approval-of-uk-binding-corporate-rules-for-data-controllers/. Acesso em: 10 mar. 2023.
377 REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/47. Acesso em: 23 fev. 2023.
378 *Ibidem*

Além disso, as normas devem conferir, de maneira expressa, direitos aplicáveis aos titulares no que diz respeito ao tratamento dos dados pessoais[379]. No Guia elaborado pelo ICO, o Órgão ressalta que as normas corporativas globais devem garantir, aos titulares de dados pessoais, direitos aplicáveis e efetivos, assegurando que os indivíduos não enfrentem quaisquer obstáculos adicionais para fazer valer tais direitos[380].

Também, estabelece-se no art. 47 do GDPR do Reino Unido, que, para serem aprovadas pelo ICO, as normas corporativas globais devem conter algumas informações[381]. Dentre elas está a estrutura e as informações de contato do grupo empresarial que realizará a transferência internacional de dados[382]. Igualmente, as normas devem conter a descrição das transferências a serem realizadas, relatando, também, as categorias de dados pessoais envolvidas; os tipos de tratamentos; as finalidades dos tratamentos; os tipos de titulares de dados afetados e a identificação dos países terceiros ou organismos internacionais[383]. No mais, o instrumento deve expressar a natureza juridicamente vinculante em âmbito interno e externo, bem como estabelecer a aplicação dos princípios gerais de proteção de dados, especialmente: (i.) a limitação da finalidade; (ii.) a minimização dos dados; (iii.) o período de armazenamento; (iv.) a qualidade dos dados; (v.) a proteção de dados *by design*[384] e *by default*[385]; (vi.) a base legal para o tratamento; (vii.) o tratamento de categorias

---

379 *Ibidem*

380 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for data Controllers**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/application-for-approval-of-uk-binding-corporate-rules-for-data-controllers/. Acesso em: 10 mar. 2023.

381 REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/47. Acesso em: 23 fev. 2023.

382 *Ibidem*

383 REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/47. Acesso em: 23 fev. 2023.

384 A proteção de dados by design, ou desde a concepção, diz respeito a implementação de medidas técnicas e organizacionais nos estágios iniciais do design das operações de tratamento de dados, de modo a salvaguardar os princípios da privacidade e da proteção de dados desde o início (UNIÃO EUROPEIA. Comissão Europeia. **What does data protection by design and by default mean?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. Acesso em: 29 mar. 2023).

385 A proteção de dados by default, ou por padrão, busca garantir que os dados pessoais tratados recebam a maior proteção possível (com o cuidado, por exemplo, de que apenas os dados necessários sejam tratados, que sejam armazenados por período curto, e tenham seu acesso limitado) (UNIÃO EUROPEIA. Comissão Europeia. **What does data protection by design and by default mean?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. Acesso em: 29 mar. 2023).

especiais de dados pessoais; (viii.) as medidas para garantir a segurança dos dados e os requisitos relativos às transferências posteriores para órgãos não vinculados às normas corporativas globais[386].

Outrossim, devem estar dispostos, nas normas corporativas globais, os direitos dos titulares de dados pessoais em relação ao tratamento dos dados e aos meios para exercer esses direitos – incluindo o direito de não serem alvos de decisões baseadas exclusivamente em tratamento automatizado de dados; o direito de apresentarem

---

[386] **Artigo 47 do General Data Protection Regulation – UK.** Tradução nossa, do original: "*Article 47.* Binding corporate rules. 1.[F1The Commissioner] shall approve binding corporate rules F2... , provided that they: (a)are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees; (b)expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and (c)fulfil the requirements laid down in paragraph 2. 2.The binding corporate rules referred to in paragraph 1 shall specify at least: (a)the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; (b)the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c)their legally binding nature, both internally and externally; (d)the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules; (e)the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with [F3the Commissioner and before a court in accordance with Article 79 (see section 180 of the 2018 Act], and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; (f)the acceptance by the controller or processor [F4established in the United Kingdom] of liability for any breaches of the binding corporate rules by any member concerned [F5not established in the United Kingdom]; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage; (g)how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14; (h)the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling; (i)the complaint procedures; (j)the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to [F6the Commissioner]; (k)the mechanisms for reporting and recording changes to the rules and reporting those changes to [F7the Commissioner]; (l)the cooperation mechanism with [F8the Commissioner] to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to [F8the Commissioner] the results of verifications of the measures referred to in point (j); (m)the mechanisms for reporting to [F9the Commissioner] any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and (n)the appropriate data protection training to personnel having permanent or regular access to personal data (REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/47. Acesso em: 23 fev. 2023).

reclamação ao ICO e o direito de obtenção de reparação por eventuais violações das normas corporativas globais[387]. Ademais, as normas devem conter a aceitação, pelo controlador ou operador, da responsabilidade por qualquer violação das normas corporativas globais por qualquer entidade do grupo titular das normas corporativas globais[388].

Também deve estar descrita no instrumento: (i.) a forma como as informações sobre as normas corporativas globais são fornecidas aos titulares de dados pessoais; (ii.) as tarefas do encarregado de proteção de dados ou qualquer outro indivíduo ou entidade encarregada de monitorar o cumprimento das nas normas corporativas globais, bem como acompanhar os treinamentos e o gerenciamento de reclamações; como se dão os procedimentos de reclamação; e (iii.) os mecanismos utilizados para assegurar o cumprimento das normas corporativas globais[389]. Vale dizer, tais mecanismos devem incluir auditorias de proteção de dados e métodos para assegurar ações corretivas para proteger os direitos dos titulares de dados, e seus resultados devem ser comunicados à pessoa ou entidade responsável pelo cumprimento das normas corporativas globais, ao conselho da empresa controladora do grupo corporativo e ao ICO, mediante solicitação[390].

Ainda, as normas devem compreender a descrição dos mecanismos utilizados para informar e registrar mudanças nas próprias normas, bem como o procedimento utilizado para comunicar tais mudanças ao ICO[391]. É imprescindível, também, que as normas incluam mecanismos de cooperação com o ICO, bem como de prestação de informações acerca de eventuais demandas legais aos quais um membro do grupo empresarial esteja sujeito em um país terceiro, que possa influenciar de forma substancial as garantias fornecidas pelas normas corporativas globais[392]. Por fim, o art. 47 estabelece que as normas devem dispor sobre treinamentos de proteção de dados conduzidos ao quadro de funcionários com acesso permanente ou regular a dados pessoais[393].

---

387 *Ibidem*
388 *Ibidem*
389 REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/47. Acesso em: 23 fev. 2023.
390 *Ibidem*
391 *Ibidem*
392 *Ibidem*
393 *Ibidem*

Outro requisito imposto pelo Órgão é que a companhia que venha a utilizar as normas corporativas globais nomeie pessoa jurídica com personalidade jurídica no Reino Unido para como a responsável por essas normas[394]. No caso de a companhia apresentar entidade que não é pessoa jurídica no Reino Unido, é necessário que se forneça provas complementares, para assegurar que os direitos dos titulares serão respeitados[395]. Dentre essas provas estão: (i.) a aceitação de encargos de qualquer procedimento legal; (ii.) a disponibilidade de ativos suficientes para atender todas as responsabilidades resultantes das normas; e (iii.) a intervenção da matriz – britânica – no caso de qualquer deficiência jurídica no Reino Unido[396].

É de suma importância que a pessoa jurídica designada arque com os deveres e responsabilidades atinentes às normas corporativas globais no Reino Unido[397]. Por esse motivo, durante o processo de análise, o ICO procura obter garantias de que as entidades britânicas indicadas sejam capazes de encarregar-se financeiramente de quaisquer violações das normas corporativas globais[398]. Ressalta-se que, em caso de qualquer violação aos direitos dos titulares de dados pessoais, a responsabilidade pelo ônus da prova é das pessoas jurídicas britânicas delegadas para as normas corporativas globais do Reino Unido[399].

No mais, a supervisão regulatória das normas corporativas globais deve ser feita por todos os membros que aderem às normas corporativas globais[400]. De qualquer sorte, o ICO almeja que as entidades jurídicas britânicas sejam capazes de sozinhas, suprir todas as necessidades relacionadas à conformidade com as normas[401].

O ICO não impõe às companhias, como parte do processo de aprovação das normas corporativas globais, que tragam evidências da realização de análises de riscos das transferências internacionais de dados pessoais[402]. No entanto, é

---

394 REINO UNIDO. Information Commissioner's Office. **Controller guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/. Acesso em: 10 mar. 2023.
395 *Ibidem*
396 *Ibidem*
397 REINO UNIDO. Information Commissioner's Office. **Controller guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/. Acesso em: 10 mar. 2023.
398 *Ibidem*
399 *Ibidem*
400 *Ibidem*
401 *Ibidem*
402 *Ibidem*

necessário que as companhias conduzam avaliações de risco de transferência sempre que houver transferências de dados pessoais do Reino Unido para um país terceiro[403]. Também é importante que tais avaliações sejam revisadas periodicamente, e as normas corporativas globais adaptadas sempre que necessário[404].

Segundo o art. 47 do GDPR do Reino Unido as normas corporativas globais, no Reino Unido, compreendem: (i.) o formulário de requerimento; (ii.) o instrumento vinculativo; (iii.) a tabela de referência; (iv.) a política de normas corporativas globais; e (v.) outras políticas e procedimentos (relevantes) referenciados dentro das normas[405].

O primeiro documento mencionado, pelo ICO, como necessário, é o formulário de solicitação. No caso, o Órgão disponibiliza dois tipos: o Formulário de Solicitação de Aprovação das Normas Corporativas Globais para Controladores do Reino Unido (Anexo A)[406] e o Formulário de Solicitação de Aprovação das Normas Corporativas Globais para Operadores (Anexo B)[407]. Tais documentos, a serem entregues para o ICO, são responsáveis por trazer informações adicionais, no intuito de garantir que os requerentes compreenderam as exigências do art. 47 do GDPR do Reino Unido e as aplicaram na prática[408]. É dizer: as companhias devem ser capazes de demonstrar como pretendem incorporar as normas corporativas globais e como estas serão gerenciadas e monitoradas[409].

As respostas fornecidas devem ser completas. Nesse sentido, quando houver mais de uma entidade legal britânica enviando dados para fora do Reino Unido, é esperado que as companhias descrevam os fluxos de dados, os tipos de titulares de

---

[403] *Ibidem*
[404] *Ibidem*
[405] REINO UNIDO. Information Commissioner's Office. **Controller guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/. Acesso em: 10 mar. 2023.
[406] REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for controllers.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021123/bcr-controller-application-form.docx. Acesso em: 10 mar. 2023.
[407] REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for processors.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021124/bcr-processor-application-form.docx. Acesso em: 10 mar. 2023.
[408] REINO UNIDO. Information Commissioner's Office. **Controller guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/. Acesso em: 10 mar. 2023.
[409] *Ibidem*

dados, as categorias de dados e os países de destino para cada uma das entidades exportadoras[410].

Primeiramente, em ambos os tipos de formulário, são solicitados os dados de contato do Requerente e a estrutura do grupo de empresas em questão[411]. Dentre as informações solicitadas estão: (i.) o nome do grupo; (ii.) o endereço da matriz; (iii.) o nome, endereço e número de registro da entidade jurídica britânica (com responsabilidade delegada) ou nome, endereço e número de registro da empresa britânica de todas as entidades jurídicas britânicas do grupo; (iv.) nome e endereço da pessoa jurídica britânica que trata das reclamações a respeito das normas corporativas globais britânicas; (v.) natureza jurídica da pessoa ou pessoas jurídicas com responsabilidade delegada; (vi.) a descrição da estrutura corporativa e localização geográfica de todos os membros a serem vinculados pelas normas corporativas globais, com documento explicando a estrutura do grupo em anexo; (vii.) nome, cargo e informações de contato do indivíduo responsável pela solicitação; e (viii.) nome, título e informações de contato de qualquer advogado externo ou consultor instruído a agir em nome do candidato[412].

A segunda seção diz respeito à descrição do fluxo das transferências de dados pessoais realizadas pelo grupo, em atenção ao art. 47(2)(b)[413] do GDPR do Reino Unido[414]. Nesse campo, é necessário incluir a categoria ou as categorias de dados pessoais transferidos, bem como o tipo de tratamento realizado e os seus objetivos[415]. Além disso, é importante que se explique os tipos de titulares de dados afetados pelo tratamento, listando-se, também, todos os países terceiros para os quais os dados são transferidos[416]. Nesta seção, o Formulário atinente aos operadores se difere do

---

410 *Ibidem*
411 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for controllers.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021123/bcr-controller-application-form.docx. Acesso em: 10 mar. 2023.
412 *Ibidem*
413 REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/47. Acesso em: 23 fev. 2023.
414 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for controllers.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021123/bcr-controller-application-form.docx. Acesso em: 10 mar. 2023.
415 *Ibidem*
416 *Ibidem*

referente aos controladores pois são realizados questionamentos adicionais, específicos sobre a dinâmica das normas corporativas globais para operadores[417].

Com efeito, questiona-se ao grupo se este permite que os terceiros controladores de dados pessoais transfiram os dados do Reino Unido diretamente para membros das normas corporativas globais sediados em outros países, ou se exige que todos os controladores terceiros enviem, primeiramente, os dados pessoais a uma entidade abrangida pelas normas corporativas globais que esteja localizada no Reino Unido, para que depois esta entidade envie às empresas sediadas em outras localidades. Além disso, é demandado que o grupo forneça garantias de que as obrigações do art. 28, do GDPR do Reino Unido[418] estão satisfeitas[419]. Ademais, é questionada ao grupo a probabilidade de que um dos seus membros realize atividades como suboperador de dados pessoais em nome de outros membros do grupo[420]. Caso a resposta seja positiva, devem ser fornecidas informações para comprovar que esta relação amparada por instrumento contratual[421].

