Impactos da **LGPD** nos Meios Alternativos de Resolução de Disputas

Coordenação: **Bernard Potsch** e **Daniel Tavela Luis**

Organização: **NewGen CAM-CCBC**

CAM·CCBC
CENTRO DE ARBITRAGEM E MEDIAÇÃO

NEW·GEN
NEW GENERATION CAM-CCBC

Impactos da **LGPD** nos Meios Alternativos de Resolução de Disputas

Autores

André Tunes do Nascimento

Ayanne Padilha

Beatriz Alaíde de Souza Assef

Denise de Araujo Berzin Reupke

Diane Brunoro Lyra

Gabriela de Ávila Machado

Giovana Carneiro

Giulia Keese Montanhesi

Julia Guimarães Rossetto

Letícia de Souza Baddauy

Mario Cesar Lobo Junior

Mariane Carvalho Amorim

Nathália Dalbianco Novaes Pereira

Nathan Correia de Azevedo

Rafael Tridico Faria

Stela Porto

Debatedores e avaliadores

Alice Moreira Franco

Chiara Teffé

Christian Augusto de Oliveira

Diego Machado

Gustavo Vaughn

Juliana Loss

Karin Klempp Franco

Laura Mendes

Marcelo Chiavassa

Maria Regina Rigolon Korkmaz

Pedro Silveira C. Soares

Rodrigo da Guia

ÍNDICE

PREFÁCIO

Autoria

Gustavo Favero Vaughn

Marcelo Chiavassa de Mello Paula Lima

Rodrigo da Guia Silva

A comunidade jurídica vivencia, atualmente, dois relevantes fenômenos cuja interconexão por vezes não recebe a devida atenção. De uma parte, verifica-se o crescimento da preocupação com a tutela da pessoa humana diante dos desafios impostos pelas novas tecnologias, em especial no que diz respeito à privacidade e proteção dos dados pessoais. No Brasil, este debate se intensificou especialmente a partir da promulgação da Lei nº. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – "LGPD"). De outra parte, nota-se o contínuo esforço de consolidação, ampliação e aperfeiçoamento dos mecanismos alternativos de resolução de disputas, propósitos situados no cerne da missão, da visão e dos valores da New Generation ("NewGen"), comissão de jovens profissionais idealizada e apoiada pelo Centro de Arbitragem e Mediação da Câmara de Comércio Brasil-Canadá ("CAM-CCBC").

Em que pese a crescente relevância de tais fenômenos na realidade contemporânea, ainda são menos frequentes do que se poderia almejar os estudos destinados à compreensão das suas conexões, que podem assumir variadas manifestações – por exemplo, desde os impactos da LGPD sobre a condução dos procedimentos de mediação e arbitragem até a própria configuração de litígios relativos à proteção de dados pessoais submetidos aos métodos alternativos de resolução de disputas, principalmente diante da possibilidade de um significativo contencioso em proteção de dados pessoais, tal qual se verifica nas relações de consumo. À luz desse contexto, cumpre, portanto, não perder de vista o questionamento: quais são os impactos da LGPD sobre os meios alternativos de resolução de disputas e, de outro lado, de que forma podem os meios alternativos auxiliarem o Estado na segurança jurídica e na pacificação dos conflitos sociais? Essa instigante e relevantíssima pergunta foi objeto de um edital de chamada de artigos acadêmicos, que foi idealizado, em momento muito oportuno, pela NewGen.

O edital, tornado público em meados de 2020, foi dividido em cinco etapas, concebidas em torno do benfazejo objetivo de adoção de um sistema mais dialético de construção do trabalho final, na contramão do tom monológico que costuma caracterizar a produção acadêmica. Todas as etapas, que listaremos a seguir, foram acompanhadas de perto pela Comissão Avaliadora, a qual tivemos a honra (e responsabilidade) de integrar ao lado das colegas Laura Mendes e Chiara Teffé.

A primeira etapa consistiu no envio de artigos acadêmicos, pelos interessados, de acordo com as normas especificadas no edital. Os trabalhos recebidos, de alta qualidade, foram submetidos à análise da Comissão Avaliadora, que, nesse primeiro momento, verificou a coerência e adequação dos textos com o tema proposto no edital, a profundidade do conteúdo, a originalidade do assunto e da abordagem, e a correção gramatical.

Após isso, como parte da segunda etapa, os artigos aprovados foram distribuídos de forma anônima aos associados da NewGen, que tiveram a oportunidade de fazer comentários críticos aos textos, a fim de contribuir para o debate e enriquecer os trabalhos.

A terceira etapa, que viria a ser reunida à quarta em razão da convergência de escopos, tinha a finalidade de reunir os comentaristas com os autores dos trabalhos, para que o debate entre eles pudesse levar a eventuais ajustes nos textos.

Na quarta etapa, desenvolvida em ambiente virtual em razão das medidas de segurança suscitadas pela pandemia da Covid-19, os autores dos belos trabalhos aprovados foram convidados a compor mesas virtuais de debates, com participação de especialistas convidados e dos membros da Comissão Avaliadora. Os autores tiveram a oportunidade de explicar ao vivo o conteúdo de seus trabalhos, o que fizeram com inegável êxito. Após isso, tanto os convidados quanto os membros da Comissão Avaliadora tiveram a oportunidade de interagir com os autores, assim como dar feedbacks sobre os trabalhos e indicar eventuais pontos que poderiam ser tratados com mais profundidade.

A quinta e última etapa consistiu no envio, pelos autores, das versões finais dos trabalhos, as quais deveriam levar em consideração os debates ocorridos por ocasião da quarta etapa.

Temos, então, a imensurável satisfação de compartilhar a lista dos nove trabalhos desenvolvidos no bojo do edital lançado pela NewGen, com a justa indicação dos nomes dos autores, que devem ser exaltados pelo que desempenharam ao longo das cinco etapas:

- Consensualidade no processo administrativo sancionador da Autoridade Nacional de Proteção de Dados Pessoais (Stela Porto e Giovana Carneiro);

- O tratamento inadequado de dados no contexto corporativo e o papel dos métodos adequados de solução de conflitos frente à preservação da reputação das empresas (Ayanne Padilha);

- Split: Brazilian arbitration and data protection in the midst of a fractured world (André Tunes do Nascimento);

- Conflito de leis na arbitragem internacional: interações entre a LGPD e outras legislações de privacidade em demandas plurilocais (Gabriela de Ávila Machado, Giulia Keese Montanhesi e Rafael Tridico Faria);

- Admissibility of evidence obtained in breach of data protection legislation in international arbitration (Mariane Carvalho Amorim);

- Procedimento arbitral e novos meios de prova: acesso à justiça eficaz em conflitos envolvendo a Lei Geral de Proteção de Dados Pessoais (Diane Brunoro Lyra e Nathan Correia de Azevedo);

- A LGPD como obrigatoriedade e oportunidade: uma aliança entre ODR e Privacy by Design (Letícia de Souza Baddauy, Mario Cesar Lobo Junior e Nathália Dalbianco Novaes Pereira);

- Arbitragem como meio alternativo de resolução de disputas oriundas da Lei Geral de Proteção de Dados Pessoais – LGPD e a compliance nas câmaras arbitrais (Denise de Araujo Berzin Reupke e Julia Guimarães Rossetto); e

- Métodos extrajudiciais e a LGPD (Beatriz Alaíde de Souza Assef).

O resultado dessa brilhante iniciativa da NewGen foi materializado com a publicação dos trabalhos no formato ora apresentado ao público. Trata-se de acervo de acentuada riqueza teórica e inegável utilidade prática, que explora, a partir de abordagens inovadoras, temas complexos situados na ordem do dia, como se pode inferir pelos títulos dos artigos acima mencionados. Temos convicção que esses trabalhos, após todas as

etapas listadas acima, serão de grande auxílio para aqueles que desejam se aprofundar no estudo dos meios alternativos e da proteção dos dados pessoais.

É muito satisfatório ver que a iniciativa da NewGen deu excelentes frutos, cumprindo assim com sua missão institucional de formação de novos profissionais e de produção de material de pesquisa de qualidade.

Parabenizamos os autores pelos trabalhos e a NewGen pela iniciativa, ao mesmo tempo em que renovamos os nossos agradecimentos pela confiança em nós depositada para compor a Comissão Avaliadora. Não hesitamos em dizer que os trabalhos ora submetidos ao apreço do público certamente contribuirão para o aperfeiçoamento da resolução de disputas no contexto da proteção de dados pessoais.

São Paulo, 8 de agosto de 2021.

CONSENSUALIDADE NO PROCESSO ADMINISTRATIVO SANCIONADOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS[1]

Autoria

Stela Porto

Giovana Carneiro

Clicar ou escanear para acesso aos debates relativos a este artigo

Debatedores

Christian Augusto S. Perrone de Oliveira

Maria Regina Rigolon Korkmaz

Rodrigo da Guia

RESUMO

Os métodos alternativos ou adequados de resolução de disputas exercem especial importância na garantia de um processo sancionatório efetivo a ser implementado pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD). A LGPD estabelece um arranjo institucional que prevê, para além da aplicação de multas, instrumentos que dão preferência à consensualidade, como já é a tendência do direito administrativo brasileiro. O primeiro tópico apresenta algumas das competências da ANPD previstas em lei. O segundo busca expor um breve panorama das multas aplicadas na Europa e dos procedimentos previstos à luz da LGPD. No terceiro tópico, refletimos sobre como a consensualidade, em especial a celebração de acordos, têm se desenvolvido no processo sancionador brasileiro. Ao final, concluímos pela proposição de uma visão menos punitivista e mais consensual da atuação da ANPD.

INTRODUÇÃO

Desde antes da entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – "LGPD"), muito se tem discutido sobre a possibilidade de

[1] As autoras agradecem os comentários e críticas ao artigo feitos por Ayanne Padilha, Christian Perrone, Maria Regina Rigolon Korkmaz e Rodrigo da Guia no evento "Impactos da LGPD nos Meios Alternativos de Solução de Disputas", organizado pelo Comitê de Gestão da New-Gen CAM-CCBC.

aplicação de multas administrativas por descumprimento às obrigações ali previstas. A aplicação de multas em outros países com base em legislações correlatas[2] e o noticiário nacional[3] em torno do tema trataram de potencializar a multa como forma de dissuasão ao descumprimento da lei e de estímulo a conformidade. Em que pese a importância desse efeito, a narrativa construída colocava em desvantagem o caráter prospectivo da sanção, se focando em uma visão meramente retributiva.[4]

De fato, o agente privado de tratamento está sujeito a perdas pecuniárias caso descumpra a legislação. Por um lado, a lei prevê, no artigo 42, que os titulares têm direito à reparação em caso de dano decorrente do exercício da atividade de tratamento de dados pessoais. Por outro, o artigo 52 prevê a competência da Autoridade Nacional de Proteção de Dados Pessoais ("ANPD") para aplicar multas simples e diária.[5] As multas, porém, constituem apenas um dos elementos do complexo arranjo sancionatório previsto pela LGPD.[6]

[2] Voltaremos ao tema no item 2.

[3] Veja, por exemplo: MONACO, Gustavo, CAMARGO, Solano, MARTINS, Amanda. Sem sanções, LGPD é inócua. Valor Econômico, abril de 2020. Disponível em: <https://valor.globo.com/legislacao/noticia/2020/04/13/sem-sancoes-lgpd-e-inocua.ghtml>. Acesso em: 04/11/2020. FRIZERA, Ricardo. LGPD, o AI-5 da inovação no Brasil. Folha Vitória, dezembro de 2019. Disponível em: <https://www.folhavitoria.com.br/economia/mundo-business/2019/12/01>. Acesso em: 04/11/2020. PIRES, Thomaz. Lei Geral de Proteção de Dados e o risco do vácuo regulatório. Valor Econômico, janeiro de 2020. Disponível em: <https://valor.globo.com/opiniao/coluna/lei-de-protecao-de-dados-e-o-risco-do-vacuo-regulatorio.ghtml>. Acesso em: 04/11/2020.

[4] A diferença finalística entre o direito administrativo e o direito penal é explorada por Alice Voronoff, que propõe um discurso de justificação, interpretação e aplicação para o direito administrativo sancionador. A autora questiona "Ao punir em âmbito administrativo, o Estado e a sociedade esperam alcançar os mesmos resultados associados à aplicação das penas? A lógica operativa desses institutos – sanções penais e administrativas – podem ser equiparadas? A resposta não é simples.", desenvolvendo a ideia base de que "(a) o direito administrativo sancionador, como regra, busca a conformação da conduta dos particulares para evitar resultados contrários a objetivos de interesse público definidos no ordenamento jurídico. Ele opera, portanto, a partir de um olhar eminentemente prospectivo e conformativo, dissociado de um juízo de condenação moral. (b) Já o direito penal tem como finalidade inerente (ainda que não seja a única) castigar o ofensor por lesão provocada a bens jurídicos caros à sociedade." (VORONOFF, Alice. *Direito administrativo sancionador no Brasil*. Belo Horizonte: Fórum, 2018, pp. 99, 102).

[5] Neste artigo, fazemos alusão às hipóteses sancionatórias aplicáveis ao setor privado. O artigo 52, §3º da LGPD excluiu as multas das hipóteses sanções aplicáveis "às entidades e aos órgãos públicos". Assim, não são cabíveis multas às pessoas jurídicas de direito público. As empresas públicas e sociedades de economia mista, à princípio, estão sujeitas a essa modalidade de sanção. Sobre o tema, ver: ZARDO, Francisco. 38. As sanções administrativas de multa simples e multa diária na LGPD, item 5. In: LGPD e administração pública: uma análise ampla dos impactos. Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

[6] Um outro aspecto desse arranjo, que não é o foco deste trabalho, se trata da multiplicidade de atores institucionais envolvidos no processo de *enforcement* da LGPD, inclusive na aplicação de sanções. O artigo 52, §2º expressamente prevê que as sanções ali dispostas não substituem a aplicação de outras sanções administrativas, civis ou penais definidas no Código de Defesa do Consumidor (Lei nº 8.078).

Os métodos alternativos de resolução de disputas, em uma concepção ampla[7], encontram seu lugar em ambas as situações às quais os agentes de tratamento estão sujeitos. Em primeiro lugar, em relação às disputas que possam advir entre o titular de dados e o controlador ou operador[8], mas também no âmbito dos processos administrativos sancionatórios decorrentes da aplicação da lei. O presente artigo se debruça sobre a segunda hipótese.

Para tanto, o primeiro tópico apresenta brevemente as competências da ANPD previstas em lei, demonstrando que o aparato institucional previsto é mais amplo do que a mera possibilidade de aplicação das multas simples e diárias. No segundo item, trataremos da aplicação de multas por autoridades estrangeiras e de algumas previsões da LGPD. Como se verá, o valor pecuniário das multas ganha destaque em relação às outras possibilidades sancionatórias existentes. No terceiro tópico, refletimos sobre como a consensualidade, em especial a celebração de acordos, têm se desenvolvido no processo sancionador brasileiro. Ao final, concluímos pela proposição de uma visão menos punitivista e mais consensual da atuação da ANPD.

1. O PAPEL DA ANPD E SUAS COMPETÊNCIAS SANCIONATÓRIAS

A LGPD, criada com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural (artigo 1º), dispõe diversos fundamentos (artigo 2º) e princípios (artigo 6º) para a tutela da proteção de dados pessoais no Brasil[9].

Conforme explica Laura Schertel, a aplicação da lei se dá em três níveis[10]. Em primeiro lugar, o tratamento de dados pessoais deve atender as "condições de legitimidade', se fundando em uma das onze (11) bases legais previstas no artigo 7º ou

[7] Métodos alternativos de resolução de controvérsias ("*alternative dispute resolution*" - ADR), em sua concepção mais ampla, incluriam métodos *consensuais* de resolução de conflitos (como mediação, neogicação e conclialiação), e arbitragem. WALLGREEN-LINDHOLM, Carita, "Chapter 1: ADR and Business". In: GOLDSMILTH, Jean-Claude, INGEN-HOUSZ, Arnold et al (eds.) *ADR in Business*: Practice and Issues across Countries and Cultures I, Kluwer Law International, 2006, p. 7

[8] Sobre essa hipótese, v. BOTTINO, Celina; PERRONE, Christian; CARNEIRO, Giovana; HERINGER, Leonardo; VIOLA, Mario. Lei Geral de Proteção de Dados Pessoais e Resolução de Conflitos: Experiências internacionais e perspectivas para o Brasil. Instituto de Tecnologia e Sociedade (ITS), Abril de 2020. Disponível em: <https://somos.itsrio.org/report-lgpd-e-resolucao-conflitos>, e demais artigos deste volume.

[9] Para saber mais sobre os princípios e fundamentos da LGPD, v.: SOUZA, Carlos Affonso; MAGRANI, Eduardo; CARNEIRO, Giovana. Lei Geral de Proteção de Dados Pessoais: uma transformação na tutela dos dados pessoais. In: MULHOLLAND, Caitlin. A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020. pp.43-64

[10] MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. Caderno Especial LGPD, p.35-56. São Paulo: Ed. RT, novembro de 2019.

no artigo 23 da lei e considerando os princípios dispostos no artigo 6º. Em segundo, é necessário que se cumpram os "procedimentos para garantir a proteção de dados pessoais", descritos pelos direitos do titular e pelas obrigações dos agentes de tratamento.

Por último – e aqui se encontra o nível mais relevante para fins deste artigo –, em caso de violação ao direito à proteção de dados pessoais, o agente de tratamento está sujeito a sanções administrativas e civis, *i.e.*, a sanções e a reparação. Como bem apontado pela autora, essa etapa é responsável pela efetividade das normas previstas na LGPD[11].

A lei prevê nove (9) hipóteses de sanções administrativas em seu artigo 52[12]: (1) advertência; (2) multa simples; (3) multa diária; (4) publicização da infração; (5) bloqueio dos dados pessoais; (6) eliminação dos dados pessoais; (7) suspensão parcial do funcionamento do banco de dados; (8) suspensão do exercício da atividade de tratamento dos dados pessoais; e (9) a proibição parcial ou total do exercício dessa atividade. Como mencionado na introdução, as multas correspondem a somente duas das nove hipóteses sancionatórias decorrentes da lei.

[11] MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. Caderno Especial LGPD, p.35-56. São Paulo: Ed. RT, novembro de 2019, p.53.

[12] Art. 52 LGPD: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

À ANPD, por sua vez, compete aplicar tais sanções[13], conforme disposto no inciso IV do artigo 55-J[14]. Como se verá no tópico 4, a lei previu parâmetros de gradação dessas sanções, que já revelam a estrutura sancionatória complexa prevista pela lei em prol de um arranjo sancionatório mais efetivo. É importante ressaltar, contudo, que a ANPD tem outras competências em paralelo à sancionatória, igualmente importantes para dar efetividade à lei. São diversas as competências, elencadas no artigo 55-J da LGPD.

O ensaio "O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD)" do projeto conjunto entre o CIPL e o CEDIS-IDP elencou oito (8) prioridades para a ANPD, quais sejam:

> *(1) Preparar a Política Nacional de Proteção de Dados Pessoais e da Privacidade;*
> *(2) Reconhecer boas práticas e exemplos de ponta em programas de governança de dados;*
> *(3) Estabelecer regras, procedimentos e diretrizes para organizações conforme requerido pela LGPD;*
> *(4) Esclarecer disposições da LGPD;*
> *(5) Incentivar a adoção de padrões técnicos da indústria e estabelecer padrões técnicos para as organizações;*
> *(6) Possibilitar transferências internacionais de dados pessoais;*
> *(7) Promover a conscientização sobre proteção de dados e educação de indivíduos e organizações; e*
> *(8) Preparação para a fiscalização regulatória.*[15]

[13] A Lei 14.010/2020 alterou a vigência de parte da lei no que tange as sanções administrativas (artigos 52 a 54), que só entram em vigor no dia 1º de agosto de 2021, conforme o artigo 65, I-A da LGPD. Na verdade, tanto a vigência da lei (todos os dispositivos, mas em especial os que versam sobre tais sanções) quanto a natureza jurídica da ANPD (se como entidade submetida a regime autárquico especial ou se como órgão integrante da Presidência da República, em regime transitório facultativo ou obrigatório) foram alvo de intenso debate no país, fruto de mudanças legislativas que envolveram o Congresso Nacional e a Presidência da República na edição de Medidas Provisórias que versavam sobre a matéria (Medidas Provisórias nº 869, de 27/12/2018 e nº 959, de 29/04/2020). Para saber mais, veja: BORDALO, Rodrigo. 33. Autoridade nacional de proteção de dados: aspectos de organização administrativa. In: LGPD e administração pública: uma análise ampla dos impactos. Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. 1. ed. São Paulo: Thomson Reuters Brasil, 2020; UOL, LGPD entra em vigor sem multa; veja 6 pontos detalhados para ficar de olho. Setembro de 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/09/19/lgpd-entra-em-vigor-sem-ter-fiscalizacao-ativa-ou-multa-entenda-o-que-muda.htm>. Acesso em: 04/11/2020. A necessidade de uma ANPD independente e autônoma também já foi defendida por diversos atores da sociedade. Por exemplo: TEFFE, Chiara Spadaccini e VIOLA, Mario. Proposta: Criação da Autoridade Brasileira de Proteção aos Dados Pessoais. Instituto de Tecnologia e Sociedade (ITS), dezembro de 2019. Disponível em: <https://itsrio.org/pt/publicacoes/proposta-anpd/>. Acesso em: 04/11/2020.

[14] Art. 55-J da LGPD: Compete à ANPD: IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

[15] O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD). *Centre for Information Policy Leadership* (CIPL) e Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP), Abril de 2020.

A última prioridade, por sua vez, é dividida no documento entre o estabelecimento de um procedimento administrativo de execução de sanções administrativas e a implementação de mecanismos para receber petições e reclamações dos titulares de dados. Quanto à primeira, conclui-se que:

> *"A ANPD deve, portanto, desenvolver e ser transparente em relação a seus procedimentos e prioridades de execução da LGPD, inclusive no que tange a como ela calculará multas. Estas devem levar em consideração a gravidade da atividade infratora, seus riscos para os indivíduos, assim como medidas de mitigação tomadas pelas organizações no contexto de seus esforços de implementação do princípio de accountability e de seus programas de governança de dados."*[16]

Como se pode ver, ainda há um longo caminho a ser percorrido para um efetivo exercício da competência sancionatória da ANPD. A coexistência de todas as outras competências em paralelo à sancionatória ressalta que o modelo previsto para a aplicação da lei não é voltado somente à aplicação de multas. Se trata, na verdade, de um arranjo holístico em que as multas são, de fato, fator importante, mas não central – como o sensacionalismo em torno da lei insiste em argumentar.

O "temor" dos diferentes atores em relação às multas, porém, não é injustificado. Como demonstraremos a seguir, autoridades de proteção de dados ao redor do globo têm aplicado diversas multas, que obviamente cumprem seu papel no estímulo dos agentes de tratamentos a se adequarem em relação à lei.

2. APLICAÇÃO DE MULTAS POR AUTORIDADES DE PROTEÇÃO DE DADOS PESSOAIS

Entre 25 de maio de 2018, data da entrada em vigor da Regulação Geral de Proteção de Dados da União Europeia (General Data Protection Regulation – "GDPR"), e 27 de janeiro de 2020, as multas aplicadas em 28 países nos quais o diploma era aplicável somavam 114 milhões de euros.[17] Considerando a gama de países e o limite máximo de multa de até 4% do faturamento anual (artigo 83 do GDPR), o número não é tão alto quanto pode parecer.

[16] O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD). *Centre for Information Policy Leadership* (CIPL) e Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP), Abril de 2020, p.17.

[17] DLA Piper GDPR data breach survey: January 2020. Disponível em: <https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/>. Acesso em 04/11/2020.

No mesmo sentido, as multas bilionárias repercutidas mundialmente não necessariamente revelam a prática das autoridades de supervisão. Por exemplo, o total aplicado pela autoridade de proteção de dados francesa (*Comission Nationale de l'Informatique et des Libertés* – "CNIL") foi apurado em 51 milhões de euros. Desse valor, 50 milhões foi referente a um caso específico. Oito meses após a entrada em vigor do GDPR, foi esse o valor da multa aplicada pela CNIL à Google LLC ("Google"), pelo uso indevido de dados pessoais de usuários, notadamente na personalização de anúncios e propagandas no sistema Android.[18]

São diversas as multas já aplicadas no contexto do GDPR, nas diferentes autoridades de proteção de dados espalhadas pela Europa[19]. O Recital 150 do GDPR[20] explicita que o Regulamento deixou a cargo de cada autoridade nacional a determinação do valor das multas, mas estabeleceu um valor máximo e alguns critérios para o cálculo das mesmas. Esses critérios são listados no artigo 83(2) do GDPR, e os itens 83(4) e (5) estabelecem dois valores máximos de multa (10 milhões de euros, ou 2% do rendimento anual, e 20 milhões de euros, ou 4% do rendimento anual, respectivamente), a depender do tipo de infração.[21]

[18] Em resumo, a CNIL baseou o mérito de sua decisão na falta de transparência de informação e na utilização dos dados, e na falta de base legal para o tratamento dos mesmos. CNIL, Deliberação do Comitê Restrito SAN-2019-001, de 21 de janeiro de 2019, proferindo uma sanção financeira contra o GOOGLE LLC. Disponível, em inglês e na íntegra, em: <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf>.

