PROTEÇÃO DE DADOS PESSOAIS NO BRASIL E NO CHILE: UMA ANÁLISE COMPARATIVA SOB A PERSPECTIVA DA DECISÃO DE ADEQUAÇÃO DA COMISSÃO EUROPEIA

Por André Ramiro

RESUMO

Considerando a influência do Regulamento Geral de Proteção de Dados da União Europeia (GDPR) na adequação de legislações de proteção de dados de outros países, o presente trabalho tem como objetivo fazer uma análise comparativa da Lei de Proteção de Dados brasileira e do atual projeto de emenda à Lei de Proteção de Dados chilena sob a perspectiva dos critérios para decisão de adequação de países terceiros previstos pelo Regulamento europeu. Para isso, de início, analisa-se os requisitos necessários para a concessão de uma decisão de adequação pela Comissão Europeia, conforme entendimento do artigo 45 do GDPR e do Grupo de Trabalho do Artigo 29 para Proteção de Dados, estabelecendo-se, em seguida, as seguintes categorias-chave para análise: (1) princípios fundamentais; (2) tratamento de dados sensíveis; (3) decisões automatizadas; (4) autoridade supervisora; (5) e mecanismos legais para proteger os direitos dos titulares de dados. Como resultado, chegou-se a parcial adequação da legislação brasileira e a total adequação do projeto de emenda à Lei de Proteção de Dados chilena, caso esta mantenha a independência da autoridade supervisora. Como conclusão, sugere-se o fortalecimento do sistema de responsabilização e campanhas públicas educativas voltadas para a conscientização sobre a importância da proteção de dados pessoais e da adequação pelas instituições em ambos os países.

INTRODUÇÃO

O Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation ou "GDPR") entrou em vigor em 25 de maio de 2018, trazendo avanços em relação ao marco jurídico anterior, a Diretiva 95/46/CE, como o fortalecimento dos direitos dos titulares de dados e o reforço na responsabilização dos agentes de tratamento de dados. O novo Regulamento europeu trouxe também um grande impacto em todo o mundo, principalmente influenciando outros países na revisão de suas legislações quanto à proteção de dados. O GDPR tornou-se o elemento-chave para essas mudanças, pois seu escopo regulatório atinge relações entre controladores, operadores e titulares de dados além das que abrangem o território da União Europeia. Assim, o não cumprimento dos padrões mínimos introduzidos pelo GDPR afeta as relações comerciais de países que ainda estão pendentes nessa questão (Scott e Cerulus, 2018).

Este é o caso do Brasil e do Chile, uma vez que ambos estão adotando ou revisando as respectivas legislações, a fim de tornar seus modelos jurídicos alinhados com o modelo europeu: o Brasil com a aprovação de sua primeira Lei Geral de Proteção de Dados; e o Chile, atualmente adaptando significativamente sua Lei de Proteção de Dados, que já completa 20 anos em vigor.

No Brasil, por conta do grande atraso na aprovação de uma Lei de Proteção de Dados em comparação com o cenário mundial, bem como pela total ausência de políticas públicas propostas ao tema e a ineficiente aplicação das leis setoriais existentes, a proteção de dados tem sido tratada apenas em casos isolados. Quanto ao Chile, embora tenha sido o primeiro país da América Latina a aprovar uma lei de proteção de dados, poucas atualizações foram feitas na lei ao longo dos anos, além de ainda existirem dificuldades para sua aplicação e para conscientização da importância do tema. Essa situação é refletida pela falta de consciência da população sobre os direitos existentes e pelos mecanismos pouco eficazes para o exercício desses direitos (Molina, 2018).

Assim, a percepção é que, seja no caso do Chile, em que a Lei de Proteção de Dados já existe há duas décadas, ou seja no caso do Brasil, em que só existiam as leis setoriais e pouco eficazes, ambos os países ainda precisavam de um avanço para a adequação do novo cenário de proteção de dados mundial destacado pela GDPR. Resta questionar, porém, se essas mudanças estão de acordo com os requisitos necessários para uma desejável decisão de adequação quanto ao nível de proteção de dados em relação aos critérios estabelecidos pelo modelo europeu.

Assim, este artigo tem como objetivo fazer uma análise comparativa do GDPR com a Lei de Proteção de Dados brasileira e com o atual projeto de emenda à Lei de Proteção de Dados chilena sob a perspectiva dos critérios para decisão de adequação de países terceiros, previstos no artigo 45 do Regulamento. Para isso, de início, analisa-se os requisitos necessários para uma decisão de adequação pela Comissão Europeia, conforme entendimento do artigo 45 do GDPR e do Grupo de Trabalho do Artigo 29 para Proteção de Dados, com o objetivo de se estabelecer as seguintes categorias-chave de análise: (1) princípios fundamentais; (2) tratamento de dados sensíveis; (3) decisões automatizadas; (4) autoridade supervisora; (5) e mecanismos legais para proteger os direitos dos titulares de dados. A partir disso, analisa-se os requisitos de cada uma das categorias citadas, para que se possa fazer um comparativo com a legislação brasileira e chilena, e, por fim, concluir se as mesmas cumprem os critérios estabelecidos para uma decisão de adequação.

1. DOS REQUISITOS NECESSÁRIOS PARA UMA DECISÃO DE ADEQUAÇÃO PELA COMISSÃO EUROPEIA PARA PAÍSES TERCEIROS (ARTIGO 45 DO GDPR)

O capítulo V do Regulamento Geral de Proteção de Dados (GDPR) dispõe sobre os tipos de transferências de dados pessoais para países terceiros ou organizações internacionais e os respectivos critérios. O capítulo apresenta no artigo 45 os critérios para as transferências realizadas com base numa decisão de adequação, dispondo que, para estes casos, as transferências só serão realizadas se o país terceiro tiver um "nível adequado de proteção" a partir de uma decisão da Comissão Europeia. O efeito da decisão concedida é que os dados pessoais podem ser transferidos dos países-membros da União Europeia para um país terceiro sem a necessidade de outras garantias e sem a exigência de uma autorização específica (Article 29 Data Protection Working Party [WP29], 2017). De acordo com o artigo 45, os critérios para avaliar a adequação do nível de proteção de países terceiros devem se basear, de forma geral, no respeito pelos direitos humanos e liberdades fundamentais; na legislação pertinente em vigor; nos direitos dos titulares de dados e nos mecanismos eficazes para que os titulares exerçam seus direitos; numa autoridade supervisora independente para garantir a aplicação da lei; e nos compromissos internacionais assumidos pelo país terceiro.