A terceira seção trata da responsabilidade civil, sendo necessária, basicamente, a confirmação de que a pessoa jurídica delegada dispõe de recursos suficientes para arcar com as responsabilidades sob as normas corporativas globais[422]. A próxima seção cuida do pessoal designado para a proteção de dados. Nesse sentido, é necessário que se traga evidências de que foi constituída equipe para supervisionar e assegurar a conformidade das normas corporativas globais[423]. Assim, importante que a companhia explique de que forma esta rede, ou equipe, opera, descrevendo a sua estrutura, responsabilidades, e funções, por meio de organograma[424].

---

417 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for processors.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021124/bcr-processor-application-form.docx. Acesso em: 10 mar. 2023.
418 REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/28. Acesso em: 23 fev. 2023.
419 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for processors.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021124/bcr-processor-application-form.docx. Acesso em: 10 mar. 2023.
420 *Ibidem*
421 *Ibidem*
422 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for controllers.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021123/bcr-controller-application-form.docx. Acesso em: 10 mar. 2023.
423 *Ibidem*
424 *Ibidem*

A seção seguinte diz respeito à conformidade e às auditorias. Nesse sentido, necessário que o requerente descreva os mecanismos utilizados para assegurar a conformidade de cada um dos membros com as normas corporativas globais, bem como a frequência na qual essas conferências são realizadas[425]. Além disso, o solicitante deve explicar como funciona o programa de *compliance* dentro do grupo, bem como esclarecer se há documento formalizando os procedimentos[426].

Na seção de relatórios e registros, o grupo requerente deve informar tudo aquilo que está em vigor para, se necessário, registrar mudanças nas normas corporativas globais ou na lista de membros[427]. Além disso, o grupo deve confirmar que, caso solicitado pelo ICO, fornecerá qualquer relatório de auditoria, sem restrições[428]. Da mesma forma, deve confirmar que o grupo – como um todo ou separadamente – cooperará com o ICO no que tange ao cumprimento das normas corporativas globais[429]. Outrossim, é necessário que o solicitante esclareça ao ICO se há exigências legais dos membros das normas corporativas globais localizados em países terceiros capazes de gerar prejuízos às garantias que estão sendo concedidas sob as normas corporativas globais do Reino Unido[430].

Por último, trata-se do treinamento e da conscientização dos funcionários das empresas do grupo corporativo. Destarte, o grupo solicitante deve fornecer documentação atinente às políticas e procedimentos para comprovar que as normas corporativas globais são comunicadas a todo o grupo[431]. Ainda, quando necessário, o requerente deve anexar evidências dos treinamentos e testes de conhecimentos realizados com seus colaboradores, bem como demonstrar que todos os funcionários que têm acesso permanente ou regular aos dados pessoais recebem treinamento sobre as normas corporativas globais[432]. Outrossim, o grupo deve explicar quem é o responsável pelo monitoramento de tais tratamentos[433]. Ainda, no caso do Formulário para Operadores, faz-se necessário que o grupo liste como notificará o controlador de dados no caso de requisitos legais das normas corporativas globais de outros países

---

425 *Ibidem*
426 *Ibidem*
427 REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for controllers.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021123/bcr-controller-application-form.docx. Acesso em: 10 mar. 2023.
428 *Ibidem*
429 *Ibidem*
430 *Ibidem*
431 *Ibidem*
432 *Ibidem*
433 *Ibidem*

gerarem efeitos adversos às garantias previstas nas normas corporativas globais do Reino Unido[434].

O segundo documento consiste no instrumento vinculativo, a ser firmado pelas empresas titulares das normas corporativas globais para controladores[435] e para operadores[436]. Destarte, o ICO destaca que, nos termos do art. 47 (1) (b), do GDPR do Reino Unido, os direitos dos titulares de dados devem ser efetivos e executáveis e, portanto, as normas corporativas globais devem ser efetivas e executáveis em âmbito interno e externo[437]. Assim, o Órgão destaca a sua preferência pela realização de um acordo intragrupo, uma vez que este instrumento é capaz de assegurar a segurança jurídica dos direitos protegidos pelas normas corporativas globais[438]. De qualquer sorte, o ICO ressalta que se o grupo requerente optar por apresentar instrumento diferente do acordo intragrupos, deve fornecer detalhes de como o instrumento será, de fato, vinculativo[439].

O terceiro documento é a política de normas corporativas globais[440]. No que tange ao seu conteúdo, o ICO ressalta que deve ser expresso de forma compreensível para os titulares de dados, lembrando o grupos de não copiarem informações de outros locais apenas por tratarem do mesmo tema[441]. Isto é, ainda que o instrumento vinculativo e a política tragam a mesma informação, as informações dentro do instrumento vinculante satisfarão a estrutura contratual prevista em Lei, enquanto as disposições da política devem atender às demandas do público[442].

No mais, o preenchimento da Tabela de Referências para as Normas Corporativas Globais para Controladores (Anexo C)[443] e a Tabela de Referências para

---

[434] REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for processors.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021124/bcr-processor-application-form.docx. Acesso em: 10 mar. 2023.

[435] REINO UNIDO. Information Commissioner's Office. **Controller guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/. Acesso em: 10 mar. 2023.

[436] REINO UNIDO. Information Commissioner's Office. **Processor guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/processor-guidance/. Acesso em: 10 mar. 2023.

[437] *Ibidem*

[438] *Ibidem*

[439] *Ibidem*

[440] *Ibidem*

[441] *Ibidem*

[442] *Ibidem*

[443] REINO UNIDO. Information Commissioner's Office. **UK BCR Referential Table.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021115/uk-bcr-referential-table.docx. Acesso em: 29 mar. 2023.

as Normas Corporativas Globais para Operadores (Anexo D)[444] são necessárias para a requisição das normas corporativas globais de ambos os agentes de tratamento. Desse modo, as tabelas trazem campos com os arts. 47 – sobre normas corporativas globais – e 28 – sobre obrigações dos operadores, no caso das normas corporativas globais para operadores – nos quais os requerentes devem sinalizar quais os documentos entregues ao ICO contêm as informações, bem como explicar onde, no documento a informação está disponível[445]. Assim, no caso de o ICO considerar que o solicitante não atendeu à requisição, há um campo no qual o Órgão explica e justifica o porquê de os requisitos não foram cumpridos[446].

Ainda, os grupos solicitantes devem incluir políticas ou procedimentos de apoio relevantes em seus requerimentos[447]. Dentre eles, algumas documentações relevantes são as atinentes aos treinamentos, às auditorias, aos procedimentos de atendimento das reclamações e à comunicação, ao público, sobre as normas corporativas globais[448]. Basicamente, as políticas e procedimentos evidenciam de forma clara a estrutura e a forma como o grupo empresarial assume as suas responsabilidades[449]. Assim, todas as políticas e procedimentos devem estar em conformidade com a GDPR do Reino Unido de forma abrangente e específica[450]. Por conseguinte, para que possamos ilustrar como se configura o instrumento de política de normas corporativas globais na prática, tratar-se-á, no próximo subcapítulo, das normas corporativas globais para controladores da multinacional Amgen, já aprovadas pelo ICO.

3.3. As Normas Corporativas Globais para controladores – caso Amgen

A Amgen, Inc. é uma empresa de biotecnologia com sede na Califórnia que se dedica à descoberta, desenvolvimento, fabricação e comercialização de terapias

---

[444] REINO UNIDO. Information Commissioner's Office. **UK BCR Referential Table – Annex 1.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021119/uk-bcr-referential-table-annex-1.docx. Acesso em: 29 mar. 2023.
[445] REINO UNIDO. Information Commissioner's Office. **UK BCR Referential Table – Annex 1.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021119/uk-bcr-referential-table-annex-1.docx. Acesso em: 29 mar. 2023.
[446] REINO UNIDO. Information Commissioner's Office. **UK BCR Referential Table – Annex 1.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021119/uk-bcr-referential-table-annex-1.docx. Acesso em: 29 mar. 2023.
[447] *Ibidem*
[448] *Ibidem*
[449] *Ibidem*
[450] *Ibidem*

humanas[451]. Seus produtos incluem as seguintes marcas: Aranesp, BLINCYTO, Corlanor, ENBREL, EPOGEN, IMLYGIC, KYPROLIS, Neulasta, NEUPOGEN, Nplate, Parsabiv, Prolia, Repatha, Sensipar, Vectibix e XGEVA[452].

Ao acessar o website da empresa, encontramos uma página especialmente dedicada às normas corporativas globais, na qual a companhia esclarece ao público que as normas corporativas globais são regras internas implementadas para viabilizar as transferências de dados pessoais dentro do grupo Amgen[453]. Nesse sentido, a empresa disponibiliza quatro modelos de normas corporativas globais: um europeu, um britânico, um argentino e, inclusive, um brasileiro[454].

O modelo britânico de normas corporativas globais (Anexo E)[455] inicia introduzindo o tema das normas corporativas globais e definindo seu escopo[456]. Assim, a empresa declara que estas normas expressam seu compromisso com a privacidade e a proteção de dados[457]. Além disso, a Amgen ressalta a obrigatoriedade dos participantes das normas corporativas globais de respeitarem tais as regras[458]. Além disso, a empresa disponibiliza lista de todas as empresas participantes das normas corporativas globais, bem como canal de contato[459]. Ainda, declara que a Amgen UK é a entidade responsável por garantir a conformidade das empresas participantes das normas corporativas globais do Reino Unido[460].

Quanto ao escopo, ressalta que as normas se aplicam a transferências e tratamentos, automatizados ou não, de todos os dados pessoais realizados por uma entidade do Grupo Amgen que atua como controladora de dados ou como operadora de dados para outra entidade do Grupo atuando como controladora[461]. Nesse sentido, as situações abrangidas pelas normas corporativas globais são: (i.) quando o operador está estabelecido no Reino Unido; (ii.) quando o operador não está

---

451 FORBES. **Amgen**. Disponível em: https://www.forbes.com/companies/amgen/?sh=6aee72f56ae3. Acesso em: 28 mar. 2023.
452 *Ibidem*
453 AMGEN. **Business Conduct and Ethics**. Disponível em: https://www.amgen.com/bcr. Acesso em: 29 mar. 2023.
454 *Ibidem*
455 **Amgen UK Binding Corporate Rules (UK BCRs).** AMGEN, November 2021. Disponível em: https://www.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-uk-bcr-final-including-appendices.pdf. Acesso em: 23 mar. 2023.
456 *Ibidem,* p.1.
457 *Ibidem,* p.1.
458 *Ibidem,* p.1.
459 *Ibidem,* p.1.
460 *Ibidem,* p.1.
461 *Ibidem,* p.1.

estabelecido no Reino Unido e recebeu as informações do controlador estabelecido no Reino Unido; (iii.) quando serão realizadas transferências futuras de dados pessoais de importadores de dados para importadores de dados[462].

Após, são tratados conceitos relativos à proteção de dados pessoais, como por exemplo, controlador de dados pessoais; operador de dados pessoais; consentimento; tratamento de dados pessoais; titular de dados; e dados pessoais sensíveis[463]. Também, esclarece-se que os dados serão tratados para finalidades explícitas, especificadas e legítimas, nos termos do art. 5 (1) (b), do GDPR do Reino Unido[464]. Além disso, informa-se que o tratamento dos dados pessoais será alterado somente mediante o consentimento dos titulares de dados pessoais ou determinação legal[465]. Ainda, ressalta-se que dados pessoais sensíveis receberão tratamento com salvaguardas adicionais[466].

No mais, informa-se que o tratamento de dados pessoais se dará de modo a limitar a coleta, o tratamento e a utilização das informações – mantendo-as apenas para razões estritamente necessárias, com anonimização ou pseudonimização dos dados quando possível[467]. São elencadas, também, as bases legais para o tratamento de dados pessoais, ressaltando ao público que o tratamento será realizado somente quando presente uma das hipóteses autorizadoras[468]. Da mesma forma, são informadas as bases legais para o tratamento de dados sensíveis, que são mais restritas[469].

Além disso, enfatiza-se a atenção ao respeito ao princípio da transparência para com os titulares de dados pessoais, estabelecendo canais de comunicação disponíveis para reclamações, solicitações de informações e retificações dos dados pessoais[470]. No mais, as normas trazem o direito dos titulares de dados de não serem submetidos a decisões baseadas unicamente no tratamento automatizado de dados, explicando, elencando, também, as exceções (execução de contrato, determinação legal ou consentimento)[471].

---

[462] *Ibidem,* p.1.
[463] *Ibidem,* p.2-4.
[464] *Ibidem,* p.4-5.
[465] *Ibidem,* p.5.
[466] *Ibidem,* p.5.
[467] *Ibidem,* p.5.
[468] *Ibidem,* p.5-6.
[469] *Ibidem,* p.6.
[470] *Ibidem,* p.7-8.
[471] *Ibidem,* p.8-9.

Ademais, a Amgen informa que implementa medidas de segurança técnicas e organizacionais, como o protocolo ISO/IEC 27002, para detectar e se proteger de incidentes de privacidade[472]. Outrossim, declara que escolherá os operadores de dados pessoais de forma cuidadosa, atentando-se às medidas de segurança utilizadas[473].

Ainda, a empresa faz ressalva sobre as transferências de dados pessoais subsequentes, aduzindo que devem estar em conformidade com as leis de proteção de dados do Reino Unido[474]. No mais, a companhia afirma conduzir treinamentos sobre proteção de dados aos seus colaboradores anualmente[475]. Nesse sentido, funcionários com acesso regular ou permanente a dados pessoais, envolvidos na coleta e tratamento de informações, recebem treinamentos específicos[476].

A Amgen também informa que são realizadas, periodicamente, auditorias abrangentes, que incluem proteção de dados em seu escopo[477]. De qualquer sorte, a empresa declara que são feitas, também, auditorias específicas, como a verificação de conformidade com o GDPR do Reino Unido, por exemplo[478]. A empresa ressalta, que o ICO pode receber cópias do resultado da auditoria, sendo que cada participante das normas corporativas globais deve aceitar serem inspecionados pelo ICO[479]. De fato, as empresas participantes das normas corporativas globais têm o dever de cooperar e ajudar umas as outras a lidar com solicitações e reclamações dos titulares de dados, bem como investigações ou auditorias realizadas pelo ICO[480].

Ademais, a Amgen declara nomear pessoal adequado para lidar com as questões de privacidade e proteção de dados[481]. Explicando um pouco da sua estrutura, a empresa atesta que possui um *Chief Privacy Officer*, responsável pela equipe de conformidade global de privacidade[482]. No mais, a empresa mantém uma rede de encarregados de proteção de dados pessoais, garantindo que cada país onde a Amgen opera, possui encarregado designado[483]. Outrossim, a empresa dispõe de

---

472 *Ibidem,* p.9.
473 *Ibidem,* p.9-10.
474 *Ibidem,* p.11.
475 *Ibidem,* p.11.
476 *Ibidem,* p.11.
477 *Ibidem,* p.11.
478 *Ibidem,* p.11.
479 *Ibidem,* p.11.
480 *Ibidem,* p.16.
481 *Ibidem,* p.12.
482 *Ibidem,* p.12.
483 *Ibidem,* p.12.

procedimento formalizado sobre eventuais reclamações, dos titulares de dados, acerca da não conformidade da Amgen com o GDPR do Reino Unido[484].

Outrossim, a empresa declara que os titulares dos dados pessoais sujeitos à transferência internacional podem buscar reparação judicial e compensação por danos resultantes de eventuais violações[485]. Nesse sentido, a Amgen do Reino Unido ressalta aceitar a responsabilidade de reparar os atos das empresas abrangidas pelas normas corporativas globais estabelecidas fora do Reino Unido[486].

Ainda, a Amgen afirma seu direito de revisar e atualizar as normas a qualquer momento, bem como manter lista atualizada das empresas participantes das normas corporativas globais e comunicar mudanças substanciais aos titulares de dados pessoais[487]. Também, a empresa manifesta que, caso as leis nacionais aplicáveis a uma empresa participante das normas corporativas globais exijam nível mais alto de proteção de dados pessoais, essas serão aplicadas[488]. No mais, havendo conflito entre as duas normas, isto deverá ser comunicado ao *Chief Privacy Officer*[489].

Finalmente, as regras trazem dois apêndices: o primeiro trata do fluxo dos dados pessoais tratados, e o segundo dos treinamentos conduzidos aos colaboradores[490]. O primeiro apêndice, busca mapear os fluxos de dados pessoais tratados pela empresa, define quem são os titulares de dados de cada tratamento, quais as categorias de dados tratados, as finalidades e, ainda, como ocorre a transferência internacional[491]. No caso, são transferidos dados pessoais de colaboradores, profissionais da área da saúde, fornecedores e voluntários de ensaios clínicos, todos da Amgen do Reino Unido para a Amgen dos Estados Unidos ou da Suíça[492]. Vale dizer, por se tratar de uma empresa que produz medicamentos, muitos dos dados transferidos são considerados sensíveis. O segundo apêndice, que trata dos treinamentos, divide-os em treinamentos gerais, que ocorrem anualmente para todos os colaboradores; treinamentos específicos para os encarregados de dados, que são feitos regularmente por uma equipe global; e treinamentos específicos, que

---

[484] *Ibidem,* p. 14.
[485] *Ibidem,* p. 15.
[486] *Ibidem,* p. 15.
[487] *Ibidem*, p. 16.
[488] *Ibidem*, p. 17.
[489] *Ibidem*, p. 17.
[490] *Ibidem*, p. 17.
[491] *Ibidem*, p. 18-19.
[492] *Ibidem,* p. 18-19.

normalmente são conduzidos para determinados grupos, de acordo com as atividades desempenhadas por eles[493].

3.4 Desafios e alternativas para a ANPD

Ao observamos o processo de aprovação da ICO para as normas corporativas globais, bem como o exemplo das normas da multinacional Amgen, aprovadas pelo Órgão, é certo que podemos aproveitar uma série de aprendizados para a experiência brasileira.

Destarte, percebe-se que o procedimento de aprovação das normas corporativas globais no Reino Unido, além de extenso, é bastante minucioso. Primeiramente, o art. 47, do GDPR do Reino Unido traz, de forma detalhada, as condições para aprovação das normas corporativas globais. Isto é, o ICO aprovará as normas corporativas globais desde que estas sejam legalmente vinculativas, confiram direitos exigíveis aos titulares de dados e sejam aplicadas por todos os membros do grupo de empresas que requer a aprovação das normas. Ainda, o grupo deve cumprir requisitos como: (i.) informar a estrutura e detalhes de contato do grupo de empresas solicitante; (ii.) informar os tipos de dados pessoais transferidos as finalidades do tratamento; (iii.) comprovar a natureza vinculativa das regras, a aplicação dos princípios de proteção de dados e o respeito aos direitos dos titulares de dados; (iv.) arcar com responsabilidade por violações das regras; (v.) cuidar dos procedimentos de reclamação; (vi.) realizar auditorias e treinamentos; e (vii.) cooperar com o ICO.

De fato, as disposições do art. 47 são refletidas no processo de aprovação das normas corporativas globais pelo ICO. A partir da análise do Guia Orientativo elaborado pelo ICO, verifica-se que o processo de aprovação das normas é cuidadoso e rigoroso. Isso porque a documentação exigida pelo Órgão – formulário, instrumento vinculativo, política de normas corporativas globais e tabela de referência – demonstra como os grupos corporativos coletam, usam, armazenam e protegem os dados pessoais dos titulares.

Ainda, ressalta-se que o ICO está apto a realizar questionamentos adicionais, caso necessário, para compreender como os requerentes lidam com solicitações de acesso, retificação e exclusão de dados pessoais, bem como de que forma garantem

---

[493] *Ibidem*, p. 20.

a conformidade com as regulamentações de proteção de dados. Com isso, o Órgão se compromete a aprovar as normas corporativas globais somente quando puder atestar que os direitos e garantias dos titulares de dados pessoais estão sendo preservados.

As normas corporativas globais para controladores da Amgen configuram um conjunto de políticas e procedimentos que visam padronizar o nível de proteção de dados em todas as empresas abrangidas pelas normas. As normas são fundamentadas no GDPR do Reino Unido e em outras regulamentações aplicáveis, como o *Data Protection Act*. Da análise, percebe-se que as normas corporativas globais da Amgen estão em conformidade com princípios legais resguardados pelo ICO.

As normas corporativas globais da Amgen referem-se aos princípios norteadores das normativas de proteção de dados, como, por exemplo, o princípio da finalidade, ao aduzir que os dados serão tratados para finalidades explícitas, especificadas e legítimas. Também diz respeito ao princípio da necessidade, informando que o tratamento de dados pessoais será feito de modo a limitar o uso dos dados, que ocorrerá apenas para aquilo que for necessário. Outrossim, a empresa destaca que o tratamento de dados sensíveis é feito com salvaguardas especiais, tal como requerem as legislações de proteção de dados.

Ademais, prezando pela transparência, as normas corporativas globais da Amgen estabelecem canais de comunicação para reclamações, solicitação de informações e retificação dos dados. Ainda, o documento trata da possibilidade de reparação judicial e compensação dos titulares de dados pessoais por danos resultantes de eventuais violações, deixando claro que a Amgen do Reino Unido aceita a responsabilidade de reparar os atos das empresas abrangidas pelas normas corporativas globais estabelecidas fora do Reino Unido. Nesse sentido, a empresa também declarou que a Amgen do Reino Unido é a entidade responsável por garantir a conformidade das empresas participantes nas normas corporativas globais.

Assim, verifica-se tanto o procedimento de aprovação das normas corporativas globais pelo ICO é abrangente e efetivo em garantir a proteção dos dados pessois, quanto as normas corporativas globais da Amgen, sob o GDPR do Reino Unido, são eficazes em definir os direitos dos titulares de dados que incluem o direito de acesso, retificação, exclusão e portabilidade dos seus dados pessoais, trazendo disposições – de forma acessível e compreensível – sobre como esses direitos serão

mantidos. Desse modo, considerando o exemplo das normas corporativas globais britânicas, é certo que estas podem fornecer boas orientações ao Brasil, sendo um exemplo bastante útil de como implementar políticas e procedimentos eficazes de proteção de dados pessoais.

Inclusive, interessante mencionar que as normas corporativas globais da Amgen aplicadas ao Brasil[494], apesar de estarem demonstrando a conformidade com a LGPD, seguem a mesma estrutura das normas britânicas, uma vez que seus dispositivos legais encontram equivalências. Tais normas são um método efetivo para que a subsidiária brasileira possa realizar transferências internacionais de dados pessoais ainda que as normas corporativas globais não tenham sido, ainda, reguladas pela ANPD.

De fato, este método de seguir a estrutura de documentos elaborados ou aprovados pelo ICO não é novidade para o Brasil. O ICO disponibilizou modelo de relatório de impacto à proteção de dados pessoais[495-496] e, utilizando esse exemplo, nosso Governo Federal publicou, em 2021, um modelo passível de ser utilizado no Brasil, que nada mais é do que uma adaptação do modelo britânico, seguindo a mesma estrutura[497].

Claro, o instrumento do relatório de impacto à proteção de dados não tem relação direta com as normas corporativas globais, mas a utilização do modelo britânico pelo governo brasileiro corrobora o fato de que o ICO é visto com seriedade e como um exemplo para os Estados que estão em processo de consolidação das legislações de proteção de dados pessoais.

---

494 **Regras Corporativas Vinculativas da Amgen Brasil (BCRs do Brasil)**. AMGEN BRASIL, São Paulo, 2020. Disponível em: https://www.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-brazil-bcr-final-including-appendices.pdf. Acesso em: 29 mar. 2023.

495 REINO UNIDO. Information Commissioner's Office. **DPIA Template**. Disponível em: https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf. Acesso em: 02 mar. 2023.

496 "O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL. Governo Federal. **Guia Template RIPD.** Brasília, DF: Governo Digital, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx. Acesso em: 02 mar. 2023).

497 BRASIL. Governo Federal. **Guia Template RIPD.** Brasília, DF: Governo Digital, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx. Acesso em: 02 mar. 2023.

Como sabemos, a ANPD ainda está em processo de amadurecimento. Isso porque, como a LGPD foi promulgada em 2018 e a ANPD foi estabelecida em 2020, a agência é relativamente nova. No entanto, desde sua criação, a ANPD tem trabalhado ativamente na implementação e fiscalização da LGPD, publicando regulamentações, orientações e notas técnicas sobre a interpretação e aplicação da lei.

De fato, o GDPR do Reino Unido e a LGPD apresentam algumas diferenças, todavia, compartilham uma série de conceitos e princípios, como a proteção da privacidade dos dados pessoais, a transparência no processamento de dados, o direito dos titulares de dados de controlar seus dados pessoais e o estabelecimento de medidas de segurança adequadas para proteger os dados pessoais.

Tal como o GDPR do Reino Unido, a LGPD estabelece que as transferências internacionais de dados pessoais só podem ser realizadas para países que ofereçam um nível adequado de proteção de dados pessoais, ou, ainda, mediante o fornecimento de mecanismos que ofereçam e comprovem garantias do cumprimento dos princípios e dos direitos do titular. Dentre essas medidas, ambas as legislações trazem a hipótese das normas corporativas globais.

Assim, tendo em vista que a LGPD e o GDPR apresentam grande semelhança no contexto, estrutura e racionalidade final, e que a LGPD foi amplamente influenciada pela Lei europeia, e que as normas corporativas globais aprovadas pelo ICO mostram-se satisfatórias para comprovar um nível apropriado de proteção de dados, certo que o Brasil pode desfrutar dos avanços legislativos da União Europeia para incorporar elementos pertinentes. Em suma, considerando que o GDPR do Reino Unido e a LGPD dispõem de uma série de semelhanças no que tange às transferências internacionais de dados pessoais, conclui-se que o modelo de aprovação, bem como o próprio modelo das normas utilizados no Reino Unido, configuram um exemplo muito útil para o Brasil.

4 CONSIDERAÇÕES FINAIS

O presente trabalho buscou responder como as normas corporativas globais aprovadas pelo ICO, bem como o seu consolidado procedimento de aprovação, podem contribuir para um futuro modelo brasileiro de normas corporativas globais, por meio do método de pesquisa dedutivo. De início, buscou-se conceituar as transferências internacionais de dados pessoais. Nesse sentido, definimo-las como um envio de dados pessoais realizado entre dois agentes legalmente independentes, localizados em territórios distintos, com o objetivo de utilizar esses dados de maneira compartilhada.

Após, relatou-se, de forma breve, a evolução das legislações de proteção de dados nos contextos europeu e brasileiro. Em resumo, as normas de proteção de dados da União Europeia tiveram início formal em 1995, com a Diretiva de Proteção de Dados Pessoais, que foi substituída, em 2018, pelo GDPR. O Brasil, por outro lado, criou normas de proteção de dados foram criadas mais recentemente, com a aprovação da LGPD em 2018. Portanto, enquanto a União Europeia dispõe de longa história em proteção de dados, e é conhecida por sua rigidez e seriedade na matéria, a norma brasileira encontra-se, ainda, em consolidação.

No mais, averiguou-se que, muito embora os mecanismos apresentem diferenças, eles compartilham uma série de princípios e elementos, como a transparência, a finalidade, o consentimento, a segurança dos dados, a minimização de dados e a proteção dos direitos dos titulares de dados pessoais. Como a legislação europeia é mais avançada, constitui um exemplo bastante útil pra o Brasil, que pode valer-se de tal exemplo para fortalecer a sua atuação em proteção de dados.

Com o aumento do fluxo de informações – também em nível transacional – verifica-se a necessidade de se regular estas transferências. Nesse ponto, tanto o GDPR quanto a LGPD possuem parte relevante de seus textos normativos tratando das transferências internacionais de dados pessoais. Nesse sentido, ambas as legislações trazem hipóteses que viabilizam as transferências internacionais. Dentre elas, além daquelas realizadas para países que proporcionem grau de proteção de dados pessoais considerado adequado. Caso o país de destino não apresente nível de proteção de dados considerado satisfatório, as legislações preveem a utilização de mecanismos de salvaguardas, ou garantias de cumprimento.

Dentre esses mecanismos, estão as normas corporativas globais. Elas constituem um instrumento legalmente vinculante que possibilita aos grupos corporativos a transferência internacional de dados pessoais no âmbito interno do grupo, sem que, para isso, tenham que ser firmados múltiplos documentos. As normas corporativas globais são um instrumento único, capaz de fornecer garantias aos titulares de dados pessoais e um alto nível de proteção à todas as transferências efetuadas dentro dos titulares das normas.

Para tanto, as normas corporativas globais devem garantir que todas as transferências realizadas dentro de um grupo corporativo apresentam princípios de proteção de dados, ferramentas eficazes para assegurar que os níveis de proteção de dados são satisfatórios e um componente que corrobore o caráter vinculativo das normas, em âmbito interno quanto externo.

No Reino Unido, é atribuição do ICO a aprovação das normas corporativas globais submetidas pelas organizações estabelecidas no Reino Unido. Assim, a avaliação e certificação das normas corporativas globais pelo ICO são uma forma de garantir que as organizações estejam em conformidade com as leis de proteção de dados. Nesse sentido, o procedimento de aprovação das normas corporativas globais pelo ICO está consolidado, uma vez que as regras para aprovação das normas já foram estabelecidas pelo GDPR do Reino Unido, no art. 47.

A ANPD, por sua vez, ainda apresenta lacunas na regulamentação dos temas envolvendo proteção de dados pessoais. As transferências internacionais de dados, especificamente, estão na Fase 1 da Agenda Regulatória do Órgão para o biênio 2023-2024. Por isso, o Brasil não possui um procedimento para aprovação das normas corporativas globais, pois estas ainda não foram regulamentadas.

No Reino Unido, o processo de aprovação das normas corporativas globais envolve a avaliação rigorosa das garantias de proteção de dados estabelecidas pelos requerentes para atender os requisitos dispostos na Lei. Ao analisar o processo de aprovação das normas corporativas globais pelo ICO, verificou-se que este mostra cuidado com os direitos dos titulares de dados pessoais. Da mesma forma, as normas corporativas globais para controladores do grupo Amgen – aprovadas pelo ICO – demonstraram cumprir todos os requisitos presentes na Lei e recomendações do ICO.

No mais, averiguou-se que a Lei brasileira foi em muito influenciada pela Lei europeia. Inclusive, sugere-se que, dada a semelhança entre a LGPD e o GDPR, há uma tendência de que a ANPD considere os países sujeitos ao GDPR e os reconhecidos como adequados à proteção de dados pela União Europeia também como dispondo de nível satisfatório. Desse modo, muitos são os fatores que levam o Brasil a se inspirar na legislação europeia de proteção de dados para consolidar o seu próprio arcabouço normativo, de forma que também na temática das normas corporativas globais, o país poderá se inspirar nos avanços já feitos pelo Reino Unido.

REFERÊNCIAS BIBLIOGRÁFICAS

Amgen UK Binding Corporate Rules (UK BCRs). AMGEN, November 2021. Disponível em: https://www.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-uk-bcr-final-including-appendices.pdf. Acesso em: 23 mar. 2023.

AMGEN. **Business Conduct and Ethics**. Disponível em: https://www.amgen.com/bcr. Acesso em: 29 mar. 2023.

BIG DATA ANALYTICS. In: INTERNATIONAL Business Machines Corporation (IBM). New York: IBM, 2023. Disponível em: https://www.ibm.com/analytics/big-data-analytics. Acesso em 22 fev. 2023.

Binding Corporate Rules (BCR). In: EUROPEAN Commission. União Europeia: European Commission, 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#:~:text=Approval%20of%20binding%20corporate%20rules,-Companies%20must%20submit&text=The%20competent%20authority%20communicates%20its,authority%20will%20approve%20the%20BCRs. Acesso em: 26 fev. 2023.

Binding Corporate Rules. The General Data Protection Regulation. PWC, 2019. Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 23 mar. 2023

BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 3 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria nº 35, de 04 de novembro de 2022**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Acesso em: 3 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº1/2021**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021. Acesso em: 3 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº2/202**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper. Acesso em: 3 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº3/2023**. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-cd/anpd-n-3-de-25-de-janeiro-de-2023-460124477. Acesso em: 3 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD nº4/2023**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077. Acesso em: 3 mar. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Tomada de Subsídios sobre Transferência Internacional.** Disponível em: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional. Acesso em: 10 mar. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 mar. 2023.

BRASIL. Governo Federal. **Guia Template RIPD.** Brasília, DF: Governo Digital, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx. Acesso em: 02 mar. 2023

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 26 fev. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 mar. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019.** Disponível: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 26 fev. 2023.

BRASIL. **Portaria nº 11, de 27 de janeiro de 2021**. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 24 mar. 2023.

BRASIL. **Projeto de Lei nº 4.060, de 2012** (Apenso PLs nos 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename. Acesso em: 25 fev. 2023.

Brexit: a saída do Reino Unido da União Europeia. **Brasil Escola**, 2023. Disponível em: https://brasilescola.uol.com.br/historiag/brexit-ou-saida-inglaterra-uniao-europeia.htm. Acesso em: 26 fev. 2023.

BREXIT. In: BRITANNICA. Londres: Britannica, 2023. Disponível em: https://www.britannica.com/topic/Brexit. Acesso em: 20 fev. 2023.

CASTELLS, Manuel. **A sociedade em rede**. 6. Ed. São Paulo: Paz e Terra, 1999.

CERVO, Amado Luiz; BERVIAN, Pedro Alcino; SILVA, Roberto da. **Metodologia cientifica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

COUNCIL OF EUROPE. In: EUROPE´S Human Rights Watchdog. União Europeia: Europe´s Human Rights Watchdog, 2023. Disponível em https://www.europewatchdog.info/en/council-of-europe/. Acesso em: 24 mar. 2023.

Data Isn't The New Oil — Time Is. **Forbes**, Nova York, 15 de julho de 2021. Disponível em: https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/?sh=1db09c1f35bb. Acesso em: 22 fev. 2023.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais.** 3. Ed. São Paulo: Editora Revista dos Tribunais, 2021, *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/215543393/v3/page/RB-3.1. Acesso em: 10 mar. 2023.2

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 24 mar. 2023.

FORBES. **Amgen**. Disponível em: https://www.forbes.com/companies/amgen/?sh=6aee72f56ae3. Acesso em: 28 mar. 2023.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2020, *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/monografias/195107452/v2/page/RB-23.1. Acesso em: 22 fev. 2023.

GDPR vs UK GDPR — what's the difference? **The Infolaw Partner Showcase**, London, 12 July 2022. Disponível em: https://www.infolaw.co.uk/partners/gdpr-vs-uk-gdpr-whats-the-difference/. Acesso em: 20 mar. 2023.
GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

Guia de Proteção de Dados Pessoais: Transferência Internacional. São Paulo: FGV, out .2020, p. 20. Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/u12834/guia_transferencia_internacional.pdf. Acesso em: 01 mar. 2023

Hamilton, Daniel S., and Quinlan, Joseph P. **The Transatlantic Economy 2022: Annual Survey of Jobs, Trade and Investment between the United States and Europe**. Washington, DC: Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network, 2022. Disponível em:

https://transatlanticrelations.org/wp-content/uploads/2022/03/TE2022_report_HR.pdf. Acesso em: 20 mar. 2023.

How do the UK's GDPR and EU's GDPR regulation compare? **GDPR EU**, 2023. Disponível em: https://www.gdpreu.org/differences-between-the-uk-and-eu-gdpr-regulations/Acesso em: 26 fev. 2023.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Big Data no projeto Sul Global: Relatório sobre estudos de caso**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2016. Disponível em: https://itsrio.org/wp-content/uploads/2017/02/ITS_Big-Data_PT-BR_v4.pdf. Acesso em: 22 fev. 2023.

KUNER, Christopher. The global data privacy power struggle. **Oxford Univesity Press's (OUPblog)**, 28 jan. 2013. Disponível em: https://blog.oup.com/2013/01/global-data-privacy-power-struggle/. Acesso em: 16 mar. 2023.

LEONARDI, Marcel. Transferência internacional de dados pessoais. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, p. 309. *E-book*. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

MANYIKA, James et al. Digital globalization: The new era of global flows. **McKinsey Global Institute**, 24 fev. 2016. Disponível em: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows. Acesso em: 20 fev. 2023.

Mecanismos de Transferência Internacional de Dados. Cláusulas-Padrão Contratuais e Regras Corporativas Vinculantes. São Paulo: Opice Blum, Bruno e Vainzof Advogados Associados, mar. 2022, p. 4. Disponível em: https://opiceblum.com.br/wp-content/uploads/2022/02/white_paper_transferencia_internacional_de_dados_v.final_.pdf. Acesso em: 20 fev. 2023.

MONTEIRO, Renato. GDPR matchup: Brazil's General Data Protection Law. **IAPP**, Portsmouth, 18 de outubro de 2018. Disponível em: https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/. Acesso em: 25 de fev. 2023.

MUNDO EDUCAÇÃO. **As redes de comunicação no mundo globalizado**. Mundo Educação, São Paulo, 2019. Disponível em: https://mundoeducacao.uol.com.br/geografia/as-redes-comunicacao-no-mundo-globalizado.htm. Acesso em: 27 mar. 2023.

OPINION OF ADVOCATE GENERAL. **Case C-101/01 Bodil Lindqvist v Åklagarkammaren i Jönköping**. TIZZANO: InfoCuria Jurisprudência, 19 September 2002. Disponível em: https://curia.europa.eu/juris/document/document.jsf?docid=47672&doclang=EN

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. [S.l.], 2013. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acesso em: 28 mar. 2023.

PRADO CHAVES, Luis Fernado. Da Transferência Internacional de Dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice**. LGPD: Lei Geral de Proteção de Dados Pessoais Comentada**. 4. Ed. São Paulo: Revista dos Tribunais, 2021, *E-book*. Disponível em: https://proview.thomsonreuters.com/launchapp/title/rt/codigos/188730949/v4/page/RL-1.10. Acesso em: 20 mar. 2023.

Proposal for an ePrivacy Regulation. União Europeia: European Commission, 2023. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation. Acesso em: 20 fev. 2023.

PROUST, Olivier; BARTOLI, Emmanuelle. Binding Corporate Rules: a global solution for international data transfers. **International Data Privacy Law**, London, November 25, 2011. Disponível em: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2011/12/International_Data_Privacy_Law-2011-Proust.pdf. Acesso em: 20 mar. 2023.

RAMOS, Pedro Henrique Soares; MONTEIRO, Renato Leite. **A Regulação Europeia de Proteção de Dados e o Impacto na Publicidade Online**. Disponível em: https://baptistaluz.com.br/regulacao-europeia-de-protecao-de-dados-e-o-impacto-na-publicidade-online/. Acesso em 23 mar. 2023.

Regras Corporativas Vinculativas da Amgen Brasil (BCRs do Brasil). AMGEN BRASIL, São Paulo, 2020. Disponível em: https://www.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-brazil-bcr-final-including-appendices.pdf. Acesso em: 29 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **About the DPA 2018**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/about-the-dpa-2018/. Acesso em: 23 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Application for approval of UK binding corporate rules for controllers.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021123/bcr-controller-application-form.docx. Acesso em: 10 mar. 2023.

REINO UNIDO. Information Commissioner´s Office. **Controllers and processors**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/. Acesso em: 02 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Controller guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/controller-guidance/. Acesso em: 10 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **DPIA Template**. Disponível em: https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf. Acesso em: 02 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/. Acesso em: 10 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Guide to Binding Corporate Rules: BCR Approvals**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/bcr-approvals/. Acesso em: 27 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Guide to the UK General Data Protection Regulation (UK GDPR)**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/. Acesso em: 01 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Information Commissioner's Office**. Disponível em: https://www.gov.uk/government/organisations/information-commissioner-s-office. Acesso em: 25 fev. 2023.

REINO UNIDO. Information Comissioner's Office. **International transfers**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/. Acesso em: 01 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **List of BCR holders approved pursuant to paragraph 9, part 3, schedule 21 to the DPA 2018**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/bcr-approvals/list-of-bcr-holders-approved-pursuant-to-paragraph-9-part-3-schedule-21-to-the-dpa-2018/. Acesso em: 27 mar. 2023.

REINO UNIDO. **Information Commissioner's Office. List of BCRs approved under UK GDPR**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/bcr-approvals/bcrs-approved-under-uk-gdpr/. Acesso em: 27 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Processor guidance**. Disponível em: https://ico.org.uk/for-organisations/guide-to-binding-corporate-rules/processor-guidance/. Acesso em: 10 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **Overview of Data Protection and the EU**. Disponível em: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/. Acesso em: 27 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **UK BCR Referential Table.** Disponível em: https://ico.org.uk/media/for-organisations/documents/4021115/uk-bcr-referential-table.docx. Acesso em: 29 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **UK BCR Referential Table – Annex 1.** Disponível em: https://ico.org.uk/media/for-

organisations/documents/4021119/uk-bcr-referential-table-annex-1.docx. Acesso em: 29 mar. 2023.

REINO UNIDO. Information Commissioner's Office. **UK BCR Requirements Table - transitioning an existing EU BCR to UK BCR**. Disponível em: https://ico.org.uk/media/for-organisations/documents/2618638/uk-bcr-requirements-to-transition-table-final.docx. Acesso em: 10 mar. 2023.

REINO UNIDO. **Regulation (EU) 2016/679** of the European Parliament and of the Council. Disponível em: https://www.legislation.gov.uk/eur/2016/679/article/47. Acesso em: 23 fev. 2023.

REINO UNIDO. UK Parliament. **Artificial intelligence and data protection**. Disponível em: https://commonslibrary.parliament.uk/research-briefings/cbp-7960/. Acesso em: 28 mar. 2023.

RODRIGUES, Cristina Barbosa; SANTOS, Jessica Mequilaine Correia dos; GAMBA, João Roberto Gorini. Dados pessoais na economia digital: análise dos impactos da proteção de dados no uso de *Big Data* pelo GAFA. **Revista DIGE - Direito Internacional e Globalização Econômica (PUC-SP)**, v. 8, n. 8, 2021. Disponível em: https://revistas.pucsp.br/index.php/DIGE/article/view/58318/40073. Acesso em: 20 fev. 2023.