[19] Para uma relação de todas as multas aplicadas com base no GDPR, veja: European Data Protection Board, National News. Disponível em: <https://edpb.europa.eu/news/national-news/2020_en>. Acesso em 04/10/2020; GDPR Enforcement Tracker. Disponível em: <https://www.enforcementtracker.com/>. Acesso em 04/11/2020.

[20] Em tradução livre: "A fim de reforçar e harmonizar as sanções administrativas para violações do presente regulamento, as autoridades de controle deverão ter competência para impor multas administrativas. O presente regulamento deverá definir as violações e o montante máximo e o critério de fixação do valor das multas daí decorrentes, que deverá ser determinado pela autoridade de controle competente, em cada caso individual, tendo em conta todas as circunstâncias relevantes da situação específica, ponderando devidamente, em particular, a natureza, a gravidade e a duração da violação e das suas consequências e as medidas tomadas para garantir o cumprimento das obrigações constantes do presente regulamento e para prevenir ou atenuar as consequências da infração. Sempre que forem impostas multas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101 e 102 do TFUE para esse efeito. Sempre que forem impostas multas a pessoas que não sejam empresas, a autoridade deverá levar em conta o nível geral de rendimentos no Estado-Membro, bem como a situação económica da pessoa em questão, no momento de estabelecer o valor adequado da multa. O procedimento de controle da coerência pode ser utilizado igualmente para a promoção de uma aplicação coerente das multas. Cabe aos Estados-Membros determinar se as autoridades públicas deverão estar sujeitas a multas, e em que medida. A imposição de uma multa ou o envio de um aviso não afetam o exercício de outros poderes das autoridades de controle ou a aplicação de outras sanções previstas no presente regulamento." (grifos nossos) (Recital 150 do GDPR).

[21] Algumas autoridades de proteção de dados têm documentos específicos detalhando as políticas regulatórias a respeito do tema. Veja, por exemplo, a da autoridade britânica, *Information Comissioner's Office* (ICO): UK, ICO, Regulatory Action Policy 2017-2021. Disponível em: < https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf>. Acesso em 04/11/2020.

A LGPD traz, no parágrafo 1º do artigo 52, parâmetros e critérios a se observar na análise do caso concreto que considere a aplicação de uma multa. São os seguintes: a gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa fé do infrator, a vantagem auferida ou pretendida e a condição econômica do infrator, a reincidência, o grau do dano e a cooperação do infrator. O parágrafo 4º dispõe que a ANPD pode considerar o faturamento total da empresa ou grupo de empresas. Os artigos 53 e 54 apresentam regras quanto à metodologia para cálculo do valor da multa, a ser definida pela ANPD após consulta pública, e requisitos procedimentais para sua aplicação.[22]

O parágrafo 7º, por sua vez, deixa clara a possibilidade de conciliação direta entre o controlador e o titular no caso de vazamentos individuais ou de acessos não autorizados[23], apesar de permanecer silente quanto ao papel da ANPD no âmbito da resolução de tal disputa.

De qualquer maneira, não se deve ignorar a possibilidade de celebração de compromisso entre a ANPD e o agente de tratamento, à luz da disposição do inciso XVII do artigo 55-J, que trata das competências da Autoridade:

> *XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;*

Nesse sentido, é cada vez mais relevante tratar da implementação da competência sancionatória da ANPD de maneira holística, considerando não apenas a possibilidade de aplicação de multas (incisos II e II do artigo 52 da LGPD), como também os parâmetros necessários para sua gradação e, principalmente, a possibilidade de celebração de compromissos com os agentes de tratamento (inciso XVII do artigo 55-J da LGPD). Essa é, afinal, a tendência vista em processos administrativos sancionadores em outras searas, como exporemos a seguir.

[22] Sobre a necessidade de parâmetros no cálculo do valor das multas, Francisco Zardo argumenta que as previsões referentes às multas simples e diária da lei são normas de eficácia limitada, aplicáveis somente após a regulamentação pela ANPD (ZARDO, Francisco. 38. As sanções administrativas de multa simples e multa diária na LGPD, item 5. In: LGPD e administração pública: uma análise ampla dos impactos. Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. 1. ed. São Paulo: Thomson Reuters Brasil, 2020).
[23] Artigo 52 da LGPD, § 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo. (grifos nossos)

3. A CELEBRAÇÃO DE ACORDOS NO ÂMBITO DE PROCESSOS ADMINISTRATIVOS SANCIONADORES NO DIREITO BRASILEIRO

Desde a década de 1970, em especial, a partir da crise do Estado-providência, teve início um debate mais intenso sobre a possibilidade de uma relação mais colaborativa entre a Administração Pública e os administrados[24]. Mesmo antes, no início do século XX, já se podia vislumbrar o surgimento de um modelo que previa uma maior participação dos indivíduos, das comunidades e da sociedade civil nas questões de natureza pública e nas decisões políticas[25]. Influenciado por essas mudanças, o direito administrativo contemporâneo tende a valorizar a participação dos administrados na formação da conduta administrativa, em detrimento da adoção de uma conduta mais autoritária e imperativa[26].

A questão, contudo, era objeto de inúmeras controvérsias. Por muitos anos, vedou-se à Administração Pública a adoção de soluções consensuais em qualquer hipótese com base (i) no princípio da legalidade[27]; (ii) em uma interpretação específica do princípio da indisponibilidade do interesse público[28]; (iii) bem como do dogma da supremacia do interesse público[29-30]. No que concerne ao primeiro óbice, tradicionalmente, adotava-se uma interpretação mais restrita do princípio da legalidade, segundo a qual todo ato da

[24] BAPTISTA, Patrícia. *Transformações do Direito Administrativo*. 2. ed. rev., ampl. e atual., Rio de Janeiro: Lumen Juris, 2018, p. 180-183; MONTEIRO, Gabriela Reis Paiva; TELÉSFORO, Rachel Lopes, "A atividade consensual da administração pública e as soluções consensuais na defesa da concorrência". In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (orgs.), *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias, Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2016, p. 310; LOPES, Paula Lino da Rocha. Atuação administrativa consensual: acordo substitutivo envolvendo atos de improbidade administrativa. *Revista de Processo*, v. 274, 2017, versão eletrônica, p. 3.

[25] GONÇALVES, Cláudio Cairo, "O Princípio da Consensualidade no Estado Democrático de Direito - Uma Introdução", *Revista de Direito Administrativo*, v. 232, 2003, p. 105.

[26] TÁCITO, Caio, "Direito administrativo participativo", *Revista de Direito Administrativo*, n. 209, 1997, p. 4.

[27] Sobre o tema, v. BERMAN, José Guilherme. Direito administrativo consensual, acordo de leniência e ação de improbidade (2015). XXIX Congresso Brasileiro de Direito Administrativo do Instituto Brasileiro de Direito Administrativo Disponível em: <http://www.bmapi.com.br/arquivos/Artigos/artigo_ibda_jgb.pdf>. Acesso em: 04/11/2020, p. 2-3.

[28] Sobre o tema, v. MOREIRA NETO, Diogo de Figueiredo, "Novos institutos consensuais da ação administrativa", *Revista de Direito Administrativo – RDA*, v. 231, 2003, p. 154; NEVES, Rodrigo Santos. Audiências de conciliação e a fazenda publica: o dogma da indisponibilidade do interesse público em juízo. *Revista dos Tribunais*, v. 990, 2018, versão eletrônica, p. 1-2.

[29] Sobre o tema, v. MOREIRA NETO, Diogo de Figueiredo, "Novos institutos consensuais da ação administrativa", *Revista de Direito Administrativo – RDA*, v. 231, 2003, p. 138; BERMAN, José Guilherme. Direito administrativo consensual, acordo de leniência e ação de improbidade (2015). XXIX Congresso Brasileiro de Direito Administrativo do Instituto Brasileiro de Direito Administrativo Disponível em: <http://www.bmapi.com.br/arquivos/Artigos/artigo_ibda_jgb.pdf>. Acesso em: 04/11/2020, p. 2-3

[30] Para uma análise mais detida sobre o tema, v. PALMA, Juliana Bonarcorsi de, "*Sanção e Acordo na Administração Pública*", São Paulo: Malheiros Editores, 2015, p. 149-150; 166-188.

Administração deveria estar embasado em uma norma legal expressa[31]. Atualmente, contudo, prevalece a teoria de que a Administração Pública está vinculada ao *bloco de legalidade*, e, consequentemente, seus atos devem se *"coadunar com os princípios, normas, leis formais e práticas informativas do regime jurídico-administrativo"*[32]. Sendo esse o caso, exceto nas hipóteses em que há comando legal expresso vendando a adoção de soluções consensuais, em geral, a Administração poderia celebrar instrumentos consensuais[33].

Quanto à indisponibilidade do interesse público, além de alguns autores apontarem a ausência de previsão normativa nesse sentido[34], vale destacar o entendimento de Diogo de Figueiredo Moreira Neto, segundo o qual "*jamais se cogita de negociar o interesse público, mas de negociar os modos de atingi-lo com maior eficiência*"[35]. Em verdade, em sendo a autocomposição uma forma eficiente de resolver conflitos, Egon Bockmann Moreira e Leila Cuéllar afirmam que haveria intenso interesse público na utilização de soluções consensuais pela Administração Pública[36]. Quanto ao ponto, registra-se que o Supremo Tribunal Federal – STF, ao menos em uma ocasião, reconheceu que a celebração

[31] BERMAN, José Guilherme. Direito administrativo consensual, acordo de leniência e ação de improbidade (2015). XXIX Congresso Brasileiro de Direito Administrativo do Instituto Brasileiro de Direito Administrativo Disponível em: <http://www.bmapi.com.br/arquivos/Artigos/artigo_ibda_jgb.pdf>. Acesso em: 04/11/2020, p. 3.

[32] SHIRATO, Vitor Rhein; PALMA, Juliana Bonacorsi. Consenso e Legalidade: vinculação da atividade administrativa consensual ao direito. *Revista Eletrônica sobre a Reforma do Estado*, n. 24, dez/jan/fev 2011, p. 20-21.

[33] SHIRATO, Vitor Rhein; PALMA, Juliana Bonacorsi. Consenso e Legalidade: vinculação da atividade administrativa consensual ao direito. *Revista Eletrônica sobre a Reforma do Estado*, n. 24, dez/jan/fev 2011, p. 20-21.

[34] PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 177.

[35] MOREIRA NETO, Diogo de Figueiredo, "Novos institutos consensuais da ação administrativa", *Revista de Direito Administrativo – RDA*, v. 231, 2003, p. 154. V. também: ARAGÃO, Alexandre dos Santos, "A consensualidade no Direito Administrativo: acordos regulatórios e contratos administrativos", *Revista de Informação Legislativa*, v. 42, n. 167, 2005, p. 293; LOPES, Paula Lino da Rocha. Atuação administrativa consensual: acordo substitutivo envolvendo atos de improbidade administrativa. *Revista de Processo*, v. 274, 2017, versão eletrônica, p. 6; SHIRATO, Vitor Rhein; PALMA, Juliana Bonacorsi. Consenso e Legalidade: vinculação da atividade administrative consensual ao direito. *Revista Eletrônica sobre a Reforma do Estado*, n. 24, dez/jan/fev 2011, p. 18-19.

[36] MOREIRA, Egon Bockamnn; CUÉLLAR, Leila, "*Administração Pública e mediação: notas fundamentais*". Disponível em: https://edisciplinas.usp.br/pluginfile.php/4241820/mod_resource/content/1/cu%C3%A9llar%2C%20leila%3B%20moreira%2C%20egon%20bockmann%20-%20administra%C3%A7%C3%A3o%20p%C3%BAblica%20e%20media%C3%A7%C3%A3o%20....pdf . Acesso em 20.mar.2020, p. 3-4. V. Também: PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 178.

de um acordo pela Administração Pública era a solução "*que melhor atenderá à ultimação deste interesse* [público]"[37].

A supremacia do interesse público, por sua vez, após intenso debate, também pode-se considerar como um conceito superado, ao menos, para parte significativa dos autores[38]. Ao invés de se falar em uma supremacia absoluta do interesse público sobre os interesses e direitos fundamentais dos indivíduos – que sequer teria previsão normativa – , dever-se-ia se valer da técnica da ponderação para adotar a solução que maximizasse o atendimento de todos os interesses em conflito[39], especialmente tendo em vista a impossibilidade de se identificar um *único* interesse público em abstrato cuja tutela deveria ser priorizada, ante a possível existência de diversos interesses públicos merecedores de guarida[40]. De toda forma, ainda que se considerasse existir uma supremacia *a priori* do interesse público, a adoção de um ato consensual pela Administração Pública poderia corresponder à *satisfação* deste interesse, e não à sua desconsideração em prol do interesse exclusivamente privado[41].

Na linha dessas considerações, parte da literatura jurídica já adotava o entendimento de Juliana de Palma, segundo a qual "a princípio a atuação administrativa consensual pode envolver qualquer objeto do direito administrativo, ressalvadas as vedações legais

[37] STF, j. 04.jun.2002, RE nº 253.885/MG, Relª. Minª. Ellen Gracie: "Poder Público. Transação. Validade. Em regra, os bens e o interesse público são indisponíveis, porque pertencem à coletividade. É, por isso, o Administrador, mero gestor da coisa pública, não tem disponibilidade sobre os interesses confiados à sua guarda e realização. Todavia, há casos em que o princípio da indisponibilidade do interesse público deve ser atenuado, mormente quando se tem em vista que a solução adotada pela Administração é a que melhor atenderá à ultimação deste interesse. Assim, tendo o acórdão recorrido concluído pela não onerosidade do acordo celebrado, decidir de forma diversa implicaria o reexame da matéria fático-probatória, o que é vedado nesta instância recursal (Súm. 279/STF). Recurso extraordinário não conhecido.". V. Também: GUERRA, Sérgio; PALMA, Juliana Bonarcosi de, "Art. 26 da LINDB. Novo regime jurídico de negociação com a Administração Pública", *Revista de Direito Administrativo*, Edição Especial: Direito Público na Lei de Introdução às Normas de Direito Brasileiro – LINDB (Lei nº 13.655/2018), 2018, p. 145.
[38] MARQUES NETO, Floriano de Azevedo; FREITAS, Rafael Véras de, *Comentários à Lei nº 13.655/2018 (Lei da Segurança para Inovação Pública)*, 2ª reimpr., Belo Horizonte: Fórum, 2019, p. 104-105.
[39] MOREIRA NETO, Diogo de Figueiredo, "Novos institutos consensuais da ação administrativa", *Revista de Direito Administrativo – RDA*, v. 231, 2003, p. 138; PALMA, Juliana Bonarcorsi de, "*Sanção e Acordo na Administração Pública*", São Paulo: Malheiros Editores, 2015, p. 170-171; BERMAN, José Guilherme. Direito administrativo consensual, acordo de leniência e ação de improbidade (2015). XXIX Congresso Brasileiro de Direito Administrativo do Instituto Brasileiro de Direito Administrativo Disponível em: <http://www.bmapi.com.br/arquivos/Artigos/artigo_ibda_jgb.pdf>. Acesso em: 04/11/2020, p. 3.
[40] SHIRATO, Vitor Rhein; PALMA, Juliana Bonacorsi. Consenso e Legalidade: vinculação da atividade administrative consensual ao direito. *Revista Eletrônica sobre a Reforma do Estado*, n. 24, dez/jan/fev 2011, p. 18; BERMAN, José Guilherme. Direito administrativo consensual, acordo de leniência e ação de improbidade (2015). XXIX Congresso Brasileiro de Direito Administrativo do Instituto Brasileiro de Direito Administrativo Disponível em: <http://www.bmapi.com.br/arquivos/Artigos/artigo_ibda_jgb.pdf>. Acesso em: 04/11/2020, p. 3.
[41] PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 171-172.

ou, ainda, os casos de vinculação administrativa"[42]. Afinal, ao ver da autora, entendimento contrário, que limitasse a possibilidade de acordos apenas aos direitos patrimoniais disponíveis, por exemplo, tornaria inviável qualquer negociação de prerrogativas públicas, como em acordos integrativos[43] e substitutivos[44-45], e inviabilizaria, por exemplo, a negociação e celebração de acordos de leniência, no qual a Administração Pública garante imunidade e/ou redução de sanções aplicáveis àqueles que se comprometem a colaborar e fornecer informações às autoridades[46].

No âmbito específico do direito administrativo sancionador, somavam-se aos óbices já mencionados[47], a ideia de que, ante a detecção de uma infração ou ilegalidade, a única alternativa disponível à Administração Pública seria a aplicação de sanções aos envolvidos, sendo-lhe vedada a opção de negociar com infratores[48]. O modelo baseado na imposição de multas, todavia, mostrou-se pouco eficiente: no âmbito específico das multas aplicadas por agências reguladoras, constatou-se que muitas das multas aplicadas não foram arrecadadas[49].

Nesse cenário, passou-se a cogitar a adoção de instrumentos que, em substituição à aplicação de multas, priorizassem a assinatura de "*compromissos, por parte dos atores regulados, de reparação de danos, alteração de comportamentos ou medidas compensatórias que tragam benefícios à sociedade e contribuam para a consecução dos*

---

[42] PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 188.

[43] "Os acordos integrativos caracterizam-se por precederem o provimento administrativo final, sem o substituir, razão pela qual também são denominados acordos endoprocedimentais ou acordos preliminaries". PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 248.

[44] "Os acordos substitutivos caracterizam-se pelo efeito terminativo do processo administrativo no qual são celebrados. Quando firmados, estes acordos substituem a decisão unilateral e imperativa da Administração Pública ou findam o processo instaurado para a conformação do provimento administrativo." PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 252.

[45] PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 185.

[46] Cf. CANETTI, Rafaela Coutinho, "Os acordos de leniência da Lei nº 12.846/2013". In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (orgs.), *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias, Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2016, p. 333; MONTEIRO, Gabriela Reis Paiva; TELÉSFORO, Rachel Lopes, "A atividade consensual da administração pública e as soluções consensuais na defesa da concorrência". In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (orgs.), *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias, Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2016, p. 325.

[47] LOPES, Paula Lino da Rocha. Atuação administrativa consensual: acordo substitutivo envolvendo atos de improbidade administrativa. *Revista de Processo*, v. 274, 2017, versão eletrônica, p. 5

[48] Cf. MARRARA, Thiago. Acordos de leniência no processo administrativo brasileiro: modalidades, regime jurídico e problemas emergentes. *Revista Digital de Direito Administrativo*, v. 2, n. 2, 2015, p. 511.

[49] Cf. RAGAZZO, Carlos Emmanuel Joppert; FRANCE, Guilherme de Jesus; VIANNA, Mariana Tavares de Carvalho. Regulação Consensual: a experiência das Agências Reguladoras de Infraestrutura com Termos de Ajustamento de Conduta. *Revista Estudos Institucionais*, v. 3, n. 1, 2017, p. 91.

objetivos de política pública"[50]. Além de proporcionar uma redução nas despesas[51], – por exemplo, de recursos despendidos em investigações e procedimentos administrativos –, outras vantagens comumente apontadas são a maior celeridade na solução das disputas[52] e o fato de que o particular teria mais incentivos a cumprir espontaneamente os termos de uma solução negociadas do que uma decisão imposta[53]. Ademais, em áreas específicas, como no direito concorrencial, a solução mais rápida também evitaria eventuais impactos negativos no mercado decorrentes do prolongamento de condutas anticompetitivas[54].

Os setores percussores na adoção do soluções consensuais foram o de antitruste, após a edição da Lei nº 8.884/1994, e o de mercado de capitais, em razão das alterações promovidas pela Lei nº 9.457/1997[55]. Na sequência, diversas agências reguladoras também passaram a prever a possibilidade de assinatura de instrumentos consensuais, como, por exemplo, a ANTT (Resoluções no 442/2004 e 847/2005), ANTAQ (Resolução no 987/2008 e, posteriormente, Resolução no 3.259/2014); ANAC (Resolução no 199/2011), ANATEL (Resolução no 629/2013)[56]. Atualmente, após a inclusão do artigo 26 na Lei de Introdução às Normas do Direito Brasileiro – LINDB (Decreto-Lei nº 4.657/1942)[57], passou a existir no ordenamento jurídico brasileiro permissivo genérico

[50] RAGAZZO, Carlos Emmanuel Joppert; FRANCE, Guilherme de Jesus; VIANNA, Mariana Tavares de Carvalho. Regulação Consensual: a experiência das Agências Reguladoras de Infraestrutura com Termos de Ajustamento de Conduta. *Revista Estudos Institucionais,* v. 3, n. 1, 2017, p. 91.

[51] PALMA, Juliana Bonarcorsi de, "*Sanção e Acordo na Administração Pública*", São Paulo: Malheiros Editores, 2015, p. 248.

[52] CF. MOREIRA NETO, Diogo de Figueiredo, "Novos institutos consensuais da ação administrativa", *Revista de Direito Administrativo – RDA*, v. 231, 2003, p. 141; SHIRATO, Vitor Rhein; PALMA, Juliana Bonacorsi. Consenso e Legalidade: vinculação da atividade administrative consensual ao direito. *Revista Eletrônica sobre a Reforma do Estado*, n. 24, dez/jan/fev 2011, p. 15.

[53] SHIRATO, Vitor Rhein; PALMA, Juliana Bonacorsi. Consenso e Legalidade: vinculação da atividade administrative consensual ao direito. *Revista Eletrônica sobre a Reforma do Estado*, n. 24, dez/jan/fev 2011, p. 5; RAGAZZO, Carlos Emmanuel Joppert; FRANCE, Guilherme de Jesus; VIANNA, Mariana Tavares de Carvalho. Regulação Consensual: a experiência das Agências Reguladoras de Infraestrutura com Termos de Ajustamento de Conduta. *Revista Estudos Institucionais,* v. 3, n. 1, 2017, p. 95.

[54] PALMA, Juliana Bonarcorsi de, "*Sanção e Acordo na Administração Pública*", São Paulo: Malheiros Editores, 2015, p. 258; MONTEIRO, Gabriela Reis Paiva; TELÉSFORO, Rachel Lopes, "A atividade consensual da administração pública e as soluções consensuais na defesa da concorrência". In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (orgs.), *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias, Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2016, p. 317.

[55] PALMA, Juliana Bonarcorsi de, *Sanção e Acordo na Administração Pública*, São Paulo: Malheiros Editores, 2015, p. 201.

[56] RAGAZZO, Carlos Emmanuel Joppert; FRANCE, Guilherme de Jesus; VIANNA, Mariana Tavares de Carvalho. Regulação Consensual: a experiência das Agências Reguladoras de Infraestrutura com Termos de Ajustamento de Conduta. *Revista Estudos Institucionais,* v. 3, n. 1, 2017.

[57] Decreto-Lei nº 4.657/1942, art. 26: "Para eliminar irregularidade, incerteza jurídica ou situação contenciosa na aplicação do direito público, inclusive no caso de expedição de licença, a autoridade administrativa poderá, após oitiva do órgão jurídico e, quando for o caso, após realização de consulta pública, e presentes razões de relevante interesse geral, celebrar compromisso com os interessados, observada a legislação aplicável, o qual só produzirá efeitos a partir de sua publicação oficial. Regulado pelo Decreto 9.830/2019.

para que que autoridade administrativa celebre compromissos, independentemente de lei ou regulamento específico[58].

4. CONCLUSÃO: POR UMA VISÃO MENOS PUNITIVISTA E MAIS CONSENSUAL DA ATUAÇÃO DA ANPD

A possibilidade de adoção de soluções consensuais no âmbito da ANPD foi expressamente incluída na lei (artigo 55-J, XVII, LGPD), na linha do disposto na LINDB e da prática de outras autoridades públicas dotadas de competência para impor sanções administrativas. Conforme disposto no tópico anterior, a solução de conflitos pela via consensual pode ser uma alternativa eficiente e vantajosa para a Administração Pública.