Para estabelecer orientações mais específicas ao que representa o designado "nível adequado de proteção", o Grupo de Trabalho do Artigo 29 para Proteção de Dados[1], órgão consultivo estabelecido na vigência da Diretiva 95/46/CE, elaborou um documento de referência relativo à adequação, publicado em 28 de novembro de 2017, durante o período de transição para o Regulamento, com o intuito de atualizar as orientações anteriores, na vigência da Diretiva, a respeito da transferência de dados pessoais para países terceiros. Conforme apresentado no documento de referência, a citação ao "nível adequado de proteção" já existia sob a Diretiva 95/46 e o documento anterior do Grupo de Trabalho, datado de 1998, juntamente com a jurisprudência do Tribunal de Justiça da União Europeia no processo Schrems, de 2015, ajudaram na construção interpretativa do conceito (WP29, 2017).

Segundo esse novo documento, a intenção da decisão não é que os países terceiros reproduzam ponto a ponto o Regulamento, mas que estabeleçam alguns requisitos essenciais que irão garantir um padrão mínimo de proteção. O Grupo de Trabalho trata no documento

---

[1] O Grupo de Trabalho do Artigo 29 para Proteção de Dados foi substituído pelo Comitê Europeu para a Proteção de Dados com a entrada em vigor do GDPR.

especificamente dos requisitos para as transferências que são baseadas numa decisão de adequação, destacando, em síntese, duas etapas fundamentais para a análise do nível de proteção: em primeiro lugar, a análise do conteúdo da legislação, e, posteriormente, a análise dos meios destinados a assegurar a efetiva aplicação.

Neste trabalho, como forma de realizar um comparativo dos principais requisitos com as normas brasileira e chilena, e se as mesmas podem indicar um nível de adequação, foram selecionadas cinco categorias-chave. As três primeiras categorias são relativas ao conteúdo da legislação, sendo a primeira os princípios fundamentais, utilizando como base o artigo 5º, nº. 1, do GDPR; a segunda, os requisitos para o tratamento de dados sensíveis; e a terceira, os critérios para decisões automatizadas. A quarta e quinta categorias se referem aos mecanismos de aplicação da lei, sendo a quarta, os critérios para uma autoridade supervisora, e a quinta, os mecanismos legais para proteger os direitos dos titulares de dados. Nas seções seguintes, serão analisadas cada uma dessas categorias e seus requisitos de acordo com a decisão de adequação.

1.1. Princípios fundamentais

O "Documento de Referência relativo à adequação" do Grupo de Trabalho do Artigo 29 estabelece que a lei de proteção de dados de um país terceiro deve apresentar princípios fundamentais relacionados ao seu conteúdo, para garantir que o nível de proteção seja essencialmente equivalente ao garantido pela União Europeia. Esses "princípios" na verdade se relacionam com todos os requisitos relativos ao conteúdo para uma lei de proteção de dados, incluindo a necessidade de definição de conceitos e alguns direitos do titular de dados, ou seja, são mais abrangentes que os princípios abordados no artigo 5º, nº. 1, do GDPR. Neste trabalho, entretanto, faremos a abordagem somente em relação aos princípios que estão elencados no artigo 5º do Regulamento.

O primeiro princípio diz respeito à licitude, lealdade e transparência (art. 5º, nº. 1, a) no tratamento de dados. Este princípio indica que os dados pessoais devem ser tratados de acordo com as leis aplicáveis e somente quando houver um fundamento legal para processá-lo, de maneira leal e transparente. O GDPR elenca as bases legais para tratamento de dados no artigo 6º, como o consentimento do titular dos dados, as disposições da legislação nacional dos países membros ou a execução de um contrato. No que diz respeito à transparência, a legislação de um país terceiro deve garantir que o titular de dados seja informado de todos os principais

elementos do tratamento de dados pessoais, como a finalidade, a identidade do controlador, seus direitos, entre outros elementos, de uma forma clara, acessível e inteligível (WP29, 2017).

O princípio da limitação das finalidades (art. 5º, nº. 1, b) estipula que os dados devem ser processados apenas para fins específicos, explícitos e legítimos, e não devem ser usados além desses fins, posteriormente, se não houver compatibilidade com as finalidades inicialmente mencionadas. O Grupo de Trabalho do Artigo 29 define mais detalhadamente no documento "Purpose Limitation" (WP29, 2013), essas características mencionadas. Quanto a ser específico, o Grupo de Trabalho indica que o propósito deve estabelecer os limites nos quais os controladores podem realizar o tratamento de dados, bem como ajudar a estabelecer as garantias necessárias para proteção de dados. Quanto a ser explícito, indica que o propósito deve ser apresentado de maneira clara, sem margem para ambiguidades. Quanto a ser legítimo, indica que o propósito deve ser não só fundamentado em uma das bases legais previstas para tratamento de dados, mas também deve ser compatível com outras leis aplicáveis.

O princípio de minimização de dados (art. 5º, nº. 1, c) define que as organizações devem coletar e processar apenas os dados pessoais necessários para atingir suas finalidades de tratamento. Segundo Filippidis (2018), a aplicação prática desse princípio abrange os conceitos de necessidade e proporcionalidade. Quanto à necessidade, o controlador deve observar se, para atingir o propósito definido, os dados poderiam ser anonimizados, por exemplo. A proporcionalidade se relaciona com a quantidade de dados coletados e se existem alternativas menos invasivas para aquela coleta específica.

O princípio da precisão (art. 5º, nº.1, d) indica que os dados devem ser exatos, precisos e, quando necessário, atualizados. Os dados pessoais que são imprecisos devem ser excluídos ou retificados imediatamente. Na prática, isso também inclui o dever de responder prontamente aos pedidos de correção realizados pelos titulares de dados (Filippidis, 2018).

O princípio de limitação de armazenamento (art. 5º, nº. 1, e) estipula que os dados devem, como regra geral, ser mantidos por não mais do que o tempo necessário para as finalidades para os quais foram definidos. O GDPR indica que os dados podem ser armazenados por períodos mais longos quando para fins de arquivamento de interesse público, pesquisa científica, histórica ou fins estatísticos.

Por fim, o princípio de integridade e confidencialidade (art. 5º, nº. 1, f) exige que qualquer entidade que processe dados pessoais assegure que os dados sejam processados de uma maneira

que garanta segurança, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando as técnicas apropriadas, como a anonimização ou pseudoanonimização, ou medidas organizacionais.

Esses princípios, como base fundamental de uma lei de proteção de dados, influenciam todo o contexto da legislação do país terceiro. Como foi dito anteriormente, o documento do Grupo de Trabalho do Artigo 29 especifica que esses princípios não devem necessariamente ser iguais em todos os termos ao GDPR, mas fornecem a base fundamental de todo processo de tratamento de dados pessoais.

1.2. Dados sensíveis

O Grupo de Trabalho do Artigo 29 estabelece que a lei de proteção de dados de um país terceiro deve apresentar maior proteção, quanto ao seu conteúdo, quando houver o tratamento de categorias especiais de dados, os denominados dados sensíveis. Essa proteção específica é indispensável, pois o tratamento desses dados pode trazer riscos significativos aos direitos e liberdades fundamentais de um indivíduo em razão das informações relacionadas a esses dados. As disposições relativas aos dados sensíveis no GDPR são apresentadas nos Considerandos nºs. 51 a 56, nos parágrafos 13, 14 e 15 do artigo 4º e no artigo 9º do Regulamento.

O parágrafo 1º do artigo 9º do GDPR define como sensíveis os tipos de dados pessoais que "origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual" de um indivíduo. Como regra geral, o Regulamento determina que esses dados não devem ser processados. Entretanto, o parágrafo 2º do artigo 9º prevê dez bases legais que servem como exceção para o tratamento de dados sensíveis, como, por exemplo, com o consentimento explícito do titular dos dados; quando o processamento é necessário para proteger seus interesses vitais; ou se o tratamento for realizado com fundamento no interesse público. Desta forma, a intenção do Regulamento é criar um nível mais elevado de proteção aos dados dessa categoria, pois, além de encontrar uma base legal no artigo 9º para o tratamento de dados dessa categoria, o controlador deve também combiná-lo com uma das bases legais do artigo 6º (Hordern, 2018), além de cumprir as demais disposições do Regulamento.

A proteção específica para o processamento de dados sensíveis é relevante, uma vez que houve um crescimento significativo no número de aplicativos e empresas que lidam com dados

sensíveis, especialmente nos serviços de saúde. Isso inclui, por exemplo, aplicativos que rastreiam dados cardíacos do usuário, prometem maior controle sobre o ciclo menstrual de uma mulher ou o uso de "tecnologias vestíveis". A vazamento e uso indevido de dados sensíveis tem mais efeitos prejudiciais principalmente pelo seu uso associado a outros dados pessoais, o que pode gerar discriminação. É por estas razões que a Comissão Europeia deve solicitar garantias específicas no processamento desta categoria de dados para países terceiros, através de medidas de segurança adicionais, no intuito de garantirem o nível de adequação necessário.

1.3. Decisões automatizadas

O Grupo de Trabalho do Artigo 29 dispõe que as decisões baseadas unicamente em tratamento automatizado, incluindo a definição de perfis, que produzirem efeitos jurídicos ou afetem de forma significativa o titular de dados, só podem ser tomadas em algumas situações, ou seja, não devem prevalecer como regra. No caso do GDPR, o artigo 22 consagra este direito do titular de dados de não ser objeto de decisão automatizada que produza efeitos jurídicos ou o afete de forma significativa como regra e estabelece três exceções: se houver o consentimento explícito do titular dos dados; se ela for necessária para a celebração ou execução de um contrato; ou quando é autorizado pela legislação da União ou de um Estado-Membro e na qual se estabelece as medidas adequadas para salvaguardar os direitos, as liberdades e os legítimos interesses do titular de dados.

O Grupo de Trabalho estabelece que a lei do país terceiro deve, em qualquer caso, prever as proteções necessárias, incluindo o direito do titular de ser informado sobre as razões específicas subjacentes à decisão e à lógica envolvida na decisão, para corrigir informações inexatas ou incompletas, e de contestar a decisão baseadas em informações incorretas. Se a decisão não cumprir as condições estabelecidas no quadro jurídico do país terceiro, o titular de dados deve ter o direito de não estar sujeito a essa decisão. Essa medida visa garantir um tratamento justo e transparente em relação ao titular dos dados, para evitar, por exemplo, decisões produzidas por algoritmos que possam reproduzir os padrões sociais de discriminação e exclusão existentes na sociedade, conforme orientação do Considerando nº 71 do GDPR.

1.4. Autoridade supervisora

Para uma análise eficaz sobre se uma legislação de proteção de dados pessoais é adequada, sob o ponto de vista do Regulamento, não é suficiente que o país terceiro tenha o conteúdo da norma nos padrões específicos, direcionada aos direitos dos titulares e princípios

fundamentais quanto ao tratamento de dados, mas que também assegure a sua aplicação efetiva. Ao avaliar um nível adequado de proteção, a Comissão Europeia avaliará todo o sistema que tornará essas disposições de países terceiros efetivamente aplicáveis. Um requisito fundamental para que essas regras sejam aplicadas é a existência de uma autoridade supervisora robusta e independente.

Para os Estados-Membros da União Europeia, o GDPR estabelece que todas as autoridades supervisoras devem agir com total independência no desempenho das suas funções, incluindo um orçamento independente. Do mesmo modo, o Regulamento prevê a necessidade de que seja criada uma autoridade supervisora independente para monitorar e fazer cumprir os requisitos de proteção de dados em países terceiros. É essencial que a autoridade aja de maneira autônoma, imparcial no exercício de seus poderes e não busque ou aceite instruções de qualquer nível governamental. Essa independência é essencial para que a autoridade possa ser protegida contra potenciais influências políticas e econômicas.

A autoridade deve ter todos os poderes e objetivos necessários para garantir o cumprimento dos direitos de proteção de dados e promover a conscientização. Além disso, a autoridade deve, por sua própria iniciativa, realizar investigações. Para tal, o sistema de proteção de dados de países terceiros exige que os responsáveis pelo tratamento de dados ou os processadores de dados cumpram e demonstrem essa conformidade à autoridade supervisora competente. Tais medidas podem incluir avaliações de impacto de proteção de dados ou a manutenção de registros ou arquivos de log de atividades de processamento de dados por um período apropriado.

1.5. Mecanismos legais para proteger os direitos dos titulares de dados

Para garantir o cumprimento das disposições relativas aos direitos e aos princípios fundamentais de proteção de dados, é também necessário que a Comissão Europeia avalie se o sistema jurídico do país terceiro fornece apoio adequado e mecanismos de proteção para que os titulares de dados exerçam os seus direitos. O titular de dados deve ter facilitado o acesso a esses mecanismos e, em caso de descumprimento da legislação, o sistema do país terceiro deve fornecer uma reparação administrativa ou judicial eficaz, incluindo a indenização por danos resultantes do tratamento ilícito dos seus dados pessoais. Isso permite que os titulares de dados possam encontrar soluções para fazer valer seus direitos de maneira rápida e eficaz.

No caso do GDPR, estão previstos no Capítulo III os direitos dos titulares de dados e a forma como os responsáveis pelo tratamento devem proceder para assegurá-los. Nos casos de descumprimento da Regulamento, para além dos mecanismos administrativos ou extrajudiciais disponíveis perante às autoridades supervisoras, os artigos 79 e 82 apresentam o direito que os titulares têm para receber indenização do responsável pelo tratamento ou do subcontratante pelos danos resultantes de uma violação. O processo judicial para o exercício do direito de receber uma indenização é instaurado nos tribunais competentes nos termos da lei de cada Estado-Membro.

Também é importante que a autoridade supervisora atue e fiscalize de forma independente, investigue as denúncias e permita que quaisquer violações dos direitos de proteção de dados sejam identificadas e punidas. O sistema deve ser eficaz, lidando com investigações preventivas e sanções que desestimulem o descumprimento da lei.

2. ANÁLISE DA LEI DE PROTEÇÃO DE DADOS BRASILEIRA

Em 14 de agosto de 2018, a primeira Lei Geral de Proteção de Dados do Brasil (LGPD) foi sancionada. Fortemente influenciada pelo GDPR, a Lei nº 13.709/2018 cria um marco para o uso de dados pessoais no país, com aplicação nos setores público e privado. Com a sua entrada em vigor, a LGPD complementará um quadro regulamentar setorial sobre proteção de dados no país, que atualmente deixa várias lacunas e insegurança jurídica.

O ex-presidente, Michel Temer, no período de aprovação da lei, vetou disposições essenciais que prejudicavam sua aplicação, como as disposições relacionadas à criação da Autoridade Nacional de Proteção de Dados, algumas penalidades e requisitos de transparência para as instituições do setor público. No entanto, na data de 28 de dezembro de 2018, já no final do mandato, foi publicada a Medida Provisória nº. 869, trazendo algumas alterações à LGPD e dispondo sobre a criação da Autoridade Nacional de Proteção de Dados, desta vez, vinculada à Presidência da República. A LGPD entrará em vigor após 24 meses de sua publicação[2], em agosto de 2020, para o período de implementação.

A Lei de Proteção de Dados do Brasil foi desenvolvida durante anos de consulta pública a entidades ligadas ao comércio, comunicação, setores da internet e organizações da sociedade

---

[2] Alteração pela Medida Provisória n° 869, de 2018, ainda em tramitação.

civil. A entrada em vigor do GDPR, em 25 de maio de 2018, e sua grande influência, contribuiu bastante para a aprovação dos projetos que tramitavam no Congresso brasileiro para a criação de uma lei de proteção de dados. Outro fator que contribuiu para a aprovação da LGPD é a intenção do Brasil de se tornar membro na Organização para Cooperação e Desenvolvimento Econômico (OCDE) (Monteiro, 2018). De acordo com as diretrizes da OCDE, entre outras condições, é necessário que o país tenha padrões robustos em relação à proteção de dados pessoais para solicitar a associação.

Nas subseções seguintes, analisam-se as categorias selecionadas anteriormente do GDPR para compará-las com as disposições da Lei Geral de Proteção de Dados do Brasil, do ponto de vista da decisão de adequação da Comissão Europeia.

2.1. Princípios fundamentais

A LGPD estipula dez princípios relativos ao processamento de dados pessoais, listados no artigo 6º, como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização. Esses princípios não são uma reprodução exata dos princípios elencados no GDPR, entretanto, contêm as principais disposições relacionadas àqueles princípios do Regulamento, conforme necessário para a decisão de adequação.

O princípio da finalidade, inciso I, indica que a atividade de tratamento de dados deve ser para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento subsequente que seja incompatível com esses com os propósitos iniciais. Este princípio é equivalente aos princípios da licitude e da limitação da finalidade do GDPR.

O segundo princípio, adequação, estipula que o tratamento de dados deve ser compatível com a finalidade informada ao titular dos dados, de acordo com o contexto do tratamento. É também equivalente ao princípio da limitação da finalidade do GDPR.

O princípio da necessidade, inciso III, indica que deve haver uma limitação da atividade de tratamento ao mínimo necessário, abrangendo dados relevantes, proporcionais e não excessivos em relação aos propósitos do tratamento. É equivalente ao princípio de minimização de dados e limitação da retenção do Regulamento.

O quinto princípio, qualidade de dados é compatível com o princípio de precisão do GDPR. Indica que o processador de dados deve garantir exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para atingir a finalidade do tratamento.

O princípio de transparência, inciso VI, dispõe que deve ser garantido aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre o tratamento e os respectivos agentes responsáveis. O princípio do livre acesso, inciso IV, dispõe que deve ser garantido aos titulares a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre seus dados pessoais. Ambos os princípios são compatíveis com o princípio da lealdade e transparência do GDPR.

O princípio de segurança, inciso VII, estabelece que o processamento de dados deve observar o uso de medidas técnicas e administrativas capazes de proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilegais de destruição, perda, alteração, comunicação ou divulgação. É compatível com o princípio de integridade e confidencialidade do GDPR.

Para uma demonstração visual dos princípios do GDPR e quais são os respectivos equivalentes da LGPD, apresentamos a seguinte tabela comparativa.

TABELA DE EQUIVALÊNCIA DE PRINCÍPIOS	
GPDR	**LGPD**
Lealdade e transparência	Livre acesso + Transparência
Licitude + Limitação das finalidades	Finalidade e Adequação
Minimização dos dados	Necessidade
Precisão	Qualidade de dados
Integridade e Confidencialidade	Segurança

O princípio de limitação de armazenamento do GDPR não tem um equivalente na LGPD, como um princípio de tratamento de dados. Entretanto, os artigos 15 e 16 da Lei brasileira dispõem que os dados pessoais serão eliminados após o término do processamento dos mesmos. Assim como o Regulamento europeu, a LGPD estabelece algumas situações em que os dados podem ser armazenados por períodos mais longos, como por exemplo, para cumprimento de uma obrigação legal ou regulatória pelo controlador. Da mesma forma, outros dois princípios da LGPD, como prevenção e não-discriminação, encontram disposições similares em outros artigos do GDPR, embora não tenham um princípio correspondente no artigo 5º do Regulamento. Como informado anteriormente, apesar de não haver uma correspondência exata dos princípios da LGPD, a legislação trata de todos aqueles que são necessários para a definição do nível adequado de proteção elencados pelo Grupo de Trabalho do Artigo 29.

2.2. Dados sensíveis

O artigo 5º, inciso II da LGPD conceitua os dados sensíveis como os dados pessoais "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Os requisitos para tratamento dessa categoria de dados estão indicados no Capítulo II, "Do tratamento de dados pessoais", Seção II e, como regra principal, o artigo 11 estabelece que os dados pessoais sensíveis só podem ser tratados quando o titular dos dados ou o seu representante legal consentirem de forma específica e destacada com o tratamento para as finalidades informadas. Quando não há consentimento, o artigo indica sete hipóteses legais em que é possível o tratamento de dados sensíveis, como quando é indispensável para o cumprimento de uma obrigação legal pelo controlador; para proteger a vida ou incolumidade física do titular dos dados ou de terceiros; ou para estudos realizados por um órgão de pesquisa.

Em relação a estudos e pesquisas relacionadas a dados sensíveis, a LGPD possui disposições similares às do artigo 89 do GDPR, especialmente no que se refere à anonimização de dados. O artigo 13 da LGPD estabelece que, na condução de estudos de saúde pública, as entidades de pesquisa que tenham acesso a bancos de dados pessoais deverão mantê-las em um ambiente controlado e seguro, de acordo com práticas de segurança e que incluirá, sempre que possível, anonimização ou pseudonimização dos dados, bem como considerando os padrões éticos apropriados relacionados a estudos e pesquisas.

De forma geral, as hipóteses para tratamento de dados sensíveis são bastante semelhantes entre o GDPR e a Lei de Proteção de Dados brasileira. Entretanto, o Regulamento europeu possui duas hipóteses exclusivas: se os dados tenham sido manifestamente tornados públicos pelo titular de dados; e quando o tratamento é realizado no âmbito das atividades legítimas, mediante as garantias adequadas, por fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, se referindo exclusivamente aos seus membros. Dessa forma, nas hipóteses que a LGPD apresenta para tratamento de dados sensíveis, pode-se concluir que a legislação cumpre os requisitos necessários quanto às garantias necessárias para o tratamento de dados sensíveis.

2.3. Decisões automatizadas

O artigo 20 da Lei de Proteção de Dados prevê que os titulares dos dados tenham o direito de solicitar uma revisão das decisões realizadas exclusivamente com base em tratamento automatizado que afetem seus interesses, incluindo decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade. Conforme análise de Bioni (2019, p. 82), a adição da expressão "e que afetem seus interesses" no texto legislativo é de extrema importância para que a lei possa ter a aplicação devida no intuito de proteger os interesses do titular de dados, mas, ao mesmo tempo, não a transformar numa proteção a "tudo", tornando a aplicação dificultada numa sociedade orientada a dados.

Este direito de solicitar revisão de decisões com base em tratamento automatizado também é previsto na Lei do Cadastro Positivo (Lei nº. 12.414/2011) e agora será estendido para o tratamento automatizado para qualquer finalidade, nas condições do artigo 20 da LGPD (Monteiro, 2018).

O artigo não prevê que exista o direito do titular de dados de se opor ao tratamento automatizado que produza efeitos na sua esfera jurídica ou que o afete significativamente, como no GDPR, mas prevê o direito de ser informado sobre os motivos específicos relativos aos critérios e procedimentos utilizados para a decisão. O entendimento do Grupo de Trabalho do Artigo 29 estabelece que, se a decisão não satisfizer as condições estabelecidas no quadro jurídico do país terceiro, o titular de dados deve ter o direito de não se submeter a ela. Portanto, a LGPD preenche este requisito apenas parcialmente.

Além disso, o artigo estabelece que, se a informação solicitada pelo titular de dados não for fornecida, com base no sigilo comercial e industrial, a autoridade supervisora poderá realizar

uma auditoria para verificar aspectos discriminatórios do tratamento automatizado. Como informado anteriormente, essas disposições quanto às decisões baseadas em tratamento exclusivamente automatizado destinam-se a proteger os direitos do titular de dados no caso de decisões que possam reproduzir aspectos discriminatórios e violar os direitos fundamentais. Além disso, o tratamento de dados, automatizado ou não, deve também obedecer ao princípio da não discriminação, previsto no art. 6, IX da LGPD.

2.4. Autoridade supervisora

O ex-presidente brasileiro, Michel Temer, vetou as disposições da LGPD relativas à instituição de uma autoridade supervisora, que teria o dever de fiscalizar e garantir a eficácia da lei. A justificativa do governo para os vetos era que a criação da autoridade era inconstitucional, já que a iniciativa veio do Congresso Nacional e o Poder Legislativo não pode criar órgãos no Poder Executivo. Alguns especialistas destacaram o fato de que a inconstitucionalidade não existiria, uma vez que um dos projetos de lei que que formaram o texto final veio da iniciativa do Poder Executivo[3]. O presidente mencionou, no entanto, que a autoridade seria criada posteriormente, o que ocorreu de 28 de dezembro de 2018, pela Medida Provisória nº. 869.

A Autoridade Nacional de Proteção de Dados é uma das disposições mais relevantes, com mais de 50 referências no texto da LGPD, especialmente porque será responsável pela regulamentação e interpretação de vários pontos da lei, como a do artigo 46, que estabelece que a Autoridade Nacional deve estabelecer os padrões técnicos mínimos a serem adotados pelos agentes de tratamento. A ausência de um sistema amplo anterior de proteção de dados no Brasil para ao menos se ter como base ou referência destaca ainda mais a importância da Autoridade nesse período de adaptação.

Junto com a Autoridade Nacional de Proteção de Dados (ANPD), também retornou ao texto da LGPD o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, um órgão multissetorial ligado à Autoridade, também foi vetado. O Conselho deve trabalhar propondo

---

[3] Entre outros, o ministro aposentado do Supremo Tribunal Federal, Ilmar Nascimento Galvão. "Ex-ministro diz que não há vício de inconstitucionalidade na criação da ANPD". Disponível em:<https://www.jota.info/docs/ex-ministro-diz-que-nao-ha-vicio-de-inconstitucionalidade-na-criacao-da-anpd-31072018>

diretrizes estratégicas e fornecendo subsídios para a elaboração de uma Política Nacional de Proteção de Dados, bem como para apoiar o desempenho da própria ANPD.

A MP nº 869, com todas as 176 emendas propostas, está atualmente em análise no Congresso Nacional. A Autoridade criada pela Medida Provisória segue um modelo vinculado à Presidência da República e algumas das emendas propostas são para alteração do modelo institucional para um modelo com independência. Como já mencionado, o entendimento do Grupo de Trabalho do Artigo 29 é que a autoridade supervisora deve atuar com total independência no desempenho de suas funções, inclusive orçamentárias. Sem esses requisitos, a Lei de Proteção de Dados do Brasil não será considerada adequada na análise da Comissão Europeia.

2.5. Mecanismos legais para proteger os direitos dos titulares de dados

Para os requisitos da decisão de adequação, a legislação do país terceiro deve dispor de mecanismos eficientes para o exercício dos direitos pelos titulares dos dados e de uma reparação administrativa ou judicial efetiva. O Capítulo IV, Seção III da LGPD, artigos 42 a 45, estipula as disposições relativas à responsabilidade e indenização por danos resultantes do processamento ilegal de dados pessoais. O Artigo 42 garante que o titular dos dados tenha o direito de receber uma indenização do controlador ou operador que cause dano material, moral, individual ou coletivo no desempenho de sua atividade de tratamento de dados pessoais, similarmente às disposições do GDPR.

Quanto aos mecanismos administrativos, a redação do artigo 55-J, inciso V, apresentada pela MP nº. 869, dispõe entre das competências da ANPD, que devem ser implementados mecanismos simplificados para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. Também entre os direitos do titular de dados, está previsto no artigo 18, §1º da LGPD que o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados perante a Autoridade Nacional. Tais previsões, cumprem os requisitos propostos pelo Grupo de Trabalho do Artigo 29, mas dependem da confirmação da estruturação da Autoridade Nacional de Proteção de Dados.

3. ANÁLISE DO PROJETO DE EMENDA À LEI DE PROTEÇÃO DE DADOS CHILENA

O Chile foi o primeiro país da América Latina a aprovar uma Lei de Proteção de Dados, em 1999. A Lei nº. 19.628, atualmente em vigor, representa um marco normativo de proteção de dados pessoais no país, com aplicação nos setores público e privado, garantindo direitos fundamentais aos titulares de dados. Entretanto, mesmo com algumas atualizações ao longo do tempo, a lei ainda apresenta várias deficiências e ainda não possui uma aplicação de forma a garantir a proteção dos direitos dos titulares de dados nela previstos, o que é motivado por alguns fatores como a inexistência de uma autoridade supervisora, a falta de regulação sobre o fluxo internacional de dados, a ausência de sanções efetivas (Violler, 2017), entre outros elementos que comprometem a aplicação efetiva da legislação.

Em março de 2017, dois novos projetos de emenda (Boletim nº 11144-07 e 11092-0, apensos) foram apresentados ao Congresso chileno com o objetivo de suplementar as deficiências da lei e atender as mais recentes tendências normativas internacionais de proteção de dados. O Chile, como membro da Organização para Cooperação e Desenvolvimento Econômico (OCDE) desde 2010, também precisa que sua lei de proteção de dados cumpra com as diretrizes atuais da OCDE em matéria de proteção de dados, o que foi exigido desde a sua adesão.

O projeto está sendo discutido no Senado e, em 3 de julho de 2018, foram apresentadas as propostas de emendas da Presidência. A criação da autoridade supervisora será uma das alterações mais significativas da atual legislação, uma vez que a sua ausência implica na falta de fiscalização e eficiência da lei, além da ausência de mecanismos administrativos para garantir os direitos dos titulares de dados. Além disso, como visto ao longo deste trabalho, a criação da autoridade supervisora é um requisito primordial para a decisão de adequação da Comissão Europeia.

A seguir, analisam-se as categorias selecionadas anteriormente do GDPR com as disposições do projeto de emenda à Lei de Proteção de Dados do Chile, bem como as propostas de emenda da Presidência.

3.1. Princípios fundamentais

O projeto de emenda prevê oito princípios relativos ao processamento de dados pessoais a serem incluídos no artigo 3º da lei chilena: licitude do tratamento, finalidade, proporcionalidade, qualidade, responsabilidade, segurança, transparência e informação, e

confidencialidade. As propostas de emenda da Presidência mantêm todos os oito princípios, embora algumas pequenas modificações de texto tenham sido sugeridas.

O princípio da licitude do GDPR tem um equivalente listado no artigo 3, alínea a, do projeto de emenda, que dispõe que o processamento de dados pessoais deve ser baseado exclusivamente na lei.

O princípio da finalidade, listado na alínea b, dispõe no texto original da emenda que os dados devem ser coletados para finalidades específicas, explícitas e lícitas, e o uso deve ser limitado ao cumprimento dessas finalidades. Entretanto, há quatro exceções previstas: quando o processamento é compatível com a finalidade original; sempre que houver uma relação contratual ou pré-contratual entre o titular dos dados e o controlador de dados que justifique o processamento de dados para finalidades diferentes; se o titular de dados autoriza novamente seu consentimento; e, finalmente, sempre que os dados provêm de fontes de acesso público e o acesso é fornecido por lei. Este princípio é equivalente à limitação das finalidades do GDPR.

Ainda quanto a este princípio, a proposta da Presidência foi acrescentar após a expressão “finalidades diferentes”, na segunda exceção, a frase “sempre que se enquadrar no escopo do contrato ou quando for consistente com as negociações anteriores”. O Executivo também sugeriu acrescentar a frase "e o seu tratamento está relacionado com os fins para os quais os dados foram recolhidos" no caso da quarta exceção (dados de fontes de acesso público).

O princípio da proporcionalidade, alínea c, indica que os dados pessoais coletados devem ser limitados aos necessários para a finalidade do tratamento. Além disso, esses dados devem ser mantidos apenas pelo período necessário para atingir os objetivos de tratamento, caso contrário, o controlador deve obter uma autorização do titular dos dados. Este princípio refere-se aos princípios de minimização e retenção de dados do GDPR.

Quanto ao princípio da qualidade, o projeto dispõe que os dados devem ser precisos, completos e atualizados em relação aos propósitos de processamento. A indicação do presidente pretende incluir um parágrafo afirmando que a empresa responsável pelo processamento deve tomar todas as medidas razoáveis para garantir que os dados pessoais que são imprecisos, incompletos ou desatualizados sejam eliminados ou corrigidos o mais rápido possível. É equivalente ao princípio da precisão do GDPR.

O princípio da transparência e informação estabelece que o processamento, as políticas e as práticas de dados pessoais devem estar permanentemente acessíveis e disponíveis a todos os interessados, de maneira clara, precisa e inequívoca. É equivalente ao princípio de transparência do Regulamento.

Finalmente, o princípio da segurança do projeto de emenda prevê que o tratamento de dados deve garantir padrões de segurança adequados, protegendo os dados pessoais contra manipulação não autorizada, perda, vazamento, dano ou destruição. Para isso, os dados precisam ser processados com aplicação de medidas técnicas e organizacionais apropriadas. O princípio de confidencialidade expressa que o controlador de dados e aqueles que têm acesso aos dados pessoais, devem mantê-lo confidencial. O controlador de dados deve estabelecer medidas apropriadas para preservar os dados e isso deve subsistir mesmo após o final do tratamento. Ambos são equivalentes ao princípio de integridade e confidencialidade do GDPR.

GPDR	**Projeto emenda à Lei de Proteção de Dados chilena**
Licitude	Licitude do tratamento
Limitação das finalidades	Finalidade
Minimização dos dados + Limitação da retenção	Proporcionalidade
Precisão	Qualidade
Integridade e Confidencialidade	Segurança + Confidencialidade
Transparência	Transparência e Informação

A disposição dos princípios previstos no projeto de emenda à Lei de Proteção de Dados chilena apresenta mais similaridades com o texto do Regulamento europeu, alguns havendo correspondência exata dos princípios, o que torna essa categoria adequada do ponto de vista do entendimento do Grupo de Trabalho do Artigo 29 e da Comissão Europeia.

3.2. Dados sensíveis

De acordo com o artigo 2º, "g", do projeto de emenda à Lei de Proteção de Dados chilena, dados pessoais sensíveis são aqueles que revelam "origem étnica ou racial, filiação política ou sindical, crenças ideológicas ou filosóficas, crenças religiosas, dados de saúde, perfil biológico humano, dados biométricos e informações sobre a vida sexual relativas à orientação sexual e identidade de gênero de uma pessoa". A emenda proposta pelo Executivo indica que os hábitos pessoais devem ser adicionados como dados sensíveis, o que proporciona maior proteção nos casos de processamento de dados que buscam rastrear padrões comportamentais e rotinas do titular de dados.

Originalmente, o texto previsto no artigo 16 do projeto de emenda, como regra geral, exige que os dados sensíveis sejam processados somente quando o titular dos dados dá expressamente seu consentimento, o qual deve ser autorizado por meios escritos, verbais ou tecnologicamente equivalentes. A proposta da Presidência sugere a alteração do texto para enfatizar a proibição de tratamento de dados pessoais sensíveis e adicionar a hipótese para autorizar o processamento de dados confidenciais quando for necessário determinar ou garantir benefícios de saúde relacionados ao titular de dados.

Quando não há consentimento, o artigo especifica algumas situações em que é lícito o tratamento, por exemplo, caso seja necessário para a defesa de um direito do titular dos dados perante os tribunais de justiça; ou quando expressamente autorizado por lei; ou sempre que seja indispensável para proteger a sua vida, saúde ou integridade física.

Além disso, algumas situações para o tratamento de dados sensíveis estão detalhadas no artigo 16-bis ao artigo 16-terceiro, tais como especificações para o tratamento de dados de saúde, dados biométricos pessoais e dados relacionados ao perfil biológico humano. O projeto de emenda também prevê que a pesquisa científica que utiliza dados sensíveis possa ser livremente publicada e divulgada, quando os dados sejam anonimizados.

Dessa forma, numa análise das hipóteses que o projeto de emenda à Lei de Proteção de Dados do Chile apresenta para tratamento de dados sensíveis, bem como dos critérios e restrições relativos ao tratamento dos mesmos, pode-se concluir que a legislação cumprirá, se aprovada nesses termos, os requisitos necessários exigidos pelo Regulamento europeu.

3.3. Decisões automatizadas

O artigo 8º-bis do projeto de emenda da Lei nº 19.628 prevê o direito de se opor a decisões baseadas exclusivamente no tratamento automatizado, incluindo a criação de perfis, que afetem negativamente ou tenham efeitos legais adversos no titular de dados. A proposta do Presidente para este artigo é remover o requisito "que os afeta negativamente ou que tenham efeitos legais adversos", o que dá mais liberdade e amplitude ao titular dos dados para se opor a qualquer tipo de tratamento automatizado.

De acordo com este artigo, os titulares dos dados podem exercer o seu direito de se opor, exceto nos seguintes casos: quando a decisão é necessária para a conclusão ou execução do contrato com o controlador de dados; quando houver consentimento prévio e expresso do titular dos dados; ou quando expressamente autorizado por lei. No segundo caso, a indicação do Presidente é que a sentença "e não ser revogada da maneira estabelecida nesta lei" deve ser incluída. O projeto de emenda estabelece que, nos dois primeiros casos, o controlador de dados deve tomar todas as medidas necessárias para garantir os direitos dos titulares de dados, especialmente o direito de obter intervenção humana para expressar seu ponto de vista e o direito de solicitar uma revisão de decisão.

A disposição dos requisitos para decisões baseadas unicamente em tratamento automatizado apresenta uma enorme similaridade com os requisitos do Regulamento europeu, o que torna essa categoria adequada do ponto de vista do entendimento do Grupo de Trabalho do Artigo 29.

3.4. Autoridade supervisora

O Título VI, artigos 30 a 36 do projeto de emenda, apresenta as disposições relativas à Agência de Proteção de Dados Pessoais. Nos termos do artigo 30, a Agência deve ser um órgão público autônomo e descentralizado, com carácter técnico, personalidade jurídica e orçamento próprio, sujeito à supervisão do Presidente da República através do Ministério da Fazenda. No entanto, essa dependência funcional da autoridade supervisora ao Poder Executivo, através do Ministério da Fazenda levantou a preocupação sobre o nível de autonomia da Agência, uma vez que especialistas e organizações da sociedade civil defenderam a necessidade de independência e conhecimento técnico do órgão supervisor (Valenzuela, 2016).

A emenda do presidente proposta para esse artigo, entretanto, é que a autoridade supervisora seja o "Conselho de Transparência e Proteção de Dados Pessoais", o atual Conselho de Transparência, criado pela Lei nº. 20.285. Esse órgão tem atualmente como uma de suas

funções a supervisão do cumprimento das regras de transparência e publicidade da informação pelos órgãos da Administração, a promoção da transparência e a garantia do direito de acesso à informação.

A preocupação com essa alternativa é que transparência e proteção de dados são questões de características diferentes e devem, portanto, ter profissionais que estejam tecnicamente preparados para cada um de forma específica. Outro fator é que o Conselho está atualmente focado na supervisão de órgãos públicos e, para cumprir os objetivos da nova lei, também precisará supervisionar instituições do setor privado.

No entanto, o benefício dessa alternativa é que o Conselho, no modelo atual, é um órgão público autônomo, com personalidade jurídica e patrimônio próprio. Como mencionado anteriormente, os padrões internacionais, incluindo aqueles exigidos pelo GDPR para a decisão de adequação, exigem que a autoridade supervisora tenha independência organizacional e financeira. Além disso, qualquer indicação futura no projeto de lei que não leve em consideração esses fatores pode prejudicar a eficácia para uma possível decisão de adequação.

3.5. Mecanismos legais para proteger os direitos do titular de dados

No que diz respeito aos mecanismos administrativos para os titulares dos dados exercerem os seus direitos, o artigo 31, "c", do projeto de emenda indica que a Agência de Proteção de Dados terá a função de resolver os pedidos e reclamações feitas pelos titulares dos dados contra o controlador de dados. Da mesma forma, o artigo 45 do projeto menciona que os titulares dos dados podem apresentar queixa à Agência quando o controlador de dados tenha expressamente ou tacitamente negado um pedido para exercer quaisquer dos seus direitos ao abrigo da lei. Além disso, o artigo 23 estabelece o exercício dos direitos dos titulares de dados de acesso, retificação, oposição e cancelamento por procedimento administrativo perante órgãos públicos.

Quanto aos mecanismos judiciais, o artigo 51 do projeto de emenda estabelece, como regra geral, que o controlador de dados deve indenizar pelos danos causados quando, em sua operação de tratamento de dados, violar os princípios, direitos ou obrigações estabelecidas na lei. Para pessoas físicas ou jurídicas que se sentem lesadas pelas decisões da Agência de Proteção de Dados, o artigo 47 determina que uma reivindicação de ilegalidade pode ser feita no Tribunal de Apelações de Santiago ou no domicílio do solicitante. Esses mecanismos

judiciais e administrativos, portanto, cumprem as características necessárias para a defesa dos direitos dos titulares de dados para uma decisão de adequação.

CONCLUSÃO

Há uma dificuldade nos contextos brasileiro e chileno em proteger efetivamente os direitos dos titulares de dados. No entanto, é perceptível a crescente preocupação de ambos os países na adequação de seus ordenamentos jurídicos, que é motivada principalmente pela importância de cumprir as novas normas de proteção de dados para as relações econômicas mundiais, influenciadas principalmente pelo novo Regulamento Europeu. No entanto, o atraso na atualização da legislação de ambos os países reflete que há, de fato, mais disposição em cumprir os requisitos, para fins econômicos, do que proteger efetivamente os direitos dos titulares de dados.

Com base na análise realizada neste artigo, pode-se inferir que a Lei de Proteção de Dados do Brasil e o projeto de emenda à Lei de Proteção de Dados do Chile se preocuparam na adequação quanto às disposições de conteúdo, relativas às principais regras estabelecidas pelo GDPR e pelo entendimento do Grupo de Trabalho do Artigo 29, entretanto, algumas recomendações específicas são necessárias quanto aos mecanismos que garantirão a eficácia da lei.

Quanto à legislação brasileira, no seu período de implementação, há a necessidade de consolidação de uma autoridade supervisora independente, uma vez que é essencial para a aplicação da lei. O modelo apresentado pela Medida Provisória nº. 869/2018, vinculado à Presidência da República, não apresenta a independência necessária para uma autoridade supervisora, na qual a autonomia institucional e orçamentária é imprescindível. Caso não haja emendas e mudança para incluir esta característica fundamental, resta prejudicada a decisão para uma adequação da lei brasileira. Por outro lado, caso emendado o texto e a Autoridade Nacional de Proteção de Dados seja criada com total independência, sua implementação e funções-chave serão refletidas num sistema administrativo eficiente para a proteção dos direitos do titular de dados.

Em relação às decisões automatizadas, o artigo 20 da LGPD prevê o direito de revisão, entretanto, não há direito expresso de oposição por parte do titular dos dados, e esse requisito é, portanto, parcialmente cumprido em relação aos requisitos para uma decisão de adequação. Isto não significa necessariamente que esta seria uma razão para a desqualificação da lei para

uma possível decisão de adequação pela Comissão Europeia, uma vez que, conforme declarado pelo Grupo de Trabalho do Artigo 29, o país terceiro não necessita de disposições que reproduzem completamente às do GDPR e outros fatores que resguardem os direitos do titular de dados podem ser considerados. Um desses fatores pode ser, por exemplo, o fato da lei brasileira considerar no seu rol de princípios o da não discriminação, previsto no art. 6, IX da LGPD.

Quanto ao projeto de emenda à Lei chilena, é necessário que o texto final mantenha as disposições sobre a autoridade supervisora e as sanções para o cumprimento da lei. É também necessário que, no debate legislativo sobre a independência ou especialidade da autoridade supervisora, seja alcançado um consenso que priorize a independência do órgão, pois, sem esse requisito, a decisão de adequação ficará comprometida. Como visto, é essencial que haja completa autonomia para que as autoridades possam ser protegidas de potenciais influências políticas e econômicas que se revelem prejudiciais ao progresso de suas atividades.

Para uma demonstração visual das categorias analisadas, e se a respectiva legislação está ou não em conformidade com o nível de adequação necessário pela Comissão Europeia, apresentamos a seguinte tabela comparativa.

DECISÃO DE ADEQUAÇÃO	**LEI DE PROTEÇÃO DE DADOS BRASILEIRA**	**PROJETO DE EMENDA À LEI DE PROTEÇÃO DE DADOS DO CHILE**
Princípios fundamentais	Cumpre	Cumpre
Garantias para tratamento de dados sensíveis	Cumpre	Cumpre
Decisões automatizadas	Cumpre parcialmente	Cumpre
Autoridade supervisora	Não cumpre	Cumpre* (se mantida a autoridade com independência)

Mecanismos legais para garantia dos direitos do titular de dados	Cumpre	Cumpre

É importante salientar que esta análise foi baseada no cumprimento dessas cinco categorias, porém, a decisão de adequação é um processo que envolve um exame mais minucioso pela Comissão Europeia, na qual a análise inclui também disposições como a avaliação do respeito e efetividade dos direitos do titular de dados, da transferência internacional de dados e de todo o sistema de responsabilização quanto ao descumprimento das normas do país terceiro.

Por fim, destaca-se que as disposições que requerem reforço na Lei brasileira e na Lei chilena não se referem às regras de conteúdo, mas aos mecanismos que tornarão as leis eficientes. Para isso, é necessário também combinar um sistema eficaz de responsabilização a ser exigido por uma autoridade supervisora independente, bem como a implementação de políticas públicas e campanhas nacionais orientadas para aumentar a conscientização sobre a importância da proteção de dados pessoais, uma vez que estes serão elementos fundamentais a serem considerados numa decisão de adequação pela Comissão Europeia.

REFERÊNCIAS

ARTICLE 29 DATA PROTECTION WORKING PARTY (2017). *Adequacy referential*. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108>

ARTICLE 29 DATA PROTECTION WORKING PARTY (2013). *Opinion 03/2013 on purpose limitation.* Disponível em: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>

BIONI, B. R. (2019). *Proteção de dados pessoais: a função e os limites do consentimento (1a ed.)*. Rio de Janeiro: Forense.

CAMERON, S. (2017). *The Digital Economy & GDPR.* Disponível em:http://www.lightreading.com/oss-bss/subscriber-data-management/the-digital-economy-and-gdpr/a/d-id/730582

FILIPPIDIS, M. (2018). Data Processing Principles. In: INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP). *European Data Protection Law and Practice.* Portsmouth, NH: International Association of Privacy Professionals.

GUIDI, G. (2018). *Modelos regulatórios para proteção de dados pessoais.* Disponível em:<https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>

HORDERN, V. (2018). Lawful Processing Criteria. In: INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP). *European Data Protection Law and Practice.* Portsmouth, NH: International Association of Privacy Professionals.

MADGE, R. (2018). *GDPR's global scope: the long story.* Disponível em: https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f

MOLINA D., O. (2018). *Chile: nuestra (pobre) cultura de privacidad de datos personales.* Disponível em: https://www.americaeconomia.com/analisis-opinion/chile-nuestra-pobre-cultura-de-privacidad-de-datos-personales

MONTEIRO, R. L. (2018). *Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?* Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>

MONTEIRO, R. L. (2018). *Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada.* Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018>

VALENZUELA, D. A. (2016). Acceso a la información pública y protección de datos personales: ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos? *Revista de derecho (Coquimbo)*, *23*(1), 51-79. https://dx.doi.org/10.4067/S0718-97532016000100003

VIOLLIER, P. (2017). *The protection of personal data in Chile.* Disponível em: <https://www.derechosdigitales.org/wp-content/uploads/the-protection-of-personal-data-in-chile_c.pdf >

SCOTT, M. CERULUS, L. (2018). *Europe's new data protection rules export privacy standards worldwide*. Disponível em: <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/>