The world's most valuable resource is no longer oil, but data. **The Economist**, Londres, 06 de maio de 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 22 fev. 2023.

UEHARA, Luiz Fernando e TAVARES FILHO, Paulo César. Transferência Internacional de Dados Pessoais: Uma Análise Crítica entre o Regulamento Geral de Proteção de Dados Pessoais da União Europeia (RGPD) e a Lei Brasileira de Proteção de Dados Pessoais (LGPD). **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 2, 2019.

UNIÃO EUROPEIA. Comissão Europeia. **Data protection**. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. Acesso em: 28 mar. 2023.

UNIÃO EUROPEIA. Comissão Europeia. **What does data protection by design and by default mean?** Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en. Acesso em: 29 mar. 2023

UNIÃO EUROPEIA. Council of Europe. **Convenção Europeia dos Direitos do Homem**. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf. Acesso em: 20 fev. 2023.

UNIÃO EUROPEIA. Council of Europe. **Convention 108 + Convention for the protection of individuals with regard to the processing of personal data**. Jun.

2018. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 Acesso em 24.03.2023

UNIÃO EUROPEIA. Council of Europe. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. 1981. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 28 mar. 2023.

UNIÃO EUROPEIA. Council of Europe (Committee of Ministers). **Resolution (74) 29**, on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector, 20 September 1974. Disponível em: https://rm.coe.int/16804d1c51 Acesso em 21.03.2023.

UNIÃO EUROPEIA. **Diretiva 95/46/CE** do Parlamento Europeu e do Conselho relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 23 fev. 2023.

UNIÃO EUROPEIA. **Directiva 2002/58/CE** do Parlamento Europeu e do Conselho relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), de 12 junho de 2002. Disponível em: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_pt.pdf. Acesso em: 01 mar. 2023.

UNIÃO EUROPEIA. **Diretiva 2018/2001** do Parlamento Europeu e do Conselho relativa à promoção da utilização de energia de fontes renováveis (reformulação), de 11 de abril de 2018. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018L2001&from=ES. Acesso em: 23 fev. 2023.

UNIÃO EUROPEIA. **Diretiva 2019/790** do Parlamento Europeu e do Conselho relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE, de 17 de abril de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0790&from=PT. Acesso em: 23 fev. 2023.

UNIÃO EUROPEIA. European Commission. **Article 29 - Data Protection Working Party**. Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on 3 June 2003. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf. Acesso em: 20 mar. 2023.

UNIÃO EUROPEIA. **Tipos de legislação**. Disponível em: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt. Acesso em: 24 mar. 2023.

VERONESE, Alexandre. Transferências internacionais de dados pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasil. In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. 1. Ed. São Paulo: Grupo GEN, 2020, *E-*

book. Disponível em: https://app.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 mar. 2023.

What is a data controller or a data processor? In: EUROPEAN Commission. União Europeia: European Commission, 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en. Acesso em: 20 fev. 2023.

What is Freedom of Information & Data Protection? **The Constitution Unit, London**, 2023. Disponível em: https://www.ucl.ac.uk/constitution-unit/research/research-archive/foi-archive/what-freedom-information-data-protection#:~:text=The%20development%20of%20Data%20Protection,to%2Ddate%20and%20lawfully%20used. Acesso em: 24 mar. 2023.

What is UK GDPR: 9 Key Things Businesses Need to Know. **Secure Privacy**, 11 april 2021. Disponível em: https://secureprivacy.ai/blog/what-is-uk-gdpr. Acesso em: 10 mar. 2023.

ANEXOS

ANEXO A: Application for Approval of UK Binding Corporate Rules for Controllers

APPLICATION FOR APPROVAL OF UK BINDING CORPORATE RULES FOR CONTROLLERS

Contact details of the Applicant and the structure of the group of undertakings, or group of enterprises engaged in a joint economic activity ('Group')
Name of the Group: Click or tap here to enter text.
Address of the Group Headquarters: Click or tap here to enter text.
Name, address and UK company registration number of the UK legal entity (with delegated responsibility) or , if exporting entity model is proposed), name, address and registered UK company number of all UK legal entities for the Group: Click or tap here to enter text.
Name and address of the UK legal entity (ies) handling complaints under UK BCRs (if different): Click or tap here to enter text.
Legal nature of the UK legal entity with delegated responsibility or legal entities if exporting entity model is being proposed Click or tap here to enter text.
A description of the corporate structure and geographical location of all members to be bound by UK BCRs, a document showing the Group structure as an annex: Click or tap here to enter text.
Name, position and full contact details of the person dealing with the application (include address, email and phone number): Click or tap here to enter text.
Name, title and full contact details of any external lawyers or other advisors instructed to act for the applicant (include address, email and phone number): Click or tap here to enter text.

Description and destinations of data flows 47(2)(b)
Describe the nature of the personal data intended to be covered by the UK BCRs. Include the category/categories of personal data, the type of processing and its purposes, the types of data subjects affected for each identified data flow and for each UK legal entity as applicable Click or tap here to enter text.
Please list all third countries to where data specified above will be transferred to under the UK BCRs. Click or tap here to enter text.

Liability
Confirm that the UK legal entity with delegated data protection responsibilities (or legal entities if exporting entity model is being proposed) has sufficient funds in place to provide the remedies and/or pay compensation for liabilities under the UK BCRs. Click or tap here to enter text.

Network of data protection officers or appropriate staff

Confirm that a network of DPOs or appropriate staff (such as a network of privacy officers) is appointed with senior management support to oversee and ensure compliance (including training and complaint handling) with the UK BCRs. Click or tap here to enter text.
Explain how the network of DPOs or privacy officers operates within the Group, Describe the internal structure of their roles and responsibilities and provide an organogram Click or tap here to enter text.

Verification of Compliance & Audits
Describe the verification mechanisms that the Group has in place to audit each of the members compliance with UK BCRs and how often compliance is examined. Click or tap here to enter text. Explain how the verification or compliance programme operates within the Group (including and not limited to information as to the recipients of any audit reports and their position within the structure of the Group) Click or tap here to enter text.
Are the verification mechanisms clearly set out in one document or other internal procedures? If so, please provide a copy of the document). Click or tap here to enter text.

Mechanisms for reporting and recording changes
Describe what is in place to record any changes to the UK BCRs and/or list of members. Please confirm what arrangements are in place to inform the Commissioner of any changes to the UK BCRs and/or to the list of UK BCRs members. Click or tap here to enter text.
Confirm that the Commissioner will be provided with any audit /verification reports, on request, without restrictions. Click or tap here to enter text.
Confirm that the Group as a whole and each of the entities of the Group who are members of the UK BCRs will co-operate with the Commissioner in relation to compliance with the UK BCRs. Click or tap here to enter text.
Please set out what mechanisms are in place for notifying the Commissioner where legal requirements of BCR members located in third countries have or could have an adverse effect on those guarantees being afforded under the UK BCRs. Click or tap here to enter text.

Training and awareness raising
Provide supporting documentation in relation to the established policies and procedures setting out the training programme demonstrating how the UKBCRs are communicated throughout the Group. Where applicable, include references to bespoke and general training programmes and testing and verification of training of UK BCRs knowledge. Click or tap here to enter text.
Confirm that all employees and other staff that have permanent or regular access to personal data receive appropriate training on the UK BCRs Please also explain whether and how different categories of employee or staff receive different training. Click or tap here to enter text.
Explain which function is responsible for monitoring the training programme in respect of UK BCRs including updating UK BCRs data protection policies and training modules, who approves and signs them off and how frequently policies and training modules are reviewed. Click or tap here to enter text.

ANEXO B: Application for Approval of UK Binding Corporate Rules for Processors

APPLICATION FOR APPROVAL OF UK BINDING CORPORATE RULES FOR PROCESSORS

Contact details of the Applicant and the structure of the group of undertakings, or group of enterprises engaged in a joint economic activity ('Group')
Name of the Group: Click or tap here to enter text.
Address of the Group Headquarters: Click or tap here to enter text.
Name, address and UK company registration number of the UK legal entity with delegated responsibility or (if exporting entity model is proposed) name, address and registered UK company number of all UK legal entities for the Group: Click or tap here to enter text.
Name and address of the UK legal entity(ies) handling complaints under UK BCRs (if different): Click or tap here to enter text.
Legal nature of the UK legal entity with delegated responsibility or legal entities if exporting entity model is being proposed Click or tap here to enter text.
A description of the corporate structure and geographical location of all members to be bound by UK BCRs, a document showing the Group structure as an annex: Click or tap here to enter text.
Name, position and full contact details of the person dealing with the application (include address, email and phone number): Click or tap here to enter text.
Name, title and full contact details of any external lawyers or other advisors instructed to act for the applicant (include address, email and phone number): Click or tap here to enter text.

Description and destinations of data flows
Describe the nature of the personal data intended to be covered by the UK BCRs. Include the expected category/categories of personal data, the type of processing and its purposes, the types of data subjects affected for each identified data flow and for each UK legal entity as applicable. (so, if an exporting entity model is proposed, we expect to see a description and the required information as against each exporting entity) Click or tap here to enter text.
Please set out the third countries to which data specified above will be transferred under the UK BCRs. (We expect to see the data flow, categories, purpose specified against each third country as necessary) Click or tap here to enter text.
Do you allow third party Controllers to transfer personal data from the UK directly to Members of the UK BCR-P based in third countries? Click or tap here to enter text.

Or do you require all third party UK Controllers to first send personal data to a UK legal entity member of the UK BCR-P who then transfers that data to a UK BCR-P member in a third country?
Click or tap here to enter text.

In either case please provide full details and a commitment that there are contractual arrangements in place ensuring:

- All Article 28 UK GDPR obligations (including but not limited to assisting the Controller in demonstrating compliance with their data protection principles), are satisfied
- A relevant contractual provision specifically dealing with direct personal data transfers from a UK Controller to an overseas member of the UK BCR exists in those contractual arrangements
- A contractual provision extending third party beneficiary rights afforded under UK BCRs has been included in those contractual arrangements in accordance with The Contract (Rights of Third Parties) Act 1999 for the benefit of Controller's and their data subjects
- A risk assessment has been undertaken and by which party (for example, external Third Party Controller or UK BCR group)
- Which BCR member is a signatory to those Article 28 contractual arrangements
- As applicable, the IGA/binding instrument reflects those Article 28 arrangements and is binding on all UK BCR members

Click or tap here to enter text.

Please confirm that a copy of the UK BCRs are annexed/referenced to contractual arrangements in place with Controllers.
Click or tap here to enter text.

Are any of the UK BCR members likely to undertake sub processing activities on behalf of other UK BCR members, or on behalf of other members of the Group who are not party to the UK BCRs?
Click or tap here to enter text.

If so, please provide further details and a commitment that contractual arrangement are in place in relation to sub processors
Click or tap here to enter text.

Liability
Confirm that the UK legal entity with delegated data protection responsibilities (or each legal entity if exporting entity model is being proposed) has sufficient funds in place to provide the remedies and/or pay compensation for liabilities arising under the UK BCRs. Click or tap here to enter text.

Network of data protection officers or appropriate staff
Confirm that a network of DPOs or appropriate staff (such as a network of privacy officers) is appointed with senior management support to oversee and ensure compliance (including training and complaint handling) with the UK BCRs. Click or tap here to enter text.

Explain how the network of DPOs or privacy officers operates within the Group. Describe the internal structure of their roles and responsibilities and provide an organogram. Click or tap here to enter text.

Verification of Compliance & Audits
Describe the verification mechanisms that the Group has in place to audit each of the members compliance with UK BCRs and how often compliance is examined. Click or tap here to enter text. Explain how the verification or compliance programme operates within the Group (including and not limited to information as to the recipients of any audit reports and their position within the structure of the Group) Click or tap here to enter text.
Are the verification mechanisms clearly set out in one document or other internal procedures? If so, please provide a copy of the document. Click or tap here to enter text.
Confirm that the Commissioner will be provided with any audit /verification reports, on request, without restrictions. Click or tap here to enter text.
Confirm that the Controller is also provided with any audit /verification reports, on request, Click or tap here to enter text.

Mechanisms for reporting and recording changes
Describe what is in place to record any changes to the UK BCRs and/or list of members. Please confirm what arrangements are in place to inform the Commissioner of any changes to the UK BCRs and/or to the list of UK BCRs members. Click or tap here to enter text.

Co-Operation with the Commissioner & Controller
Confirm that the Group as a whole and each of the entities of the Group who are members of the UK BCRs will co-operate with the **Commissioner** in relation to compliance with the UK BCRs. Click or tap here to enter text.
Confirm that the Group as a whole and each of the entities of the Group who are members of the UK BCRs will co-operate with the **Controller** in relation to compliance with the UK BCRs. Click or tap here to enter text.
Please set out what mechanisms are in place for notifying the **Commissioner** where legal requirements of BCR members located in third countries have or could have an adverse effect on those guarantees being afforded under the UK BCRs. Click or tap here to enter text.
Please set out what mechanisms are in place for notifying the **Controller** where legal requirements of BCR members located in third countries have or could have an adverse effect on those guarantees being afforded under the UK BCRs.

Click or tap here to enter text.

Training and awareness raising
Provide supporting documentation in relation to the established policies and procedures setting out the training programme demonstrating how the UK BCRs are communicated throughout the Group. Where applicable, include references to bespoke and general training programmes and testing and verification of training of UK BCRs knowledge. Click or tap here to enter text.
Confirm that all employees and other staff that have permanent or regular access to personal data receive appropriate training on the UK BCRs Please also explain whether and how different categories of employee or staff receive different training. Click or tap here to enter text.
Explain which function is responsible for monitoring the training programme in respect of UK BCRs including updating UK BCRs data protection policies and training modules, who approves and signs them off and how frequently policies and training modules are reviewed. Click or tap here to enter text.

ANEXO C: UK BCR Referential Table – for completion by ALL Applicants (updated July 2022)

UK BCR Referential Table – for completion by ALL Applicants
(updated July 2022)

Applicants should ensure they read the updated Guidance before completing the referential table and the BCR documentation pack.

NAME OF ORGANISATION	Click or tap here to enter text.			
Article	**Comments**	**Document which must contain the required information**	**BCR Applicant to complete** **Documents in which the Article 47 requirement is met/satisfied**	**ICO to complete Requirement met Y/N** **If No, ICO to summarise why not met**
Art. 47.1(a)		• IGA/binding instrument only	Click or tap here to enter text.	Click or tap here to enter text.
Art. 47.1(b)	The IGA and BCR Policy must expressly confer third party beneficiary rights as specified in 47.2(c), 47.2(e) 47.2(f), Art. 47.2(g), and Art. 47.2(i). The content of the BCR Policy must ensure data subjects understand they have enforceable rights against	• IGA/binding instrument and • BCR Policy (summary form in BCR)	Click or tap here to enter text.	Click or tap here to enter text.

	BCR members.			
Art 47(2)(a)		• Application form only	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(b)		• Application form and • BCR Policy (in summary form)	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(c)		• IGA • BCR Policy (in summary form) • Supporting Policies & Procedures	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(d)		• BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(e)		• IGA and • BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(f)	IGA must contain a commitment regarding the UK entity/entities	• Application form • IGA and • BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(g)		• BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(h)		• Application Form • Supporting policies and	Click or tap here to enter text.	Click or tap here to enter text.

		procedures		
Art 47(2)(i)		• BCR Policy and • Supporting Policies and procedures	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(j)		• Application form • IGA • Supporting Policies and procedures	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(k)		• Application Form • Supporting Policies and procedures	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(l)		• Application form • IGA • Supporting Policies and procedures	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(m)		• Application form • IGA /binding instrument • Supporting Policies and procedures	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(n)		• Application form	Click or tap here to enter text.	Click or tap here to enter text.

		• Supporting Policies and procedures		

ANEXO D: UK BCR Referential Table - Annex 1
Additional elements for completion by BCR-P Applicants only
(updated July 2022)

UK BCR Referential Table - Annex 1
Additional elements for completion by BCR-P Applicants only (updated July 2022)

Applicants should ensure they read the updated UK BCR Processor Guidance before completing this Annex.

NAME OF ORGANISATION	Click or tap here to enter text.

Article	**Comments**	**Document**	**FOR COMPLETION BY APPLICANT:** **Where (document and section) does this requirements appear in the application form, BCR Policy or IGA/binding instrument or other supporting policies and procedures**	**FOR COMPLETION BY ICO:** **Requirement met Y/N** **If No, ICO to summarise why not met**
Art. 47.1(b)	IGA and BCR Policy must contain commitment that individuals can enforce certain rights directly against Processor and include a provision in respect of	• Application Form • IGA/binding instrument and • BCR (summary of directly enforceable rights in BCR)	Click or tap here to enter text.	Click or tap here to enter text.

	Third Party Contract Rights Act 1999			
Art 47(2)(d)	Commitment by Processor towards Controller	• Application Form • BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(e)		• Application Form • IGA/binding instrument and • BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(f)	IGA must contain a specific liability clause in respect of sub processors where engaged	• Application Form • IGA • BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(g)	BCR-Ps made available to Controllers and data subjects	• Application Form • BCR Policy	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(l)	Includes a commitment towards Controller and Commissioner	• Application form • IGA • Supporting Policies and procedures	Click or tap here to enter text.	Click or tap here to enter text.
Art 47(2)(m)	Includes a commitment towards Controller and	• Application form • IGA /binding instrument	Click or tap here to enter text.	Click or tap here to enter text.

	Commissioner	• Supporting Policies and procedures		
Art. 28 UK	Commitment that all Art 28 UK GDPR obligations between processor and Controller contain third party beneficiary rights in accordance with The Contract (Rights of Third Parties) Act 1999	• Application form • IGA	Click or tap here to enter text.	Click or tap here to enter text.

ANEXO E: Amgen UK Binding Corporate Rules (UK BCRs)

Amgen UK Binding Corporate Rules (UK BCRs)

Introduction

Amgen is a biotechnology leader committed to serving patients with grievous illness. These UK Binding Corporate Rules ("**UK BCRs**") express Amgen's commitment to privacy and data protection as it strives to provide adequate protection for the transfers and Processing of Personal Information between Amgen Participating Companies.

All Amgen Participating Companies and all Personnel are committed to respecting, and are legally bound by, these UK BCRs in respect of Personal Information within the UK BCRs' scope. Non-compliance can lead to disciplinary sanctions, as permitted by local law. The Chief Compliance Officer in liaison with the Chief Privacy Officer ensures that the UK BCRs will be enforced. A list of Participating Companies can be found here: https://wwwext.amgen.com/-/media/Themes/CorporateAffairs/amgen-com/amgen-com/downloads/amgen-bcr/amgen-BCRs-participating-companies.pdf. All Participating Companies can be contacted at privacy@amgen.com for any question concerning these UK BCRs.

These UK BCRs have been adopted in reference to the UK Data Protection Laws. Amgen UK is responsible for ensuring compliance by the Amgen Participating Companies with these UK BCRs. Individuals can enforce these UK BCRs against Amgen UK as a third-party beneficiary as described below. These UK BCRs are available on Amgen's website: www.amgen.com/bcr. Alternatively, please contact Amgen on privacy@amgen.com to request a copy.

1 – Scope

Amgen UK BCRs apply to transfers and Processing, automated or manual, of all Personal Information of Data Subjects performed by an Amgen Participating Company operating as Data Controller or operating as a Data Processor for another Amgen Participating Company acting as Data Controller in any of the following cases:

a) the Amgen Participating Company which Processes the Personal Information is established in the UK; or

b) the Amgen Participating Company which Processes the Personal Information is not established in the UK and has received the Personal Information from an Amgen Participating Company established in the UK; or

c) to onward transfers of Personal Information from Data Importers to Data Importers.

An overview of the data flows pursuant to these UK BCRs is available at Appendix 1.

2 – Definitions

Terms	*Definitions*
Amgen UK	Amgen Limited, a company incorporated in England and Wales under company number 02354269 and whose registered office is at 216 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire, England, CB4 0WA.
Applicable Law	The law of the United Kingdom or a part of the United Kingdom (including without limitation the UK Data Protection Laws).
Compliance Lead	A person within the Healthcare Compliance division of the Worldwide Compliance and Business Ethics department at an Amgen Participating Company who has delegated responsibility for data protection and privacy and, where distinct from the local Data Protection Officer, supports the local Data Protection Officer with its responsibilities and tasks.
Consent	Any freely given specific, informed and unambiguous indication of a Data Subject's wishes, by which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Information relating to him/her.
Data Controller	Any entity which makes decisions with regard to the collection and Processing of Personal Information, including decisions about the purposes for, and manner in which, Personal Information is Processed.
Data Exporter	An Amgen Participating Company operating as a Data Controller established in the UK that transfers Personal Information to a Data Importer.
Data Importer	An Amgen Participating Company which is not established in the UK that either (a) receives Personal Information from a Data Exporter or (b) receives an onward transfer of Personal Information pursuant to Article 1(c) of these UK BCRs.
Data Processor	A person or entity that processes Personal Information on behalf of a Data Controller.
Data Protection Officer	A person who has been nominated by Amgen's Chief Privacy Officer as being responsible for the oversight of Privacy and Data Protection at local level as well as the implementation of appropriate and required controls.
Data Subject	A natural person who can be identified, directly or indirectly, by reference to Personal Information. A Data Subject may be (without limitation): • a patient / clinical trial data subject (which may include a child under the age of 18)

Terms	***Definitions***
	• a healthcare professional • an employee • a vendor or supplier
Participating Company	A legal entity from the Amgen group that is bound by the UK BCRs.
Personal Information	Any information relating to a Data Subject such as a name, an identification number, location data, an online identifier or to one or more factors specific to or information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of Personal Information may include the following: • A Data Subject's name, address, social security number, driver's license number, financial account information, family information, or medical data, • The name, professional education, and prescribing practices of a healthcare professional, • The email address and other identifying information provided by someone visiting an Amgen website. The above list is indicative only and not exhaustive.
Personnel	All staff members and contingent workers (including consultants, temporary agency workers and contract workers) of any Amgen Participating Company.
Privacy Incident	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed.
Processing	Any operation or set of operations which is performed on Personal Information (or sets of Personal Information), whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Sensitive Personal Information	Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Separately to the UK Data Protection Laws, Amgen also considers financial information and information that could be used to perpetrate

Terms	*Definitions*
	identity theft (e.g., Social Security Number, driver's license number, credit card or other bank account information) as Sensitive Personal Information.
Technical and Organizational Security Measures	Technological and organizational measures aimed at protecting Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.
Third Party	A natural or legal person, public authority, agency or any other body other than the Data Subject, the Amgen Participating Company acting as Data Controller and an Amgen Participating Company acting as Data Processor. At Amgen, a Vendor is considered a Third Party. Depending on the circumstances, a Third Party may act as a Data Controller or a Data Processor in relation to the Processing of Personal Information.
Vendor	Any natural or legal person, business or organization that provides goods and/or services to an Amgen Participating Company under a contractual relationship and/or is a recipient of Personal Information from such Amgen Participating Company in order to render those good and/or services.
UK ICO	The UK Information Commissioner's Office, as the UK's independent data protection authority.
UK	The United Kingdom.
UK Data Protection Laws	The UK GDPR, the Data Protection 2018 and any other data protection law or regulation applicable in the UK from time to time.
UK GDPR	The retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020/1586).

Amgen shall interpret the terms in these UK BCRs in accordance the UK Data Protection Laws.

3 – Purpose Limitation

Personal Information shall be Processed for explicit, specified and legitimate purposes pursuant to Article 5(1)(b) of UK GDPR.

Personal Information will not be Processed in ways that are incompatible with the legitimate purposes for which the Personal Information was collected or Applicable Law. Data Importers are obligated to adhere to original purposes when storing and/or further Processing or Processing Personal Information transferred to them by another Participating Company. The purpose of Personal Information Processing may only be changed with the Consent of the Data Subject or to the extent permitted by Applicable Law.

Sensitive Personal Information will be provided with additional safeguards such as provided by the UK Data Protection Laws.

4 - Data Quality and Proportionality

Personal Information must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Information that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

Personal Information shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed, pursuant to Article 5(1)(c) of the UK GDPR.

Personal Information Processing will be guided by the objective of limiting the collection, Processing and/or usage of Personal Information to only what is necessary, i.e. as little Personal Information as possible. The possibility of anonymous or pseudonymous data must be considered, provided that the cost and effort involved is commensurate with the desired purpose.

Personal Information which is no longer required for the business purpose for which it was originally collected and stored, must be deleted according to Amgen's Record Retention Schedule. In the event that statutory retention periods or legal holds apply, the data will be blocked rather than deleted. At the end of the retention period or the legal hold, the data will be deleted.

5 – Legal Basis for Processing Personal Information

Processing of Personal Information is only permissible if at least one of the following prerequisites is fulfilled:

- The Data Subject has given his or her Consent to the Processing of his or her Personal Information for one or more specific purposes.

- The Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.

- The Processing is necessary for compliance with a legal obligation to which the Data Controller is subject under Applicable Law.

- The Processing is necessary in order to protect the vital interests, such as life, health or safety, of the Data Subject or of another natural person.

- The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

- The Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

6 – Processing of Sensitive Personal Information

If, according to a specific and legitimate purpose, the Amgen Participating Company needs to Process Sensitive Personal Information, the Amgen Participating Company will only do so if:

- The Data Subject has given explicit Consent to the Processing of those Sensitive Personal Information for one or more specified purposes, except where Applicable Law provides that the prohibition in Article 9(1) of the UK GDPR may not be lifted by the Data Subject.

- The Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller in the field of employment and social security and social protection law in so far as it is authorized by Applicable Law or by a collective agreement pursuant to Applicable Law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving his Consent.

- The Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the Consent of the Data Subjects.

- The Processing relates to Sensitive Personal Information which are manifestly made public by the Data Subject.

- The Processing of Sensitive Personal Information is necessary for the establishment, exercise or defence of legal claims.

- The Processing is necessary for reasons of substantial public interest, on the basis of Applicable Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

- The Processing of the Sensitive Personal Information is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Applicable Law or pursuant to contract with a health professional, and where those Sensitive Personal Information are Processed by or under the responsibility of a health professional such professional must be subject to the obligation of professional secrecy under Applicable Law or rules established by competent bodies in the UK or by another person also subject to an obligation of secrecy under Applicable Law or rules established by competent bodies in the UK.

- The Processing of Sensitive Personal Information is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Applicable Law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy.

- The Processing of Sensitive Personal Information is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on Applicable Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

7 – Transparency and Information Rights

All Participating Companies shall process Personal Information in a transparent manner. Amgen is committed to making the UK BCRs, including contact information, readily available to every Data Subject and to informing Data Subjects of the transferring and Processing of their Personal Information. These UK BCRs are available on Amgen's website: www.amgen.com/bcr. Alternatively, please contact Amgen on privacy@amgen.com to request a copy. Amgen will also use various communication means such as corporate websites, including internal websites and newsletters, contracts, and specific privacy notices to meet this requirement.

Data Subjects whose Personal Information is Processed by a Participating Company shall be provided with the information set out in Articles 13 and 14 of the UK GDPR.

Where the Personal Information is not received from a Data Subject, the obligation to inform the Data Subject does not apply if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law.

8 – Rights of Access, Rectification, Erasure and Restriction of Data

Every Data Subject has the right to obtain from the Participating Company confirmation as to whether or not Personal Information concerning him or her are being Processed, and, where that is the case, access to the Personal Information and the information required to be provided by Article 15(1) of the UK GDPR. The follow up on this request, including the possibility to charge a fee or the time frame to answer such a request, will be subject to Applicable Law and communicated appropriately to the Data Subject when he/she submits his/her request.

Every Data Subject has the right to obtain the rectification, erasure or restriction of data in particular because the data are incomplete or inaccurate.

Every Data Subject has the right to object, at any time on grounds relating to their particular situation, to the Processing of their Personal Information based on the performance of a task carried out in the public interest or the legitimate interests of the Participating Company or a Third Party (including profiling based on those grounds). The Participating Company shall no longer Process the Personal Information unless it demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

Every Data Subject has the right to object (free of charge) to the Processing of Personal Information relating to him or her for the purposes of direct marketing, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject exercises their right to object to the Processing of Personal Information relating to him or her for the purposes of direct marketing, the Participating Company must cease Processing the Personal Information for that purpose.

Every Data Subject has the right to obtain the notification to Third Parties to whom the Personal Information have been disclosed of any rectification, erasure, or restriction, pursuant to Article 19 of the UK GDPR.

Every Data Subject has the right to know the logic involved in any automatic Processing of data, pursuant to Article 13(2)(f) of the UK GDPR.

Where Processing is based on Consent, every Data Subject has the right to withdraw their Consent at any time. The withdrawal of Consent shall not affect the lawfulness of Processing based on Consent before its withdrawal.

Every Data Subject has the right to complain to the Participating Company regarding the Processing of Personal Information through the internal complaint mechanism provided pursuant to Article 17.

Any requests under this Article 8 (or Article 9 below) should be sent to the Participating Company at: privacy@amgen.com. While making requests by email is strongly encouraged, this does not preclude a Data Subject making a verbal request. The Participating Company shall inform the Data Subject without delay of the outcome of their request and at the latest within one month of receipt of the request (including where applicable the reasons for not taking action and the possibility of lodging a complaint with the UK ICO and/or seeking a judicial remedy). That period of one month may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Participating Company shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Any communication, action and/or information provided in relation to a request under this Article 8 (or Article 9 below) shall be provided to the Data Subject free of charge. Where requests from a Data Subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Participating Company may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The Participating Company shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

9 – Automated Individual Decisions

The Data Subject shall have the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless that decision:

- is necessary for entering into, or performance of, a contract between the Data Subject and the Participating Company;

- is required or authorized by Applicable Law which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests (including at least the right to obtain human intervention on the part of the Participating Company, to express his or her point of view and to contest the decision); or

- is based on the Data Subject's explicit Consent.

10 – Security and Confidentiality

Amgen implements appropriate Technical and Organizational Security Measures, to protect against and detect Privacy Incidents. International frameworks, such as ISO/IEC 27002, are used by Amgen to determine these security measures.

Amgen has processes in place to ensure that Privacy Incidents are subject to reporting, tracking and appropriate corrective actions, as necessary. Any Privacy Incident shall be documented (including the facts relating to the Privacy Incident, its effects and the remedial action taken) and the documentation shall be made available to the UK ICO on request. Furthermore, Participating Companies shall notify without undue delay any Privacy Incident to Amgen UK and the Chief Privacy Officer and the other relevant privacy officer/function and, where the Privacy Incident is likely to result in a high risk to their rights and freedoms, Data Subjects.

Information Security Risk Assessments are used to identify potential threats to Sensitive Personal Information and implementation of additional security controls as appropriate.

The implementation of the measures will be done having regard to the state of the art, pursuant to Article 32 of the UK GDPR.

The Chief Information Security Officer works jointly with the Chief Privacy Officer in order to ensure the security and confidentiality of Personal Information.

The Technical and Organizational Security Measures shall be designed to implement the data protection principles under Article 5 of the UK GDPR, data protection by design and default principles pursuant to Article 25 of the UK GDPR and to facilitate compliance with the requirements set up by these UK BCRs in practice.

11 – Relationships with Data Processors (Amgen Data Importer or Vendor)

The Amgen Participating Company (acting as Data Controller) will carefully choose a Data Processor that can be either another Amgen Participating Company or a Vendor. The Data Processor must provide sufficient guarantees regarding their Technical and Organizational Security Measures governing the Processing to be carried out and must ensure compliance with those measures.

When outsourcing is deemed necessary after assessing the business needs and risks of such an outsourcing, the process of choosing the Data Processor will include an evaluation of privacy risk factors and balance business needs against potential risks.

The Amgen Participating Company (acting as Data Controller), utilizing written contractual means will, in accordance with Applicable Law (and in particular the requirements of Article 28(3) of the UK GDPR), instruct the Data Processor that, among other things:

(i) the Data Processor shall act only on instructions from the Amgen Participating Company acting as Data Controller and that the Processing of Personal Information for the Data Processor's own purposes or for the purposes of a Third Party is prohibited;

(ii) on the rules relating to the security and confidentiality to be incumbent on the Data Processor and to implement appropriate Technical and Organisational Measures to ensure a level of security appropriate to the risk of the Processing;

(iii) persons authorised to Process the Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iv) the Data Processor shall not engage another Data Processor without the prior specific or general written authorisation of the Amgen Participating Company acting as Data Controller and, where such authorisation is given, the same data protection obligations as set out in the contract or other legal act between the Amgen Participating Company acting as Data Controller and the Data Processor shall be imposed on that other Data Processor;

(v) taking into account the nature of the Processing, it must assist the Amgen Participating Company acting as Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Amgen Participating Company's obligation to respond to requests for exercising the Data Subject's rights;

(vi) it must assist the Amgen Participating Company acting as Data Controller in ensuring compliance with the obligations relating to security of Processing, notification of a Privacy Incident to the ICO, communication of a Privacy Incident to the Data Subject, data protection impacts assessments and prior consultation with the ICO, taking into account the nature of Processing and the information available to the Data Processor;

(vii) at the choice of the Amgen Participating Company acting as Data Controller, it must delete or return all the Personal Information to the Amgen Participating Company acting as Data Controller after the end of the provision of services relating to the Processing, and delete existing copies unless UK Data Protection Law requires storage of the Personal Information;

(viii) it must make available to the Amgen Participating Company acting as Data Controller all information necessary to demonstrate compliance with the obligations laid down in this Article 11 and allow for and contribute to audits, including inspections, conducted by the Amgen Participating Company acting as Data Controller or another auditor mandated by it.

The Amgen Participating Company acting as Data Controller shall ensure that the Data Processor remains fully compliant with the agreed Technical and Organizational Security Measures.

The Amgen Participating Company acting as Data Controller retains responsibility for the legitimacy of Processing and is still liable for the Data Subject's rights. To the extent the Data Processor is subject to the UK Data Protection Laws, it shall also be liable for its obligations and responsibilities as a Data Processor under such laws.

In order to provide for the contractual obligations set out in this Article on Data Processors, a contractual template titled the Data Privacy Schedule is provided for use by Amgen Participating Companies acting as Data Controller. The Amgen Participating Company acting as Data Controller may, depending on the specific circumstances of each contractual arrangement, negotiate different provisions to those set out in the Data Privacy Schedule, but the contractual provisions must still cover, at a minimum, the obligations set out above in this Article 11.

12 – Restrictions on Transfers and Onward Transfers

All transfers of Personal Information to Third Parties located outside of the UK shall respect the UK Data Protection Laws on transfers and onward transfers of Personal Information either by making use of the standard contractual clauses authorized under Paragraph 7 of Schedule 21 of the Data Protection Act 2018 or by another adequate means according to Chapter V of the UK GDPR.

All transfers of Personal Information to Data Processors located outside of the UK shall respect the UK Data Protection Laws relating to Data Processors (and the requirements set out in Article 11 above) in addition to the rules on transfers and onward transfers of Personal Information set out in this Article 12 and in the UK Data Protection Laws.

13 – Training Program

As described in Appendix 2, Amgen provides appropriate training on privacy principles and more specifically on the UK BCRs to all Personnel. This training also includes information regarding the consequences under criminal and employment law and/or their contract for services for Personnel who breach the UK BCRs.

The training is mandatory and repeated annually. Successful participation in training will be documented.

Specific trainings will be provided on a case by case basis to Personnel who have permanent or regular access to Personal Information, or who are involved in the collection of Personal Information or in the development of tools used to Process Personal Information.

In addition, Amgen's Global Privacy Compliance Team provides appropriate information and resources related to privacy, for instance, on the Amgen intranet portal.

14 – Audit and Monitoring Program

The Chief Privacy Officer ensures that all Participating Companies (and their compliance with these UK BCRs) are included within the audit and monitoring program from a privacy and data protection perspective. Comprehensive audits are carried out on a regular basis, no less frequent than every 2 to 3 years (for Amgen Participating Companies with a medium to high risk profile based on the Audit department's risk assessment methodology) and every 4 to 5 years (for Amgen Participating Companies with a low risk profile based on the Audit department's risk assessment methodology), by the Internal Audit Team or independent, external certified auditors. Comprehensive audits include data protection and privacy matters within their scope (including compliance with these UK BCRs, where applicable to and used by a Participating Company). In addition to comprehensive audits, and without prejudice to the timeframes set out above, other scopes of audit are carried out including cross-functional or issue-specific audits (e.g., compliance with the UK BCRs), a limited audit of one or more Personal Information Processing systems and/or a limited audit of one or more functional departments (e.g., the Global Privacy Compliance Team). The audit program is developed and agreed to in cooperation with the Chief Audit Executive and the Chief Compliance Officer who is a Senior Vice-President. The Chief Privacy Officer, the Chief Compliance Officer, and the Chief Information Officer can initiate ad hoc UK BCR-related audits at any time. For example, in response to any identified compliance issue or a report of substantive non-compliance, a Privacy Incident and/or a substantive change in the UK Data Protection Laws. The audit program covers all aspects of the UK BCRs including methods of ensuring that corrective actions will take place.

All UK BCR audit reports are communicated to the Chief Compliance Officer and to the Chief Privacy Officer in a timely manner. The UK BCR audit summaries and findings, as well as other relevant information, are also regularly reported to the Board of Directors of Amgen Inc. via appropriate committees (e.g., Corporate Responsibility and Compliance Committee and/or Audit Committee of the Board), to the board of directors of Amgen UK and (where appropriate, for example, in relation to a finding requiring remedy) to the relevant Participating Company. The Corporate Responsibility and Compliance Committee of the Board of Directors of Amgen, Inc. meets five times a year. Privacy & Data Protection is covered annually, typically in the October meeting.

The UK ICO can receive a copy of UK BCR-related audit reports upon request.

Each Participating Company shall cooperate with and shall accept, without restrictions, to be audited by the UK ICO. Each audited entity must inform the Chief Privacy Officer immediately if it receives notice of such audit or such an audit takes place.

15 – Compliance and Supervision of Compliance

Amgen appoints appropriate Personnel, including where applicable a network of Data Protection Officers, with top management support to oversee and ensure compliance with data protection rules. The Chief Privacy Officer is in charge of the Global Privacy Compliance Team which is a global team providing expert support worldwide for Amgen entities (including Participating Companies).

At Amgen, the Chief Privacy Officer's responsibilities, among others, include:

- advising the board of management;
- ensuring data protection compliance at a global level (including having overall responsibility for the UK BCRs);
- reporting regularly on data protection compliance (including to the Chief Compliance Officer); and
- working with the UK ICO's investigations.

The Global Privacy Compliance Team includes the Chief Privacy Officer, Head of Global Privacy (who reports to the Chief Privacy Officer and oversees the global network of Data Protection Officers), the European Data Protection Officer and other local Data Protection Officers. The Global Privacy Compliance Team has overall responsibility for data protection and privacy compliance worldwide at Amgen.

The European Data Protection Officer has been appointed by Amgen as the Data Protection Officer for the EU/EEA, the UK and Switzerland. The European Data Protection Officer has the tasks set out in Article 39 of the UK GDPR. The European Data Protection Officer has a direct reporting line to the Head of Global Privacy and the Chief Privacy Officer as well as senior management at Amgen UK and is supported by the local Compliance Lead in the UK.

At the local level, Data Protection Officers are responsible for handling local privacy requests from Data Subjects, for ensuring compliance at a local level with support from the Global Privacy Compliance Team and for reporting major privacy issues to the Chief Privacy Officer. Amgen maintains a Data Protection Officer network and ensures that a DPO is appointed or assigned for

each country where Amgen has a corporate entity (the Participating Company) and the applicable law of the jurisdiction of such Participating Company require such appointment.

Usually, Data Protection Officers either are, or are supported by, the local Compliance Leads who report into the Worldwide Compliance and Business Ethics department. The Global Privacy Compliance Team is a part of, and reports into, the Worldwide Compliance and Business Ethics department for which is headed by the Chief Compliance Officer. The Chief Compliance Officer has overall responsibility for the Amgen group's legal and regulatory compliance worldwide. Rarely, due to the specific circumstances of an Amgen Participating Company or other special circumstances, the Data Protection Officer may come from another function, for example Regulatory. In any event, the Global Privacy Compliance Team ensures that the Data Protection Officers and Compliance Leads are trained appropriately and have a sufficient level of management and expertise to fulfil his or her role. In addition, the Data Protection Officers have a direct reporting line to the Chief Privacy Officer and are supported by Global Privacy Compliance Team Personnel in the event they need any additional guidance.

Every Participating Company acting as Data Controller shall be responsible for and be able to demonstrate compliance with the UK BCRs. As part of this requirement, all Participating Companies:

- must maintain a record of all categories of Processing activities carried out in line with the requirements as set out in Article 30(1) of the UK GDPR. This record should be maintained in writing, including in electronic form, and shall be made available to the Chief Privacy Officer and the UK ICO on request;

- carry out data protection impact assessments for Processing operations that are likely to result in a high risk to the rights and freedoms of natural persons in accordance with Article 35 of the UK GDPR. Where a data protection impact assessment under Article 35 indicates that the Processing would result in a high risk in the absence of measures taken by the Participating Company to mitigate the risk, the Chief Privacy Officer must be consulted prior to Processing, who shall then consult with the UK ICO in accordance with Article 36 of the UK GDPR.

16 – Actions in Case of National Legislation Preventing Respect of the UK BCRs

Where a Participating Company has reason to believe that the laws applicable to it prevents the Participating Company from fulfilling its obligations under the UK BCRs or has a substantial effect on the guarantees provided by the rules, it will promptly inform the Chief Privacy Officer (except where prohibited by a law enforcement authority, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation) and Amgen UK.

Where there is conflict between local national law and the commitments in the UK BCRs, the Chief Privacy Officer in liaison with local legal counsel and the local Data Protection Officer will determine what legally appropriate action is required. If necessary, the Chief Privacy Officer will also consult with the UK ICO.

Where any legal requirement a Participating Company is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by the UK BCRs, the Chief Privacy Officer (and Amgen UK) shall be promptly notified, and the Chief Privacy Officer shall notify the UK ICO. This includes any legally binding request for disclosure of the Personal Information by a law enforcement authority or state security body. In such a case, the UK ICO should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure (unless otherwise prohibited, such as a prohibition under criminal law to preserve the

confidentiality of a law enforcement investigation). If in specific cases the suspension and/or notification are prohibited, the Participating Company receiving the request will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so. If, despite having used its best efforts, the Participating Company receiving the request is not able to notify the UK ICO, the Participating Company, in conjunction with the Chief Privacy Officer, shall annually provide general information on the requests it receives to the UK ICO.

In any event, transfers of Personal Information by a Participating Company to any public authority shall not be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

17 – Internal Complaint Mechanisms

Amgen will expand and utilize its existing complaint handling process to incorporate handling of any UK BCRs-related complaints or concerns.

Any Data Subject may complain, at any time, that any Participating Company is not complying with the UK BCRs. Such complaints will be handled by the Global Privacy Compliance Team under the direction of the Chief Privacy Officer and in cooperation with the relevant local Data Protection Officer.

Amgen recommends that such complaints are provided in writing either by postal mail or email directly to the Global Privacy Compliance Team or to the Participating Company. The Global Privacy Compliance Team may be contacted using the contact details below:

Address: Amgen Limited, 216 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire, CB4 0WA, UK. Email: privacy@amgen.com

Amgen Personnel may as well, when acceptable according to the laws applicable to the Participating Company, use the Business Conduct Hotline to report a UK BCRs complaint.

If the complaint is received locally by the Participating Company, the DPO will translate if necessary and forward it without undue delay to the Global Privacy Compliance Team.

An initial response will be provided to the Data Subject within ten (10) working days informing that his/her complaint is under consideration and that he or she will receive substantive response without undue delay and in any event within one month of receipt of the request. Taking into account the complexity and number of the requests, the one-month period may be extended by a maximum of two further months, in which case the Data Subject shall be informed accordingly. The substantive response will include details about our findings and any action Amgen has or proposes to take. If Amgen determines that no action should be taken, this shall be explained to the Data Subject together with reasons for this determination.

If the complaint is upheld by Amgen, then Amgen will implement appropriate remedial measures. Those measures will be decided on a case by case basis by the Chief Privacy Officer and the Global Privacy Compliance Team, the local DPO and, where applicable, any other relevant department. Furthermore, if the Global Privacy Compliance Team discovers individual wrongdoing, appropriate disciplinary measures will be taken, up to and including termination of employment or engagement, to the extent permitted by Applicable Law.

The Data Subject will receive an answer informing him/her of the outcome of his complaint. This shall be without undue delay and in any event within one month of receiving the complaint (with sufficient details for Amgen to identify the nature of the complaint and, only where reasonably necessary, with any information requested to confirm the complainant's identity). Taking into account the complexity and number of the requests, the one-month period may be extended by a maximum of two further months, in which case the Data Subject shall be informed accordingly.

The Data Subject will be informed that if he/ she is not satisfied by Amgen's answer, he/she can lodge a claim before the UK courts or the UK ICO. However, it is not a requirement that a Data Subject first go through Amgen's complaint handling process before he or she can complain to the UK ICO or bring a claim before the UK courts.

This complaint handling process will be made public through the publication of the UK BCRs as mentioned in Article 7 above.

18 - Third Party Beneficiary Rights and Liability

A Data Subject whose Personal Information originates from the UK or is protected by the UK Data Protection Laws and is transferred to Participating Companies outside the UK shall have the right to enforce the UK BCRs as a third-party beneficiary and shall have the right to seek judicial redress, obtain remedies and, where appropriate, compensation for actual damage suffered as a result of breach of these UK BCRs. Any such claims can be brought by the Data Subject before the UK ICO. Data Subjects may also bring a claim before a competent court in the UK. The Data Subject shall be able to enforce the following Articles as a third party beneficiary:

- Articles 1, 2, 3, 4, 5 and 6;
- Article 7;
- Articles 8 and 9;
- Article 10, 11 and 12;
- Articles 16 and 21;
- Article 18; and
- Article 19.

For the avoidance of doubt, the third party beneficiary rights do not extend to those Articles and elements of these UK BCRs which pertain to internal mechanisms implemented within Participating Companies or the Amgen group such as details regarding training (including Appendix 2), audit programmes, internal compliance networks and structure and the mechanism for updating the UK BCRs.

Amgen UK accepts responsibility for and agrees to take such action as is reasonably necessary to remedy the acts of Participating Companies established outside the UK. Amgen UK shall pay compensation for any material or non-material damages resulting from the violation of these UK BCRs, unless it can demonstrate that the Participating Company established outside the UK is not responsible for the event giving rise to the damage. Amgen UK has sufficient financial means and insurance cover to cover damages under the UK BCRs.

Any Data Subject who has suffered damage arising from a breach of these UK BCRs by a Participating Company not established in the UK is entitled, where appropriate, to receive compensation from Amgen UK for the damage suffered and the courts or other competent authorities in the UK shall have jurisdiction. The Data Subject shall have the rights and remedies against Amgen UK as if the

violation had been caused by Amgen UK in the UK instead of the Participating Company not established in the UK. If the Participating Company not established in the UK is responsible or held liable for such breach, it will to the extent to which it is responsible or liable, indemnify Amgen UK for any cost, charge, damage, expense or loss Amgen UK incurs in relation to such breach.

In the event of a claim by a Data Subject that he/she has suffered damage and has established it is likely that such damage occurred because of a breach of these UK BCRs, the burden of proof to show that the damages suffered by the Data Subject due to a breach of these UK BCRs are not attributable to relevant Participating Company shall rest with Amgen UK. If Amgen UK can demonstrate that the Participating Company established outside the UK is not responsible for the event giving rise to the damage, it shall not be liable or responsible for the damage.

19 – Mutual Assistance and Cooperation with the UK ICO

Participating Companies shall cooperate and assist each other to handle a request or complaint from a Data Subject or an investigation or inquiry by the UK ICO.

Participating Companies will answer, in collaboration with the Chief Privacy Officer, UK BCRs-related requests from the UK ICO within an appropriate timeframe in view of the circumstances of the request (and in any event no later than any deadline imposed by the UK ICO) and in an appropriate detail based on the information reasonably available to the Participating Company. In relation to the implementation and ongoing application of the UK BCRs, Participating Companies shall give due consideration to the communications and recommendations of the UK ICO and shall comply with any formal decisions or notices issued by the UK ICO.

20 – UK BCRs Updating and Changes

Amgen reserves the right to change and/or update these UK BCRs at any time. Such update of the UK BCRs may be necessary specifically as a result of new legal requirements, significant changes to the structure of the Amgen group or official requirements imposed by the UK ICO.

Amgen will promptly report any significant changes to the UK BCRs or to the list of Participating Companies to all other Participating Companies and to the UK ICO to take into account modifications of Applicable Law, the regulatory environment and/or the Amgen group structure. Some modifications might require a new approval from the UK ICO.

The Chief Privacy Officer will keep a fully updated list of the Participating Companies of the UK BCRs and track any updates to the rules as well as provide the necessary information to the Data Subjects or the UK ICO upon request. Any administrative changes to the UK BCRs will be reported to Participating Companies on a regular basis.

Amgen is committed that no transfer is made to a new Participating Company under the guarantees of the UK BCRs until the new Participating Company is effectively bound by the UK BCRs and in compliance with the UK BCRs.

Any administrative changes to the UK BCRs or to the list of Participating Companies will be reported to the Participating Companies on a regular basis and reported at least once a year to the UK ICO with a brief explanation regarding the reasons for the update.

Substantial modifications to the rules will also be communicated to the Data Subjects by any means according to Article 7 of the UK BCRs.

21 – Relationship between National Laws and the UK BCRs

Where the local national laws applicable to a Participating Company require a higher level of protection for Personal Information it will take precedence over the UK BCRs. If the local national laws applicable to a Participating Company provide a lower level of protection for Personal Information than the UK BCRs, the UK BCRs will be applied.

In the event that obligations arising from the local national laws applicable to a Participating Company are in conflict with the UK BCRs, the Participating Company shall inform the Chief Privacy Officer without undue delay and shall comply with the additional requirements set out in Article 16 above.

In any event, Personal Information shall be Processed in accordance with the Article 5 of the UK GDPR and relevant local legislation.

22 – Final Provisions

The UK BCRs shall be effective upon approval by the UK ICO and be applicable to the Amgen Participating Companies upon signing the UK BCRs Adoption Agreement.

23 – Appendices

The attached appendixes are integrally part of the UK BCRs.

Appendix 1: Overview of Amgen UK's Data Flows

Appendix 2: Overview of Amgen Training Program

Appendix 1: Overview of Amgen UK Data Flows

Data subjects	Categories of data	Purposes	Transfer
Employee	Identification data such as name, address, date and place of birth, hire date, social security numbers, credit card numbers, bank account and financial information, and driver's license and government-issued identification card numbers Vacations and benefits, grievances, bonuses, promotions, reviews and evaluations, work records, information related to health and welfare coverage, retirement plan and stock option details Tax and Finance Personal information Sensitive data such as national origin, when permitted by local law	Personnel management, information technology support and administration purposes in connection with the employment relationship and benefits, or the administration of post-employment benefits, as well as to comply with Amgen's legal, administrative and corporate obligations	Amgen global data bases are located in the USA where Amgen Inc., the headquarters, is based. Data are flowing from Amgen UK (or the relevant Data Exporter) to Amgen Inc. in the United States or to Amgen Participating Companies in Switzerland. Then, the data may: - simply be stored and maintained there - be analyzed to provide global statistics and reports - be shared onward inside the Amgen group to other Participating Companies where there is a business need for such access by specific personnel or business functions at those Amgen Participating Companies (ex: an employee applying for a job outside his country or having to report to a manager based outside of his country). In most cases, such Participating Companies will act as Data Controllers, but depending on the business need, Participating Companies may also act as Data Processors (ex: in providing IT Help Desk support or providing support relating to the HR Connect Service Centre).
Healthcare Professionals	Name, business phone number, business email address and Field of expertise Professional background (resume) Participation to other research Financial information (billing and payment information)	Administration and management of Amgen's professional and scientific activities – R&D (for example, participation in medical research, clinical studies, professional meetings or congresses Promotion of Amgen's products and services Disclosure of financial information when required by applicable "sunshine act" Regulatory compliance such as safety monitoring, adverse event reporting or transparency requirements	
Vendors / Suppliers	Individual name, organization name, business contact information Billing and payment information	Processing of payments to vendors and suppliers Regulatory compliance such as tax law	
Clinical Trial Data Subjects / Patients (which may include children under the age of 18 where (1) there is a pediatric patient involved in a clinical	Coded data, health data, date of birth, place of birth, sex, weight, height, ethnicity, family situation (such as marital status, children), financial situation such as reimbursement, professional situation such as job, unemployment, participation to other research;	Administration and management of biomedical research (clinical trial, observatory studies) Regulatory compliance such as safety monitoring and adverse event reporting (when permitted by local law)	

study sponsored by Amgen, or (2) there is an adverse event involving the use of an Amgen product with a pediatric indication)	commutes, consumption of drugs, alcohol, drugs, and general habits or behaviors (when permitted by local law)		

Appendix 2: Overview of Amgen Training Program

Privacy and Data Protection Training / Awareness Program

The Privacy and Data Protection Training Program strives to ensure that all Amgen Personnel are properly trained regarding Amgen UK BCRs as well as any legal obligations that impact Processing of Personal Information. This program contains various elements.

General training for all Amgen Personnel

All Amgen Personnel must perform an annual online training on data protection as part of the Code of Conduct Training. This training is mandatory and monitored and usually takes around 75 minutes to complete. By the end of Q2 2022, this training will also include the UK BCRs and information regarding the consequences under criminal and employment law and/or their contract for services for Personnel who breach the UK BCRs. See "Specific training to Personnel" below for the specific training on the UK BCRs which will be provided in the interim.

Specific training to DPOs

All Amgen DPOs are regularly trained on new processes through regular DPO calls performed by the Global Privacy Compliance Team and privacy workshops onsite and/or online on a need-to-know basis. All DPOs have access to a wiki page that answers the most frequently asked questions and provides guidance as well as links to external resources. Specific training on UK BCRs will be provided to the DPOs, including a communication package to cascade the UK BCRs requirements to their local management team.

Specific training to Personnel

Specific training may be delivered on a need-to-know basis either online or onsite or through posting information on the Amgen intranet. This training may be focused on specific groups that may either Process Personal Information on a daily basis or support other groups that Process Personal Information. For instance, the audit group, R&D functions, and the legal department are regularly trained. This training can happen either at a regional level or on a country level. Prior to the inclusion of UK BCRs training as part of the Code of Conduct Training in 2022, the UK BCRs will be assigned as an online read and acknowledge training to existing and new Personnel promptly following the approval of the UK BCRs by the ICO. This training must be completed within 30 days of assignment. Further specific UK BCRs training may be developed on a need-to-know basis.

Awareness

Amgen has a dedicated page on its intranet on Privacy and Data Protection that provides links to other resources either internally or externally.

Amgen's Global Privacy Compliance Team collaborates with the Information Security department on the Sentinel program which is a global program to raise awareness of Amgen Personnel on information security.

Training support

All privacy-related trainings are developed by the Global Privacy Compliance Team and approved by the Chief Privacy Officer. The training may either be directly performed by a Global Privacy Compliance Team member or by a local DPO on a "train the trainer" model.