A mera previsão legal, todavia, não é suficiente para assegurar que soluções consensuais serão implementadas, tampouco que os potenciais benefícios serão gozados. Conforme apontam Carlos Ragazzo, Guilherme France e Mariana Vianna, que realizaram um amplo estudo dos instrumentos consensuais implementados no âmbito das agências reguladoras, para que a adoção de métodos consensuais ofereça as vantagens descritas, é necessário que suas regras e condições sejam previstas de forma clara e objetiva[59]. Seria importante, portanto, que fossem elaboradas normas mais específicas regulando o procedimento para celebração de acordos no âmbito de um processo administrativo na ANPD.[60]

Ademais, para assegurar que o interesse público não seja desconsiderado para satisfazer exclusivamente interesses privados no âmbito de uma negociação, é importante que sejam impostos limites ao administrador[61]. Como não poderia deixar de ser,

---

[58] GUERRA, Sérgio; PALMA, Juliana Bonarcosi de, "Art. 26 da LINDB. Novo regime jurídico de negociação com a Administração Pública", *Revista de Direito Administrativo*, Edição Especial: Direito Público na Lei de Introdução às Normas de Direito Brasileiro – LINDB (Lei nº 13.655/2018), 2018, p. 140.

[59] RAGAZZO, Carlos Emmanuel Joppert; FRANCE, Guilherme de Jesus; VIANNA, Mariana Tavares de Carvalho. Regulação Consensual: a experiência das Agências Reguladoras de Infraestrutura com Termos de Ajustamento de Conduta. *Revista Estudos Institucionais*, v. 3, n. 1, 2017, p. 95.

[60] A ANPD elencou o estabelecimento de normativos para aplicação do artigo 52 e seguintes da LGPD como um dos temas prioritários da Agenda Regulatória 2021-2022, a partir da Portaria ANPD nº 11, de 27 de janeiro de 2021. Segundo o cronograma disponibilizado, a previsão de início do processo de regulamentação é o 1º semestre de 2021. O prazo parece ter se materializado, tendo em vista a publicação, em 28 maio de 2021, de minuta da norma de fiscalização da ANPD no portal eletrônico Participa + Brasil e abertura de consulta pública para comentários e sugestões ao documento. A minuta foi tímida ao tratar do tema do presente artigo, dispondo, no artigo 52, que "o termo de ajustamento de conduta no âmbito do processo administrativo sancionador seguirá regulamentação própria da ANPD e legislação aplicável.". Disponível em: <https://www.gov.br/participamaisbrasil/norma-de-fiscalizacao-da-anpd>. Acesso em: 30/06/2021.

[61] MONTEIRO, Gabriela Reis Paiva; TELÉSFORO, Rachel Lopes, "A atividade consensual da administração pública e as soluções consensuais na defesa da concorrência". In: LEAL, Fernando;

procedimentos consensuais e a celebração de acordos com a Administração Pública devem sempre observar os princípios da legalidade, impessoalidade e a moralidade[62] e, de forma mais específica, devem garantir o cumprimento da objetividade e da isonomia[63].

Esses foram alguns entre os tantos outros questionamentos que circundam o exercício da competência sancionatória da ANPD. A proteção de dados pessoais, apesar de muitas vezes tratada como disciplina autônoma, guarda relação com outros institutos já desenvolvidos na doutrina e na prática jurídica, sendo necessário resgatar e relacionar avanços e teses construídas em outros momentos. Esperamos, assim, que a ANPD busque, junto a outras autoridades e agências reguladoras brasileiras, a execução de um processo sancionatório aberto à consensualidade.

REFERÊNCIAS

ARAGÃO, Alexandre dos Santos, A consensualidade no Direito Administrativo: acordos regulatórios e contratos administrativos. *Revista de Informação Legislativa*, v. 42, n. 167, 2005.

BAPTISTA, Patrícia. *Transformações do Direito Administrativo*. 2. ed. rev., ampl. e atual., Rio de Janeiro: Lumen Juris, 2018.

BERMAN, José Guilherme. Direito administrativo consensual, acordo de leniência e ação de improbidade (2015). XXIX Congresso Brasileiro de Direito Administrativo do Instituto Brasileiro de Direito Administrativo Disponível em: <http://www.bmapi.com.br/arquivos/Artigos/artigo_ibda_jgb.pdf>. Acesso em: 04/11/2020.

MENDONÇA, José Vicente Santos de (orgs.), *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias, Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2016, p. 315. V. também: ARAGÃO, Alexandre dos Santos, "A consensualidade no Direito Administrativo: acordos regulatórios e contratos administrativos", *Revista de Informação Legislativa*, v. 42, n. 167, 2005, p. 298.

[62] ARAGÃO, Alexandre dos Santos, "A consensualidade no Direito Administrativo: acordos regulatórios e contratos administrativos", *Revista de Informação Legislativa*, v. 42, n. 167, 2005, p. 298; MONTEIRO, Gabriela Reis Paiva; TELÉSFORO, Rachel Lopes, "A atividade consensual da administração pública e as soluções consensuais na defesa da concorrência". In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (orgs.), *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias, Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2016, p. 315.

[63] MONTEIRO, Gabriela Reis Paiva; TELÉSFORO, Rachel Lopes, "A atividade consensual da administração pública e as soluções consensuais na defesa da concorrência". In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (orgs.), *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias, Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2016, p. 315.

BOTTINO, Celina; PERRONE, Christian; CARNEIRO, Giovana; HERINGER, Leonardo; VIOLA, Mario. Lei Geral de Proteção de Dados Pessoais e Resolução de Conflitos: Experiências internacionais e perspectivas para o Brasil. Instituto de Tecnologia e Sociedade (ITS), Abril de 2020. Disponível em: <https://somos.itsrio.org/report-lgpd-e-resolucao-conflitos>. Acesso em: 04/11/2020.

CANETTI, Rafaela Coutinho. Os acordos de leniência da Lei nº 12.846/2013. In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (orgs.). *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, 2016.

DLA Piper GDPR data breach survey: January 2020. Disponível em: <https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/>. Acesso em: 04/11/2020.

GONÇALVES, Cláudio Cairo, "O Princípio da Consensualidade no Estado Democrático de Direito - Uma Introdução", *Revista de Direito Administrativo*, v. 232, 2003.

GUERRA, Sérgio; PALMA, Juliana Bonarcosi de. Art. 26 da LINDB. Novo regime jurídico de negociação com a Administração Pública. *Revista de Direito Administrativo, Edição Especial*: Direito Público na Lei de Introdução às Normas de Direito Brasileiro – LINDB (Lei nº 13.655/2018), 2018.

LOPES, Paula Lino da Rocha. Atuação administrativa consensual: acordo substitutivo envolvendo atos de improbidade administrativa. *Revista de Processo*, v. 274, 2017, versão eletrônica, p. 1-18.

MARQUES NETO, Floriano de Azevedo; FREITAS, Rafael Véras de, *Comentários à Lei nº 13.655/2018 (Lei da Segurança para Inovação Pública)*, 2ª reimpr., Belo Horizonte: Fórum, 2019.

MARRARA, Thiago. Acordos de leniência no processo administrativo brasileiro: modalidades, regime jurídico e problemas emergentes. *Revista Digital de Direito Administrativo*, v. 2, n. 2, 2015, p. 509-527. Disponível em: http://www.revistas.usp.br/rdda/article/view/99195. Acesso em: 04/11/2020.

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. Caderno Especial LGPD, p.35-56. São Paulo: Ed. RT, novembro de 2019.

MONTEIRO, Gabriela Reis Paiva; TELÉSFORO, Rachel Lopes. A atividade consensual da administração pública e as soluções consensuais na defesa da concorrência. In: LEAL, Fernando; MENDONÇA, José Vicente Santos de (Orgs.). *Transformações do direito administrativo*: consequencialismo e estratégias regulatórias. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2016.

MOREIRA NETO, Diogo de Figueiredo, "Novos institutos consensuais da ação administrativa", *Revista de Direito Administrativo – RDA*, v. 231, 2003.

MOREIRA, Egon Bockamnn; CUÉLLAR, Leila, "*Administração Pública e mediação: notas fundamentais*". Disponível em: https://edisciplinas.usp.br/pluginfile.php/4241820/mod_resource/content/1/cu%C3%A9llar%2C%20leila%3B%20moreira%2C%20egon%20bockmann%20-%20administra%C3%A7%C3%A3o%20p%C3%BAblica%20e%20media%C3%A7%C3%A3o%20....pdf. Acesso em: 04/11/2020.

NEVES, Rodrigo Santos. Audiências de conciliação e a fazenda publica: o dogma da indisponibilidade do interesse público em juízo. *Revista dos Tribunais*, v. 990, 2018, versão eletrônica.

O papel da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) conforme a nova Lei Geral de Proteção de Dados Pessoais (LGPD). Centre for Information Policy Leadership (CIPL) e Centro de Direito, Internet e Sociedade do Instituto Brasiliense de Direito Público (CEDIS-IDP), abril de 2020.

PALMA, Juliana Bonarcorsi de, "Sanção e Acordo na Administração Pública", São Paulo: Malheiros Editores, 2015.

RAGAZZO, Carlos Emmanuel Joppert; FRANCE, Guilherme de Jesus; VIANNA, Mariana Tavares de Carvalho. Regulação Consensual: a experiência das Agências Reguladoras de Infraestrutura com Termos de Ajustamento de Conduta. *Revista Estudos Institucionais*, v. 3, n. 1, 2017.

SHIRATO, Vitor Rhein; PALMA, Juliana Bonacorsi. Consenso e Legalidade: vinculação da atividade administrativa consensual ao direito. *Revista Eletrônica sobre a Reforma do Estado*, n. 24, dez/jan/fev 2011.

SOUZA, Carlos Affonso; MAGRANI, Eduardo; CARNEIRO, Giovana. Lei Geral de Proteção de Dados Pessoais: uma transformação na tutela dos dados pessoais. In:

MULHOLLAND, Caitlin. A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020. pp.43-64.

TÁCITO, Caio. Direito administrativo participativo. *Revista de Direito Administrativo*, n. 209, 1997.

UK, ICO, Regulatory Action Policy 2017-2021. Disponível em: < https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf>. Acesso em: 04/11/2020.

VORONOFF, Alice. *Direito administrativo sancionador no Brasil*. Belo Horizonte: Fórum, 2018.

ZARDO, Francisco. 38. As sanções administrativas de multa simples e multa diária na LGPD, item 5. In: LGPD e administração pública: uma análise ampla dos impactos. Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

O TRATAMENTO INADEQUADO DE DADOS NO CONTEXTO CORPORATIVO E O PAPEL DOS MÉTODOS ADEQUADOS DE SOLUÇÃO DE CONFLITOS FRENTE À PRESERVAÇÃO DA REPUTAÇÃO DAS EMPRESAS

Autoria
Ayanne Padilha

Debatedores
Christian Augusto S. Perrone de Oliveira
Maria Regina Rigolon Korkmaz
Rodrigo da Guia

Clicar ou escanear para acesso aos debates relativos a este artigo

RESUMO

O desenvolvimento da tecnologia, o crescente uso e a manipulação das informações demonstraram a necessidade da concretização do direito à autodeterminação informativa. A partir da entrada em vigor da LGPD no ordenamento jurídico, passaram a ser exigidos os direitos dos titulares dos dados e por conseguinte, os deveres dos empresários em operações que envolvam o tratamento de informações pessoais. Nesse sentido, as obrigações impostas pela legislação deverão ser observadas, sob pena de sanções. O presente estudo analisa o sistema multiportas como alternativa eficaz para a solução de conflitos oriundos da referida matéria, em razão do alto nível de morosidade do sistema judiciário e das vantagens que tais técnicas poderão oferecer para determinadas questões. Além disso, este projeto também possui a finalidade de apresentar hipóteses que poderão impactar os ativos empresariais das organizações, tal como a reputação da corporação e o diferencial competitivo da companhia no mercado.

1. INTRODUÇÃO

Os avanços da tecnologia e o crescimento da utilização de dados na economia, evidencia a necessidade de o indivíduo ter controle dos seus próprios dados pessoais. Mesmo antes da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) entrar em

vigência, o ordenamento jurídico do Brasil já possuía alguns diplomas legais que discutiam a matéria da privacidade e proteção dos dados pessoais no país, como a Constituição Federal de 1988, a lei que disciplina o Habeas Data (Lei nº 9.507/97), o Marco Civil da Internet (Lei nº 12.965/14), o Código de Defesa do Consumidor (Lei nº 8.078/90), a Lei do Cadastro Positivo (Lei nº 12.414/11), a Lei de Acesso à Informação (Lei nº 12.527/11), de modo que a LGPD somente fortaleceu e ampliou tais direitos.

Apesar da existência de legislações que já disciplinavam a matéria de privacidade e a proteção de dados, foi a partir da publicação da LGPD que o tema passou a ser visto com mais pertinência para aqueles que realizam o tratamento de informações pessoais. Nessa perspectiva, deverão se adequar à referida legislação toda pessoa física ou jurídica, de direito privado ou público, que realizar qualquer tipo de operação que envolva o processamento de dados pessoais.

É fundamental enxergar a implementação das normas de privacidade e proteção de dados como uma janela de oportunidades à instituição, assim estar aberto à inovação poderá fazer com que a empresa se destaque e se posicione no mercado através de um diferencial competitivo, obtendo, por exemplo, uma maior confiança dos clientes, um maior domínio das atividades que estão sendo realizadas na companhia, o desenvolvimento de novos produtos e entre outras séries de benefícios.

A reputação é um ponto que merece destaque, pois esse fator, quando não observado pela empresa, poderá gerar danos incalculáveis ao negócio. Apesar de serem necessárias a adoção de mitigação de riscos em um projeto de adequação à LGPD, não podemos dispensar a possibilidade de ocorrer algum incidente de segurança que envolva as informações pessoais dos titulares de dados no âmbito da organização e que possa causar algum tipo de dano ao titular.

Sabemos que o crescimento de ações no Poder Judiciário e a sua morosidade é uma realidade enfrentada pelo país, portanto o sistema de justiça brasileiro ainda apresenta um ritmo lento, quando se trata de solução de litígios. Por este motivo, o sistema multiportas pode ser uma alternativa eficiente para a resolução de conflitos oriundos da referida matéria, conforme veremos nos próximos capítulos.

Observa-se que essas poderão ser técnicas viáveis em face do sigilo dos procedimentos, da especialidade do profissional, da flexibilização dos métodos utilizados e da solução eficaz da disputa, benefícios estes que poderão atender à necessidade das partes.

Assim, além da importância do tratamento adequado de dados no contexto corporativo, será esclarecida também a relevância do sistema multiportas e a contribuição que este possui frente à preservação da imagem das empresas.

2. DA AUTODETERMINAÇÃO INFORMATIVA AOS DIREITOS DOS TITULARES E DEVERES DO EMPRESÁRIO

De acordo com a Lei Geral de Proteção de Dados, toda pessoa natural tem assegurada a titularidade de seus dados, sendo garantidos o direito fundamental à liberdade, intimidade e privacidade.

Nesse sentido, a LGPD concretiza o direito de obter controle acerca de suas informações pessoais, garantia intitulada como autodeterminação informativa[1], fundamento incluso no art. 2º, II da referida norma.

Também reconhecida em decisões internacionais como a sentença sobre o Censo Alemão, a autodeterminação informativa, é um direito fundamental que coloca o sujeito no controle dos seus dados pessoais, como aponta o entendimento de Danilo Doneda[2]:

> *A autodeterminação informativa é, inclusive, um dos fundamentos da disciplina da proteção de dados de acordo com a LGPD. Concebido como um direito fundamental, na esteira do direito geral de personalidade, o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações.*

Nesse mesmo cenário ensina Bruno Bioni[3] que o fluxo das informações do sujeito deve atender somente às legítimas expectativas do titular, este não devendo ultrapassar os limites legais estabelecidos e atingir o livre desenvolvimento da pessoa humana.

Nesse prisma, a LGPD[4] define os princípios essenciais da norma, os quais deverão ser observados na atividade de tratamento de dados, isto posto, deverão ser constatados em toda operação de tratamento a boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e por último, a responsabilização e prestação de contas.

---

[1] BODIN de MORAES, Maria Celina. Apresentação. In: RODOTÀ, Stefano. A vida na sociedade de vigilância. Privacidade hoje. Rio de Janeiro: Renovar, 2008, p.15.
[2] DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 168.
[3] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020, p.104
[4] Art. 6, LGPD.

Em que se pese o desenvolvimento da disciplina no Brasil, é importante observar as disposições expressas no texto legal[5], assim são deveres do empresário e direitos do titular de dados: o acesso facilitado às informações sobre o tratamento, que deverão ser disponíveis de forma adequada, ostensiva e com clareza, além de outros tópicos previstos na regulamentação.

A matéria da proteção de dados possui como um dos seus pontos principais a liberdade da informação, portanto é necessário entender que, se por um lado a comunicação adequada é uma obrigação do empresário, por outra vertente, o controle da informação é uma garantia legal do indivíduo[6].

Além do mais, cabe destacar que o empresário tem responsabilidade de informar ao titular das informações pessoais quais são as medidas técnicas e administrativas utilizadas na organização, se estas possuem capacidade de resguardar os dados em caso de acessos não autorizados, bem como circunstâncias acidentais ou até mesmo ilícitas de acesso, eliminação, divulgação, perda ou modificação, de acordo com o que determina o princípio da segurança[7].

A segurança também é uma obrigação que possui como probabilidade a ocorrência de responsabilidade civil da companhia e o possível direito a indenização de acordo com o que a LGPD[8] afirma, desde que seja caracterizado o fato ilícito, o nexo causal e ensejado o dano.

Face ao exposto, é primordial compreendermos que com a ampliação da discussão da temática no cenário nacional, bem como de compartilhamentos de casos envolvendo tratamentos inadequados e incidentes de segurança, a sociedade da informação desenvolve, cada vez mais, consciência acerca da importância que deve ser dada a defesa da privacidade e proteção de dados pessoais.

Dessa forma, é fundamental que o a instituição esteja ciente dos direitos dos titulares e de suas obrigações como controlador ou como operador, sob pena de responsabilização na forma da lei. Isto posto, passaremos abordar sobre a possibilidade

[5] Art. 9, LGPD.
[6] BORELLI, Alessandra; ZAMPERLIN, Emelyn. A importância da conscientização do tema privacidade e proteção de dados nas empresas. In: Blum, Renato Opice; Vainzof, Rony; Moraes, Henrique Fabretti (Org). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1. ed. São Paulo: Thomson Reuters Brasil, 2020, p 367.
[7] Art. 6, VII, LGPD.
[8] Art. 42, LGPD.

da ocorrência de sanções administrativas e judiciais envolvendo a operação inadequada de tratamento de dados pessoais.

3. A Aplicação de Sanções Administrativas e o Crescimento das Ações Judiciais em Virtude do Tratamento Inadequado dos Dados

O sistema de responsabilidade e ressarcimento de danos da LGPD, segundo Maria Celina Moraes et. al., se baseia no disposto pelo princípio da responsabilização e prestação de contas, em outros termos, este corresponde a demonstração de medidas seguras e suficientes que tenham capacidade de certificar o cumprimento da legislação de proteção de dados. Desse modo, podemos concluir que o legislador optou por prevenir e evitar a ocorrência de danos, além de incluir a hipótese do ressarcimento[9].

O regime de responsabilidade civil definido na referida legislação[10] se rege conforme três elementos cruciais, sendo estes: a ocorrência do dano, que decorre do ato ilícito praticado; a violação do instrumento legal pelo agente de tratamento de dados; e a culpa[11].

Pode-se concluir que a imposição do dever de indenizar surge com o enquadramento dos itens citados acima, além disso, cabe ressaltar que o controlador e o operador poderão ser os responsabilizados solidariamente por tais condutas, conforme define a regulamentação[12].

Excepcionalmente, o dispositivo legal apresenta hipóteses em que há exclusão da responsabilidade dos agentes de tratamento, isto posto, estes não serão enquadrados quando provarem que o dano originou de culpa exclusiva do titular ou de terceiros, na hipótese de não haver violação à norma, e quando esses não realizarem a operação de tratamento de dados que lhes é atribuída.[13]

Por outro lado, ficam subordinados às sanções administrativas, os agentes de tratamento que cometerem as infrações previstas no dispositivo legal. Estas serão

[9] MORAES, MARIA CELINA; QUEIROZ, JOÃO QUINELATO. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD, 2019, p.126. Disponível em: https://www.academia.edu/41132175/Autodetermina%C3%A7%C3%A3o_informativa_e_responsabiliza%C3%A7%C3%A3o_proativa_novos_instrumentos_de_tutela_da_pessoa_humana_na_LGDP. Acesso em 01 out 2020.
[10] Art. 42 ao 45, LGPD.
[11] MORAES, MARIA CELINA; QUEIROZ, JOÃO QUINELATO. Op. Cit. p.126.
[12] Art. 42, LGPD.
[13] Art. 43, LGPD.

aplicadas pela Autoridade Nacional de Proteção de Dados, que possui a competência de fiscalizar, zelar, penalizar aquele que desrespeitar o disposto na LGPD[14].

As penalidades serão promovidas após procedimento administrativo conforme esclarece melhor a Minuta de Resolução de Fiscalização para Consulta Pública da ANPD[15], sendo assegurada a ampla defesa, conforme a situação específica do caso, e observado os parâmetros e critérios indicados no escopo normativo da LGPD[16].

Em face da lei nº 14.010/20, as sanções administrativas foram prorrogadas para 01 de agosto de 2021. Assim, mesmo com prazo adiado em um ano até o início da aplicação das sanções administrativas, que são competências exclusivas da ANPD, a judicialização de temas impostos na legislação já é uma realidade no país, no que se tange a responsabilidade civil com os titulares que tiveram seus direitos violados pelos agentes de tratamento, como foi o caso da Construtora Cyrela[17], a qual foi condenada pela justiça ao compartilhar os dados pessoais de um cliente com um parceiro sem a autorização do próprio.

É importante reforçar que as sanções administrativas estabelecidas pela lei são de competência exclusiva da ANPD, todavia é possível que seja promovida ações no Poder Judiciário que versem a respeito de direitos morais e materiais oriundos de um dano provocado pelo tratamento inadequado das informações.

A Lei geral de Proteção de Dados traz uma espécie de diálogo regulamentário que associa tais componentes e demostra a importância do equilíbrio entre estes, assim como estabelecem as parcerias realizadas da ANPD com órgãos do direito do consumidor e com o Conselho Administrativo de Defesa Econômica.

Com isso, podemos constatar que os referidos órgãos poderão atuar em cooperação com a ANPD, fiscalizando as organizações na medida de suas atribuições, com base em sanções de outra natureza e com fundamentos distintos das sanções atribuídas à Autoridade Nacional de Proteção de Dados. Isto posto, a primeira ação promovida no país

[14] Art. 55, J, LGPD.
[15] BRASIL. Autoridade Nacional de Proteção de Dados. Minuta de Resolução de Fiscalização para Consulta Pública. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-publica-sobre-norma-de-fiscalizacao/2021.05.29___Minuta_de_Resolucao_de_fiscalizacao_para_consultapblica.pdf/@@download/file/2021.05.29___Minuta_de_Resolucao_de_fiscalizacao_para_consultapblica.pdf.
[16] Art 52, caput e §1º, LGPD.
[17] AUTOR DESCONHECIDO. Cyrela é condenada a indenizar cliente por violar LGPD. ISTO É dinheiro.Disponível em: https://www.istoedinheiro.com.br/cyrela-e-condenada-a-indenizar-cliente-por-violar-lgpd/.

com os fundamentos da lei, é proposta pelo Ministério Público do Distrito Federal e dos Territórios[18].

Em razão disso, é de se concluir que a judicialização da matéria em proteção de dados no Brasil, provocará um crescimento de demandas no poder judiciário, situação que poderá ser evitada, caso os titulares de dados e os agentes de tratamento desejem utilizar outras vias para a resolução do problema, situação que será tratada nos próximos capítulos.

4. A ADEQUAÇÃO DA LGPD COMO UM DIFERENCIAL COMPETITIVO E A REPUTAÇÃO DA EMPRESA FRENTE AO TRATAMENTO INADEQUADO DE DADOS

A gestão baseada em inovação e competitividade de mercado, pode ser caracterizada como um diferencial da organização frente aos demais concorrentes, desse modo, é importante avistar o procedimento da adequação à Lei Geral de Proteção de Dados como um benefício para os negócios.

Além de buscar as medidas preventivas para estar de acordo com o que a LGPD determina, o processo de conformidade faz com que a empresa esteja aberta à inovação, local onde poderá ser desenvolvido novos produtos e revisões de modelos do negócio, sendo esses pontos significativos que poderão contribuir com o avanço da empresa no mercado[19].

Em consonância com a temática envolvida, o estudo realizado pelo Cisco chega à conclusão de que: "O percentual de empresas que afirma receber benefícios comerciais significativos devido à privacidade (por exemplo, eficiência operacional, agilidade e inovação) cresceu para mais de 70%". Tal pesquisa revela que, apesar do investimento adicional, elevar os níveis de privacidade na organização poderá trazer aos investimentos um retorno positivo para o negócio.

Nessa concepção, a temática da reputação destaca-se por ser um bem intangível e de extrema relevância para as corporações. Podemos trazer à baila o caso da Netshoes[20],

[18] BRASIL. Ministério Público do Distrito Federal e dos Territórios. Ação Civil Pública nº 0730600-90.2020.8.07.0001. Brasília, 2020. Disponível em: https://pje.tjdft.jus.br/consultapublica/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=fb4a04b5a693503d66bf1e444688de24b4b253efd0929626. Acesso em: 25 set 2020.
[19] BIONI, Bruno Ricardo. Inovar pela lei. Revista FGV Executivo, 2019, p.33.
[20]Ministério Público do Distrito Federal e Territórios. MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-

que após ter enfrentado um incidente de segurança no ambiente da empresa, trouxe consigo um impacto positivo para a imagem da empresa.

Ao se utilizar de medidas eficazes para mitigar os riscos da operação, o estabelecimento seguiu as orientações do Ministério Público e por fim acabou realizando um TAC - termo de ajuste de conduta, no valor de R$ 500.000,00 (quinhentos mil reais).

Em contrapartida, diferentemente do incidente sofrido pela Netshoes, o Banco Inter[21] não obteve uma boa repercussão após a negar a ocorrência de vazamento de dados pessoais de seus clientes. Em razão disto, a instituição bancária recebeu a proposta de TAC correspondente a R$ 1.500.000,00 (um milhão e meio), como forma de reparar os danos provocados pelo ocorrido.

Nota-se que além de danos financeiros, um incidente de segurança pode gerar impactos incalculáveis para a imagem do estabelecimento.

De acordo com Viviane Nóbrega Maldonado, é extremamente complexo estimar um valor monetário correto ao dano reputacional da empresa. Não obstante, conforme o Reputation Institute, entidade que classifica e acompanha as reputações de cerca de 7 mil corporações reconhecidas em escala mundial, fatores intangíveis representam 81% da quantia de mercado da empresa, de modo que sua deterioração enseja impacto tangível na performance.[22]

A cultura da conscientização pode chegar a impactar os ativos empresariais, não só em termos da reputação da companhia, mas também sendo provável classificar o referido bem intangível, através das escolhas dos clientes, parceiros de negócios, compras e fusões[23].

Levando em consideração a possibilidade de ocorrência de incidente de segurança no âmbito interno da organização, as práticas adotadas pela empresa serão levadas em consideração com base no que determina a lei, estas podendo atenuar ou agravar a

2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados. Acesso em 15 set 2020.

[21] Ministério Público do Distrito Federal e Territórios. Banco Inter: acordo destinará R$ 1,5 milhão para caridade e combate a crimes cibernéticos. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31.Acesso em: 15 set 2020.

[22] MALDONADO, Viviane. A Lei Geral de Proteção de Dados: objeto, âmbito de aplicação, requisitos, segurança e a necessidade de sua correta implementação. LGPD: Lei Geral de Proteção de Dados pessoais: manual da implementação. In: Maldonado, Viviane Nóbrega (Org). Thomson Reuters Brasil, 2019, p. 29.

[23] BORELLI, Alessandra; ZAMPERLIN, Emelyn. Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. Renato Opice Blum, Rony Vainzof, Henrique Fabretti Moraes, coordenadores. 1. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 382.

responsabilidade dos agentes de tratamentos, como abordado anteriormente nos capítulos anteriores.

É indispensável preservar o entendimento de que é fundamental manter um bom nível de segurança da informação da instituição, pois as sanções promovidas pela ausência de utilização de tais critérios poderão causar penalidades consideráveis para a corporação além do dano reputacional, valor inestimável para a empresa.

Além de tudo, as empresas que possuem uma boa comunicação com público sobre os assuntos que envolvem a segurança da informação, à proteção e aos dados pessoais, são organizações que tendem a se destacar perante as demais.

5. O PAPEL DOS MÉTODOS ADEQUADOS DE SOLUÇÃO DE CONFLITOS EM FACE DE LITÍGIOS ENVOLVENDO PROTEÇÃO DE DADOS

Como se sabe, o sistema multiportas são meios alternativos e eficazes para solucionar conflitos. Em razão do alto índice de litígios concentrados no Poder Judiciário, a arbitragem, mediação, conciliação e negociação surgem como instrumentos viáveis, que visam facilitar a resolução da controvérsia com celeridade e sem a necessidade de as partes utilizarem obrigatoriamente o sistema comum de justiça.

Sendo assim, o sistema multiportas, incentivado pelo Novo Código de Processo Civil[24], aponta uma maior flexibilidade no procedimento e incentiva a cooperação das partes.

Nesse sentido, a Lei Geral de Proteção de dados em seu art. 52, §7, também menciona a possibilidade de utilizar a conciliação direta entre conflitos entre controlador e titular como mecanismo para solução de conflitos em decorrência de vazamento de dados individual ou acessos não autorizados.

De acordo com o que determina o dispositivo, podemos interpretar que também há margem para a utilização da mediação e da negociação, em detrimento da natureza da matéria não impedir o uso das técnicas de tais institutos. Por outro lado, é possível a utilização da arbitragem, desde que o conflito específico atenda aos requisitos do procedimento, que também serão abordados neste capítulo.

[24] MATTOS NETO, Antônio José de. Direitos patrimoniais disponíveis e indisponíveis à luz da arbitragem. In: WALD, Arnoldo (Org.). Doutrinas essenciais: arbitragem e mediação. São Paulo: Revista dos Tribunais, 2014. v. 2, p. 413-431.

Nessa perspectiva, serão abordadas as viabilidades dos meios adequados de resolução de disputas em matéria de proteção de dados, visto que estas poderão ser hipóteses válidas face a realização de acordos advindos da referida temática, para que a sociedade como todo seja beneficiada com a tutela de seus direitos frente à uma eventual violação dados pessoais.

5.1. A possibilidade de realização do procedimento arbitral em disputas envolvendo dados pessoais

O art. 1º da Lei de Arbitragem brasileira[25] dispõe acerca dos critérios para submissão de um determinado conflito à Arbitragem, assim, temos os critérios objetivos e subjetivos. Este se refere a "quem" pode ser parte litigante na arbitragem, ou seja, somente pessoas consideradas capazes podem litigar no procedimento, é a chamada Arbitrabilidade Subjetiva. Enquanto aquele, trata da conhecida Arbitrabilidade Objetiva, o direito posto em disputa, para ser objeto da arbitragem, dispõe de dois critérios, quais sejam: o direito tem que ser patrimonial; e, necessita ser disponível.

Sendo assim, o critério da patrimonialidade não comporta muitos mistérios, o litígio na arbitragem necessita versar acerca de valores pecuniários, de cunho patrimonial. Por sua vez, a doutrina ressalta alguns aspectos acerca da disponibilidade, assim, exemplifica Antônio Mattos Neto[26], que:

> *Direito disponível é o alienável, transmissível, renunciável, transacionável. A disponibilidade significa que o titular do direito pode aliená-lo; transmiti-lo inter vivos ou causa mortis; pode, também, renunciar ao direito; bem como, pode, ainda, o titular transigir seu direito.*

Nesse sentido, de acordo com o que aponta o ensinamento, nota-se que para a efetivação do instituto, há a necessidade de o mérito em questão estar definido como um direito patrimonial disponível. Portanto, a realização do procedimento arbitral está diretamente ligada ao objeto do litígio, ou seja, o conteúdo específico necessita estar alinhado com a arbitrabilidade objetiva e subjetiva.

[25]Art. 1, da lei nº 9307/96: "As pessoas capazes de contratar poderão valer-se da arbitragem para dirimir litígios relativos a direitos patrimoniais disponíveis".
[26]MATTOS NETO, Antônio José de. Direitos patrimoniais disponíveis e indisponíveis à luz da arbitragem. In: WALD, Arnoldo (Org.). Doutrinas essenciais: arbitragem e mediação. São Paulo: Revista dos Tribunais, 2014. v. 2, p. 413-431.

Podemos constatar que na Constituição Federal do Brasil[27], em seu art. 5º, X, o direito à privacidade pertence ao rol de direitos fundamentais. Em contrapartida, o direito a proteção de dados pessoais ainda não possui previsão no texto constitucional, apesar de já haver Proposta de Emenda à Constituição (PEC 17/2019), propondo a inclusão do referido direito na norma mencionada, nesse ponto tal revisão "altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais[28]".

Desse modo, o direito da proteção de dados ainda não se enquadra formalmente como direito fundamental no país, todavia em legislações infraconstitucionais, como no Marco Civil da Internet[29] (Art. 3, III), tal direito pertence ao rol de princípios que disciplinam o uso da internet no país.

Há posicionamentos doutrinários como o de Danilo Doneda, que sugere a proteção de dados como um direito fundamental implícito na Constituição, uma vez que:

> *Contando ou não com a previsão expressa na Constituição Federal, o esforço a ser empreendido pela doutrina e jurisprudência deve se consolidar pelo favorecimento de uma interpretação dos incisos X e XII, do art. 5º mais fiel ano nosso tempo, isto é, reconhecendo a íntima ligação que passam a ostentar os direitos relacionados à privacidade e à comunicação de dados. Dessa forma, seria dado o passo necessário à integração da personalidade em sua acepção mais completa nas vissitudes da Sociedade da Informação.* [30]

Vale ressaltar que face as abordagens legais e teóricas, podemos citar o caso do IBGE[31], julgado pelo Supremo Tribunal Federal em face das Ações Diretas de Inconstitucionalidade de nº 6.387, 6.388, 6.389, 6.390 e 6.393. As ADIs foram propostas em detrimento da inconstitucionalidade da Medida Provisória 954, que previa o compartilhamento de informações pessoais por empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística (IBGE).

---

[27]BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 29 ago 2020.

[28] BRASIL. Proposta de Emenda à Constituição 17/2019. Brasília, Senado Federal. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A95C937D1F1839CF11D6A4904DC09559.proposicoesWebExterno1?codteor=1773684&filename=PEC+17/2019. Acesso em 04 set 2020.

[29] BRASIL. Lei nº 12.965/14. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 30 ago 2020.

[30] DONEDA, Danilo. Op. Cit. p. 264.

[31] Supremo Tribunal Federal. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1. Acesso em 23 set 20.

Tal conflito promoveu o entendimento do tribunal em favor do direito à autodeterminação informativa e consequentemente à proteção dos dados pessoais. Sobre a decisão do STF, comenta Laura Shertel Mendes que:

> *As ADIs se mostram também como uma oportunidade de instituir os parâmetros constitucionais da proteção de dados no Brasil, que poderiam ser aproveitados para os casos de processamento e uso de dados relacionados durante e depois da pandemia. Assim, o reconhecimento expresso de um direito fundamental à proteção de dados pelo STF, por exemplo, seria de grande contribuição. Dessa tutela constitucional poder-se-iam extrair não somente os procedimentos de segurança, transparência e proporcionalidade/necessidade para tratamento de dados*[32]

Não obstante, o direito mencionado já se classifica como direito fundamental em normas internacionais, como na Convenção de 108 de 1981 modernizada[33], Carta de Direitos Fundamentais da União Europeia[34], o Tratado sobre o Funcionamento da União Europeia (TFUE)[35] e entre outros dispositivos estrangeiros.

Por se tratar de um direito da personalidade, dado a natureza da matéria, assim como determina o Relatório LGPD Resolução de Conflitos, promovido pelo Instituto de Tecnologia & Sociedade do Rio (ITS), o procedimento arbitral não é adequado para solucionar conflitos que versem sobre proteção de dados pessoais entre titulares e controladores.[36]

Porém, existem casos que poderão ser passíveis de arbitragem, desde que o objeto em questão retrate aspectos patrimoniais disponíveis. Como exemplo, podemos descrever o surgimento de um conflito entre o controlador e o operador, oriundo da relação contratual entre os agentes de tratamento, sendo este conflito uma consequência patrimonial. Por este motivo, aponta o relatório que tal instituto ainda é uma questão aberta para a legislação brasileira. Todavia, o material aponta que a doutrina internacional

---

[32] MENDES, Laura Shertel. A encruzilhada da proteção de dados no Brasil e o caso do IBGE, 2020 Disponível em: https://www.conjur.com.br/2020-abr-24/laura-shertel-mendes-encruzilhada-protecao-dados. Acesso em 29 set 2020.

[33] UNIÃO EUROPEIA. Convenção 108 +. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 11 set 2020.

[34] UNIÃO EUROPEIA. Carta dos Direitos Fundamentais. Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f. Acesso em: 11 set 2020.

[35] UNIÃO EUROPEIA. Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia. Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12012E%2FTXT. Acesso em: 11 set 2020.

[36] INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. Lei Geral de Proteção de Dados Pessoais e Resoluções de Conflitos: Experiências internacionais e perspectivas para o Brasil.
BOTTINO, Celina; PERRONE, Christian; CARNEIRO, Giovana; HERINFER, Leonardo; VIOLA, Mario (Org.). Relatório LGPD: Resolução de Conflitos. Disponível em: https://itsrio.org/wp-content/uploads/2020/04/Relatorio_LGPDResolucaoConflitos.pdf. Acesso em: 29 ago 2020.

já se inclina a respeito da submissão de litígios referentes à dados pessoais à arbitragem, especialmente em sede de arbitragem comercial internacional[37].

Dessa maneira, pode-se concluir que se tratando de conflito de natureza indisponível e não patrimonial, não há como tal matéria ser passível de arbitragem, todavia caso a temática se demonstre um conflito patrimonial e disponível, não há qualquer óbice para a adoção do procedimento arbitral.

5.2. Mediação, negociação e conciliação

A possibilidade de autocomposição é autorizada mediante o art. 52, § 7º da LGPD, dessa maneira, nos termos do artigo, os vazamentos individuais ou os acessos não autorizados poderão ser matéria de conciliação direta entre as partes envolvidas. Vale ressaltar ainda que, caso não seja realizado acordo, o controlador estará subordinado à aplicação das sanções administrativas da norma.

Contudo, não podemos deixar de mencionar a possibilidade de realização da mediação e negociação nos conflitos envolvendo o direito à proteção de dados, pois estes são métodos de solução de conflitos, que diferentemente da arbitragem, se caracterizam por ter em seus procedimentos a atuação ativa das partes na solução do problema, isto é, uma decisão construída pelas partes é mais eficaz que uma decisão imposta por um terceiro,, assim, a figura do mediador ou dos negociadores auxiliará as partes na finalidade de obter a resolução do mérito de forma consensual.

Assim, o instituto da mediação é um método que conta com a participação de um terceiro imparcial entre as partes. A ideia é que ela restabeleça o diálogo entre os envolvidos, de modo que eles enxerguem, por si mesmos, outros aspectos do impasse, de modo a chegar a uma solução[38]. Nesse caso, o mediador estimulará as partes para que estas possam chegar a uma solução. Enquanto, o mediador deve cooperar para que as próprias partes formulem suas próprias alternativas, o conciliador pode propor soluções no instituo da conciliação.

[37] Ibdem., p 29.
[38] SALLES, Carlos Alberto de. Negociação, mediação, conciliação e arbitragem: curso de métodos adequados de solução de controvérsias. Forense, 2020, p. 44

Por outro lado, a negociação é uma forma de autocomposição direta entre as partes, diferentemente da mediação e conciliação, que são formas de autocomposição assistidas por terceiro – o mediador e o conciliador[39].

Por se tratar de métodos de natureza auto compositiva, ambas as partes poderão chegar a um acordo benéfico, isto posto, uma das maiores características contidas pela LGPD é o "empoderamento" do indivíduo sobre suas próprias informações, consoante o aponta o relatório ITS[40]. Sendo assim, o uso do sistema multiportas frente a esses conflitos, passam a representar uma ideia de autonomia do titular.

Ademais, de acordo com crescente número de demandas impostas no Poder Judiciário e seguindo a tendência dessas técnicas, este não pode ser enfrentado apenas como a única forma de resolver os litígios ocasionados pela LGPD, sendo plausível a inclusão de sessões envolvendo os métodos utilizados para solução de disputas.

Ressalte-se, por fim, que a resolução do conflito no contexto de proteção de dados pessoais também poderá ser buscada pelo poder público, e pela própria ANPD, além da iniciativa privada.

Logo, não existe qualquer óbice a utilização desses meios para realização de acordos a respeito da matéria em destaque. Além disso, o incentivo desses institutos poderá beneficiar o titular, o controlador e operador, em face do sigilo dos procedimentos, da celeridade do processo e da busca por uma solução efetiva para todos polos envolvidos.

6. CONSIDERAÇÕES FINAIS

Em razão da ampliação da discussão da temática no cenário nacional, bem como de compartilhamentos de casos envolvendo tratamentos inadequados de dados e incidentes de segurança, a sociedade da informação desenvolve, cada vez mais, consciência acerca da importância que deve ser dada a defesa da privacidade e dos dados pessoais.

Dessa forma, é fundamental que o administrador esteja ciente dos direitos dos titulares das informações e de suas obrigações como controlador, sob pena de responsabilização na forma da lei. Porém não devemos ficar subordinados apenas as

[39] SALLES, Carlos Alberto de. Negociação, mediação, conciliação e arbitragem: curso de métodos adequados de solução de controvérsias. Forense, 2020, p.122

[40] INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. Lei Geral de Proteção de Dados Pessoais e Resoluções de Conflitos: Experiências internacionais e perspectivas para o Brasil. BOTTINO, Celina; PERRONE, Christian; CARNEIRO, Giovana; HERINFER, Leonardo; VIOLA, Mario (Org.). Relatório LGPD: Resolução de Conflitos. Disponível em: https://itsrio.org/wp-content/uploads/2020/04/Relatorio_LGPDResolucaoConflitos.pdf. p. 31.

penalidades inclusas na lei, pois o projeto de implementação da legislação, poderá abrir novas janelas à organização.

Portanto, desenvolver a concepção de que a prevenção e a adoção de medidas eficazes de tratamento de dados, poderá elevar o nível da organização em termos de reputação, inovação, maior confiança com o cliente, entre outras séries de benefícios.

Por outro lado, quanto à ocorrência de vazamento de dados na empresa por qualquer contexto que seja, é viável que a instituição, além de utilizar as medidas adotadas no projeto de conformidade com a LGPD, observe que os métodos alternativos solução de disputas poderão contribuir para a resolução do mérito em destaque.

Em face disso, tais técnicas poderão demonstrar maior eficácia em razão de suas especificidades, como a confidencialidade, a especialidade do profissional, a busca pela solução do litígio, a celeridade do processo, a qualidade e a flexibilização dos procedimentos.

REFERÊNCIAS

AUTOR DESCONHECIDO. **Cyrela é condenada a indenizar cliente por violar LGPD**. ISTO É dinheiro. Disponível em: https://www.istoedinheiro.com.br/cyrela-e-condenada-a-indenizar-cliente-por-violar-lgpd/. Acesso em 10 jun 2021.

BIONI, Bruno Ricardo. **Inovar pela lei**. Revista FGV-Executivo, 2019.

_____. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BODIN de MORAES, Maria Celina. Apresentação. In: RODOTÀ, Stefano. **A vida na sociedade de vigilância. Privacidade hoje**. Rio de Janeiro: Renovar, 2008.

BORELLI, Alessandra; ZAMPERLIN, Emelyn. **A importância da conscientização do tema privacidade e proteção de dados nas empresas**. In: Blum, Renato Opice; Vainzof, Rony; Moraes, Henrique Fabretti (Org). Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e o GDPR. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. **Minuta de Resolução de Fiscalização para Consulta Pública**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-publica-sobre-norma-de-

fiscalizacao/2021.05.29___Minuta_de_Resolucao_de_fiscalizacao_para_consultapblica.pdf/@@download/file/2021.05.29___Minuta_de_Resolucao_de_fiscalizacao_para_consultapblica.pdf. Acesso em 28 jun 2021.

_____. **Lei nº 9307, de 23 de setembro de 1996**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9307.htm. Acesso em: 29 ago 2020.

_____. **Lei nº 13.709/18**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 30 ago 2020.

_____. **Lei nº 12.965/14**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 30 ago 2020.

_____. **Lei nº 14.010/20**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm#art20. Acesso em 2 set 2020.

_____. Ministério Público do Distrito Federal e dos Territórios. **Ação Civil Pública nº 0730600-90.2020.8.07.0001**. Brasília, 2020. Disponível em: https://pje.tjdft.jus.br/consultapublica/ConsultaPublica/DetalheProcessoConsultaPublica/listView.seam?ca=fb4a04b5a693503d66bf1e444688de24b4b253efd0929626. Acesso em: 25 set 2020.

_____. **Proposta de Emenda à Constituição nº 17/2019**. Brasília, Senado Federal, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=A95C937D1F1839CF11D6A4904DC09559.proposicoesWebExterno1?codteor=1773684&filename=PEC+17/2019. Acesso em 04 set 2020.

CISCO. **From Privacy to profit: Achieving Positive Returns on Privacy Investments**. Cisco Data Privacy Benchmark Study, 2020. Disponível em: https://web.archive.org/web/20200821184234/https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf. Acesso em: 01 out 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei geral de proteção de dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

MALDONADO, Viviane. **A Lei Geral de Proteção de Dados: objeto, âmbito de aplicação, requisitos, segurança e a necessidade de sua correta implementação**. In: Nóbrega, Viviane (Org). LGPD: Lei Geral de Proteção de Dados pessoais: manual da implementação. São Paulo: Thomson Reuters Brasil, 2019.

MATTOS NETO, Antônio José de. **Direitos patrimoniais disponíveis e indisponíveis à luz da arbitragem**. In: WALD, Arnoldo (Org.). Doutrinas essenciais: arbitragem e mediação. v. 2. São Paulo: Revista dos Tribunais, 2014.

MENDES, Laura Shertel. **A encruzilhada da proteção de dados no Brasil e o caso do IBGE**, 2020 Disponível em: https://www.conjur.com.br/2020-abr-24/laura-shertel-mendes-encruzilhada-protecao-dados. Acesso em 29 set 2020.

Ministério Público do Distrito Federal e Territórios. **Banco Inter: acordo destinará R$ 1,5 milhão para caridade e combate a crimes cibernéticos, 2018**. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31.Acesso em: 15 set 2020.

Ministério Público do Distrito Federal e Territórios. **MPDFT e Netshoes firmam acordo para pagamento de danos morais após vazamento de dados, 2019.** Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados. Acesso em 15 set 2020.

MORAES, MARIA CELINA; QUEIROZ, JOÃO QUINELATO. **Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD**, 2019. Disponível em: https://www.academia.edu/41132175/Autodetermina%C3%A7%C3%A3o_informativa_e_responsabiliza%C3%A7%C3%A3o_proativa_novos_instrumentos_de_tutela_da_pessoa_humana_na_LGDP. Acesso em 01 out 2020.

SALLES, Carlos Alberto de. **Negociação, mediação, conciliação e arbitragem: curso de métodos adequados de solução de controvérsias**. 3 ed. Rio de Janeiro: Forense, 2020.

SUPREMO TRIBUNAL FEDERAL. **STF suspende compartilhamento de dados de usuários de telefônicas com IBGE** Disponível em:

http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442902&ori=1. Acesso em 23 set 20.

UNIÃO EUROPEIA. **Convenção 108 +**. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. Acesso em: 11 set 2020.

_____. **Carta dos Direitos Fundamentais.** Disponível em: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f. Acesso em: 11 set 2020.

_____. **Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia**. Disponível em:https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A12012E%2FTXT. Acesso em: 11 set 2020.

SPLIT: BRAZILIAN ARBITRATION AND DATA PROTECTION IN THE MIDST OF A FRACTURED WORLD

Author

André Tunes do Nascimento

Debated by

Diego Machado

Karin Klempp Franco

Pedro Silveira C. Soares

Click or scan to access the debates on this article

ABSTRACT

Whilst the Brazilian arbitration market bloomed in a world of convergence, legal fracturing comes once again in its heels. After decades of legal reforms, in a lengthy and costly harmonisation process, laws regulating arbitrations' raw material – data – are enacted in a myriad of different countries. The next in line is Brazil, once arbitration's 'belle of the ball'[1], whose Data Protection Law, DPL (Lei Geral de Proteção de Dados, LGPD) came recently into force.

This paper intends to briefly explore one of the most urgent, pressing issues which the Brazilian new regulation gave rise: the international transfer of personal data within arbitration procedures. Chapter I is dedicated to the emergence of data concerns in Brazil and the entanglement of arbitration and personal data issues; Chapter II addresses the rules of the Brazilian DPL on data transfer; Chapter III approaches the challenges that regulatory fragmentation raises, whereas Chapter IV discusses alternatives to practitioners in tackling legal discrepancies and is followed by a brief conclusion.

[1] *"Brazil As 'La Belle Of The Ball': The Brazilian Courts' Pro-Arbitration Stance* (2011-2012)". Wald, Arnoldo And M. Vieira in The Paris Journal of International Arbitration/Les Cahiers de l'Arbitrage 2013-2.

I. BRAZIL, GLOBAL ARBITRATION, AND THE DISCOVERY OF 'DATA'

Before the pandemic and the abrupt extinction of the world we used to know, there was a time when arbitration was a synonym to the duo 'paper - flash drive'. Practitioners reserved a considerable amount of its own time to operate all the aspects related to the submission of a client's allegation. The saving-printing-contacting-a-courier modus operandi contrasted with the fast, online, encrypted submission forms of the Brazilian state courts. With the pandemic, most arbitration chambers were forced to change adopting submissions mainly by e-mail[2].

The adaptations to a society in crisis highlighted dilemmas that arbitration in Brazil seemed to avoid for years, as if embracing some Freudian mechanism of repression (*Verdrängung*)[3]. The first fact that emerged from the depths of arbitration's subconscious was its vulnerability, the fragility of a system that – while usually depending on secrecy – relies on data transfer mechanisms which do not substantially differ from those used by practitioners in their private lives, such as e-mail[4]. The understanding that arbitration may be affected by data processing issues in the form of safety concerns, however, is only part of a greater realisation.

Arbitration, as dispute resolution by state courts, is not merely intertwined with data processing. Arbitration *is* data processing. Arbitrators gather data (agents, conducts, circumstances) and qualify them in light of a paradigm, the law. There is no fundamental difference between arbitration and e.g. computer programming to that matter. Both have in its matrix deontic logics to ordinate data.

The potential major impacts of personal data protection regulation towards arbitration should then come as no surprise: what it is been regulated is arbitration's raw material, which may affect practitioners in the same way e.g. mining companies are affected by environmental law. At the international level, just as environmental regulation

[2] For instance, CAM-CCBC Administrative Resolution n. 39 and Chamber of Conciliation, Mediation and Arbitration CIESP FIESP Resolution n. 2.

[3] '*Es kann das Schicksal einer Triebregung werden, daß sie auf Widerstände stößt, welche sie unwirksam machen wollen. Unter Bedingungen, deren nähere Untersuchung uns bevorsteht, gelangt sie dann in den Zustand der Verdrängung*'. 'An impulse might be fated to oblivion. Under certain conditions, which will be subject of our closer scrutiny, this impulse assumes the condition of a 'repression' (*Verdrängung*)' (translated by the author). FREUD, Sygmund. *Die Verdrängung*, Public Domain, 1915. Obtained in http://www.psychanalyse.lu/. Acessed on 3rd October 2020.

[4] '(…) data breaches are not only exposed when storing data, but also when sending it through email. Email is not a safe courier to send data such as the request for arbitration, memorials, or exhibits.' RODRÍGUEZ, Santiago Enrique. 'The what, the why, and the how: Blockchain as a solution for Institutional Arbitration', Spain Arbitration Review, Revista del Club Español del Arbitraje, Club Español del Arbitraje; Wolters Kluwer España 2020, vol. 2020, Issue 37, p. 82.

may induce or discourage investors; personal data protection regulation adds complexity to litigation becoming either an asset or a hindrance in a country's quest to conquer the legal market[5].

Brazil's successful story with arbitration has then a new chapter. The country already hosts one of the most important arbitration chambers in the world (CAM-CCBC)[6] and it is ranked 6th amongst countries with most ICC proceedings[7]. The recently in force DPL, as one more character of this story, introduces new elements to take into account while recalculating Brazilian's route to success. In order to understand which role the new law will play in the country's legal market's expansion, it is particularly relevant to assess how the DPL will interact with international players. In other words, it is time to have a glance at where the DPL meets the world: the international transfer of data.

II. THE BRAZILIAN DPL AND THE INTERNATIONAL TRANSFER OF DATA

Before delving into the more complex issues that the Brazilian DPL poses – issues that inexorably touch the arbitration market – one must take a step back in order to better define the subject at hand: the 'international transfer of data'. A task that first and foremost falls within the realms of law, as 'international transfer of data' is, somewhat counterintuitively, a legal concept that does not necessarily relate to an IT-expert understanding of the same phenomenon.

The Brazilian DPL didactically erects the notion of 'international transfer of data' out of smaller 'blocks', i.e., normative factors laid down by the DPL as premises of the regulation as a whole[8]. The first chapters of the DPL are exclusively dedicated to these key conceptual definitions, which shall be more thoroughly explained so as to clearly establish the contours of the rule at hand. More specifically, there is a need to briefly recollect what the Brazilian DPL regards as ***(a)*** 'international'; ***(b)*** 'transfer'; and ***(c)*** 'data'.

[5] On the development of arbitration global 'market' and the rationale under the selection of its 'products', see: MATTLI, Walter. *Private Justice in a Global Economy:* From Litigation to Arbitration International, Organization 55, The IO Foundation and the Massachusetts Institute of Technology, pp. 919–947, 2001.
[6] 2018 International Arbitration Survey: The Evolution of International Arbitration, School of International Arbitration, Queen Mary University and White & Case LLP, p. 13.
[7] ICC Annual Report 2019, p. 14.
[8] About 'normative factors': ALCHOURRON, Carlos e BULYGIN, Eugenio. *Introducción a la metodologia de las ciencias jurídicas y sociales*, Editorial Astrea de Alfredo y Ricardo Depalma: Buenos Aires, 1993, p. 29.

(a). Internationality in the Brazilian DPL. As if making a mockery of our Westphalian ancestors, the notion of 'territory' poorly conforms to a system of information exchange – the internet – that is nowhere and everywhere at the same time[9], a quality that some could attribute to arbitration itself[10]. In a way, the internet only adds up to an already strained relationship between the modern state and reality. It is indeed telling that the Brazilian DPL, as other data protection laws, resorts to the once rare instruments of extraterritoriality to circumvent issues related to its geographic scope of application.

The Brazilian DPL, as per its art. 3, applies to data processing operations within the Brazilian territory; to all data processing activities whose purpose is to offer or provide goods and services in Brazil; and to the processing of data collected in Brazil. The Brazilian DPL is similar to the European GDPR as it applies regardless of a data processing entity's location[11]. It also follows its European counterpart, as well as its neighbouring Argentinean DPL, as it binds anyone who processes data with the objective of offering goods or services in Brazil[12]. What might characterise 'offering of goods or services in Brazil' is another debate, although language and currency may be taken as guidance[13].

***(b).* Transfer of data in the Brazilian DPL**. The Brazilian DPL does not expressly define what shall be considered as 'transfer'. It does, however, as the European GDPR, describe 'cross-border processing' (Art. 4, (23), GDPR) or as in the Brazilian version, '*international* data transfer' (Art. 5, XV). The concept of 'transfer' is thus only defined in its *qualified* form. An omission that is certainly not a result of accident: facing a similar problem whilst examining the history of transborder data flow, Prof. Kuner refrains from

[9] To be fair with our Westphalian ancestors, the legal notion of territory is a 20th century creation: 'Das Land, auf welchem der staatliche Verband sich erhebt, bezeichnet seiner rechtlichen Seite nach den Raum, auf dem die Staatsgewalt ihre spezifische Tätigkeit, die des Herrschens, entfalten kann. In diesem rechtlichen Sinne wird das Land als Gebiet bezeichnet'. 'The land over which the state organisation erects itself indicates, under a legal perspective, the space over which that state power exercises the specific activity enshrined within its ruling. In such a legal sense this land is named 'territory''. (translated by the author). JELLINEK, Georg. Allgemeine Staatslehre, O. Häring: Berlin, 1914, p. 394.

[10] See Gaillard's 'transnational' representation of international arbitration. GAILLARD, Emannuel. *The representations of international arbitration*, in Journal of International Dispute Settlement, vol.1, n. 2, pp. 271-281, p.278.

[11] On the comparison of the Brazilian DPL and the GDPR: *Comparing privacy laws: GDPR v. LGPD*, DataGuidance by OneTrust with Baptista Luz Advogados.

[12] Art. 4.1, (c), Argentinean DPL.

[13] As referred to by Mr. Igor Mostnyi in the International Congress on Law and Technology held virtually from August 11th to August 13th. CHAGAS, Beatriz Uchôas. TUNES, André. *Report on the International Congress on Law and Technology*. Revista de Arbitragem e Mediação. vol. 67, ano 17, p. 395-413. São Paulo, ed. RT, out-dez. 2020.

resorting to a crystallised definition of 'transfer' in light of the rapid '*evolution of technologies*'[14].

Given the inherent broadness of any attempt of conceptualisation of 'transfer', an alternative would be to adopt a typological approach. A 'type' (*Typus*), in contrast to a concept, is dynamic and works on approximations towards a model rather than on subsumption to a given rule[15]. The fluidity of types is ideal to describe legal phenomena in a changing world. To the extent of establishing or unveiling rules as it is here intended, however, types are less useful[16].

Assuming the risks of tautology and crystallisation, one may resort then to a systematic view of the Brazilian DPL as to understand what 'transfer' might enshrine. To the Brazilian DPL 'transfer' equals 'processing' (art. 5, X), as any '*operation carried out with personal data*'. The agent responsible for this operation is in its turn a '*processing agent*' (art. 5, IX), i.e. a processor or its controller, which coordinate a processing operation (art. 5, VI).

With due regard to the framing already laid down by the Brazilian DPL and its correlated definitions, and to the purposes of this article, 'transfer' might be apprehended as an '*exchange of personal data between processing agents*'. This is an unofficial definition of 'transfer' but carries practical value in the arbitration context as an easily recognisable data processing activity that causes the Brazilian DPL to apply.

***(c)*. Data in the Brazilian DPL**. 'Data' to the Brazilian DPL equals 'personal data' as information related to an identified or identifiable natural person (art.5, I). The definition is identical to the one portrayed in the GDPR (art. 4, I). As in the GDPR, in the Brazilian DPL personal data may also be qualified as 'sensitive' whenever it regards e.g. 'racial or ethnic origin', 'religious belief' or 'political opinion'.

The array of information that may be understood as 'personal data' is unsurprisingly enormous. From a person's name and image standing as the most obvious examples, to a

[14] KUNER, Christopher. *Regulation of Transborder Data Flows under Data Protection and Privacy Law:* Past, Present and Future". OECD Digital Economy Papers, No. 187, OECD Publishing, 2011, p.14.
[15] On the concept of '*typus*': SCHMIDT, Jürgen. *Das Denken in Standards: Zu einer Publikation von Karl-Heinz Strache*. ARSP: Archiv für Rechts- und Sozialphilosophie . vol. 59, n. 2, 1973, pp. 257-264.
[16] LARENZ, Karl. CANARIS, Claus-Wilhelm. *Methodenlehre der Rechtswissenschafts*, Springer, 1995, p. 71.

person's walking movements[17] and body temperature[18] as the newcomers in the seemingly ever-growing list of what may be classified as personal data.

After briefly visiting the key concepts that structure the international transfer of data in the Brazilian DPL, it is arrived the moment to lay down the – by the norm acknowledged – preconditions to its application. In other words, it is time to reveal the pieces that compose the frame of the Brazilian DPL. This exercise has practical meaning: facing a potential transfer of data, practitioners in international arbitration may ascertain the DPL's scope of application through a fast – though not thoroughly comprehensive – manner.

$$I \wedge T \wedge D \rightarrow Br^{DPL}$$

Where 'I' is the norm factor 'international', 'T' amounts to 'transfer', 'D', 'data' and 'Br^{DPL}', the Brazilian Data Protection Law.

$$I \wedge T \wedge D \rightarrow Br^{DPL} \therefore (Bo \vee O \vee C) \wedge (E \wedge Pa) \wedge (Id \vee Ib) \rightarrow Br^{DPL}$$ [19]

Where 'Bo' represents 'data processing within Brazilian borders', 'O' means an 'offer to provide goods or services in Brazil', and 'C' 'collected data in Brazil'. In its turn, 'E' is the act of 'exchange' and 'Pa' indicates two or more processing agents. Finally, 'Id' evinces 'information regarding an identified natural person' and 'Ib', information related to an identifiable natural person[20].

Naturally the abovementioned sentence is a simplification of the norm which may reduce its perceived scope of application. Nonetheless, one can already establish some typical situations where the transfer of data in an international arbitration proceeding might trigger the application of the law. As such, ***(i)*** the sending of memorials of a Brazilian party to an arbitration institution overseas; ***(ii)*** the exchange of communications or documents between parties and arbitrators seated in different countries, one of them being in Brazil; ***(iii)*** the exchange of communications or documents between parties and external experts, with at least one of them seated in Brazil; ***(iv)*** the sending of procedural

[17] As referred to by Mr. Takashi Nakazaki in the International Congress on Law. CHAGAS, Beatriz Uchoas. TUNES, André. op. cit.
[18] Idem note 13.
[19] Where "∧" stands for the connective "and","∨", stands for the connective "or" and " ∴" stands for "therefore".
[20] The qualifier 'sensitive' (art. 5°, II, Brazilian DPL) is irrelevant in the task of assessing the Brazilian DPL application in this context as it is encompassed by the larger concept of 'personal data'.

orders or awards from an arbitral institution to parties, if the parties, the arbitral institution or at least one of the arbitrators is seated in Brazil; or ***(v)*** the providing of a sharing platform accessible from Brazil; are some of the examples of facts that the Brazilian DPL may regulate[21].

As it is noticeable, in an international arbitration in which at least one of its *players* – parties, arbitrators, experts, assistants or arbitral institution – has connections with Brazil, virtually all exchange of data concerned gives rise to the Brazilian DPL to apply. This expansive approach has its benefits. The level of protection that the Brazilian DPL avails is unprecedented. Problems may arise, however, when different, but equally expansive, protective laws collide.

III. THE PROBLEM: THE WORLD IS NOT GDPR

Although nationality itself is an irrelevant application criterion under both the Brazilian DPL and e.g. the GDPR, the territory in which a nation is confined is not[22]. Other DPLs around the globe follow the same pattern[23]. Data processing activities or data collection within a country's borders may give rise to the application of data regulation that might drastically vary from country to country.

During the discussions that led to the approval of the DPL in the Brazilian Congress the fear of enacting an idiosyncratic law was tangible. As to curb Brazilian representatives' purported eagerness for isolationism, a prominent lawyer suggested an objective standard to the approval of amendments in the Brazilian DPL. Resorting to a Brazilian indigenous fruit ('*jabuticaba*') as a common metaphor to Brazilian – negatively regarded – peculiarities, he defended[24]:

> *Everything that brings the Brazilian law closer to the GDPR must be approved.*
> *Everything that distances the Brazilian law from the GDPR shall be deemed as a 'jabuticaba'*[25].

[21] PAISLEY, Kathleen. *It's All About the Data:* The Impact of the EU General Data Protection Regulation on International Arbitration, Fordham International Arbitration & Mediation Conference, Volume 41, Issue 4, 2018, pp. 864-865.
[22] BUCHAIN, Luiz Carlos. *A Lei Geral De Proteção De Dados:* Noções Gerais, Revista dos Tribunais, vol. 1010/2019, 2019, p.8.
[23] As is the case, for instance, of Australia (Privacy Act, Sections 5A and 5B), Mexico (Reglamento De La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, art. 4) and Argentina (Ley 25.326, art. 44).
[24] LEMOS, Ronaldo. *Lei de Dados Deve Evitar Jabuticabas*, Folha de São Paulo, 18 February 2019.
[25] Translated by the author.

Apart from Brazilians apparent despise for its own fruits or the discussion over the phenomenon of regulation import in developing countries[26], it is almost naïve to assume that legislators across the globe would think in the same way as our prominent lawyer. In fact, there are good reasons to believe that they do not. National laws may inevitably reflect countries' needs, cultures or political moments[27].

A brief overview of data protection regulations in other countries evinces a wide diversity of solutions in comparison with the GDPR. The Australian Privacy Act, for instance, does not distinguish data controllers and processors, a fundamental distinction in the GDPR, nor does it establish the need to appoint a data protection officer[28]. The Indian Personal Data Protection Bill does not consider the performance of a contract as a legal basis for processing data[29]. In Mozambique – a country that might be a potential market to Brazilian practitioners, such as Angola[30] – there is still no Data Protection Law, though data protection itself may be regarded as a human right[31]. In contrast, the Singaporean legal framework has a business centred approach on data protection and does not regard it a human right[32]. Even countries where similarities between their Data Protection Laws and the GDPR may be more easily drawn differences arise: while in Japan there is a much more strict understanding of a 'right to be forgotten'[33], in Brazil GDPR's concept of establishment is not encompassed by the law.

[26] Latin America had already its share of regulatory importation, which is viewed by some as costly effective: POSNER, Richard. *Creating a Legal Framework for Economic Development*, The World Bank Research Observer, Vol. 13, No. 1, 1998. To a Brazilian criticism on the subject: *Regulação da Propriedade Privada: Inovações na Política Agrária e a Redução dos Custos de Equidade*, PORTUGAL GOUVEIA, Carlos. in Regulação e Desenvolvimento Novos Temas, SALOMÃO FILHO, Calixto (Org.).

[27] As Professor Legrand's advice to legal comparatists goes: "The comparatist must adopt a view of law as a polysemic signifier which connotes inter alia cultural, political, sociological, historical, anthropological, linguistic, psychological and economic referents". Ultimately, this view of law challenges the very idea of a 'legal transplant': LEGRAND, Pierre. The Impossibility of Legal Transplants, Maastricht Journal of European and Comparative Law, 1997, vol. 4, p. 116.

[28] On the comparison of the Australian Privacy Act and the GDPR: *Comparing privacy laws: GDPR v. The Australian Privacy Act*, Data Guidance by One Trust with Mills Oakley.

[29] WIMMER, Kurt, MALDOFF, Gabe, LEE, Diana. *Comparison*: Indian Personal Data Protection Bill 2019 vs. GDPR, International Association of Privacy Professionals.

[30] As an example of the Brazil-Angola relationship and arbitration, CAM-CCBC representative, Patricia Kobayashi, participated in the VIII International Arbitration Congress held in Luanda: https://ccbc.org.br/cam-ccbc-centro-arbitragem-mediacao/noticias-cam-ccbc/novidades-cam-ccbc/noticias-cam/roadshow-africa/. Access on 3 October 2020.

[31] As referred to by Ms. Rita Donato in the International Congress on Law and Technology. CHAGAS, Beatriz Uchoas. TUNES, André, op. cit.

[32] As referred to by Mr. Chong Kim Lim in the International Congress on Law and Technology. CHAGAS, Beatriz Uchoas. TUNES, André, op. cit.

[33] On a Japanese perspective of a right to be forgotten, an important precedent of the Japanese Supreme Court: *Japanese court rules against paedophile in 'right to be forgotten' online case.* The Guardian, 2 February 2017. In Brazil, the existence of a right to be forgotten within the Brazilian constitution has been denied by its Supreme Court, which stated that occasional abuses should be assessed *in casu*: see 'Recurso Extraordinário n° 1.010.606', rel. Dias Toffoli, Supremo Tribunal Federal, 2021.

The Brazilian legislators surely knew of the legal discrepancies that reign across different countries on what regards data protection. In regulating the international transfer of data the Brazilian DPL provides a hybrid solution: it is – as the GDPR – both a geographically and organisationally based regulation[34]. Art. 33 of the Brazilian DPL states that international transfer of data is allowed insofar as its destination is a *"country or international organisations that provide a level of protection of personal data that is adequate to the provisions of this Law"* (Art. 33, I). At the same time, international transfer of data is also allowed where "*the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in this Law*" (Art. 33, II).

The Brazilian DPL then bets on global regulation uniformity as it explicitly refrains from applying to the processing of data originated outside Brazilian borders if "*the country of origin provides a level of personal data protection adequate to that established in this Law*" (Art. 4, IV). The adequacy of extraneous national regulations is to be ascertained by the Brazilian NDPA (National Data Protection Authority, Autoridade Nacional de Proteção de Dados) that in fulfilling such duty shall have regard not only to a country's legal framework but also the nature of the transferred data and specific circumstances which a particular transfer might be entangled.

The twofold answer of the Brazilian DPL to the problem of multiplicity gives due consideration to different – but yet compatible – legal regimes. It also leaves room for private regulation, which is welcomed inasmuch as it concurs with state led policy[35]. The Brazilian DPL, however, still does not eliminate doubt on what regards the transfer of international data. Intense data-reliant activities such as arbitration may struggle in maintaining the delicate balance between distinct national regulations.

International proceedings may potentially involve a diversity of data protection regulations. Addressing this issue Bhaipaj and Kala draw attention to the hypothetical example of an arbitration administered by a Singaporean Arbitral Institution between EU and Indian parties: three distinct legal regimes would potentially apply to data-related issues regarding the proceedings[36]. A Brazilian arbitral institution administering a

[34] Idem note 14, p. 20.
[35] UEHARA, Luiz Fernando. TAVARES FILHO, Paulo César. *Transferência Internacional De Dados Pessoais*: Uma Análise Crítica Entre O Regulamento Geral De Proteção De Dados Pessoais Da União Europeia (RGPD) E A Lei Brasileira De Proteção De Dados Pessoais (LGPD), Revista de Direito e as Novas Tecnologias, vol. 2/2019, 2019, p. 7.
[36] BAIPAI, Ananya. KALA, Shambhavi. *'Data Protection, Cybersecurity and International Arbitration: Can they Reconcile?*', Indian Journal of Arbitration Law Volume VIII, Jodhpur Issue 2 2019, p. 8.

proceeding between e.g. a Portuguese and an Angolan party would face the same challenge. In this example, the Brazilian DPL would apply pursuant to art.3, I, as there is data processing within the Brazilian territory. Also, the GDPR would apply as the controller of (at least some) of the data provided in the context of a proceeding has its establishment in Europe (art.3 (1) of the GDPR). Following a similar rationale, the Angolan law would apply as well (art. 3, 2, *a*, of the Angolan DPL).

The potential for conflict amidst an already established dispute between parties is evident. This author is not aware of any case law in which data protection issues were raised by any of the parties during international commercial proceedings. One such absence may be due to the secrecy that generally applies to commercial arbitration. Two relatively recent decisions in international investment arbitration proceedings, however, may hint what lies ahead[37].

In *Tennant Energy v. Canada*, an arbitration under NAFTA Chapter 11, parties discussed whether the Permanent Court of Arbitration would be bound to the GDPR[38]. It was argued that the PCA, being an international organisation, would not be subject by the GDPR. As Lavranos points out this reasoning deserves criticism: the GDPR – as the Brazilian DPL – also applies to international organisations[39].

In *Elliot v. Korea*, an arbitration under the KORUS FTA, Korea argued that according to its DPL (the Korean Personal Information Protection Act, PIPA) personal information disclosed in the proceedings should be redacted. The Claimant, however, contested the assertion that the arbitral institution, the PCA, or the arbitral tribunal could be considered data-controllers, as Korea could not prove either one of them "*arrange or organize the personal information of individuals in a systematic manner so as to enable "easy access to the personal information"*[40]. In light of the fact that the PIPA has a definition of data-controller very similar to the one portrayed by the GDPR – which, in turn, is similar to the Brazilian DPL definition – Claimant's argument lacked persuasiveness[41]. In fact, the arbitral tribunal of Elliot v. Korea dismissed Claimant's

[37] LAVRANOS, Nikos. *The need for a Data Protection Protocol for arbitration proceedings*, Thomson Reuters, Practical Law Arbitration Blog, 2019. Available at: http://arbitrationblog.practicallaw.com/the-need-for-a-data-protection-protocol-for-arbitration-proceedings/Access on 4 October 2020.
[38] Case documents available at: https://www.italaw.com/cases/7250 Access on 3rd October 2020.
[39] Idem note 38.
[40] PCA Case N° 2018-51, Procedural Order n° 4, p. 6, § 23.
[41] As per the DataGuidance database. Available at: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Access on 4 October 2020.

thesis allowing personal information throughout the proceedings to be duly anonymised[42].

Apart from the specificities of investment arbitration, these two cases leave important lessons to commercial arbitration. First, in both cases the need for arbitration practitioners to be well-acquainted to national normative frameworks that may seem totally irrelevant to the dispute was rendered conspicuous[43]. Second, both cases also shed light on the responsibilities of arbitral tribunals and institutions: ultimately data protection laws rely on them to protect third person's rights (e.g. the right of anonymisation) that may be only indirectly affected by the dispute. It is an internalisation of policy costs that arbitration must get used to. Finally, both cases prove that the intersections of data protection and proceeding-administration are not merely a theoretical approach and may impact real life disputes.

IV. ALTERNATIVES: WAYS THROUGH A FRACTURED WORLD

International arbitration arose as to meet the demands of an also international arbitration community[44]. That is, there is nothing inherently international in arbitration itself: it is international inasmuch as it meets such a demand. Arbitration suitability to proceedings with elements of transnationality was earned, not given. Every time change – whether of a legal or economic nature – emerges, there is a need to readaptation in order to assure practitioners and potential clients that the system is still better than the alternative (national courts, regularly).

Data protection adds new costs and risks to international arbitration. *Ad terrorem*, facing the current complexity of different legal frameworks, data-reliant companies would prefer the national courts of countries with clear data protection rules to arbitration. Resorting to national courts would be a solution to avoid the uncertainties of data protection application and the kind of discussion which was seen in *Tennant Energy v. Canada*. In fact that might be an alternative to the problem of legal multiplicity.

[42] Idem note 41, *passim.*
[43] Such was the case of *Tennant Energy v. Canada*.
[44] 2021 International Arbitration Survey: Adapting Arbitration to a Changing World, Queen Mary University of London, White & Case, 2021, p. 2: "*International arbitration is the preferred method of resolving cross-border disputes for 90% of respondents*".

A return to courts is, however, not the only or necessarily the best alternative. Although data protection may apply irrespective of choice of law clauses in a contract[45], as data protection obligations fall on arbitral participants rather than governing proceedings[46], flexibility might still be sided with arbitration. Practitioners may then model proceedings taking data protection in consideration. Initiatives such as the ICCA-IBA Task Force on Data Protection[47] work exactly on that premise: they seek to assess risks involved with personal data protection regulation and to offer practical guidelines.

One of the most appealing recommendations of the ICCA-IBA task force, which has particular relevance in addressing the issue of data transfers, is the creation of a "data protection protocol"[48]. According to the task force, a data protection protocol *"refers to a document agreeing on how data protection is going to be applied in a particular context"*[49]. The protocol thus does not change nor alter the effect of the applied data protection regulation; it simply recognises the legal frameworks at play addressing data concerns in the form of a declaration, a procedural order or a contract[50].

Correctly, the ICCA-IBA task force suggests that the data protection protocol should be established at the outset of the proceedings. Indeed, acknowledging and addressing data protection tension zones right from the start may prevent the use of data concerns as a strategy to eschew enforceable awards, a new dimension of *guerrilla* tactics in the pandemic world[51]. A protocol in the form of a contract executed at the case management conference after thoroughly discussions between all participants, including e.g. third party funders would estop parties from attacking the validity of decisions on the ground of data concerns or imposing unjustified restrictions to document production.

---

[45] As seen, application criteria of data protection laws such as the GDPR and the Brazilian DPL do not consider the will of the parties in a contract as they refer to e.g. the territory in which data processing is performed. This view was already adopted in German law even before the GDPR, see: BURIANSKI, Markus, REINDL, Martin. '*Truth or Dare?* The conflict between e-discovery in international arbitration and German data protection rules, in SchiedsVZ, vol.8, issue 4, pp.182-200, Kluwer Law International, C.H. Beck, 2010, p.192.

[46] The ICCA-IBA Roadmap to Data Protection in International Arbitration, p. 34.

[47] Idem note 46, *passim.*

[48] Data protection protocols, as a form of private regulation, amount to what may be identified as "non-state law". To a legal pluralistic approach of non-state laws, see: MICHAELS, Ralf. *What is non-state law?* In Negotiating State and Non-State Law: the challenge of global and local legal pluralism, Cambridge University Press, 2015, p.41-58.

[49] Idem note 46, p. 41.

[50] CERVENKA, Anja. SCHWARZ, Philipp. *Datenschutz im Schiedsverfahren – die Rolle des Schiedsgerichts'* in Jörg Risse , Guenter Pickrahn , et al. (eds), SchiedsVZ, German Arbitration Journal, Kluwer Law International; Verlag C.H. Beck oHG 2020, vol. 18, issue 2, p. 82.

[51] As referred to by Ms. Marike Paulsson in the International Congress on Law and Technology. CHAGAS, Beatriz Uchoas. TUNES, André, op. cit.

On what regards the international transfer of data, a protocol ought to map all potential data flows between arbitral participants in order to detect the application of distinct data protection laws[52]. The 'map' should also include data storage intermediators: the fundamental idea is to keep track of all data exchange so as to avoid surprises e.g. the application of a data protection law which was not deemed relevant at the outset of the proceedings. During the proceedings the protocol may be amended with the purpose of integrating other actors whose participation could not have been predicted, for instance, experts.

All participants provided in a data protection protocol may be held accountable for data protection violations. In this scenario, tribunals will have a prominent role: as Cervenka and Schwarz assert, '*[d]em Schiedsgericht kommt eine Schlüsselrolle im Zusammenhang mit der Einhaltung der datenschutzrechtlichen Bestimmungen zu*'[53] This 'key role' in protecting data during arbitration proceedings involves, as per the same authors, duties to ***(i)*** inform subjects to data protection norms; ***(ii)*** foster data safety, which includes a risk assessment to be performed in conjunction to the parties; and ***(iii)*** minimise data, imposing document production to be reduced to a minimum, a principle already enshrined within the Prague rules[54]. A tribunal's failure to protect data might result in sanctions to its arbitrators. If data protection violations may effectively taint an award is another discussion that lies outside the scope of this paper, although the mentioned authors deny the possibility.

Bearing in mind the abovementioned considerations, how the Brazilian DPL will coexist with a data protection protocol designed to arbitration proceedings is still an open issue. Until the moment this paper was written, this author was also not aware of particular case law involving the Brazilian DPL and arbitration. The fact is that in contrast to the GDPR (Art. 26) the Brazilian DPL does not expressly acknowledge agreements between controllers. The absence of a dedicated provision shall not be an obstacle to the using of data protection protocols in proceedings where the Brazilian DPL might apply: the protocol is a private agreement with procedural repercussions that do not substantially

[52] Idem note 21, p.891.
[53] 'The arbitral tribunal has a key role to the compliance of data protection provisions' (Translated by the author).
[54] Rules On The Efficient Conduct Of Proceedings In International Arbitration (Prague Rules), Note from the Working Group, p.2.

differ from any other procedural contracts agreed by the parties in the context of arbitration[55].

Brazil, as an emergent legal market, should not, however, exclusively rely on private parties' initiative to find balance amongst conflicting data protection rules and arbitration. Different layers of harmonising regulatory framework should ground a concatenated movement in order to promote safe data transfer in arbitration proceedings, selling thereby Brazilian arbitration as the product it is.

A harmonic understanding of the applicable laws is the first step to properly 'map' data flows through a data protection protocol. And that is the task of the Brazilian NDPA, which should offer guidelines specifically designed to arbitration proceedings. In a second layer of specificity, Brazilian arbitral institutions – possibly already taking the NDPA guidelines into account – should in conjunction draft a clarifying document directed to foreign arbitral participants on the relationship of the Brazilian DPL and other data protection laws. In a third layer of regulation, each arbitral institution – with the assistance of its DPO – should disclose its own guidelines on data transfer[56], preferably also making a data protection protocol sample available, similar to the one provided by the ICCA-IBA Task Force. Finally, resorting to this multi-layered framework, arbitral tribunals should design their data protection protocols in a casuistically manner and with due consideration to the input of all arbitral participants.

V. CONCLUSION

This paper journeyed from an abstract realisation to a practical understanding. Under a Brazilian perspective, it has exposed the ubiquity of personal data concerns within international arbitration procedures and suggested a mechanism to address legal diversity. Acknowledging the variety of personal data protection regulations that fall on each arbitral participant individually, data protection protocols present themselves as an effective instrument to minimise occasional friction amongst legal orders.

A more obvious but in this paper unexplored alternative to legal fracturing is standardisation through a treaty. An internationally encompassing solution to the problem of distinct data protection regulations is not in sight in the foreseeable future, though.

[55] Interesting to notice that procedural contracts are expressly provided for in the Brazilian Procedural Code, Art. 190.
[56] Arbitral Institutions such as the ICC and the Vienna International Arbitration Centre expressly encourage the agreement of a data protection protocol at the outset of proceedings.

While harmonising solutions would be ideal, as of now, practitioners will have to embrace diversity. And to Brazilian arbitration that might be actually good.

The Brazilian DPL should be seen not as mere cause for additional costs to proceedings but as an asset. It places the country in the world's vanguard on data protection, granting market agents the clarity and safety they need to process data. Arbitral participants will take that into consideration while choosing arbitral institutions or even contractual partners. Instead of attempting to patch the differences between various national regulations, the still relatively small Brazilian arbitration community has the unique opportunity to set an example of harmony in a coordinated response to a inexorably split world.

REFERENCES

2021 International Arbitration Survey: Adapting Arbitration to a Changing World, Queen Mary University of London, School of International Arbitration White & Case, 2021.

2018 International Arbitration Survey: The Evolution of International Arbitration, School of International Arbitration, Queen Mary University and White & Case LLP

ALCHOURRON, Carlos e BULYGIN, Eugenio. *Introducción a la metodologia de las ciencias jurídicas y sociales*, Editorial Astrea de Alfredo y Ricardo Depalma: Buenos Aires, 1993.

BAIPAI, Ananya. KALA, Shambhavi. *'Data Protection, Cybersecurity and International Arbitration: Can they Reconcile?*', Indian Journal of Arbitration Law Volume VIII, Jodhpur Issue 2, 2019.

BUCHAIN, Luiz Carlos. *A Lei Geral De Proteção De Dados:* Noções Gerais, Revista dos Tribunais, vol. 1010/2019, 2019.

BURIANSKI, Markus, REINDL, Martin. '*Truth or Dare?* The conflict between e-discovery in international arbitration and german data protection rules, in SchiedsVZ, vol.8, issue 4, pp.182-200, Kluwer Law International, C.H. Beck, 2010.

CERVENKA, Anja. SCHWARZ, Philipp. *Datenschutz im Schiedsverfahren – die Rolle des Schiedsgerichts'* in Jörg Risse , Guenter Pickrahn , et al. (eds), SchiedsVZ, German Arbitration Journal, Kluwer Law International; Verlag C.H. Beck oHG 2020, Volume 18 Issue 2.

CHAGAS, Beatriz Uchôas. TUNES, André. *Report on the International Congress on Law and Technology*. Revista de Arbitragem e Mediação. vol. 67, ano 17, p. 395-413. São Paulo, ed. RT, out-dez. 2020.

Comparing privacy laws: GDPR v. LGPD, DataGuidance by OneTrust with Baptista Luz Advogados.

Comparing privacy laws: GDPR v. The Australian Privacy Act, DataGuidance by OneTrust with Mills Oakley.

DATAGUIDANCE DATABASE. Available at: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Access on 4 October 2020.

FREUD, Sygmund. *Die Verdrängung*, Public Domain, 1915. Obtained in http://www.psychanalyse.lu/. Acessed on 3rd October 2020.

GAILLARD, Emannuel. *The representations of international arbitration*, in Journal of International Dispute Settlement, vol.1, n. 2, pp. 271-281.

ICC Annual Report 2019.

JELLINEK, Georg. *Allgemeine Staatslehre*, O. Häring: Berlin, 1914.

KUNER, Christopher. *Regulation of Transborder Data Flows under Data Protection and Privacy Law:* Past, Present and Future". OECD Digital Economy Papers, No. 187, OECD Publishing, 2011.

LARENZ, Karl. CANARIS, Claus-Wilhelm. *Methodenlehre der Rechtswissencschafts*, Springer, 1995.

LAVRANOS, Nikos. *The need for a Data Protection Protocol for arbitration proceedings*, Thomson Reuters, Practical Law Arbitration Blog, 2019.

LEGRAND, Pierre. *The Impossibility of Legal Transplants*, Maastricht Journal of European and Comparative Law, vol. 4, 1997.

LEMOS, Ronaldo. *Lei de Dados Deve Evitar Jabuticabas*, Folha de São Paulo, 18 February 2019.

MATTLI, Walter. *Private Justice in a Global Economy:* From Litigation to Arbitration International Organization 55, The IO Foundation and the Massachusetts Institute of Technology, pp. 919–947, 2001.

MICHAELS, Ralf. *What is non-state law?* In Negotiating State and Non-State Law: the challenge of global and local legal pluralism, Cambridge University Press, 2015, p.41-58.

PAISLEY, Kathleen. *It's All About the Data:* The Impact of the EU General Data Protection Regulation on International Arbitration, Fordham International Arbitration & Mediation Conference, Volume 41, Issue 4, 2018.

PCA Case N° 2018-51, Procedural Order n° 4.

PORTUGAL GOUVEIA, Carlos. *Regulação da Propriedade Privada: Inovações na Política Agrária e a Redução dos Custos de Equidade*, in Regulação e Desenvolvimento Novos Temas, SALOMÃO FILHO, Calixto (Org.).

POSNER, Richard. *Creating a Legal Framework for Economic Development*, The World Bank Research Observer, Vol. 13, No. 1, 1998.

RODRÍGUEZ, Santiago Enrique. 'The what, the why, and the how: Blockchain as a solution for Institutional Arbitration', Spain Arbitration Review, Revista del Club Español del Arbitraje, Club Español del Arbitraje; Wolters Kluwer España 2020, Volume 2020, Issue 37.

Rules On The Efficient Conduct Of Proceedings In International Arbitration (Prague Rules), Note from the Working Group

SCHMIDT, Jürgen. *Das Denken in Standards: Zu einer Publikation von Karl-Heinz Strache*. ARSP: Archiv für Rechts- und Sozialphilosophie . Vol. 59, No. 2 (1973), pp. 257-264.

THE GUARDIAN, 2 February 2017. *Japanese Court Rules Against Paedophile In 'Right To Be Forgotten' Online Case.*

The ICCA-IBA Roadmap to Data Protection in International Arbitration.

UEHARA, Luiz Fernando. TAVARES FILHO, Paulo César. Transferência Internacional De Dados Pessoais: Uma Análise Crítica Entre O Regulamento Geral De Proteção De Dados Pessoais Da União Europeia (RGPD) E A Lei Brasileira De Proteção De Dados Pessoais (LGPD), Revista de Direito e as Novas Tecnologias, vol. 2/2019, 2019.

WALD, Arnoldo and M. Vieira in The Paris Journal of International Arbitration/Les Cahiers de l'Arbitrage 2013-2. *"Brazil as 'La Belle of the Ball': The Brazilian Courts' Pro-Arbitration Stance* (2011-2012)".

WIMMER, Kurt, MALDOFF, Gabe, LEE, Diana. *Comparison*: Indian Personal Data Protection Bill 2019 vs. GDPR, International Association of Privacy Professionals.

CONFLITO DE LEIS NA ARBITRAGEM INTERNACIONAL: INTERAÇÕES ENTRE A LGPD E OUTRAS LEGISLAÇÕES DE PROTEÇÃO DE DADOS EM DEMANDAS PLURILOCAIS

Clicar ou escanear para acesso aos debates relativos a este artigo

Autoria

Gabriela de Ávila Machado

Giulia Keese Montanhesi

Rafael Tridico Faria

Debatedores

Diego Machado

Karin Klempp Franco

Pedro Silveira C. Soares

RESUMO

Tendo em vista a vasta aplicabilidade da Lei Geral de Proteção de Dados, do Regulamento Europeu e de outras normas de proteção de dados, demandas arbitrais que envolverem atividades com dados pessoais tratados em mais de um território se encontrarão sob a incidência de múltiplas leis. A Lei Geral de Proteção de Dados, assim como toda as outras normas congêneres, deseja resguardar os dados de seus cidadãos nacionais, porém, não dispõe sobre seu alcance dentro da ordem jurídica transnacional. Através desta perspectiva, pretende-se analisar a interação e eventual conflito das leis de proteção de dados pessoais no âmbito da arbitragem internacional, em casos hipoteticamente contratuais, sob a ótica da autonomia das partes e dos atuais mecanismos de definição da lei aplicável na resolução de controvérsias.

INTRODUÇÃO

A Lei Geral de Proteção de Dados – Lei nº 13.709/2018 ("LGPD") foi introduzida no cenário mundial da proteção de dados com uma abrangência ampla, com alcance extraterritorial.

Ocorre que neste meio, normas de proteção de dados como o GDPR (*General Data Protection Regulation* ou "Regulamento Geral sobre a Proteção de Dados", da União Europeia) e outras, também possuem ampla aplicabilidade e podem, a depender do caso concreto, superar as fronteiras de seus países e cidadãos e interagir com a nova norma brasileira.

Muito se discute na arbitragem internacional sobre a lei aplicável às demandas plurilocais. Como veremos a seguir, demandas que envolvem proteção de dados pessoais, e não apenas aquelas que envolvem questões de comércio internacional, também suscitam discussões desta natureza.

Portanto, o artigo buscará analisar a interação e eventual conflito das leis internacionais de proteção de dados pessoais no âmbito da arbitragem internacional e da arbitragem institucionalizada que envolver tratamento de dados pessoais em mais de um território. A análise será feita sob a perspectiva da legislação brasileira e normas da União Europeia como as mais relevantes à presente discussão.

1. A EVOLUÇÃO DA PROTEÇÃO DE DADOS: UMA PERSPECTIVA GLOBAL

A evolução tecnológica e as novas formas de comunicação e de compartilhamento de informação no mundo globalizado permitiram avanços científicos, políticos, econômicos e mudanças sociais expressivas. O fluxo transacional de informações se tornou um recurso de enriquecimento nesta nova realidade econômica, que se convencionou denominar *data driven economy*.

A despeito dos benefícios trazidos por esse fluxo, o uso do espaço cibernético e a difusão desgovernada de informações entre agentes privados, que se deu especialmente em detrimento da privacidade e da proteção aos dados pessoais individuais, tornou-se um motivo de preocupação aos legisladores ao redor do globo.

A indefinição de fronteiras reais no ciberespaço provocou intensos debates jurídicos envolvendo soberania, territorialidade, propriedade e jurisdição dos Estados e evidenciou o interesse comum em regular o ambiente virtual e, consequentemente, a própria tutela da privacidade e proteção de dados de seus nacionais.[1]

[1] MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo. Thomson Reuters, Revista dos Tribunais, Brasil, 2019.
REVISTA DO ADVOGADO: Lei Geral de Proteção de Dados Pessoais. São Paulo: Associação dos Advogados de São Paulo, v. 144, nov. 2019. Mensal.

As primeiras proposições legislativas sobre o tema têm origem na década de 1970[2] e o primeiro consenso internacional a respeito da coleta e do gerenciamento da informação pessoal é do ano de 1980, quando entraram em vigor as *Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais* (as "Diretrizes sobre a Privacidade"), pela Organização para a Cooperação e Desenvolvimento Econômicos ("OCDE").[3]

As Diretrizes sobre a Privacidade se tornaram referência para muitos países, como Canadá, Austrália, Estados Unidos e aos integrantes da União Europeia, criarem seus modelos regulatórios mais recentes, vide a Diretiva 46 de 1995, emitida pelo European Parliament[4].

No Canadá foram instituídas políticas nacionais, como o *The Privacy Act*[5] que tratou dos dados tratados por entidades governamentais e o *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[6], relativo ao tratamento de dados por agentes privados. Buscando coerência com as diretrizes nacionais e supressão de lacunas e omissões, surgiram regulamentações regionais sobre o assunto nas suas diversas províncias.

Diferentemente do Canadá, os Estados Unidos se propuseram a implementar políticas nacionais direcionadas ao uso de determinados tipos de dados ou de setores específicos, como *Driver's Privacy Protection Act* ("DPPA"), *Children's Online Pivacy Protection Act* ("COPPA"), *Fair Credit Reporting Act* ("FCRA"), *Health Insurance Portability and Accountability Act* ("HIPAA") e *Family Educational Rights and Privacy* ("FERPA"), ressalvada a autonomia de cada estado para legislar de forma complementar.

---

[2] Hessen (Alemanha), seguido da França, Noruega, Suécia e Áustria foram os primeiros países europeus a desenvolver legislações nesta temática, além das manifestações estadunidenses através do "Fair Information Practice Principles" ou (FIPPs).

[3] Também são denominadas "OECD Guidelines on The Protection of Privacy and Transborder Flows of Personal Data"

[4] UNIÃO EUROPEIA. Parlamento Europeu e Conselho da União Europeia. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Relativa à proteção de dados das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 01 set. 2020.

[5] CANADA. Privacy Act R.S.C., 1985, c. P-21. <https://laws-lois.justice.gc.ca/eng/acts/P-21/index.html>. Acesso em: 10 set. 2020.

[6] CANADA. Personal Information Protection and Electronic Documents Act. S.C. 2000, c. 5. Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html>. Acesso em: 10 set. 2020.

A União Europeia, por sua vez, adotou modelo diverso. Como evolução da Diretiva 46, aprovou em 2016 o GDPR[7], que entrou em vigor em 2018 e trata o tema de forma ainda mais completa, a iniciar com a aplicabilidade em todos os seus estados-membros (que, por sua vez, poderão adotar normas complementares).

O GDPR se tornou referência mundial em termos de proteção de dados pessoais. Seus princípios guardam semelhanças com diversas outras legislações, inclusive, influenciaram na construção de dezenas de leis de proteção de dados de outras nações, dentre elas a própria lei brasileira.[8]

Em uma perspectiva nacional, a construção do marco regulatório no Brasil teve início com a Constituição Federal de 1988, que introduziu garantias e direitos à proteção da intimidade e da vida privada. Estas foram defendidas em diplomas subsequentes, como o Código do Consumidor[9] em 1990 e o Marco Civil da Internet[10] em 2014.

No entanto, a regulamentação específica se consolidou apenas em 2018, com a promulgação da Lei Geral de Proteção de Dados (ou "LGPD"), Lei nº 13.709/2018[11].

Em 2019, a LGPD passou por sua primeira alteração, quando a Medida Provisória n° 869/2018 foi convertida em Lei, nº 13.853/19, para fins de instituir a Autoridade Nacional de Proteção de Dados ("ANPD"), órgão fiscalizatório, sancionador e interpretador de suas normas.

Após diversas alterações e discussões sobre adiamento, a LGPD entrou em vigor em setembro de 2020[12] e, de acordo com sua redação final, tem por objetivo "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".[13]

---

7 UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 01 set. 2020.

8 REVISTA DO ADVOGADO: Lei Geral de Proteção de Dados Pessoais. São Paulo: Associação dos Advogados de São Paulo, v. 144, nov. 2019. Mensal.

9 BRASIL. Lei nº 8.078, 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em: 01 set. 2020.

10 BRASIL. Lei nº 12.956, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 set. 2020

11 BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm Acesso em: 01 set. 2020.

12 Os artigos 52, 53 e 54, referente à sanções administrativas, entrarão em vigor apenas em agosto de 2021.

13 FEIGELSON, Bruno. SIQUEIRA, Antonio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. São Paulo. Thomson Reuters, Revista dos Tribunais, Brasil, 2019.

1.1. LGPD: aplicabilidade e abrangência

A aplicabilidade da LGPD está prevista no seu artigo 3º:

> *Art. 3º: Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados desde que:*
> *I - a operação de tratamento seja realizada no território nacional;*
> *II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou*
> *III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.*

Quanto a extensão jurídica da norma, o referido artigo esclarece que seus comandos serão dirigidos às operações de tratamento realizadas na forma física ou digital, que estabeleçam conexão e vínculo com o território nacional, seja o tratamento realizado em território brasileiro ou não, desde que a origem dos dados seja local, bem como se envolver bens, serviços ou indivíduos brasileiros.

Dessa forma, a lei prevê a possibilidade de estrangeiros violarem a LGPD, ainda que fora do território brasileiro ou realizando tratamento de dados em ambiente virtual, em razão da dimensão atribuída ao artigo 3º.

1.2. Coexistência e interação entre normativas de proteção de dados

A par da vasta extensão da aplicabilidade LGPD, demonstrada acima, é plenamente possível nos depararmos com a interação desta com outras normas internacionais de proteção de dados, a depender da situação concreta.

O GDPR, por exemplo, preconiza em seu artigo 3º que será aplicável "ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União Europeia, independentemente de o tratamento ocorrer dentro ou fora da União Europeia"[14]. Ou seja, ainda que o controlador ou operador esteja na Europa, mas a guarda dos dados, ou tratamento seja realizado no Brasil, o GDPR é aplicável.

[14] Article 3, GDPR "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

A toda evidência, há uma tendência global de formação de um direito transnacional e relativização do estado soberano, já anunciada pelo direito internacional, também vista neste segmento em razão da pluralidade de sujeitos envolvidos no tratamento de dados internacionais.

A multiplicidade de agentes de diversas nacionalidades envolvidos em uma mesma situação fática pode permitir a incidência de múltiplas normativas em matéria de proteção de dados, criando uma interação entre estas normas, seja de natureza harmoniosa ou conflituosa.

A imprecisão de fronteiras no ciberespaço também faz com que este se torne um *locus* de permanente reflexão quanto a sua regulação. Tanto a LGPD, quanto o GDPR e outras normas de proteção de dados estrangeiras cuidam de disciplinar os dados tratados neste universo se demonstrado algum vínculo com seus nacionais. Vejamos um exemplo.

O comércio internacional -- na sua atual configuração -- permite ao cidadão brasileiro comprar um produto canadense em um site de uma empresa sediada nos Estados Unidos, que, por sua vez, armazena os dados pessoais de seus consumidores em um servidor contratado e situado em um país da União Europeia.

Nesta situação hipotética, é possível verificar a interação de quatro normas de proteção de dados concomitantemente. Situações como estas estão cada vez mais presentes na sociedade globalizada e eventuais litígios decorrentes de relações jurídicas similares irão suscitar, inevitavelmente, uma discussão sobre a lei aplicável ao caso concreto.

Portanto, entende-se que a sistemática da aplicação de normas de proteção de dados em situações de violação de direitos envolvendo mais de uma nacionalidade, quer seja em uma arbitragem ou não, deve passar pela análise dos limites de cada legislação e pela discussão doutrinária e casuística da lei aplicável.

Para compreender como essas interações ocorrem dentro da disputa submetida à arbitragem, importante delimitar, em primeiro plano, quais casos envolvendo violação de proteção de dados são relevantes a este método de resolução de disputas.

2. ARBITRAGEM INTERNACIONAL E A PROTEÇÃO DE DADOS EM DISCUSSÃO

Quais tipos de conflitos podem surgir em matéria de proteção de dados e em quais destes a arbitragem pode se colocar para resolver adequadamente é uma questão

primordial, especialmente no Brasil, onde o interesse público desta matéria atrai a competência do Judiciário de plano.

Por essa razão e pelo histórico das demandas consumeristas se desenvolverem ao judiciário (ainda que diante da existência de cláusulas compromissórias), entendemos que conflitos emergentes da relação entre titulares e controladores/operadores é mais difícil ser passível de arbitragem, sendo muito provável que seja conduzida pelo Poder Judiciário.

Ainda assim, existem dois outros focos de conflitos que, emergindo de cláusulas contratuais, podem suscitar a aplicação deste método, sendo eles, conflitos entre controladores e conflitos entre controlador e operador.

É cada vez mais comum nos depararmos com previsões contratuais extensas para dispor sobre o tratamento de dados pessoais em determinado acordo comercial, alocação de responsabilidade em *Data Processing Agreements*, assim como as cláusulas contratuais padrão (ou "*Standards Contractual Clauses"*) no âmbito da transferência internacional de dados.

Dessa forma, centralizamos a discussão que está por vir pensando nesses casos hipotéticos, como ferramenta de afunilar o debate e explorar a autonomia das partes dentro do procedimento arbitral que contém múltiplas nacionalidades.

2.1. Autonomia e convenção das partes

A autonomia das partes é um dos fundamentos basilares da arbitragem internacional. Isso porque, sendo sua natureza predominantemente contratual, um tribunal arbitral apenas tratará de solucionar determinado conflito se assim for a expressa vontade das partes.[15]

Segundo a definição da Convenção de Nova Iorque, a convenção de arbitragem é "*o acordo escrito pelo qual as partes se comprometem a submeter à arbitragem todas as divergências que tenham surgido ou que possam vir a surgir entre si no que diz respeito*

[15] CARMONA, Carlos Alberto. Arbitragem e processo: um comentário à lei no 9.307/96. 3. ed. São Paulo: Atlas, 2009

a um relacionamento jurídico definido, seja ele contratual ou não, com relação a uma matéria passível de solução mediante arbitragem"[16].

São espécies de acordo a cláusula compromissória e o compromisso arbitral. Através de uma cláusula compromissória, a arbitragem pode ser instituída pelas partes antes do surgimento do conflito, ao passo que o compromisso arbitral prevê sua instauração a partir de uma controvérsia determinada.

Na arbitragem internacional, as partes se utilizam destes instrumentos para traçar as regras gerais: escolher a modalidade da arbitragem (institucional ou *ad-hoc*), critérios de designação de árbitros, a lei regente, o idioma, além da sede da discussão e outros. [17]

A ampla liberdade, indissociável desta forma de resolução de disputas, também vem acompanhada da grande responsabilidade de não comportar desistência ou arrependimento do compromisso, sendo possível a anulação da convenção somente em limitadas hipóteses previstas em lei, por exemplo, se constatada violação à soberania nacional, aos bons costumes e à ordem pública.

Apesar da convenção, por qualquer que seja a cláusula, criar lei entre as partes, a autonomia não é absoluta e nem sempre é suficiente para resolver o conflito ou garantir dos direitos dos titulares envolvidos na disputa.

Como veremos, ainda que as partes expressamente convencionem pela aplicação de determinada legislação em matéria de proteção de dados, como o GDPR ou a LGPD, caso possuam algum elemento de conexão com a realidade fática, ambas deverão ser inevitavelmente aplicadas.

2.2. Lei aplicável e conflito de normas

Conforme exposto, a autonomia das partes e os preceitos básicos da arbitragem internacional permitem às partes escolher a lei que governará suas relações contratuais e, por consequência, a lei aplicável a determinado conflito.[18] Não é tarefa simples quando

[16] BRASIL. Decreto nº 4.311, de 23 de julho de 2002. Promulga a Convenção sobre o Reconhecimento e a Execução de Sentenças Arbitrais Estrangeiras. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4311.htm Acesso em: 01 set. 2020.
[17] DECCACHE, Antonio Carlos Fernandes. Cláusula de arbitragem nos contratos comerciais internacionais. 1. ed. São Paulo: Atlas, 2015.
[18] BORN, Gary B. International arbitration: law and practice. 2. ed. The Netherlands: Kluwer Law International, 2015.

envolver duas ou mais nacionalidades ou caso parte do tratamento dos dados pessoais se dê em mais de um território.

No âmbito da arbitragem comercial, é consenso entre os países de *common law* e *civil law*, que em contrato devem ser determinadas a (i) lei que rege o direito em disputa ou o contrato principal celebrado entre as partes; (ii) lei que rege o procedimento arbitral; e (iii) lei que rege a convenção de arbitragem ou cláusula arbitral.

A lei que rege o direito em disputa ou o contrato principal celebrado entre as partes é o denominado direito substantivo. Neste sentido, a lei de regência deve ser escolhida para governar a interpretação e a validade do contrato principal, os direitos e deveres das partes, a forma de execução, e as consequências do descumprimento.

A lei que rege o procedimento arbitral ou a *lex arbitri*, por outro lado, diz respeito ao foro, geralmente optado por local neutro, mas que pode ser qualquer um que as partes aceitem, geralmente atrelado à escolha de determinada instituição que manterá o controle da disputa e todos os dados pessoais inerentes a esta.

Por fim, deverá ser determinada a lei que rege a convenção de arbitragem, decisão tão fundamental quanto a escolha lei do contrato principal, uma vez que "constitui negócio jurídico autônomo, com vida própria" e que pode suscitar discussões acerca de validade e competência, antecedentes ao mérito, conforme as lições de Antônio Carlos Fernandes Deccache[19].

A escolha desta última, em específico, pode acarretar discussões relacionadas a própria competência de determinado tribunal arbitral para resolver litígios envolvendo normas de proteção de dados, portanto, deve ser tratado com cautela.

Ocorre que, por vezes, as partes se omitirão ou não chegarão a um consenso quanto à lei aplicável a estas matérias, especialmente à lei da cláusula arbitral, de modo que compete aos árbitros decidir, através dos documentos e elementos fáticos que estão à disposição face ao caso concreto.

No sentido da jurisprudência, vem sendo utilizada para determinação da lei aplicável à cláusula arbitral a metodologia trifásica estabelecida pelo tribunal inglês, no caso "Sulamérica CIA Nacional de Seguros v. Enesa Engenharia S.A. 54" (caso Jirau),

[19] DECCACHE, Antonio Carlos Fernandes. Cláusula de arbitragem nos contratos comerciais internacionais. 1. ed. São Paulo: Atlas, 2015.

que tratou da cobertura securitária de sinistros ocorridos durante a construção da usina hidrelétrica de Jirau, no estado brasileiro de Rondônia, em março de 2011.[20]

Em suma, antes mesmo do debate de direito material, houve uma dúvida quanto a lei aplicável à convenção de arbitragem e a corte inglesa determinou a prevalência da lei inglesa, aplicando o que ficou conhecido como metodologia trifásica.

Na primeira fase da metodologia deve ser examinada a escolha expressa sobre a lei aplicável à convenção de arbitragem. Caso não haja determinação expressa, aplica-se a segunda fase, em que será analisada uma escolha implícita de lei, podendo ser àquela escolhida pelas partes para reger o mérito da demanda, por exemplo.

Inexistente lei explícita ou implícita, o tribunal deve verificar qual sistema jurídico guarda vínculos mais estreitos com a convenção de arbitragem. A terceira fase busca elementos concretos de conexão para se aproximar da realidade e da autonomia das partes.

Entendemos que, para os fins do presente estudo, os testes desenvolvidos para solucionar questões da espécie poderão não só contribuir para assegurar a competência arbitral em litígios envolvendo normas de proteção de dados, como para dirimir dúvidas entre normas conflitantes.

3. APLICABILIDADE DE NORMAS DE PROTEÇÃO DE DADOS NA ARBITRAGEM INTERNACIONAL.

A aplicabilidade de normas em uma arbitragem doméstica – contrato entre nacionais, envolvendo dados tratados em um único país e titulares nacionais -- não nos remete a quaisquer dúvidas. A lei aplicável será àquela da origem das partes e da disputa.

A arbitragem internacional, por outro lado, guarda maiores complicações, a medida em que dois ou mais sistemas legais são capazes de competir entre si como sendo o direito substantivo a ser observado.

À primeira vista, a aplicação das leis de proteção de dados no meio da arbitragem internacional não nos parece concorrentes. Isto é, defende-se que não há predileção de uma legislação de proteção de dados em detrimento de outra em demandas plurilocais, e

[20] CORTE DE APELAÇÃO INGLESA. Sulamérica Cia Nacional De Seguros S.A. and others v Enesa Engenharia S.A and others. EWCA Civ 638. Londres, 16 maio 2012. Disponível em: http://www.bailii.org/ew/cases/EWCA/Civ/2012/638.html. Acesso em: 10 set. 2020.

sim, a complementariedade de seus significados, dispositivos e princípios para maior efetividade da proteção dirigida às pessoas naturais e seus dados.

Por serem normativas tipicamente garantidoras de direitos fundamentais, legislações como o GDPR, LGPD e outras leis mundialmente conhecidas possuem princípios e regras muito harmoniosos entre si, quando não idênticas.

Vê-se, de outro lado, que algumas legislações são mais robustas que outras (algumas mais centralizadoras, outras mais delegatórias), criando neste caso, uma subsidiariedade entre as disposições e complementação lógica dos sentidos de seus textos. Esse caráter suplementar pode vir a impedir eventual invalidade da sentença arbitral, por exemplo.

Como já mencionado brevemente, a arbitragem no Brasil não poderá, de qualquer forma, ofender a soberania nacional, os bons costumes e a ordem pública. Neste cenário, se adotadas pelas partes normas que confrontem disposições de ordem pública brasileira (isto é, não elegendo a LGPD), eventual decisão poderá ser considerada nula, perdendo sua eficácia executiva.

Assim, vemos a complementação como forma de superar a discussão sobre uma única lei aplicável soberana e de preservação da ordem pública das nações envolvidas no debate.

Além disso, empresas multinacionais, quando se veem sob a ordem de normas distintas, optam por ajustar seus modelos e políticas de conduta perante todos os países em que operam, buscando a máxima conformidade.

Nos parece que esta prática é a mais adequada e a que mais atende aos desígnios das leis de proteção de dados desenvolvidas até então. Grande parte possui influência dos conceitos de *Privacy by Design* e *Privacy by Default*, que prevê a proteção e a privacidade dos dados em sua configuração mais restritiva possível e definida a cada fase do desenvolvimento de um projeto.

Portanto, espera-se que após efetiva incorporação da LGPD no ordenamento jurídico, seu órgão fiscalizador consolidado e sua integração sistêmica no cenário internacional, seremos contemplados com um cenário mais harmonioso, com normas integradas, semelhantes e concordantes.

Nada obstante, as normas podem vir a colidir. Isso porque o conflito concreto pode se dar tanto com relação à autoridade legitimada para processar e julgar a violação

concreta, ou seja, um conflito da competência em matéria de proteção de dados pelas autoridades identificadas em cada norma, como pelo conflito entre determinados dispositivos legais, sanções aplicáveis, obrigações conflitantes, etc.

Os conflitos podem surgir principalmente quando falamos nas diferenças entre a LGPD e o GDPR. Por exemplo: a LGPD estabelece que o tratamento de dados pessoais deve ser feito com segurança, sob orientações da ANPD, sendo omissa, contudo, sobre as técnicas de segurança obrigatórias, em termos de segurança digital. De outro lado, o GDPR estabelece formas para manter a segurança dos dados digitais através da encriptação e a pseudoanonimização. Se, porventura, a ANPD, no Brasil, estabelecer que outras técnicas são mais seguras, em oposição à encriptação e a pseudoanonimização, poderá haver um conflito sobre qual regramento é o mais adequado a ser aplicável a uma determinada situação.

Ainda, a pluralidade de significados e como as normas atribuem diferentes definições para um mesmo conceito também chama atenção: é o que acontece com a definição de estabelecimento, tratada de forma distinta pela LGPD e pelo GDPR.

Outros temas também podem representar um conflito entre as normas por suas divergências de regramento, como o marketing direto ou comercialização direta, a relação entre controlador e operador ou mesmo a definição dos dados sensíveis[21]. Estes assuntos são abordados diferentemente na LGPD e no GDPR.

Portanto, verificado um conflito entre as duas ou mais normas aplicáveis a determinada demanda arbitral, entendemos que deve ser feita a devida ponderação entre as normas, para resolução da controvérsia real. Nestas circunstâncias, a cláusula compromissória, o compromisso arbitral e a determinação da lei aplicável pelos próprios árbitros assumem relevante papel.

3.1. Resolvendo conflitos entre normas de proteção de dados.

Sem prejuízo do entendimento que ainda veremos consolidar na jurisprudência das cortes, nos casos práticos futuros, o conflito entre normas pode ser solucionado através da expressa convenção entre as partes (cláusula compromissória ou compromisso arbitral)

[21] No GDPR, onde há proibição de tratamento de dados sensíveis, salvo exceções, o regulamento os define apenas como “dados de saúde”, “dados biométricos” e “dados genéticos”, enquanto a LGPD fala uma gama ampla de dados, incluindo convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

ou dirimido pelo próprio tribunal arbitral, a partir das técnicas de aferição e determinação da lei aplicável, conforme a doutrina e jurisprudência.

Na perspectiva da convenção entre as partes, recomenda-se que haja uma análise global de todos os dados envolvidos, seu local de tratamento, de seus titulares e sua nacionalidade, assim como todas as normas que podem manter conexão com a lide.

Além de fazer constar no compromisso ou na cláusula quais leis mantêm conexão e serão aplicadas à matéria, defende-se a previsão de complementação das normas aplicáveis e, em casos de conflitos entre suas disposições, a opção final das partes.

Interessante ressalvar que as partes são livres e autônomas para convencionar a aplicação de determinada legislação, contudo, pela natureza especial destas normas, essencialmente de ordem pública, a legislação não eleita poderá ser aplicável às partes sob outros vieses de responsabilidade (como criminal, administrativa, em tutela coletiva, trabalhista, etc.).

Ainda que a autonomia das partes seja uma das bases da arbitragem, nada obsta um determinado País suscitar a competência sob a ótica da ordem pública e do caráter coletivo da lei de proteção de dados.

Caso as partes falhem em optar por uma norma para contrapor às demais em caso de conflito, caberá ao tribunal ponderação das normas para resolução da controvérsia, assim como analisar o conjunto probatório, a situação fática, a doutrina e jurisprudência internacional aplicável.

Importante notar que esta prática ainda se consolidará com os primeiros casos advindos da vigência da LGPD, já que não sabemos até que ponto ela poderá causar controvérsias reais no cenário internacional.

Por fim, é possível utilizar a orientação jurisprudencial do método trifásico utilizada nos casos Sulamérica Cia Nacional De Seguros S.A. and others v. Enesa Engenharia S.A and others, First Link Investments Corp. Ltd. v. GT Payment Pte. Ltd. (Singapura), BCY v. BCZ, dentre diversos outros[22].

[22] SUPREMO TRIBUNAL DA REPÚBLICA DE SINGAPURA. BCY v. BCZ. SGHC 249. Singapura, 9 nov. 2016. Disponível em: https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/bcy-v-bcz-(for-release)-(08-11-2016)-pdf.pdf Acesso em: 10 set. 2020.
SUPREMO TRIBUNAL DA REPÚBLICA DE SINGAPURA. FirstLink Investments Corp Ltd v. GT Payment Pte Ltd and others. SGHCR 12. Singapura, 19 jun. 2014. Disponível em: http://www.newyorkconvention.org/11165/web/files/document/1/7/17749.pdf. Acesso em: 10 set. 2020

Isso porque apesar de não tratar da determinação da lei aplicável a cláusula arbitral em si, é plenamente viável buscar resolver um conflito entre normas de lei de proteção de dados através de uma aplicação análoga da terceira fase.

A partir de sua concepção original, sugere-se que o tribunal responsável pelo julgamento verifique qual sistema jurídico guarda vínculos mais estreitos com a situação real, levando em consideração a natureza da controvérsia, a localidade das partes, do tratamento dos dados pessoais e dos titulares envolvidos.

3.2. ANPD e fiscalização na arbitragem institucional

Se as demandas plurilocais envolvem discussão e aplicação de diversas bases regulamentares para alcançar seu desfecho, é certo que nas câmaras arbitrais, os envolvidos terão grande responsabilidade para com estas diversas bases, assim como as secretarias e agentes destas instituições, à medida em que sofrerão fiscalização pelos respectivos órgãos.

Assim como os Estados Unidos tem Federal Trade Comission (FTC) e na União Europeia há Data Protection Commission (DPC) e outras autoridades de controle, o Brasil constituiu a ANPD, órgão que conta com a tríplice função de "zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional"[23].

A LGPD prevê que quanto maior o conjunto de dados tutelados sob o artigo 3º, mais responsabilidade perante a ANPD as Câmaras de Arbitragem possuirão. Neste aspecto, as próprias Câmaras podem ser comparadas com os tribunais judiciais brasileiros, em função da substancial quantidade de dados pessoais tratados nos seus procedimentos arbitrais.

Além da quantidade expressiva de dados, a pluralidade de sujeitos e nacionalidades envolvidas nas demandas internacionais é um fator de extrema atenção, pois aumenta as possibilidades de mais de uma legislação ser aplicável.

As Câmaras brasileiras ao lidar com disputas internacionais não estão de qualquer forma isentas da fiscalização e acompanhamento da Autoridade Nacional de Proteção de Dados, mesmo que em determinadas demandas se busque lei diversa da LGPD para reger a demanda.

[23] Art. 5º, inciso XIX, LGPD.

Pelo contrário, a arbitragem internacional poderá demandar mais atenção do que as arbitragens domésticas, em matéria de proteção de dados, não só pela grande quantidade de dados tratados, mas por reunir regulamentações estrangeiras, igualmente aplicáveis.

Nesse sentido, ainda que a confidencialidade já seja parte do procedimento arbitral, primordial revisitar e atualizar procedimentos e políticas para a arbitragem institucionalizada cumprir com suas atividades-fim, uma vez que estão sujeitas a aplicação das normas e a ainda desconhecida, porém inevitável atuação da ANPD.

Notamos, por fim, que ainda há muito que ser definido pela ANPD, inclusive no que diz respeito à transferências internacionais de dados e forma de fiscalização. Não há, no entanto, pelo menos por ora, que se falar em fiscalização, pela ANPD, de cumprimento de legislação estrangeira. Essa fiscalização deverá ser realizada apenas pela autoridade competente, nos limites de suas atribuições e competências, não estando excluída a possibilidade de compartilhamento de informações entre autoridades para fins de fiscalização e investigação.

CONSIDERAÇÕES FINAIS

A partir destas reflexões, conclui-se que os procedimentos de arbitragem internacional não estão desvinculados da ordem jurídica nacional e que as interações entre leis de proteção de dados em conflitos concretos na arbitragem internacional podem gerar diversas controvérsias quando se discutem cláusulas contratuais e instrumentos particulares entre agentes de tratamento.

Dessa forma será importante harmonizar as decisões e os métodos que os procedimentos arbitrais adotarão em face dos conflitos de aplicabilidade entre diversas normas nacionais que regem o mesmo tema, proteção de dados.

Nunca houve a regulamentação de um assunto tão intrinsicamente pulverizado em todo o globo quanto a proteção de dados pessoais, em uma época em que a transnacionalidade dos dados de indivíduos faz parte do cotidiano das empresas e seus negócios.

A discussão sobre a soberania estatal para assegurar os direitos de seus nacionais enfrentará grandes testes quando houver colidência entre as legislações. Não por acaso as próprias normas são tão similares, facilitando assim a complementariedade entre si, ao invés de um conflito entre si.

Neste novo cenário que está se construindo a cada dia, as partes, árbitros e câmaras de arbitragem devem estar cientes dos riscos inerentes ao processo de implementação das normas de proteção de dados das diversas nações que passam por seus procedimentos, especialmente quanto a LGPD, quando em solo brasileiro.

REFERÊNCIAS:

BORN, Gary B. International arbitration: law and practice. 2. ed. The Netherlands: Kluwer Law International, 2015.

BRASIL. Decreto nº 4.311, de 23 de julho de 2002. Promulga a Convenção sobre o Reconhecimento e a Execução de Sentenças Arbitrais Estrangeiras. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4311.htm Acesso em: 01 set. 2020.

BRASIL. Lei nº 9.307, de 23 de setembro de 1996. Dispõe sobre a arbitragem. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9307.htm. Acesso em: 01 set. 2020.

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm Acesso em: 01 set. 2020.

BRASIL. Lei nº 12.956, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 01 set. 2020.

BRASIL. Lei nº 8.078, 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em: 01 set. 2020.

CANADA. Personal Information Protection and Electronic Documents Act. S.C. 2000, c. 5. Disponível em: <https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html>. Acesso em: 10 set. 2020.

CANADA. Privacy Act R.S.C., 1985, c. P-21. <https://laws-lois.justice.gc.ca/eng/acts/P-21/index.html>. Acesso em: 10 set. 2020.

CARMONA, Carlos Alberto. Arbitragem e processo: um comentário à lei no 9.307/96. 3. ed. São Paulo: Atlas, 2009.

CORTE DE APELAÇÃO INGLESA. Sulamérica Cia Nacional De Seguros S.A. and others v Enesa Engenharia S.A and others. EWCA Civ 638. Londres, 16 maio 2012. Disponível em: http://www.bailii.org/ew/cases/EWCA/Civ/2012/638.html. Acesso em: 10 set. 2020.

DECCACHE, Antonio Carlos Fernandes. Cláusula de arbitragem nos contratos comerciais internacionais. 1. ed. São Paulo: Atlas, 2015.

FEIGELSON, Bruno. SIQUEIRA, Antonio Henrique Albani. Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. São Paulo. Thomson Reuters, Revista dos Tribunais, Brasil, 2019.

MALDONADO, Viviane Nóbrega. BLUM, Renato Opice. LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo. Thomson Reuters, Revista dos Tribunais, Brasil, 2019.

REVISTA DO ADVOGADO: Lei Geral de Proteção de Dados Pessoais. São Paulo: Associação dos Advogados de São Paulo, v. 144, nov. 2019. Mensal.

SUPREMO TRIBUNAL DA REPÚBLICA DE SINGAPURA. BCY v. BCZ. SGHC 249.

Singapura, 9 nov. 2016. Disponível em: https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/bcy-v-bcz-(for-release)-(08-11-2016)-pdf.pdf Acesso em: 10 set. 2020.

SUPREMO TRIBUNAL DA REPÚBLICA DE SINGAPURA. FirstLink Investments

Corp Ltd v. GT Payment Pte Ltd and others. SGHCR 12. Singapura, 19 jun. 2014. Disponível em: http://www.newyorkconvention.org/11165/web/files/document/1/7/17749.pdf. Acesso em: 10 set. 2020.

TRAKMAN, Leon and Walters, Robert and Zeller, Bruno, Is International Arbitration Prudent when Dealing with Personal Data Challenges? (August 1, 2019). Forthcoming (2019) Transnational Dispute Management, UNSW Law Research Paper No. 19-95, Available at SSRN: https://ssrn.com/abstract=3503176 or http://dx.doi.org/10.2139/ssrn.3503176

UNIÃO EUROPEIA. Parlamento Europeu e Conselho da União Europeia. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Relativa à proteção de dados das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>. Acesso em: 01 set. 2020.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 01 set. 2020.

ADMISSIBILITY OF EVIDENCE OBTAINED IN BREACH OF DATA PROTECTION LEGISLATIONS IN INTERNATIONAL ARBITRATION[1]

Autoria

Mariane Carvalho Amorim

Debatedores

Alice Moreira Franco

Gustavo Vaughn

Clicar ou escanear para acesso aos debates relativos a este artigo

ABSTRACT

Through the last decade, there has been an ongoing trend to edit national and international data protection legislations. Although national legislations do not necessarily apply to international arbitration, some of them, like the LGPD and the GDPR, are deemed to apply for practically all private entities within the territory. As these norms come into force, they must be bore in mind by arbitrators throughout proceedings. Thus, this paper intends to examine how data protection law will influence the admissibility of evidence, particularly the ones unlawfully obtained in breach of its provisions. This issue will be analyzed comparatively through the experience already obtained in the European Union (EU) aiming at assuming how these breaches will be treated in face of the Brazilian Data Protection Act (LGPD).

INTRODUCTION.

Two years after it was sanctioned by the former president Michel Temer, the Brazilian General Data Protection Act (hereafter 'LGPD') finally came into force[2]. As the beginning of its efficacy had been postponed for several times, the subtle decision to bring the starting date for September 2020 put all LGPD subjects in a race for becoming compliant.

[1] Artigo não atualizado após a realização dos debates.

[2] "*Lei Geral de Proteção de Dados entra em vigor*", Senado Notícias, Published: 18 September 2020, Access: 02 October 2020, Available at: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor.

In this sense, international arbitrations involving Brazilian entities must also be able to fulfil all requirements that from now on secure parties' right to privacy and data protection. Admissibility of evidence may be one of the factors affected the most by the regulation. As there are new grounds for obtaining, maintaining, and passing on personal data, a great part of information that was used to construct legal forms of evidence, may now be considered unlawful.

Therefore, the author intends to discuss the impacts caused by the coming into force of the LGPD and other national data protection legislations in international arbitration, especially regarding the concept of admissible evidence. Accordingly, this paper will answer the following questions: (i) how can data protection legislations make evidence unlawful?; (ii) considering the EU privacy law experience, how can we assume Brazil will treat documents obtained through breaches of the LGPD?; and, consequently and conclusively, (iii) will unlawfully obtained evidence, especially the ones in breach of these norms, be admitted in arbitration regulated by the LGPD?

The methodology chosen for this paper is one of comparative nature. First, the data protection legislation from the selected regions will be analyzed, especially regarding document production and evidence. Then, the doctrine of admissibility of unlawfully obtained evidence will be approached, verifying how evidence obtained from data breaches had been treated in arbitration. Finally, these matters will be analyzed jointly, concluding how privacy law might influence the admissibility of evidence.

1. REGIONAL ANALYSIS OF DATA PROTECTION REGULATIONS

On the one hand, considering that the LGPD has only recently come into force, there is still minimum doctrine and precedents regarding its scope and application. On the other hand, the EU adopted a directive pertaining data protection matters as early as in 1995, by means of the Directive 95/46/EC. This directive has then been superseded by the General Data Protection Regulation (GDPR), which became national law for all member states since May 2018. Thus, this chapter intends to dive into the history of the GDPR and the LGPD, looking for intersections and mismatches.

1.1. GDPR

Before the EU enacted the GDPR, data protection was ruled by Directive 95/46/EC. Even then, the regulation was already a model of general ruling on the matter of privacy,

different from countries like the United States, which until the present date still lack a general regulation on personal data and privacy[3]. Since the GDPR was implemented, it became the legal backbone of data protection and privacy in the EU. Both the GDPR and Directive 95/46/EC were meant to unify the data protection regulations for the member states, so that data could freely flow among them[4].

The GDPR contains a broad material scope, which extends its effects to almost every private organization and practitioner within the EU[5]. Recital 20 and 91 guarantee its applicability to judicial authorities and lawyers, assuring its reach to arbitration[6]. An entire paper could be written about the issues and adaptation needs for complying with the GDPR in arbitral proceedings. However, this paper focus is on how evidence might be tainted with illegality if it breaches this legislation. Thus, the rules for processing and sharing personal data must be looked at.

In this sense, Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime. These principles are laid out at the beginning of the code, as they contain its spirit, and must guide individual case analysis when verifying compliance by covered entities. Also, Article 83(5)(a) GDPR sets forth the highest fines for breach of the basic principles, as they constitute the core protections to subjects' personal data. The principles are the following:

Article 5(1) GDPR: [personal data shall be]

> *"(**a**) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency'); (**b**) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research*

[3] Esteve, Asunción. "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA." International Data Privacy Law 7.1 (2017): 36-47. P. 38.
[4] Titiriga, Remus. (2020). "*EU protection of the right to privacy and right to personal data and their connection to the Gonzales case and beyond*." SSRN Electronic Journal. KLRI (Korea Legislation Research Institute) Journal of Law and Legislation, 10. 139-164. P. 149.
[5] Zahariev, Martin. "*GDPR Issues in Commercial Arbitration and How to Mitigate Them*". Kluwer Arbitration Blog. Published: 07 September 2019. Access: 02 October 2020. Available at: http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/?doing_wp_cron=1593176922.7666449546813964843750
[6] Cf. Recital (20) "While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making." and Recital (91) "[…] The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory."

> *purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation'); (**c**) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (**d**) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (**e**) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation'); (**f**) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

One of the issues that arise out of these principles is the high costs involved in producing documents in a compliant manner. This was highlighted in the case Finjan, Inc. v. Zscaler, Inc., decided by a Federal Court in California in January 2019. In that case, Finjan ("Plaintiff") alleged that Zscaler ("Defendant") infringed its patent on a computer security technology. The accusation was based on the fact that Mr Warner, a former director from Plaintiff's company, had started working for Defendant and, according to the allegations, illegally disclosed details about Plaintiff's patented technology to Defendant. In order to support its claims, Plaintiff required the production of Mr. Warner's e-mails.

Defendant objected to said request by asserting that it could not produce such documents without breaching the GDPR. Considering the duties set forth by the GDPR, especially the one regarding data minimization, Defendant alleged that it would have to incur unreasonable costs to clean out the excessive data and provide the documents in a compliant manner. The Court ruled that, despite the alleged costs, Defendant could not avoid document production in the US, based on compliance to a statutory provision from the EU.

In circumstances such as the latter, entities will find themselves "between a rock and a hard place".[7] On the one hand, they might produce the evidence in breach of the

[7] Pearce, Alex. "*Between a Rock and a Hard Place? How GDPR Can Affect Discovery in US Litigation*". Ellis & Winters LLP Attorneys at Law. What's Fair Blog. Published: 19 February 2019. Access: 02 October 2020. Available at: https://www.elliswinters.com/trade/rock-hard-place-gdpr-can-affect-discovery-us-litigation/

GDPR and face the fines[8]. On the other hand, they can disrespect the authority demanding the document and face the legal consequences, which might be of even greater amount, depending on the circumstances. This issue might also arise in arbitration, in cases of document production demanded by the Tribunal, which can also impose penalties for noncompliance with its orders, or even when there is a request by one of the parties to produce evidence that is substantial for the case but which production costs are excessive in view of compliance. The arbitrators might face a situation of legal and financial impossibility, in which the evidence can not reasonably be expected to be produced.

Another matter that arbitrators might face is where one of the documents were obtained in breach of such principles but the requesting party had no influence on. The tribunal will have to balance the fact that the document is already available in the public domain[9] with the other party's right to be forgotten, recognized by the GDPR[10] and which would compel entities to make the data unavailable at the party's request, subject to sanctions. In any case, there are no straight answers or limits to how will the GDPR apply to document production.

1.2. LGPD

The LGPD is not that much innovative in face of the GDPR, having in mind that the project was inspired by the latter. Yet, there might be greater space to solve the issues previously raised, as the LGPD, in comparison, is leaner than the GDPR. In this sense, an entity compliant to the European legislation, will most likely easily comply with the LGPD. As the GDPR, the LGPD also has a broad scope, encompassing not only Brazilian subjects but basically any entity which practice somehow involves them[11].

[8] The fines for breaches of these principles have been reaching shocking amounts, as it was when Google was condemned to pay a 57 million dollars fine in France. Cf. also. Brasseur, Kyle. "*French court upholds Google's $57M GDPR fine*". Compliance Week. Published: 22 June 2020. Access: 02 October 2020. Available at: https://www.complianceweek.com/gdpr/french-court-upholds-googles-57m-gdpr-fine/29096.article

[9] "Public domain implies to be a state wherein the evidence is accessible to the public at large without undue hardship." Jain, Nitya. "*Can an Arbitral Tribunal Admit Evidence Obtained through a Cyber-Attack?*". Kluwer Arbitration Blog. Published: 27 January 2019. Access: 02 October2020. Available at: http://arbitrationblog.kluwerarbitration.com/2019/01/27/can-an-arbitral-tribunal-admit-evidence-obtained-through-a-cyber-attack/

[10] IT Pro Team. "*What is the 'right to be forgotten'?*". IT Pro. Published: 08 January 2020. Access: 02 October 2020. Available at: https://www.itpro.co.uk/general-data-protection-regulation-gdpr/what-is-the-right-to-be-forgotten

[11] KOCH, Richie. "*What is the LGPD? Brazil's version of the GDPR*". GDPR.EU. Access: 02 October 2020. Available at: https://gdpr.eu/gdpr-vs-lgpd/

The differences between the legislations relevant for the present paper are, first, the greater number of lawful bases for processing data set forth by the LGPD. Whereas the European Law only admits six reasonings for lawfully processing data, while the Brazilian Act lists ten[12]. One of the additional bases added to the LGPD in comparison with the GDPR is especially relevant to the present analysis. Article 7(VI) admits that data processing might occur to exercise rights in judicial, administrative or arbitration procedures.

Although the LGPD only recently came into force and there are still no available precedents regarding Article 7(VI), it can be assumed that in cases such as Finjan, Inc. v. Zscaler, Inc., the Brazilian Act would have greater flexibility to allow the party to duly fulfill the Court's order. Accordingly, in cases that an essential evidence for the regular exercise of the party's right was unlawfully made available with no bad faith involved, Article 7 (VI) might also serve as foundation to request the admissibility of the evidence.

2. ADMISSIBILITY OF UNLAWFULLY OBTAINED EVIDENCE

In the previous chapters, the author has analyzed how data protection regulations might make evidence unlawful. But even in the cases where the taint of illegality may not be removed, can arbitral tribunals admit such evidence? It must be clarified that there is not a sure answer to this question, but a common "*lawyerish"* one: it depends. There are different approaches to the admissibility of evidence, and it might be influenced by where the award will be enforced.

Considering the purpose of the present study, which is focused on European and Brazilian Law, doctrines like the Exclusionary Evidentiary Rule from the United States will not be considered, as it ultimately prevents evidence collected or analyzed in violation of the party's rights from being used in a court of law, considering it a "Fruit of the poisonous tree"[13]. When not dealing with these jurisdictions, e.g. in European

[12] Article 7. Personal data might only be processed in the following hypothesis: I – With the consent of the data subject; II - To comply with a legal or regulatory obligation of the controller; III - To execute public policies provided in laws or regulations, or based on contracts, agreements, or similar instruments; IV - To carry out studies by research entities that ensure, whenever possible, the anonymization of personal data; V - To execute a contract or preliminary procedures related to a contract of which the data subject is a party, at the request of the data subject; VI - To exercise rights in judicial, administrative or arbitration procedures; VII - To protect the life or physical safety of the data subject or a third party; VIII - To protect health, in a procedure carried out by health professionals or by health entities; IX - To fulfill the legitimate interests of the controller or a third party, except when the data subject's fundamental rights and liberties, which require personal data protection, prevail; or X - To protect credit (referring to a credit score).

[13] J.H. Boykin, M. Havalic (2014), "Fruits of the Poisonous Tree: The Admissibility of Unlawfully Obtained Evidence in International Arbitration" Transnational Dispute Management, (Provisional Issue).

countries, Tribunals may be more open to admit unlawfully obtained evidence, that is the case in *Cutajar v. Caruana*, which will be further explained in the next chapter. In countries which highly value principles such as good faith in a traditional and protective view, these evidences are also not likely to be considered, which is the case for Brazil, as an example. However, precautions must always be made, considering that, policy-wise, although arbitral tribunals must decide based on the most accurate description of the facts, the admissibility of this kind of evidence might lead to an incentive for parties to obtain documents unlawfully.[14]

Thus, the decision on the admissibility of unlawfully obtained evidence will always depend on the applicable law, including the law which governs the contract and specially the lex arbitri, which must be a part of the answer for such question. Regarding soft law mechanisms that discipline evidence production, the International Bar Association Rules on the Taking of Evidence in International Arbitration (hereafter "the IBA Rules") provides general standards on the admissibility of evidence. According to the preamble, it intends to "*to provide an efficient, economical and fair process for the taking of evidence in international arbitrations, particularly those between Parties from different legal traditions*".[15]

Article 9(1) of the IBA Rules grants the Arbitral Tribunal the power to decide on the admissibility, relevance, materiality, and weight of evidence. The broadness of this power is guided by the assumption that when deciding on admissibility of evidence, arbitrators are seeking to establish the necessary facts to get to the truth, not limited by technicalities[16]. Although this wide discretionary powers are also conferred by other international arbitration regulations, such as the UNCITRAL Model Law on International Commercial Arbitration[17] (hereafter "the Model Law"), they must be exercised sparingly, as admitting evidence in some circumstances might render the award unenforceable.

[14] Nicole, S Ng. "*Illegally Obtained Evidence in International Arbitration: Protecting the Integrity of the Arbitral Process.*" Singapore Academy of Law Journal. Published: 10 July 2020. Access: 04 October 2020. Available at: https://journalsonline.academypublishing.org.sg/e-First/Singapore-Academy-of-LawJournal/ctl/efirstCurrentArticleList/mid/568/ArticleId/1274?Citation=Published+on+eFirst+10+July+2020.

[15] "*IBA Rules on The Taking of Evidence*". Adopted by a resolution of the IBA Council. 29 May 2010. International Bar Association. Preamble. P. 4.

[16] Blackaby, Nigel; Partasides, Constantine; Redfern, Alan; Hunter, Martin. Redfern and Hunter on International Arbitration. 6th Edition. Oxford University Press (2015), p. 377.

[17] Article 19(2) of the Model Law states: "Failing such agreement, the arbitral tribunal may, subject to the provisions of this Law, conduct the arbitration in such manner as it considers appropriate. The power conferred upon the arbitral tribunal includes the power to determine the admissibility, relevance, materiality and weight of any evidence."

Therefore, the Tribunal might also consider the law, or at least the public policy, of the place of enforcement when deciding on the admissibility of unlawfully obtained evidence.

Having these remarks in mind, international doctrine has developed a system of topics that must be analyzed to conclude whether to admit or dismiss unlawfully obtained evidence. Thus, when facing this sort of issue, arbitrators must consider and balance: i) the relevance and materiality of the evidence; ii) the means used to obtain the evidence and the presence of "good faith", if applicable; iii) the nature of the law violated; and, iv) the risks to the enforceability of the award. In this sense, even though a straight answer to the question about the admissibility of evidence in international arbitration does not exist yet, there are a set of principles that may assist the tribunal in answering, in a case by case analysis.[18]

Diving into the step by step analysis set forth by the doctrine, the first topic is probably the most relevant one. Any jurisdiction will be gravely reluctant to admit evidence obtained illegally if there is no prove that such evidence is relevant for the case. This position is due to the exceptional nature of the admission of such evidence, which generally is based on parties' fundamental rights to fairness, to be heard and to properly present its case. If the evidence does not prove to be material, there is no reason why the Tribunal would risk the whole proceedings by applying such exception.

Following from that, investigating the means that the evidence was obtained, in particular in respect to good faith by the submitting party is also of essential nature. The obligation to act in good faith constitutes a general principle in international arbitration.[19] Moreover, most jurisdictions prohibit a party to benefit of its own unlawful behavior. Consequently, the second step of the examination intends to inhibit the parties to commit trespass and other illegalities aiming at proving their case.[20] The situations in which the submitting party proves to be in good faith includes the ones where the information to be admitted is already in public domain.

The third step is more technical and strictly connected to the fourth, the nature of the law violated will interfere directly in the enforceability of the award. Whenever deciding on the admissibility of evidence, the Tribunal is balancing, on the one hand,

[18] Fallah, Sara Mansour. "*The Admissibility of Unlawfully Obtained Evidence before International Courts and Tribunals*". In the Law & Practice of International Courts and Tribunals, vol. 19, issue 2. Online version. Brill | Nijhoff. 26 Aug 2020.
[19] Fouchard, Philippe; Gaillard, Emmanuel; Goldman, Berthold. "*International Commercial Arbitration*", Kluwer Law International, (1999), § 1479.
[20] Fallah. "The Admissibility of Unlawfully Obtained Evidence…". Online version.

parties' procedural guarantees, and on the other hand, the right or law violated in obtaining the evidence. The nature of such right, among the other previous factors, will certainly determine the weight of admitting the evidence.

3. PRIVACY AND DATA PROTECTION LEGISLATIONS' IMPACTS ON ADMISSIBILITY OF EVIDENCE.

A famous quote when discussing privacy and data protection law states that "There is a new mantra in cybersecurity today: It's when not if."[21] The increasing number of cyber-attacks suggest that arbitrators will be ever more frequently faced with questions of admissibility of evidence obtained in breach of data protection legislations. Considering the requisites for complying with the GDPR and the LGPD, as well as the test to analyze if an unlawfully obtained evidence may be admitted in international arbitral proceedings, the existence of a breach and it tainting the evidence with inadmissibility will depend on a case-by-case study.

In this sense, member states of the EU have already ruled in favor of the admissibility of evidence obtained in breach of the GDPR. That was the case in *Cutajar v. Caruana*, decided on February 2019. One of the parties alleged that one of the evidence submitted, a phone call recording, could not be admitted, as it did not consent to the recording and, thus, the evidence was obtained in breach of the GDPR. The Court recognized that the recording did constitute processing of personal data but considered that it did not have the competence to judge on data protection breaches.[22] The Maltese Court also highlighted that "the 'Exclusionary Rule' under US law was alien to the Maltese legal system and had not developed in the same way in Malta."[23] Thus, it considered that evidence obtained unlawfully, improperly or unfairly could be admitted.

The LGPD contains a less comprehensive scope then the GDPR, even permitting the processing of data for the regular exercise of rights in arbitral proceedings. In view of the possibility to admit evidence obtained in breach of the GDPR, it is most likely that this understanding will extend to the application of the LGPD. Nevertheless, when deciding upon the matter, the arbitrators should always consider the step by step analysis,

[21] David Reis, ABA Tech Report 2017, American Bar Association, Published: 01 December 2017. Access: 04 October 2020. Available at: https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html

[22] Bugeja, Thomas. "*Can evidence obtained in breach of GDPR be lawfully used as evidence?*". Times of Malta. Published: 30 June 2019. Access: 04 October 2020. Available at: https://timesofmalta.com/articles/view/can-evidence-obtained-in-breach-of-gdpr-be-lawfully-used-as-evidence.718126

[23] Ibid.

to avoid encouraging unlawful behavior by the parties and to fulfill the ultimate duty of filling an enforceable award.

CONCLUSION.

Regulating privacy and data protection in a world where technology develops million times faster than the law may seem like an impossible journey. The rush to encompass all possible scenarios have led most jurisdictions into having a messy net of independent regulations that do not connect or dialog with each other. The recent initiatives, starting with the EU and followed by Brazil, to consolidate and contemplate all data protection in a general act is essential to keep law comprehensive and to make it viable for data subjects to be aware of their rights and for processors and controllers to be compliant.

From the various sectors impacted by these regulations, for sure jurisdictional entities will be one of which faces the greater challenges. The matter of admitting evidence that breach data protection regulations is at its core a balancing principles activity, e.g. due process, the right to be heard and the general interest of the legal order. Although there are no straight answers, the following years will enrich the discussion, as the GDPR's enlarges its experience with matters of this nature and the LGPD creates its own.

BIBLIOGRAPHY

Blackaby, Nigel; Partasides, Constantine; Redfern, Alan; Hunter, Martin. Redfern and Hunter on International Arbitration. 6th Edition. Oxford University Press (2015).

Brasseur, Kyle. "French court upholds Google's $57M GDPR fine". Compliance Week. Published: 22 June 2020. Access: 02 October 2020. Available at: https://www.complianceweek.com/gdpr/french-court-upholds-googles-57m-gdpr-fine/29096.article

Bugeja, Thomas. "Can evidence obtained in breach of GDPR be lawfully used as evidence?". Times of Malta. Published: 30 June 2019. Access: 04 October 2020. Available at: https://timesofmalta.com/ articles/view/can-evidence-obtained-in-breach-of-gdpr-be-lawfully-used-as-evidence.718126

Esteve, Asunción. "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA." International Data Privacy Law 7.1 (2017): 36-47.

Fallah, Sara Mansour. “The Admissibility of Unlawfully Obtained Evidence before International Courts and Tribunals”. In the Law & Practice of International Courts and Tribunals, vol. 19, issue 2. Online version. Brill | Nijhoff. 26 Aug 2020.

Fouchard, Philippe; Gaillard, Emmanuel; Goldman, Berthold. “International Commercial Arbitration”, Kluwer Law International, (1999).

IT Pro Team. “What is the 'right to be forgotten'?”. IT Pro. Published: 08 January 2020. Access: 02 October 2020. Available at: https://www.itpro.co.uk/general-data-protection-regulation-gdpr/what-is-the-right-to-be-forgotten

“IBA Rules on The Taking of Evidence”. Adopted by a resolution of the IBA Council. 29 May 2010. International Bar Association. Preamble. P. 4.

J.H. Boykin, M. Havalic (2014), “Fruits of the Poisonous Tree: The Admissibility of Unlawfully Obtained Evidence in International Arbitration” Transnational Dispute Management, (Provisional Issue).

Jain, Nitya. “Can an Arbitral Tribunal Admit Evidence Obtained through a Cyber-Attack?”. Kluwer Arbitration Blog. Published: 27 January 2019. Access: 02 October2020. Available at: http://arbitrationblog.kluwerarbitration.com/2019/01/27/can-an-arbitral-tribunal-admit-evidence-obtained-through-a-cyber-attack/

KOCH, Richie. “What is the LGPD? Brazil’s version of the GDPR”. GDPR.EU. Access: 02 October 2020. Available at: https://gdpr.eu/gdpr-vs-lgpd/

“Lei Geral de Proteção de Dados entra em vigor”, Senado Notícias, Published: 18 September 2020, Access: 02 October 2020, Available at: https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor.

Nicole, S Ng. “Illegally Obtained Evidence in International Arbitration: Protecting the Integrity of the Arbitral Process.” Singapore Academy of Law Journal. Published: 10 July 2020. Access: 04 October 2020. Available at: https://journalsonline.academypublishing.org.sg/e-First/Singapore-Academy-of-LawJournal/ctl/efirstCurrentArticleList/mid/568/ArticleId/1274

Pearce, Alex. “Between a Rock and a Hard Place? How GDPR Can Affect Discovery in US Litigation”. Ellis & Winters LLP Attorneys at Law. What’s Fair Blog. Published: 19 February 2019. Access: 02 October 2020. