RELATÓRIO

Cláusulas-Padrão Contratuais:

Transferências Internacionais de Dados Pessoais em Perspectiva

AUTORES
FLÁVIA PARRA
TAINÁ AGUIAR JUNQUILHO
PEDRO GUEIROS

REVISÃO E EDITORAÇÃO
CELINA BOTTINO
CHRISTIAN PERRONE

PROJETO GRÁFICO
MARIANA BERTOLUCI

ITS

Sumário

RESUMO EXECUTIVO

Em meio à heterogeneidade de ordenamentos jurídicos ao redor do mundo, encontrar um denominador comum à garantia de confiança e proteção de fluxos transfronteiriços de dados pessoais, é de fato muito complexo. É nesse contexto que as instrumentos contratuais se apresentam como uma opção fundamental a empresas e organizações que realizam tratamentos de dados em diversos e variados países do globo, especialmente, as **Cláusulas-Padrão Contratuais (CPCs)**.

Neste relatório você encontrará **quatro principais exemplos que regulamentam CPCs**, quais sejam, da União Europeia, Reino Unido, Singapura e Nova Zelândia. A partir destes casos concretos, será possível compreender como e porquê diferentes abordagens de CPCs contribuem para um maior ou menor nível de proteção de dados e, de igual modo, de participação dos países no ecossistema global de transferências internacionais. Para tanto, será apontado objetivamente as **principais convergências e divergências dos respectivos instrumentos contratuais**. E, uma vez identificadas, apresenta-se, por fim, **no que consistem os critérios de proteção mínimo e máximo em termos de CPCs**.

Para além de uma compreensão essencial de como diferentes países do mundo exercem influência no sistema global de trocas de dados, o estudo tem um propósito bem claro. Apoiar o processo de regulamentação das CPCs pela Autoridade Nacional de Proteção de Dados (ANPD) no Brasil. Este tão esperado passo a ser dado no país, deverá inserir e definir o Brasil como relevante ator desse cenário internacional.

Inicialmente são levantadas as perspectivas da União Europeia trazidas pelo Regulamento Geral de Proteção de Dados Pessoais da União Europeia (“GDPR”). Em seguida, apresenta-se o panorama normativo do Reino Unido. Em seguida, a perspectiva da Associação das Nações do Sudeste Asiático (ASEAN e, mais especificamente, a de Singapura) e, por fim, da Nova Zelândia. Tudo isso com a finalidade principal de levantar iniciativas existentes no tema e para melhor compreender as particularidades de cada ordenamento e sugerir quais os modelos possíveis para o Brasil, diante de suas peculiaridades, pode adaptar-se às demais iniciativas.

Comparando os diversos ordenamentos, nota-se que as Cláusulas-Padrão Contratuais (CPCs) são de longe os mecanismos mais utilizados. A teia estruturante do comércio internacional tem por base que a maior parte das transações que se direcionam a fluxos transfronteiriços de dados se dá por arranjos contratuais.

É importante que instrumentos desse tipo sejam de fácil uso e com as garantias necessárias para proteger dados pessoais sem que criem exigências que impeçam o desenvolvimento de atividades e serviços e da inovação. É ainda mais importante esse aspecto no que tange às micro e pequenas empresas, pois estas devem cumprir com as exigências de proteção sem que os custos altos a levem a ficar excluídas dos fluxos internacionais.

Igualmente importa notar que as redes negociais podem ser bastante complexas, logo, é significativo que exista possibilidade de estruturação das CPCs para refletirem essa complexidade, levando em consideração o potencial de flexibilidade prática de adequação às diversas formas de organizações empresariais.

Por outro lado, as Normas Corporativas Globais (NCGs) parecem ser mais adequadas às grandes corporações e conglomerados econômicos. Curioso observar que, no contexto europeu, mesmo diante da complexidade do mecanismo e da necessidade de adequação a múltiplos sistemas, ainda existem poucas organizações que utilizem esses sistemas. No entanto, já é notável um salto significativo no seu uso desde a maior flexibilização do mecanismo de chancela pela União Europeia, com a entrada em vigor do GDPR. O que tende a indicar uma demanda que pode vir a chegar ao Brasil.

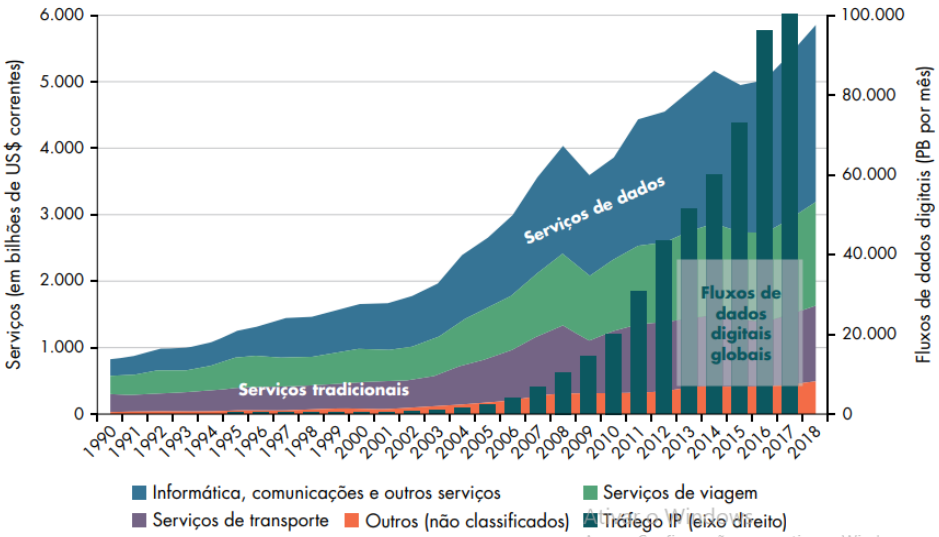
Conclui-se, que para melhor equilíbrio e promoção de transferências internacionais de dados que, ao mesmo tempo, respeitem proteção de dados pessoais e não restrinjam essa atividade importante, atingindo, em especial, pequenos empreendedores, é necessário construir parâmetros mínimos à proteção de dados pessoais a ser observada pelas empresas. Assim, o Brasil deve prever de forma clara e objetiva os limites da responsabilização dos agentes de tratamento da cadeia de tratamento de dados, assegurando os direitos, liberdades e garantias dos titulares de dados.

1 . Introdução

Quando o assunto é transferências internacionais de dados, as controvérsias parecem surgir quase instantaneamente. Afinal, quais são as regras aplicáveis ao importar ou exportar informações pessoais de um país para outro? A resposta está longe de ser simples e atinge muito mais as pessoas do que se imagina. Basta verificar que a mera utilização de um aplicativo com armazenamento de nuvem para *smartphones* já pode configurar em si um fluxo expressivo de dados.

O fluxo de transação internacional de dados aumenta ano a ano, como apontam Relatório produzido pelo Banco Mundial em 2021[1] e a figura a seguir:

Figura O.5 Desde 1990, o comércio global de serviços de dados aumentou imensamente e já representa metade de todo o comércio de serviços



Fonte: Cálculos da equipe do RDM 2021 baseados no banco de dados da Solução Comercial Integrada Mundial (WTIS, na sigla em inglês) do Banco Mundial

Diante desse contexto, o presente Relatório busca traçar um panorama normativo global de como ordenamentos jurídicos ao redor do mundo lidam com transferências internacionais. Nesse sentido, o objetivo é compreender, em perspectiva comparada, modelos e cláusulas que possibilitam a transferência internacional de dados, seja para países ques regulam internamente essa transferência, seja aqueles que

[1] WORLD BANK GROUP. *The World Bank Open Knowledge Repository*. Disponível em: <https://openknowledge.worldbank.org/>. Acesso em: 02.11.2022.

possibilitam que países que não possuem normativas protetivas de dados, transfiram por meio de Cláusulas-Padrão Contratuais (CPCs). O relatório finaliza sugerindo, com base nas diferentes perspectivas apresentadas, horizontes de adequação para o Brasil.

Os critérios sugeridos são: **a) Cláusulas-Padrão Contratuais (CPCs):** há a necessidade de estipulação de regras claras e flexíveis que sejam compatíveis com as diferentes responsabilidades e atribuições de Controladores e Operadores, projetando um espaço de uma maior variação às diferentes realidades empresariais, isto é, desde pequenas e médias empresas a grandes corporações. Sob este alcance, a Autoridade Nacional de Proteção de Dados (ANPD) pode considerar estruturá-las sob uma abordagem com marco comum de cláusulas, conteúdo mínimo essencial e uniforme, e uma ulterior gama de cláusulas com disposições que se adequem aos diferentes agentes e situações presentes nos fluxos transnacionais de dados; **b) Cláusulas Contratuais Específicas (CCEs):** há que se notar que a abordagem frente a esses mecanismos deve levar em consideração que a "especificidade" buscada pode se referir a certas peculiaridades existentes em determinados setores (e.g. saúde, financeiro etc.). Portanto, a abordagem da ANPD deve comportar a possibilidade dessas adaptações também; **c) Normas Corporativas Globais (NCGs):** uma abordagem mais teleológica e flexível, focada mais no "espírito" e nos princípios das normas de proteção de dados pode ser o caminho para uma maior adesão a esse mecanismo. As diferentes instituições que podem se interessar a propor esses mecanismos tendem a harmonizar normas de múltiplas jurisdições, o que na prática pode levar a escolhas difíceis sobre os caminhos a serem usados para a proteção e segurança de dados. Eventual exigência de um padrão muito rígido para a aprovação destas NCGs pode ter como resultado inibir a atuação de empresas no país ou ainda aumentar os custos de funcionamento.

2. Panorama quanto às Cláusulas-Padrão Contratuais em diferentes ordenamentos jurídicos

As decisões de adequação ou não das normas (ou contratos) do país (ou empresa/órgão) remetente de dados, varia em cada país ao redor do mundo. Existem modelos rígidos com cláusulas pré-determinadas, cujas principais vantagens são a garantia de um nível mínimo como padrão de proteção e a clareza nas obrigações; modelos flexíveis, cujas cláusulas podem ser negociadas e que têm como vantagens principais a possibilidade de focar na melhor forma de proteção e de adaptação ao fluxo global e aos seus múltiplos atores e os modelos híbridos, em que se preveem previamente cláusulas que podem ser discutidas.

Em um segundo momento, será realizada uma comparação entre as cláusulas obrigatórias do modelo rígido previsto pela União Europeia e para se compreender quais dessas cláusulas são consideradas obrigatórias ou estão também previstas por cada país.

2.1. União Europeia

A União Europeia possui modelo de regulação e viabilização da transferência internacional de dados que estabelece "gradações". As decisões de adequação encontram-se no primeiro "nível", nas quais se reconhecem graus de equivalência na proteção de dados ao país remetente. De forma secundária, há outras maneiras que representam as garantias no cumprimento à proteção de dados pessoais. Menciona-se por exemplo as CPCs, as quais são instrumentos jurídicos que vinculam agentes de tratamento que, fora do Espaço Econômico Europeu (EEE), operam transferências de dados.

2.1.1. Panorama normativo

O Parlamento Europeu tem notória tradição e maturidade em proteção de dados, tanto é assim que possui, desde os anos 1990, a Diretiva 95/46/CE já regulava a coesão entre os países do bloco europeu no tratamento de dados pessoais. A Diretiva

foi substituída em 2016 pelo GDPR aprovado pelo Parlamento Europeu, tendo entrado em vigor em 25 de maio de 2018.

O GDPR traz, para além das cláusulas fixas, que não são passíveis de sofrerem modificações, os novos arranjos contratuais que permitem maior dinamismo às diferentes modalidades de transferências internacionais de dados, levando em consideração as múltiplas formas de relações entre Controladores e Operadores[2]. Além disso, em recentes modificações ocorridas na legislação em 2021, foram incluídos anexos em branco, que devem ser preenchidos com informações adicionais, com detalhes a respeito das categorias de dados tratados, categorias de titulares de dados, dentre outros elementos relativos aos contornos da relação formalizada[3].

2.1.2. As cláusulas, sua aplicação e dificuldades

Mesmo diante de um grande avanço para que a implementação de CPCs seja progressivamente facilitada, fato é que as exigências do modelo europeu trazem muitos custos à realidade empresarial. Basta inferir que se trata de uma gama de cláusulas pré-formatadas que devem necessariamente ser inseridas a contratos celebrados sob as mais diversas finalidades e objetivos.

As constantes revisitações também impõem certo desgaste. A partir de 27 de dezembro de 2022, agentes de tratamento poderão continuar com as CPCs estabelecidas sob o regime anterior para contratos celebrados antes de 27 de setembro de 2021, desde que as operações de tratamento permaneçam as mesmas. Some-se ainda ao fato de que, conforme uma lista de perguntas e respostas disponibilizadas em maio desde ano, as CPCs deverão ser revistas já em 2024[4].

---

[2] Os módulos para transferências delineadas dividem em 4 opções: i) controlador-controlador (C2C); ii) controlador-operador (C2P); iii) operador-operador (P2P) e ainda; iv) operador-controlador (P2C).

[3] A teor do Anexo I.B.

[4] EUROPEAN COMMISSION. *The New Standard Contractual Clauses – Questions and Answers Overview*. Disponível em: <https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf>. Acesso em: 28.06.2022.

Até essa revisão prevista para 2024, as CPCs mínimas que devem prever "garantias em matéria de proteção de dados" quando da transferência internacional são: **(i)** Limitação das finalidades, isso é, o importador de dados deve proceder ao tratamento dos dados pessoais apenas para a(s) finalidade(s) específica(s) da transferência; **(ii)** Transparência, que determina o dever de informação, pelo exportador de dados aos titulares, a fim de permitir que os titulares dos dados exerçam efetivamente os seus direitos; **(iii)** Exatidão e minimização dos dados, ou seja, coleta do mínimo de dados possíveis, atualizados e corretos; **(iv)** Limitação da conservação apenas durante o tempo necessário para a(s) finalidade(s) para a(s) qual(is) são tratados; **(v)** Segurança do tratamento por meio de adoção de medidas técnicas e organizativas adequadas; **(vi)** Dados sensíveis, os quais exigem garantias adicionais; **(vii)** Transferências ulteriores só pode ser realizado com consentimento do titular e seguindo aos princípios do GDPR; **(viii)** Tratamento sob a autoridade do importador de dados, isso é, o importador de dados deve assegurar que qualquer pessoa que atue sob a sua autoridade, incluindo um subcontratante, só procede ao tratamento dos dados mediante as suas instruções; **(ix)** Documentação e cumprimento, demonstrando que as garantias e determinações foram adotadas na transferência.

Nota-se que diante de tantos ônus, pequenas e médias empresas parecem lidar sensivelmente com mais prejuízos. Isso porque, grandes corporações gozam de formas mais especializadas para enquadramento à sistemática, a exemplo das Regras Corporativas Globais (NCGs). Estas nada mais são do que políticas a serem adotadas por conglomerados e grupos econômicos estabelecidos na UE para transferir dados para fora do bloco.

2.2. Reino Unido

2.2.1. Panorama normativo

À época da edição do GDPR, o Reino Unido ainda era parte da União Europeia, já que a sua saída da UE (evento que ficou conhecido como "Brexit") só ocorreria em 31 de janeiro de 2020. Em razão disso, a GDPR foi incorporada às leis do Reino

Unido pelo *Data Protection Act* de 2018[5] (ou "UK DPA"), que atualizou as regras aplicáveis à proteção de dados no território por meio da substituição do *Data Protection Act* de 1998.[6]

Após o Brexit, houve um **período de transição**, durante o qual as regulações da União Europeia continuaram a ser aplicáveis ao Reino Unido, que durou até 31 de dezembro de 2020 em razão do termos do "Acordo sobre a saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia Atômica".[7] Ou seja, até 31 de dezembro de 2020, o GDPR, em sua versão da União Europeia, seguiu como plenamente aplicável ao Reino Unido, não sendo necessárias quaisquer alterações em termos de transferência de dados, já que o Reino Unido seguiria adequado em matéria de proteção de dados. No entanto, a partir de 01 de janeiro de 2021, transferências de dados pessoais para o Reino Unido passaram a ser regidas pelo *EU-UK Trade and Cooperation Agreement*,[8] acordado entre a União Europeia e o Reino Unido. O acordo previu regime interno (conhecido como *bridging clause*) que garantiu a continuidade de transferências de dados pessoais entre o Espaço Econômico Europeu ("EEE") e o Reino Unido, sem a necessidade de serem postas em prática outros mecanismos de transferência.[9]

Para fins do *EU-UK Trade and Cooperation Agreement*, contudo, uma das condicionantes previa que o Reino Unido não poderia alterar seu regime de proteção de dados pessoais, o qual ainda era baseado nas regras da União Europeia.[10] Nesse contexto, também em 01 de janeiro de 2021, entraram em vigor **as**

---

[5] Reino Unido. *Data Protection*. Disponível em: https://bit.ly/3vmdL0Q. Acesso em: 17.04.2022.

[6] O *Data Protection Act* de 1998 é a internalização, no Reino Unido, da Diretiva 95/46/CE.

[7] União Europeia. Acordo sobre a saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia Atômica (2019/C 384 I/01). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C:2019:384I:FULL&from=EN. Acesso em: 16.04.2022.

[8] União Europeia e Reino Unido. Acordo de Comércio e Cooperação entre a União Europeia e a Comunidade Europeia da Energia Atómica, por um lado, e o Reino Unido da Grã-Bretanha e da Irlanda do Norte, por outro. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22021A0430(01)&from=EN. Acesso em: 17.04.2022.

[9] Comissão Europeia. Brexit. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/brexit_en. Acesso em: 17.04.2022.

[10] Ibid.

emendas feitas ao *Data Protection Act* de 2018, a fim de refletir o *status* do Reino Unido fora da União Europeia.[11] Ademais, entrou em vigor, ainda em 01 de janeiro de 2021, a chamada **UK GDPR**, ou seja, a Regulação Geral de Proteção de Dados do Reino Unido, a qual define os princípios, direitos e obrigações para o tratamento de dados no Reino Unido, com a exceção dos regimes aplicáveis a agências de inteligência e autoridades.[12] A UK GDPR é muito baseada na GDPR da União Europeia, tendo sido feitas breves modificações para que a lei fosse melhor aplicável ao contexto interno do Reino Unido.

Por conseguinte, o regime aplicável à proteção dos dados pessoais, hoje, no Reino Unido, está previsto no UK DPA de 2018 e na UK GDPR enquanto leis próprias, e não mais no GDPR. Porém, é inegável que as referidas leis guardam muita semelhança com o GDPR aplicável à UE, uma vez que o Reino Unido a incorporou quando ainda fazia parte da UE. Justamente por esse motivo, e outros postos sob análise, a Comissão Europeia, em decisão de 28 de junho de 2021, confirmou a adequação do Reino Unido em matéria de proteção de dados pessoais. Conforme o texto:

> *The Commission has carefully analysed the law and practice of the United Kingdom. Based on the findings developed in recitals (8) to (270), the Commission concludes* ***that the United Kingdom ensures an adequate level of protection for personal data transferred*** *within the scope of Regulation (EU) 2016/679 from the European Union to the United Kingdom.*[13] (*grifos nossos*)

Portanto, atualmente, há um fluxo livre de dados entre Reino Unido e União Europeia com base na decisão de adequação concedida pela Comissão Europeia. Ademais, o Reino Unido reconhece a adequação dos países vistos como adequados para fins de transferências de dados com a UE. Porém, os demais países ainda devem adotar um dos mecanismos previstos na UK GDPR para a transferência de dados, dentre os

---

[11] 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/#2. Acesso em: 17.04.2022.

[12] Ibid.

[13] Comissão Europeia. *Commission implementing decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 30.04.2022.

quais se destacam as cláusulas contratuais padrão. Assim, na medida em que o Reino Unido deixou a União Europeia, coube à ICO a elaboração de CPCs que sejam específicas ao território de sua atuação, analisadas abaixo.

Finalmente, cabe ressaltar que, assim como na União Europeia, em conformidade com a GDPR, as CPCs **são apenas um dos mecanismos possíveis para a transferência internacional de dados** perante a UK GDPR. No entanto, especialmente após o julgamento do caso Schrems II, as CPCs despontam como um dos principais meios para transferências, atrás das situações em que já há uma decisão de adequação acerca da jurisdição para a qual os dados serão transferidos.[14] Para os fins da UK GDPR, as transferências internacionais de dados podem ser realizadas a partir de: **(i)** instrumentos juridicamente vinculantes e com força executiva acordados entre autoridades públicas ou outros órgãos públicos; **(ii)** NCGs; **(iii)** CPCs a serem especificadas pelo Secretário de Estado do Reino Unido; **(iv)** CPCs a serem especificadas pela ICO; **(v)** código de conduta acompanhado de compromissos vinculativos e com força executiva do controlador e do operador que estejam em um país terceiro para que apliquem as salvaguardas apropriadas, inclusive aquelas referentes a direitos dos titulares; ou **(vi)** procedimento de certificação junto aos compromissos vinculantes e com força executiva do controlador e operador no país terceiro em que garantam a aplicação das salvaguardas apropriadas, inclusive aquelas referentes a direitos dos titulares.[15] Portanto, o caso analisado aqui se refere ao item **(iv)** acima, disposto no artigo 46 (2) (d) da UK GDPR, qual seja, as CPCs especificadas pela ICO.[16]

---

[14] A decisão do Tribunal de Justiça da União Europeia no caso Schrems II reafirmou a validade das SCCs para que se possa realizar transferências internacionais de dados, ao mesmo tempo em que afirmou que as empresas possuem a obrigação de se verificar, em análises específicas, se as leis locais do país para o qual os dados serão transferidos são capazes de prover um grau de proteção adequado, segundo os parâmetros da União Europeia. Caso as leis locais não o garantam, pode-se necessitar de salvaguardas adicionais para garantir a proteção ou suspender transferências. Ver Processo C-311/18. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-311/18. Acesso em: 30.04.2022.

[15] Information Commissioner's Office. *International transfers after the UK exit from the EU Implementation Period*. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/. Acesso em: 01.05.2022.

[16] Information Commissioner's Office. *Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018*. Version A1.0. p. 32. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. Acesso em: 01.05.2022.

2.2.2. As cláusulas, sua aplicação e dificuldades

O documento contendo as cláusulas disponibilizadas pela ICO é dividido em **quatro partes**, são elas: **(i)** tabelas (*tables*, em inglês); **(ii)** cláusulas proteção adicional (*extra protection clauses,* em inglês); **(iii)** cláusulas comerciais (*commercial clauses*, em inglês); e **(iv)** as cláusulas obrigatórias (*mandatory clauses*, em inglês).

A linguagem se vale dos mesmos termos das cláusulas da União Europeia, como *data importer* (quem recebe os dados) e *data exporter* (quem envia os dados). Além disso, o texto é mais *user-friendly* quando comparado às cláusulas da União Europeia, sendo a sua escrita mais simples. O objetivo central é estabelecer em quais condições se dá o Acordo de Transferência Internacional de Dados (*International Data Transfer Agreement*, em inglês, ou "IDTA").

Existem algumas tabelas, logo no início, que guiam a aplicação das cláusulas com base em seu preenchimento (e.g. indicação de quem seria o controlador, qual a relação entre as partes etc.). As tabelas ainda promovem uma visão geral da relação entre *data importer* e *data exporter* ao questionarem se existem outros acordos ou contratos entre eles, o que é interessante tendo em vista que demais contratos firmados podem vir a influenciar as disposições de proteção de dados (e.g. quem se configura como Controlador ou como Operador). Nesse sentido, parece haver uma compreensão mais explícita sobre as interconexões entre os diversos documentos firmados no âmbito de uma relação jurídica e como esses podem influenciar obrigações relacionadas ao GDPR do Reino Unido. Portanto, as tabelas, em um primeiro momento, apresentam uma preocupação em deixar os pressupostos da transferência internacional de dados entre as partes claros (e.g. a parte que pode rescindir o IDTA, quais dados são transferidos, quem são os titulares de dados, a finalidade da transferência, requisitos de segurança para a transferência etc.).

As partes 2 e 3 do documento, as cláusulas proteção adicional e as cláusulas comerciais, por sua vez, são de preenchimento

por parte do importador e do exportador de dados, variando a partir das relações jurídicas especificamente estabelecidas entre as partes. No entanto, a parte 4 é de aplicação obrigatória e constitui, de fato, as cláusulas contratuais padrão para as transferências internacionais. Ou seja, o documento do Reino Unido **conta com partes adicionais** que guiam a aplicação das CPCs e as transferências em si. As partes 1, 2 e 3, nesse sentido, atuam de forma a contextualizar, em uma relação jurídica específica, a aplicação dessas cláusulas. É um formato interessante na medida em que fornece mais subsídios ao importador e exportador de dados quando da elaboração do IDTA, reforçando, como já afirmado, que se trata de documento mais *user-friendly* que as cláusulas aplicáveis no âmbito da União Europeia.

O conteúdo geral das cláusulas versa sobre, na sequência do documento[17]:

- **Possibilidade de alterações às cláusulas obrigatórias:** de forma geral, não seria possível modificar as cláusulas, havendo poucas exceções, como para garantir que as referências da parte 4 estejam conformes às partes 1, 2 e 3 do documento e para retirar as cláusulas que não sejam aplicáveis às partes;
- **Aplicação e interpretação do IDTA:** disposições dos pressupostos sobre como aplicar e interpretar o IDTA (e.g. se houver uma inconsistência entre o IDTA e as leis de proteção de dados do Reino Unido, essas últimas serão aplicáveis; se houver uma inconsistência entre eventual acordo relacionado ao tratamento de dados e o IDTA, os termos do IDTA prevalecem etc.);
- **Lei que rege o IDTA:** correspondente à lei do país aplicável do Reino Unido;
- **Salvaguardas apropriadas estabelecidas pelo IDTA:** estabelece as obrigações das partes em relação à adequação das salvaguardas – o exportador precisa, por exemplo, garantir que o IDTA provê salvaguardas adequadas, e o importador de dados deve, por exemplo, fornecer, ao exportador de dados, informações a respeito das leis locais, práticas, riscos e proteções aos dados que serão transferidos.

[17] Information Commissioner's Office. *Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018*. Version A1.0. p. 9-32. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. Acesso em: 01.05.2022.

- **Revisões do IDTA para garantia das salvaguardas:** estabelece que, eventualmente, são necessárias revisões para assegurar que as salvaguardas ainda sejam adequadas (e.g. se o IDTA não mais as prover, as partes podem alterar seus termos, pausar a transferência etc.);
- **Sujeição das partes à ICO:** estabelece prerrogativas da ICO em relação ao IDTA (e.g. ICO pode requerer informações a ambas as partes sobre o IDTA);
- **Obrigações do exportador:** dentre as quais se encontram cumprir com leis de proteção de dados do Reino Unido, cumprir possíveis acordos relacionados ao IDTA, garantir que o importador tenha capacidade de seguir as disposições do IDTA etc.;
- **Obrigações do importador:** as obrigações do importador são mais amplas que aquelas do exportador, variando caso a UK GDPR seja ou não aplicável ao importador. Ademais, há obrigações e especificações a respeito de princípios de proteção de dados, ocorrência de violação aos dados tratados pelo importador, possibilidade de transferir os dados já transferidos ao importador e a subcontratação de outros agentes enquanto Operadores ou Suboperadores pelo importador.
- **Direitos dos titulares em relação ao IDTA:** o titular possui direitos como receber cópia do IDTA, informações sobre o importador de dados e os tratamentos por ele realizados, exercer seus direitos de forma geral – a serem cumpridos pelo controlador de dados. O IDTA também prevê exceções nas quais não é necessário cumprir com tais direitos (e.g. se não for possível verificar a identidade do titular etc.);
- **Acesso por terceiros aos dados transferidos conforme leis locais:** trata-se dos casos em que os dados poderão ser acessados em razão de obrigação local por autoridades, sendo que, se for o caso, o importador de dados deverá informar as partes envolvidas sobre o pedido de acesso, dentre outras obrigações;
- **Violações ao IDTA:** estabelecimento de obrigações ao exportador e ao importador caso o IDTA seja violado pelas partes;
- **Término do IDTA:** estabelecimento de casos em que o IDTA terminará e o que as partes devem fazer se o IDTA terminar (e.g. parar de tratar os dados transferidos assim que as leis locais permitirem etc.);
- **Aspectos a respeito de ações que podem ser ajuizadas em face do IDTA:** disposições a respeito da responsabilidade das

partes, como e em quais matérias os titulares de dados e a ICO podem ajuizar ações, previsão sobre as cortes que podem julgar ações e sobre a possibilidade de arbitragem para resolução de conflitos advindos do IDTA.

Os pontos acima, portanto, trazem uma visão geral sobre o conteúdo das CPCs.

Ademais, é importante ressaltar que o IDTA permite que as transferências sejam feitas entre os Controladores, Operadores e Suboperadores. Em relação ao tratamento dos dados pessoais que são transferidos, o exportador de dados pode ser o Controlador, Operador ou Suboperador. Já o importador de dados pode ser o Controlador, o Operador ou Suboperador do exportador ou não ser o Operador ou Suboperador do exportador (caso em que o importador de dados é instruído por uma terceira parte). Assim, há considerável flexibilidade quanto à aplicação do IDTA em face da classificação das partes enquanto agentes de tratamento. Além disso, o IDTA permite que as partes acrescentem obrigações adicionais e suplementares, o que pode vir a incluir orientações do EDPB ou pontos relacionados ao caso Schrems II, como destacado acima – ponto de diferenciação quanto às CPCs da União Europeia.

Uma questão, inclusive, que as CPCs da ICO esclarecem, quando comparadas às CPCs da União Europeia é que as primeiras são aplicáveis tanto quando o importador de dados deve observar as regras postas pela UK GDPR, quanto quando a UK GDPR não se aplica ao importador de dados. Do contrário, no caso das CPCs da União Europeia, elas só se aplicam quando a GDPR não é a lei de proteção de dados aplicável ao importador no âmbito das cláusulas. Por conseguinte, resta uma incerteza a respeito de como devem ser as CPCs se o GDPR for aplicável ao importador por causa da aplicação extraterritorial do regulamento, de acordo com seu artigo 3(2).

Ainda, é pouco claro como as CPCs propostas pela ICO têm sido aplicadas. Isso porque tais CPCs entraram em vigor em 21 de março de 2022, após a sua aprovação pelo Parlamento inglês.[18] Por esse motivo, **as cláusulas ainda são recentes e é**

[18] Information Commissioner's Office. *IDTA and guidance*. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. Acesso em: 09.05.2022.

incerto como as empresas as implementarão. Além disso, junto ao IDTA publicado, o qual constitui a parte essencial das CPCs, **a ICO também publicou o chamado *UK Addendum***.[19] Trata-se de documento simplificado que funciona como um adendo às novas CPCs da UE, permitindo que empresas que já adotaram essas cláusulas só incluam o adendo aos acordos já existentes para estarem adequados perante a UK GDPR. O *UK Addendum* é mais flexível e oferece diferentes formas de utilização com estrutura tabular, sendo possível escolher quais cláusulas se aplicam às transferências específicas. Contudo, dentre suas desvantagens, há de se destacar que se trata de documento aplicável somente à UE, sem levar em conta outras regiões, como a própria ASEAN. Ademais, é possível que parte das empresas, e em especial aquelas que possuem estabelecimentos na UE e no Reino Unido, utilizem apenas o *UK Addendum* em vez do IDTA proposto pela ICO já que, em diversas vezes, já teriam as CPCs da UE implementadas.

Outro ponto de destaque é que as transferências de dados que sejam realizadas com base nas CPCs antigas, firmadas até 21 de setembro de 2022, **seguirão válidas até 21 de março de 2024**, conforme as disposições transitórias publicadas pela ICO quanto a transferências internacionais de dados.[20] As CPCs antigas são as desenvolvidas a partir da Diretiva 95/46/CE, de 24 de outubro de 1995, a qual versava sobre proteção de dados pessoais e foi substituída pelo GDPR. Ou seja, elas não abarcam completamente as modificações do GDPR ou a decisão do Tribunal de Justiça da União Europeia no caso Schrems II. Isso significa que as empresas que já tenham em vigor as CPCs antigas para transferências de dados apenas precisarão implementar as novas CPCs da ICO a partir de 2024, caso não o façam voluntariamente antes dessa data. Com base

---

[19] Information Commissioner's Office. *International Data Transfer Addendum (IDTA) to the EU Commission Standard Contractual Clauses*. Disponível em: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf. Acesso em: 10.05.2022.

[20] Nos termos das disposições transitórias da ICO: "*Contracts **concluded on or before 21 September 2022** on the basis of any Transitional Standard Clauses shall continue to provide appropriate safeguards for the purpose of Art 46(1) of the UK GDPR **until 21 March 2024**, provided that the processing operations that are the subject matter of the contract remain unchanged and reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards*." (*grifos nossos*) Information Commissioner's Office. I*nternational Data Transfer Agreements. Transitional Provisions*. Disponível em: https://ico.org.uk/media/for-organisations/documents/4019534/scc-transitional-provisions.pdf. Acesso em: 09.05.2022.

nesses pontos, é possível que a aplicação massiva das CPCs da ICO ainda demore.

De forma geral, ainda parece cedo para afirmar quais seriam as dificuldades na implementação das CPCs da ICO, principalmente pelos motivos expostos acima. Pode-se, mesmo assim, colocar breves considerações a seu respeito, em especial sobre suas diferenças quanto às CPCs da UE.

Nesse sentido, as CPCs da ICO não cobrem as obrigações previstas no artigo 28 do GDPR quanto aos Operadores de dados, as quais estão expressamente incluídas nas CPCs da UE. A ideia, com base no texto do IDTA, é que os acordos adicionais ou outros contratos (os *linked agreements*) cobririam esses pontos. No entanto, a inclusão das obrigações no IDTA poderia ter simplificado esse aspecto. Conjuntamente, **antes que se realize qualquer transferência de dados**, deve-se elaborar um ***Transfer Risk Assessment*** (TRA) a fim de avaliar a adequação do país do importador dos dados, especialmente após a decisão Schrems II. Se o país não tiver um nível adequado de proteção de dados, é um caso em que seria possível a inclusão de cláusulas suplementares para cobrir os aspectos necessários.

2.3. Associação das Nações do Sudeste Asiático

2.3.1. Panorama normativo

A Associação das Nações do Sudeste Asiático (conhecida como "ASEAN") foi fundada em 1967 a partir da assinatura da **Declaração da ASEAN** ou Declaração de Bangkok. Os países que faziam parte da ASEAN no primeiro momento eram: Indonésia, Malásia, Filipinas, Singapura e Tailândia. Posteriormente, juntaram-se à ASEAN: Brunei, em 1984; Vietnã, em 1995; Laos e Mianmar, em 1997; e Camboja, em 1999.[21] Esses países, juntos, compõem a ASEAN hoje.

[21] ASEAN. *The Founding of ASEAN*. Disponível em: https://asean.org/about-asean/the-founding-of-asean/. Acesso em: 19.05.2022.

Os propósitos da ASEAN, quando do seu surgimento, eram voltados à **cooperação** em termos econômicos, sociais, culturais, técnicos, educacionais e nos demais campos a fim de **promover a estabilidade regional** por meio do respeito à justiça e da aderência aos princípios da Carta das Nações Unidas.[22] A Declaração da ASEAN afirmava que a Associação representaria:

> *the collective will of the nations of Southeast Asia to bind themselves together in friendship and cooperation and, through joint efforts and sacrifices, secure for their peoples and for posterity the blessings of peace, freedom and prosperity*.[23]

Atualmente, a estrutura jurídica da ASEAN é regida pela Carta da ASEAN, a qual entrou em vigor em 15 de dezembro de 2008, após sua ratificação por todos os países do bloco.[24] A Carta trouxe modificações ao funcionamento da ASEAN em eixos centrais, como econômico, sociocultural e político. Além disso, de acordo com dados de 2018, os países-membros da ASEAN, em conjunto, tinham uma população de 634 milhões, um Produto Interno Bruto (PIB) de USD 2.55 trilhões e, enquanto ASEAN, formavam a sexta maior economia do mundo com transações que somavam USD 3.7 trilhões.[25] Assim, a ASEAN, enquanto bloco econômico, possui a capacidade para **atrair oportunidades enquanto um mercado unificado**, ressaltando sua relevância atual, inclusive no ramo da tecnologia,[26] e sendo seu mercado digital um dos que mais cresce no mundo.[27]

A título exemplificativo, a ASEAN implementou políticas relevantes nos últimos anos, incluindo: AEC *Blueprint 2025*, *Masterplan on* ASEAN *Connectivity 2025* e e-ASEAN *Framework*

---

[22] ASEAN. *The Founding of ASEAN*. Disponível em: https://asean.org/about-asean/the-founding-of-asean/. Acesso em: 19.05.2022.

[23] Ibid.

[24] ASEAN. *Significance of the ASEAN Charter*. Disponível em: https://asean.org/about-asean/asean-charter/. Acesso em: 19.05.2022.

[25] GAN, Thio Tse. Deloitte: *Data and privacy protection in ASEAN – what does it mean for businesses in the region*. p. 4. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf. Acesso em: 19.05.2022.

[26] Ibid.

[27] World Economic Forum. Digital ASEAN. Disponível em: https://www.weforum.org/projects/digital-asean. Acesso em: 19.05.2022.

Agreement, todos com o objetivo de endereçar as questões envolvidas na tecnologia e conectividade de seus países-membros. Especificamente sobre proteção de dados, em 2016, **a ASEAN implementou o ASEAN *Framework on Personal Data Protection***, um documento que reconhece importância da proteção de dados, inclusive para a promoção e crescimento de relações comerciais e fluxo de informação entre países-membros da ASEAN em um contexto de economia digital.[28]

Nesse sentido, é importante compreender que, ainda que o ASEAN *Framework on Personal Data Protection* tenha como seu objetivo fortalecer a proteção de dados como um tema de relevo no âmbito da ASEAN, **não se trata propriamente de uma lei ou de regulação a respeito do tema**. O *Framework* em questão, portanto, funciona mais como um registro a respeito das **intenções** dos países-membros da ASEAN em torno da proteção de dados pessoais, sem que constitua ou mesmo crie quaisquer obrigações no nível doméstico ou internacional a esses países-membros. Ou seja, **trata-se de documento não vinculante**.

Ocorre, a partir do *Framework*, o estabelecimento de alguns princípios de proteção de dados pessoais que precisam ser levados em consideração por parte dos países-membros quando da implementação e elaboração de legislações internas, tais como: **(i)** notificação, consentimento e propósito específico (os titulares de dados precisam ser notificados sobre o uso de seus dados pessoais, além de consentirem para tal uso em propósitos apropriados); **(ii)** precisão dos dados pessoais (eles precisam ser adequados, corretos e completos na medida do que for necessário); **(iii)** salvaguardas em termos de segurança da informação (os dados devem estar protegidos de acessos indevidos e outros incidentes); dentre outros aspectos.[29]

Assim, apesar do *Framework* e dos seus pressupostos gerais terem de ser seguidos pelos países-membros da ASEAN, cada um deles pode ter **leis específicas e internas a respeito da**

---

[28] ASEAN. *Framework on Personal Data Protection* aprovado a partir da ASEAN *Telecommunications and Information Technology Ministers Meeting* (TELMIN), ocorrida em 25 de novembro de 2016. Disponível em: https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf. Acesso em: 10.06.2022.

[29] Ibid.

proteção de dados pessoais. Por conseguinte, é uma situação diferente da União Europeia em relação ao GDPR, que é vinculante a todos os países-membros, constituindo um regulamento uniforme no tema. Em todo caso, a legislação interna dos países-membros, quando existente, de fato reflete os princípios estabelecidos por meio do ASEAN *Framework on Personal Data Protection*.[30]

A imagem demonstra a situação, em março de 2021, das leis em proteção de dados na ASEAN:

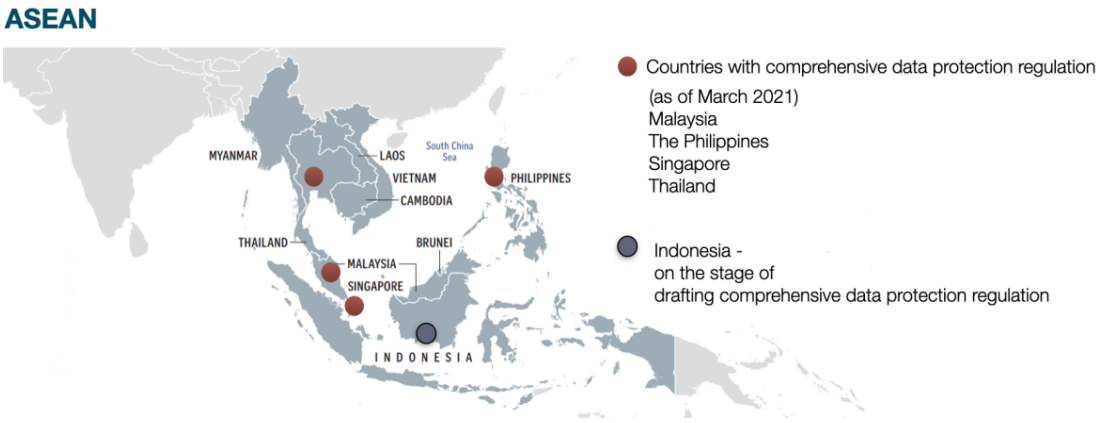


Imagem 1: *Status* das legislações em proteção de dados pessoais nos diversos países-membros da ASEAN[31]

A diferença de níveis de implementação de leis a respeito de proteção de dados dentre os países que compõem o bloco foi até mesmo reconhecida durante a **ASEAN *Telecommunications And Information Technology Ministers Meeting*** (TELMIN), instância da ASEAN hoje chamada **ASEAN *Digital Ministers Meeting*** (ADGMIN). Trata-se de um encontro anual dos ministros das pastas de telecomunicações e tecnologia da informação de todos os países-membros da ASEAN. Assim, no

[30] KHUMON, Prapanpong. Overview of the Data and Privacy Protection in the ASEAN region, presented at the U.S. – Thailand Cybersecurity and Data Protection Standards Workshop. Disponível em: https://share.ansi.org/Shared%20Documents/U.S.-Thailand%20Cybersecurity%20and%20Data%20Protection%20Standards%20Workshop/Overview%20of%20Data%20and%20Privacy%20Protection%20in%20ASEAN,%20Office%20of%20Personal%20Data%20Protection%20Committee.pdf. Acesso em: 25.06.2022.

[31] KHUMON, Prapanpong. Overview of the Data and Privacy Protection in the ASEAN region, presented at the U.S. – Thailand Cybersecurity and Data Protection Standards Workshop. Disponível em: https://share.ansi.org/Shared%20Documents/U.S.-Thailand%20Cybersecurity%20and%20Data%20Protection%20Standards%20Workshop/Overview%20of%20Data%20and%20Privacy%20Protection%20in%20ASEAN,%20Office%20of%20Personal%20Data%20Protection%20Committee.pdf. Acesso em: 25.06.2022.

encontro em que foi aprovado o ASEAN *Framework on Personal Data Protection*, afirmou-se que:

> ***Implementation***
>
> *7.* ***Recognising the different levels of development of the Participants, a Participant may delay the application of this Framework until such time that it is ready to implement it*** *by informing the other Participants in writing.* (grifos nossos)

Por esse motivo, a situação jurídica quanto às transferências internacionais de dados nos países-membros da ASEAN não é harmônica. Especificamente nos que possuem regulação em proteção de dados pessoais, o *status* do tema é o seguinte:

Country	Regulation	Cross-border data transfer grounds	Regulator
Malaysia	Comprehensive	Adequacy protection level of destination country, consent, contracts, appropriate safeguards, vital interests.	Ministry of information, culture, and communication (MIC)
Philippines	Comprehensive	Accountability is placed to a data controller to ensure contracts or other means that provide a comparable protection level.	National privacy commission (NPC)
Singapore	Comprehensive	Comparable protection level of destination country, consent, contracts, binding corporate rules (BCRs)	Personal data protection commission (PDPC)
Thailand	Comprehensive	Adequacy protection level of destination country, consent, contracts, legal obligation, important public task, vital interests.	Office of Personal Data Protection Committee
Indonesia	Sectoral (but now drafting comprehensive law)	Report to regulator - Banking sector, report to Bank of Indonesia - MOCI	Ministry of communication and informatics (MOCI)

Common grounds: Contracts for cross-border data transfers

Imagem 2: Regulação a respeito de transferências internacionais de dados nos países-membros da ASEAN que possuem leis de proteção de dados estabelecidas ou incipientes[32]

Ademais, além do ASEAN *Framework on Personal Data Protection,* a ASEAN juntou esforços para consolidar outras medidas que auxiliassem nas transferências de dados pessoais entre os países do grupo, o que originou os ***Cross Border Data Flows Mechanisms*** **da ASEAN**, divididos: na **(i)** ASEAN *Certification*; e nas **(ii)** ASEAN *Model Contractual Clauses* (as

[32] KHUMON, Prapanpong. Overview of the Data and Privacy Protection in the ASEAN region, presented at the U.S. – Thailand Cybersecurity and Data Protection Standards Workshop. Disponível em: https://share.ansi.org/Shared%20Documents/U.S.-Thailand%20Cybersecurity%20and%20Data%20Protection%20Standards%20Workshop/Overview%20of%20Data%20and%20Privacy%20Protection%20in%20ASEAN,%20Office%20of%20Personal%20Data%20Protection%20Committee.pdf. Acesso em: 25.06.2022.

"MCCs da ASEAN"), as quais constituem o foco da presente análise, aprovadas em sua versão final por meio do **ASEAN *Digital Senior Officials' Meeting*** (ADGSOM).[33]

2.3.2. As cláusulas, sua aplicação e dificuldades

As MCCs da ASEAN, que possuem um formato semelhante às CPCs que são adotadas na União Europeia e no Reino Unido, foram aprovadas em 22 de janeiro de 2021, junto à aprovação do ASEAN *Data Management Framework* ("ASEAN DMF"). As iniciativas foram elaboradas pelo *Working Group on Digital Data Governance* da ASEAN, liderado por Singapura.[34] Enquanto o ASEAN DMF serve como um instrumento a fim de auxiliar as empresas e negócios a estabelecerem um sistema de governança e manejo de dados (inclusive por meio de estruturas de governança e implementação de salvaguardas aos tratamentos de dados pessoais), as MCCs da ASEAN são as CPCs e condições gerais que podem ser implementadas no âmbito de acordos entre empresas que permitam a transferência internacional de dados.

O pressuposto é que as MCCs da ASEAN reduzam os custos de negociação e *compliance*, além de economizar o tempo envolvido na elaboração de contratos, especialmente para as Pequenas e Médias Empresas ("PMEs"), garantindo a proteção dos dados pessoais envolvidos.[35] As MCCs da ASEAN, por sua vez, baseiam-se no ASEAN *Framework on Personal Data Protection*, porém, há uma diferença central entre o seu modelo e o adotado na União Europeia e no Reino Unido, tendo em vista que a sua adoção é **opcional**.[36] Isso significa que as empresas

[33] World Economic Forum. Digital ASEAN. Disponível em: https://www.weforum.org/projects/digital-asean. Acesso em: 19.05.2022.

[34] Personal Data Protection Commission of Singapore (PDPC). *Data Management Framework and Model Contractual Clauses on Cross Border Data Flows*. Disponível em: https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows. Acesso em: 10.06.2022.

[35] Ibid.

[36] ASEAN. *Framework on Personal Data Protection* aprovado a partir da ASEAN *Telecommunications and Information Technology Ministers Meeting* (TELMIN), ocorrida em 25 de novembro de 2016. Disponível em: https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf. Acesso em: 10.06.2022.

sujeitas às leis de proteção de dados aplicáveis aos países-membros da ASEAN ou as que façam parte de países da ASEAN que ainda não possuem tais legislações podem continuar a utilizar outros instrumentos para transferências internacionais de dados, o que inclui cláusulas que tenham sido elaboradas internamente, sem a necessidade de modificar os modelos já adotados.[37] Ainda assim, o uso das MCCs é incentivado por parte da ASEAN a fim de cumprir com o panorama de proteção de dados na região e tornar sua aplicação mais harmônica. Nesse sentido:

> ***Parties are also free to use any other valid data transfer mechanisms recognised within ASEAN**, if or when they are available or relevant to AMS. ASEAN recognises that these mechanisms include, but are not limited to, self-assessment that transfer of data overseas shall be protected to a comparable level of protection, consent, codes of conduct, binding corporate rules, certifications, such as ISO series relating to security and privacy techniques, APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems, or other legally enforceable mechanisms. **Companies have the flexibility to choose the most appropriate personal data protection or privacy-enhancing data transfer mechanism for a particular context**.*[38] (grifos nossos)

Além disso, as MCCs da ASEAN foram pensadas, de forma inicial, no contexto das transferências internacionais entre os próprios países-membros da ASEAN, sendo possível sua adaptação para transferências internacionais a outros países, especialmente aqueles que adotem o APEC *Privacy Framework*[39] ou OECD *Privacy Guidelines*.[40] Trata-se de formato que difere de forma significativa das CPCs previstas no âmbito da União Europeia e do Reino Unido, uma vez que o objetivo dessas, conforme estabelecido acima, é serem de aplicação obrigatória para as transferências internacionais de dados que

---

[37] Personal Data Protection Commission of Singapore (PDPC). *Guidance for Use of ASEAN Model Contractual Clauses for Cross Border Data Flows in Singapore*. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.ashx?la=en. Acesso em: 10.06.2022.

[38] ASEAN. *Model Contractual Clauses for Cross Border Data Flows* (MCCs). Disponível em: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf. Acesso em: 26.06.2022.

[39] APEC *Privacy Framework*. Disponível em: https://www.apec.org/docs/default-source/publications/2005/12/apec-privacy-framework/05_ecsg_privacyframework.pdf?sfvrsn=d3de361d_1. Acesso em: 15.06.2022.

[40] OECD *Privacy Guidelines*. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 15.06.2022.

envolvam os demais países que não tenham níveis de adequação reconhecidos a partir de decisões das autoridades responsáveis, sendo as CPCs um dos mecanismos possíveis a fim de tornar válidas as transferências em questão.

Nesse sentido, destaca-se que o próprio texto das MCCs afirma que:

> *Recognising the different levels of development of AMS, private sector parties in AMS* ***may voluntarily adopt the MCCs****, in the transfer of data to other parties in other AMS. While the MCCs are primarily designed for intra-ASEAN flow of personal data, parties* ***may adapt these clauses with appropriate modifications at their discretion for transfers between businesses intra-country in AMS, or transfers to non-AMS*** (….).[41]

Ou seja, há um grau considerável de flexibilidade em relação ao uso das MCCs da ASEAN quando comparado ao cenário da União Europeia e Reino Unido, nos quais há a obrigatoriedade de uso das CPCs, caso elas sejam o mecanismo para transferência internacional de dados adotado por parte das empresas em questão. Isso se soma ao fato de que as partes **podem alterar, de modo relativamente simplificado, as MCCs**, desde que elas se mantenham em conformidade com os princípios de proteção de dados estabelecidos por meio do ASEAN *Framework on Personal Data Protection* ou conforme os requisitos das leis nacionais dos países-membros da ASEAN, variando de acordo com as legislações aplicáveis ao caso específico sob análise.[42] Também é possível que as partes adicionem cláusulas às MCCs conforme necessário aos seus modelos negociais ou aos seus arranjos comerciais. Ainda assim, a inclusão de quaisquer disposições não pode contradizer ou anular as obrigações relacionadas à proteção de dados pessoais que estejam estabelecidas a partir das MCCs da ASEAN.[43]

Ou seja, a partir de tais indicações da ASEAN, resta claro a importância de as partes modelarem a aplicação das MCCs da

---

[41] ASEAN. *Model Contractual Clauses for Cross Border Data Flows* (MCCs). Disponível em: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf. Acesso em: 20.06.2022.

[42] Personal Data Protection Commission of Singapore (PDPC). *Guidance for Use of ASEAN Model Contractual Clauses for Cross Border Data Flows in Singapore*. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.ashx?la=en. Acesso em: 10.06.2022.

[43] Ibid.

ASEAN às especificidades das transferências de dados que estejam sob análise, especialmente em razão do contexto delas e dos países para os quais os dados pessoais serão enviados. Isso porque, como afirmado, **as MCCs foram pensadas em conformidade com a lógica aplicável à ASEAN, sendo necessárias adequações caso outros países funcionem como os receptores dos dados pessoais, por exemplo**. Ademais, há de se considerar particularidades das jurisdições envolvidas dentro da própria ASEAN, já que, como foi ressaltado, a proteção de dados pessoais na região não é garantida a partir de um regulamento unificado, tal qual é o caso da União Europeia por meio do GDPR. Assim, ainda que haja princípios no assunto estabelecidos a partir da ASEAN *Framework on Personal Data Protection*, os seus países-membros possuem autonomia para formularem suas próprias legislações no tema.

Um outro ponto que deve ser observado é se existem explicações por parte das autoridades de proteção de dados responsáveis por cada uma das jurisdições da ASEAN a respeito do uso das MCCs ao país-membro que se encontre em análise. Um exemplo é a autoridade de proteção de dados de Singapura, a ***Personal Data Protection Commission of Singapore*** (ou "PDPC"). A PDPC publicou, no dia 22 de janeiro de 2021, o *Guidance for use of ASEAN Model Contractual Clauses for Cross Border Data Flows In Singapore*, que tem como objetivo esclarecer e guiar a aplicação das MCCs envolvendo as transferências em Singapura.[44]-[45] Documento semelhante também foi proposto pela autoridade de proteção de dados das Filipinas, a ***National Privacy Commission***.[46] Por esses motivos,

[44] Personal Data Protection Commission of Singapore (PDPC). *Guidance for Use of ASEAN Model Contractual Clauses for Cross Border Data Flows in Singapore*. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.ashx?la=en. Acesso em: 10.06.2022.

[45] Especificamente de modo a tornar a aplicação das MCCs da ASEAN conforme à legislação de proteção de dados da Singapura, a PDPC orientou agentes de tratamento de dados: **(i)** a especificar a definição de titular de dados a fim de indicar que esses podem ser pessoas vivas ou falecidas, tendo em vista que a lei do país se aplica em ambos os casos; **(ii) a** especificar qual o prazo de notificação caso alguma das partes do contrato sofra um incidente de segurança; **(iii)** a incluir obrigações para a notificação dos titulares afetados pelo incidente de segurança, tendo em vista que esse é um requisito perante a legislação de proteção de dados de Singapura; e **(iv)** que não seria necessário, perante as leis de proteção de dados de Singapura, incluir o *Addendum of Additional Terms* às MCCs da ASEAN.

[46] National Privacy Commission of the Republic of the Philippines. *NPC Advisory No. 2021 – 02. Guidance for the Use of the ASEAN Model Contract Clauses and ASEAN Data Management Framework*. Disponível: https://www.privacy.gov.ph/wp-content/uploads/2021/06/Advisory-ASEAN-MCC-DMF_FINAL-signed.pdf. Acesso em: 25.06.2022.

caso as partes optem por utilizar as MCCs da ASEAN em suas transferências internacionais de dados, **é importante que a implementação das mesmas seja bem pensada e reflita as condições de cada caso**.[47]

As obrigações gerais previstas nas MCCs da ASEAN correspondem àquelas já estabelecidas pela ASEAN *Framework on Personal Data Protection*, as quais incluem: **(i)** existência de licitude e de uma base legal adequada para a coleta, uso e transmissão de dados pessoais; **(ii)** cláusulas sobre coleta, notificação, finalidade, acurácia, segurança da informação, acesso e correção dos dados, transferências, retenção e responsabilização; e **(iii)** notificações de incidentes de segurança que tenham ocorrido.[48] Ademais, as MCCs da ASEAN cobrem basicamente as transferências que se dão entre: **(i)** controlador que exporta dados para operador, que tratará os dados pessoais que foram recebidos em conformidade com as instruções do controlador; e **(ii)** controlador que faz a transferência de dados para outro controlador, que tratará os dados pessoais conforme seus próprios propósitos e finalidades.[49]-[50]

O documento que traz as MCCs aprovadas pela ASEAN possui uma parte introdutória sobre seu uso e aplicação, explicando pontos relevantes às partes que optarem pelas MCCs. As cláusulas em si, por sua vez, são divididas em relação aos dois módulos possíveis, como descrito acima: **(i)** transferência internacional de Controlador para Operador; ou **(ii)** transferência internacional de Controlador para Controlador. Junto a isso, as cláusulas também podem possuir uma indicação a respeito de

---

[47] SUN, Abe; LECK, Andy; BERRY, Arwen; LIM, Ren Jun. ASEAN: Adopting the ASEAN Model Contractual Clauses for cross-border data transfers. Disponível em: https://insightplus.bakermckenzie.com/bm/data-technology/asean-adopting-the-asean-model-contractual-clauses-for-cross-border-data-transfers_1. Acesso em: 25.06.2022.

[48] National Privacy Commission of the Republic of the Philippines. *NPC Advisory No. 2021 – 02. Guidance for the Use of the ASEAN Model Contract Clauses and ASEAN Data Management Framework*. Disponível: https://www.privacy.gov.ph/wp-content/uploads/2021/06/Advisory-ASEAN-MCC-DMF_FINAL-signed.pdf. Acesso em: 25.06.2022.

[49] Ibid.

[50] KHUMON, Prapanpong. Overview of the Data and Privacy Protection in the ASEAN region, presented at the U.S. – Thailand Cybersecurity and Data Protection Standards Workshop. Disponível em: https://share.ansi.org/Shared%20Documents/U.S.-Thailand%20Cybersecurity%20and%20Data%20Protection%20Standards%20Workshop/Overview%20of%20Data%20and%20Privacy%20Protection%20in%20ASEAN,%20Office%20of%20Personal%20Data%20Protection%20Committee.pdf. Acesso em: 25.06.2022.

serem ou não opcionais, sendo que as opcionais não precisam ser implementadas pelas partes.[51]

O conteúdo geral das cláusulas sobre proteção de dados pessoais versa sobre o seguinte, sendo que tais disposições podem variar em conformidade com os módulos das MCCs:[52]

- **Definições aplicáveis às MCCs:** como conceitos de incidente de segurança, importador e exportador de dados, além de outros;
- **Obrigações do exportador de dados:** que incluem observar as leis de proteção de dados que sejam aplicáveis; adotar as medidas técnicas e organizacionais para garantir que os dados transferidos estejam protegidos; e responder a requisições das autoridades e dos titulares de dados;
- **Obrigações do importador de dados:** como seguir as instruções lícitas do controlador e não transferir os dados para outra parte sem a autorização do Controlador, caso se trate de Operador de dados; além de adotar medidas técnicas e organizacionais a fim de que os dados recebidos estejam protegidos e informar sobre incidentes de segurança, caso se trate tanto de importador que é Operador quanto de Controlador.

Assim, ao que tudo indica, as MCCs não seriam tão adequadas para fins de transferências entre operadores de dados ou entre um operador de dados e um controlador, por exemplo. Trata-se de aspecto que pode dificultar a implementação das MCCs em situações práticas que envolvem transferências internacionais, possivelmente reduzindo a proteção dos titulares nos casos que não estejam abarcados por meio dos módulos atuais das MCCs da ASEAN. Junto a esse ponto, é importante destacar que, como visto, as MCCs da ASEAN se baseiam no ASEAN *Framework on Personal Data Protection*, o que pode gerar algumas contradições com as leis locais dos países-membros da ASEAN, inclusive no sentido de estabelecer obrigações por meio das MCCs que sejam **mais protetivas e restritivas** que as próprias legislações domésticas. Isso pode gerar certo grau de dificuldade na aplicação das MCCs. Um exemplo disso é o fato

[51] ASEAN. *Model Contractual Clauses for Cross Border Data Flows* (MCCs). Disponível em: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf. Acesso em: 26.06.2022.

[52] Ibid.

de que, na cláusula 2.1. das MCCs, estabelece-se a necessidade de obtenção de consentimento para a transferência ocorrer – o que não necessariamente é obrigação prevista em leis de proteção de dados locais na ASEAN.

Ademais, a seção chamada *Additional Terms for Individual Remedies*, das MCCs, prevê que os titulares de dados podem tomar algumas medidas contra as partes a fim de garantir que certas disposições das MCCs sejam cumpridas – ponto que também pode gerar resistência das partes em utilizar as MCCs em seus contratos. Ou seja, ainda que as MCCs sejam um avanço em termos de transferências internacionais de dados na ASEAN, é bem provável que elas precisem de dadas modificações para serem utilizadas em diversos cenários.[53]

2.4. Nova Zelândia

2.4.1. Panorama normativo

A proteção de dados pessoais é regulamentada na Nova Zelândia a partir do *Public Act* 2020 nº 31 (conhecido como ***Privacy Act 2020***).[54] Trata-se de legislação que estabelece regras quanto a como entidades governamentais e demais organizações devem lidar com informações e quais os direitos dos indivíduos quando do uso de suas informações pessoais,[55] como direito de acesso e o de correção.[56] Para fins da aplicação do *Privacy Act 2020*, informações pessoais são aquelas que se referem a um indivíduo identificável, como as que se referem a características da pessoa (e.g. cor do olho) e demais informações que possam a identificar (e.g. nome completo). Não há a necessidade de que a informação

[53] LIU, Anthony; CHAN, Jacqueline; PARSONS, Mark. *International: Comparing contractual clauses - ASEAN MCCs v. EU SCCs*. Disponível em: https://www.dataguidance.com/opinion/international-comparing-contractual-clauses-asean. Acesso em: 26.06.2022.

[54] O *Privacy Act* 2020 substitui e complementa as disposições do *Public Act* 1993 nº 28 (ou *Privacy Act* 1993), que era o responsável por regular o tema de proteção de dados anteriormente na Nova Zelândia.

[55]

[56] Nova Zelândia. *Data privacy*. Disponível em: https://www.data.govt.nz/toolkit/privacy-and-security/data-privacy/. Acesso em: 26.06.2022.

identifique diretamente o indivíduo, bastando que, a partir dela, ele seja **identificável**.[57] Além desses pontos, é interessante também destacar que, desde o ano de 2012, a Nova Zelândia é considerada como um país que oferece um nível de proteção de dados compatível com o da União Europeia, tendo recebido sua decisão de adequação por parte da Comissão Europeia.[58]-[59]

Além disso, o *Privacy Act 2020* prevê treze princípios que precisam ser observados por aqueles que utilizem informações pessoais, são eles: **(i)** deve haver propósito para coleta de informações pessoais, que só podem ser coletadas para finalidades lícitas e caso a coleta seja necessária; **(ii)** de forma geral, as informações pessoais devem ser coletadas a partir de um contato direto com o indivíduo, a menos que uma exceção do *Privacy Act 2020* seja aplicável (e.g.: se a informação for publicamente acessível); **(iii)** devem ser dadas informações adequadas aos indivíduos cujas informações pessoais serão coletadas (e.g.: a finalidade da coleta e as entidades e organizações que irão utilizar as informações, dentre outros); **(iv)** a coleta de informações precisa ocorrer por meios lícitos e que não interfiram na privacidade dos indivíduos; **(v)** é necessário implementar as medidas adequadas para garantir a segurança e integridade das informações; **(vi)** o indivíduo tem direito à confirmação sobre se as entidades ou organizações detêm as suas informações e o direito a acessá-las; **(vii)** o indivíduo tem direito a corrigir suas informações pessoais, além de as entidades ou organizações terem o dever de prezar pela precisão das informações utilizadas; **(viii)** quem utilizar as informações pessoais deve se certificar de que sejam precisas, relevantes, atualizadas e completas; **(ix)** as informações pessoais não podem ser retidas por um tempo além do que o necessário para o cumprimento dos propósitos de seu uso; **(x)** devem ser observados os limites para o uso de informações pessoais, sendo que elas devem ser utilizadas apenas para os

[57] Nova Zelândia. *Data privacy*. Disponível em: https://www.data.govt.nz/toolkit/privacy-and-security/data-privacy/. Acesso em: 26.06.2022.

[58] Comissão Europeia. 2013/65/EU: *Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand*. Disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013D0065. Acesso em: 26.06.2022.

[59] A decisão de adequação da Comissão Europeia foi concedida à Nova Zelândia tendo em vista o *Privacy Act* de 1993. Houve, portanto, dúvidas sobre se a decisão de adequação seria mantida em face das modificações trazidas por meio do *Privacy Act* de 2020. Até o momento não houve sinalização de que essa seria revogada, continuando válida.

propósitos para os quais foram coletadas, a menos que alguma exceção do *Privacy Act 2020* seja aplicável (e.g.: se a informação for utilizada sem identificar o indivíduo em questão); **(xi)** de forma geral, a entidade ou organização não pode divulgar as informações pessoais, a menos que alguma exceção do *Privacy Act 2020* seja aplicável (e.g.: se o indivíduo permitir que a divulgação ocorra); **(xii)** pode haver a transferência internacional de informações, caso as obrigações postas no *Privacy Act 2020* sejam observadas; e, por fim, **(xiii)** entidades e organizações podem atribuir um identificador único aos indivíduos se necessário, se as disposições do *Privacy Act 2020* forem observadas.[60]

Junto aos princípios em proteção de dados, o *Privacy Act 2020* traz disposições específicas sobre segurança da informação e incidentes de segurança, além de descrever quais os papéis a serem exercidos pela *Privacy Commissioner* da Nova Zelândia, que é a autoridade de proteção de dados do país. A possibilidade de transferência internacional de dados, por sua vez, pauta-se, de modo central, no chamado *Information Privacy Principle 12* ("IPP 12"), disposto acima. Portanto, para os fins do *Privacy Act 2020*, as transferências internacionais de dados podem ocorrer caso suas regras e obrigações sigam cumpridas.

3. Convergências e divergências entre os modelos apresentados

3.1. Comparando os modelos:

Os modelos aqui listado apresentam convergências e divergências, como se nota na tabela comparativa a seguir:

[60] Nova Zelândia. *Public Act* 2020 nº 31 (*Privacy Act* 2020), Parte 3, *Information privacy principles and codes of practice*. Disponível em: https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23331. Acesso em: 26.06.2022.

Tabela 1 - Normatização de Transferência Internacional de dados

País/ Organismo	Norma	Vinculação	Previsão
Parlamento Europeu	GDPR Regulamento Geral de Proteção de Dados da União Europeia	Vinculante	O modelo europeu de transferências internacionais de dados pessoais comporta gradações com relação à viabilidade do envio de dados. Em um primeiro "degrau", tem-se as decisões de adequação, em que se reconhece um nível equivalente de proteção de dados ao país remetente. E, subsidiariamente, existem outras formas que expressem garantias no cumprimento à proteção de dados, tais como as mencionadas CPCs. Estas, nada mais são do que instrumentos jurídicos vinculativos a agentes de tratamento ao operar as transferências de dados fora do Espaço Econômico Europeu (EEE).
Reino Unido	UK GDPR	Vinculante	As transferências internacionais de dados podem ser realizadas a partir de: (i) instrumentos juridicamente vinculantes e com força executiva acordados entre autoridades públicas ou outros órgãos públicos; (ii) regras vinculativas aplicáveis a empresas (denominadas binding corporate rules, em inglês); (iii) CPCs a serem especificadas pelo Secretário de Estado do Reino Unido; (iv) CPCs a serem especificadas pela ICO; (v) código de conduta acompanhado de compromissos vinculativos e com força executiva do controlador e do operador que estejam em um país terceiro para que apliquem as salvaguardas apropriadas, inclusive aquelas referentes a direitos dos titulares; ou (vi) procedimento de certificação junto aos compromissos vinculantes e com força executiva do controlador e operador no país terceiro em que garantam a aplicação das salvaguardas apropriadas, inclusive aquelas referentes a direitos dos titulares.[61] Portanto, o caso analisado aqui se refere ao item (iv) acima, disposto no artigo 46 (2) (d) da UK GDPR, qual seja, as CPCs especificadas pela ICO.[62]
Nova Zelândia	Privacy Act 2020	Vinculante	pode haver a transferência internacional de informações, caso as obrigações postas no Privacy Act 2020 sejam observadas

[61] Information Commissioner's Office. *International transfers after the UK exit from the EU Implementation Period*. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/. Acesso em: 01.05.2022.

[62] Information Commissioner's Office. *Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018*. Version A1.0. p. 32. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. Acesso em: 01.05.2022.

Associação das Nações do Sudeste Asiático (conhecida como "ASEAN")	ASEAN Data Management Framework ("ASEAN DMF")	Não vinculante	Cross Border Data Flows Mechanisms da ASEAN, divididos: na (i) ASEAN Certification; e nas (ii) ASEAN Model Contractual Clauses (as "MCCs da ASEAN"), as quais constituem o foco da presente análise, aprovadas em sua versão final por meio do ASEAN Digital Senior Officials' Meeting (ADGSOM). As MCCs da ASEAN, que possuem um formato semelhante às cláusulas-padrão contratuais que são adotadas na União Europeia e no Reino Unido, foram aprovadas em 22 de janeiro de 2021, junto à aprovação do ASEAN Data Management Framework ("ASEAN DMF"). As iniciativas foram elaboradas pelo Working Group on Digital Data Governance da ASEAN, liderado por Singapura.[63] Enquanto o ASEAN DMF serve como um instrumento a fim de auxiliar as empresas e negócios a estabelecerem um sistema de governança e manejo de dados (inclusive por meio de estruturas de governança e implementação de salvaguardas aos tratamentos de dados pessoais), as MCCs da ASEAN são as cláusulas contratuais padrão e condições gerais que podem ser implementadas no âmbito de acordos entre empresas que permitam a transferência internacional de dados.

Fonte: elaborada pelo ITS Rio.

Em resumo, a União Europeia traz modelo que vincula os países integrantes do bloco europeu e comporta gradações com relação à viabilidade do envio de dados. Em um primeiro "degrau", tem-se as decisões de adequação, em que se reconhece um nível equivalente de proteção de dados ao país remetente. E, subsidiariamente, existem outras formas que expressem garantias no cumprimento à proteção de dados, tais como as mencionadas CPCs. Estas, nada mais são do que instrumentos jurídicos vinculativos a agentes de tratamento ao operar as transferências de dados fora do Espaço Econômico Europeu (EEE).

Já o modelo adotado pela Nova Zelândia além de oferecer uma estrutura rígida, com princípios e fundamentos mínimos para que a serem assegurados à proteção de dados pessoais, a Autoridade Nacional de Proteção de Dados neozelandesa (OPC) oferece uma opção *built to suit*, em que após preencher um questionário com os aspectos particulares à realidade do agente de tratamento, oferece-se um modelo próprio, mais bem estruturado às necessidades individuais.

[63] Personal Data Protection Commission of Singapore (PDPC). *Data Management Framework and Model Contractual Clauses on Cross Border Data Flows*. Disponível em: https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows. Acesso em: 10.06.2022.

A Associação das Nações do Sudeste Asiático (conhecida como "ASEAN") apresenta modelo mais flexível, tendo em vista que as diretrizes apresentadas no **ASEAN *Data Management*** servem de guia para orientação dos países integrantes e não é vinculante. A partir, entretanto do ***Cross Border Data Flows Mechanisms* da ASEAN**, divididos: na **(i)** ASEAN *Certification*; e nas **(ii)** ASEAN *Model Contractual Clauses* (as "MCCs da ASEAN"), as quais constituem o foco da presente análise, aprovadas em sua versão final por meio do **ASEAN *Digital Senior Officials' Meeting*** (ADGSOM). As MCCs da ASEAN, que possuem um formato semelhante às cláusulas contratuais padrão que são adotadas na União Europeia e no Reino Unido, foram aprovadas em 22 de janeiro de 2021, junto à aprovação do ASEAN *Data Management Framework* ("ASEAN DMF"). As iniciativas foram elaboradas pelo *Working Group on Digital Data Governance* da ASEAN, liderado por Singapura.[64] Enquanto o ASEAN DMF serve como um instrumento a fim de auxiliar as empresas e negócios a estabelecerem um sistema de governança e manejo de dados (inclusive por meio de estruturas de governança e implementação de salvaguardas aos tratamentos de dados pessoais), as MCCs da ASEAN são as cláusulas-padrão contratuais e condições gerais que podem ser implementadas no âmbito de acordos entre empresas que permitam a transferência internacional de dados.

3.2 Comparando as cláusulas:

Além dos diferentes modelos, é importante comprar as cláusulas que visam garantir minimamente a proteção de dados quando da transferência internacional de dados. Abaixo comparam-se as garantias mínimas previstas no GDPR, verificando-se quais delas estão ou não presentes em cada país para compreender o que é mínimo comum e no que cada um diverge.

[64] Personal Data Protection Commission of Singapore (PDPC). *Data Management Framework and Model Contractual Clauses on Cross Border Data Flows*. Disponível em: https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows. Acesso em: 10.06.2022.

Tabela 2 - Comparativo de cláusulas mínimas para transferência internacional de dados

Aspecto	União Europeia	ASEAN	Nova Zelândia
De quantos itens são compostos os modelos regulatórios?	18 cláusulas, um apêndice e dois anexos.	nove cláusulas e um termo adicional.	16 itens.
Há módulos específicos para diferentes arranjos nas relações entre agentes de tratamento?	Sim, há quatro módulos: 1- Controlador-Controlador; 2- Controlador-Operador; 3- Operador-Operador e; 4- Operador-Controlador.	Sim, há dois módulos: 1- Controlador-Operador e; 2 - Controlador-Controlador.	Não.
No âmbito do envio transfronteiriço de dados, há prévia definição de qual lei local é hierarquicamente superior?	Não, apenas estabelece-se que independentemente de previsões de leis locais estrangeiras, os agentes devem garantir o compliance com as determinações das cláusulas.	Não, mas caso a lei local entre em contradição com as cláusulas, as cláusulas prevalecem.	Não.
As regras voltadas à Segurança da Informação obedecem a algum padrão?	Deve-se adotar todas as medidas técnicas e organizacionais. Recomenda-se ainda a encriptação e a pseudoanonimização.	Sugere-se à adequação a normas da ISO relacionadas a medidas de segurança e privacidade.	Recomenda-se a adoção das melhores práticas, com padrões geralmente esperados internacionalmente.
Há regras voltadas à comunicação em caso de incidentes de segurança?	Sim, deve-se adotar preventivas a incidentes, inclusive para mitigar seus efeitos. Em havendo riscos às liberdades dos titulares de dados, eventual incidente provocado pelo importador de dados deve ser procedido à comunicação para o exportador de dados e à Autoridade Nacional competente.	Sim, eventual incidente provocado pelo importador de dados deve ser procedido à comunicação para o exportador de dados e à Autoridade Nacional competente.	Sim, a parte responsável deve notificar os titulares afetados. A notificação poderá ser ser uma comunicação pública, caso venha envolver muitos titulares de dados; A notificação poderá ser retardada, caso implique em riscos à segurança da informação ou ainda, quando a lei local não exigir notificações ou comunicações públicas.

Há obrigações específicas quanto ao envio de dados pessoais sensíveis?	Sim, devem ser adotadas salvaguardas adicionais, tais como limitações no acesso aos dados, medidas de segurança como pseudoanonimização e outras possíveis restrições.	Não.	Sim, sugere-se a adoção de precauções adicionais.
Há interfaces nos modelos regulatórios que auxiliam o agente a construir as cláusulas passo a passo?	Não.	Não.	Sim, é possível estruturar as próprias cláusulas sob medida dentro do site da Autoridade Nacional de Proteção de Dados.

Fonte: elaborada pelo ITS Rio.

Nota-se que no geral existem cláusulas mínimas comuns a serem respeitadas quando da transferência internacional, em especial no que tange a limitação de finalidade, exatidão e minimização, limitação da conservação e segurança no tratamento.

Em recente colaboração entre a ASEAN e a Comissão Europeia, foi elaborado um Guia[65] voltado à compreensão das diferentes nuances entre as CPCs previstas pelo bloco asiático e pelo bloco europeu. O guia evidencia, essencialmente, as regras aplicáveis aos diferentes arranjos de relações entre a exportação e importação de dados pessoais, na qualidade de agentes Controladores e Operadores. Incluem-se, nesse sentido, as respectivas obrigações, medidas de salvaguardas, direitos dos Titulares de Dados, *compliance*, resolução de disputas e encerramento de atividades de compartilhamento transfronteiriço.

[65] ASEAN; EUROPEAN COMMISSION. *Joint Guide to ASEAN Model Contractual Clauses and EU Standard Contractual Clauses*. Disponível em: <https://commission.europa.eu/system/files/2023-05/%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf>. Acesso em: 31.07.2023.

4. Perspectivas para o cenário brasileiro

No Brasil, a LGPD traz as normativas sobre transferência internacional nos artigos 33 a 35. O artigo 33 enumera as hipóteses legais de transferência internacional:

> 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;

Nota-se que as disposições da Lei nº 13.709/18 assimilam-se ao regime normativo do tema previsto no GPDR. Isso é, a legalidade das transferências internacionais em princípio a partir de prévia autorização da Autoridade competente, por meio do reconhecimento de níveis de equivalência entre o país emitente e receptor dos dados pessoais. Não havendo compatibilidade, a lei prevê mecanismos técnicos que assegurem um nível adequado de proteção além-fronteiras. Alguns instrumentos contratuais são relevantes, nesse aspecto, pois integram e assessoram as relações ocorridas entre agentes de tratamento interessados em enviar ou receber as informações pessoais internacionalmente.

A exemplo das CPCs e das NCGs, destinadas à verificação de conformidade no tratamento de dados pessoais, atores privados passam a promover no âmbito de suas atividades internas, a inserção de comandos normativos que regulam a forma de tratamento de dados pessoais, em consonância com os pressupostos da legislação de seus respectivos países de origem das operações.

Sob um viés particularmente mais liberal e consequentemente flexível, a sistemática de cláusulas contratuais mais maleáveis, torna a proteção de dados menos efetiva, dando azo a potenciais descumprimentos à privacidade dos titulares de dados. Noutro giro, em uma ótica mais paternalista e resultantemente mais rígida, comandos muito limitados às negociações privadas, impõe ônus capazes de refrear as atividades entre particulares, levando a significativa diminuição do fluxo de informações.

Nesse sentido, entende-se que a perspectiva em torno da viabilidade dos fluxos transfronteiriços de dados pessoais deve ser estimulada, por meio de uma maior confiança e alinhamento entre diferentes países.

Isso porque, posições mais conservadoras na construção de instrumentos contratuais tendem a levar a maior isolamento e dificuldades no estabelecimento de relações comerciais, projetando consequências que levam a uma "localização forçada" de dados pessoais. Ainda assim, uma expressiva relativização de instrumentos contratuais tende a dificultar o reconhecimento de países como nível equivalente de proteção em relação a outros países de proteção de dados mais amadurecida;

No que tange às CPCs, um equilíbrio entre modelos mais rígidos e flexíveis parece coerente sob o panorama das transferências internacionais, especialmente pautado em um núcleo duro comum e irretratável de princípios e garantias fundamentais de proteção de dados, atrelado à disponibilização de cláusulas adaptáveis às diferentes realidades de atores privados;

Com relação às NCGs, por oferecerem formas mais fáceis de adaptação a grandes grupos e conglomerados econômicos, deveriam ser construídos sob condições que possibilitem a inclusão de outros agentes como pequenas e médias empresas, tornando o ecossistema de concorrência e inovação mais favorável.

Isso é, eventual regulamentação excessiva, nesse viés, parece resultar em dois cenários possíveis. De um lado, pode-se excluir a efetiva participação de pequenos e médios atores que não possuam condições em adequar-se às altas exigências estabelecidas. E, por outro lado, como as condições

acentuadas são capazes de deflagrar um descumprimento generalizado, onde o fluxo transfronteiriço, diga-se, irrefreável, encontrará outras formas de seguir seu curso.

Conclusões

Este documento objetivou trazer panorama atual de como alguns ordenamentos jurídicos ao redor do mundo lidam no que tange às cláusulas-padrão contratuais e finaliza sugerindo, com base nas diferentes perspectivas apresentadas, horizontes de adequação para o Brasil.

A partir das diversas previsões aqui apresentadas, conclui-se que para o melhor fluxo de dados, aponta-se à perspectiva de construir parâmetros mínimos à proteção de dados pessoais a ser observada pelas empresas, prevendo de forma clara e objetiva os limites da responsabilização dos agentes de tratamento da cadeia de tratamento de dados, assegurando os direitos, liberdades e garantias dos titulares de dados.

Fora desse contexto, as CPCs são os mecanismos mais utilizados. Ainda que em alguns casos possa ser questionada a sua efetividade, deve ser compreendido que a teia estruturante do comércio internacional, e de fato a maior parte das transações que se direcionam a fluxos transfronteiriços de dados, baseia-se em arranjos contratuais.

Nesse sentido, é importante que este instrumento seja de fácil uso e com o mínimo necessário de exigências e demais burocracias. Quanto maiores as existências de burocracias, maiores são os custos e, consequentemente, mais micro e pequenas empresas podem ficar excluídas dos fluxos, tendendo à concentração dos fluxos somente em empresas maiores, por terem mais capacidades para absorver custos.

Igualmente importa notar que as redes negociais podem ser bastante complexas, logo, é significativo que exista possibilidade de estruturação das CPCs para refletirem essa complexidade, tendo em vista que este modelo parece ser mais apropriado às pequenas e médias empresas, levando em consideração o potencial de flexibilidade prática de adequação às diversas formas de organizações empresariais.

Por outro lado, as NCGs parecem ser mais adequadas às grandes corporações e conglomerados econômicos. Curioso observar que, no contexto europeu, mesmo diante da complexidade do mecanismo e da necessidade de adequação a múltiplos sistemas, ainda existem poucas organizações que utilizem esses sistemas. No entanto, já é notável um salto significativo no seu uso desde a maior flexibilização do mecanismo de chancela pela União Europeia, com a entrada em vigor do GDPR. O que tende a indicar uma demanda que pode vir a chegar ao país.

Assim, os pressupostos para a edificação da convergência e interoperabilidade devem levar em consideração: (i) a necessidade de convivência harmônica entre diferentes ordenamentos jurídicos por meio da adoção de mecanismos de proteção; (ii) o alcance da proteção em meio ao fluxo transfronteiriço sem necessariamente exigir uma equivalência nos mecanismos específicos de proteção de dados.

Tem-se como consequência a busca por um grau de flexibilidade para se permitir a convivência paralela entre modelos distintos de proteção de dados em nível internacional. A ANPD deve apontar de forma clara quais elementos são primordiais à proteção de dados diante de situações transfronteiriças e quais são acessórios.

Externamente, a cooperação internacional com outras Autoridades de Proteção de Dados é fundamental, assim como a publicização ampla, clara e acessível dos posicionamentos adotados, de modo que as respectivas Autoridades estrangeiras também estabeleçam as diferentes discussões da regulação transfronteiriça de dados frente ao Brasil.

Seria igualmente interessante monitorar continuamente os diferentes foros de discussões da regulação transfronteiriça de dados, posicionando-se de forma notória as propostas de discussões, inclusive submetendo ideais que conversem com as diferentes jurisdições.

Ainda, torna-se importante ter atenção às discussões travadas em tratados de livre comércio, pois, na atualidade, estes instrumentos estão firmando entendimentos do nível de proteção ou abordando a proteção de dados entre países.

A partir desse relatório, nota-se que quaisquer dos modelos

adotados, assegura garantias mínimas de proteção de dados pessoais, comuns às cláusulas exigidas nos países analisados. Nesse sentido, o Brasil pode espelhar-se em um dos modelos apresentados (rígido, flexível ou híbrido) ou criar o seu próprio, desde que asseguradas as garantias fundamentais no que tange a proteção dos dados pessoais no país importador.

Sobre os autores

Celina Bottino é graduada em Direito pela PUC-Rio, mestre em Direitos Humanos pela Universidade de Harvard. Especialista em Direitos Humanos e tecnologia. Foi pesquisadora da Human Rights Watch, em Nova York. Supervisora da Clínica de Direitos Humanos da FGV Direito-Rio. Foi consultora da Clínica de Direitos Humanos de Harvard e pesquisadora do ISER. É associada ao Centro de Defesa dos Direitos da Criança e Adolescentes do Rio de Janeiro. Atualmente, desenvolve pesquisas na área de Direitos Humanos e tecnologia coordenando projetos na área de liberdade de expressão e privacidade. É filiada ao Berkman Klein Center de Harvard e diretora de Projetos do ITS.

Christian Perrone é Pesquisador Fulbright (Universidade de Georgetown, EUA), Doutor (UERJ) em Direito Internacional e Direito Digital; mestre LL.M. -- em Direito Internacional (Universidade de Cambridge, Reino Unido); Diplomado em Direito Internacional dos Direitos Humanos pelo Instituto Universitário Europeu (EUI, Itália). Ex-secretário da Comissão Jurídica Interamericana da OEA e especialista em Direitos Humanos da Comissão Interamericana de Direitos Humanos e da Corte Interamericana de Direitos Humanos. Atualmente, advogado, consultor de Políticas Públicas e head das áreas de Direito & Tecnologia e GovTech no ITS.

Flávia Parra é Advogada Associada no VMCA Advogados e Contingent Worker - Privacy no Meta. É graduada em Direito pela USP.

Mariana Bertolucci é Designer e artista visual, graduada pela Universidade Federal de Mato Grosso do Sul (UFMS). Se motiva por trabalhos que possuam o propósito de transformação, por isso busca desenvolver habilidades estratégicas que possam somar à produção de materiais gráficos. Tem interesse pela interseção entre a tecnologia e educação, além de desenvolver pesquisa nos campos de estudos do marketing e do webdesign. É designer sênior e pesquisadora na área de Mídias do ITS.

Tainá Aguiar Junquilho é Doutora em Direito com ênfase em Inteligência Artificial pela UnB. Foi bolsista da FINATEC no

Projeto de Pesquisa & Desenvolvimento de aprendizado de máquina (machine learning) sobre dados judiciais das repercussões gerais do Supremo Tribunal Federal - STF (Projeto Victor). Advogada e Pesquisadora GovTech do ITS Rio. Vice líder do Grupo de Estudos Observatório em Políticas Públicas (GEOPP UnB). Professora de Direito e Tecnologia do Mestrado IDP e da graduação.

Pedro Gueiros é Mestre em Direito Civil pela PUC-Rio. Ex-bolsista da Fundação Konrad Adenauer. Pesquisador em Direito e Tecnologia do ITS Rio. Advogado Orientador do Núcleo de Prática Jurídica do Ibmec-RJ. Integrante do Núcleo Legalite da PUC-Rio. Graduado em Direito pelo Ibmec-RJ.

Acesse nossas redes

itsrio.org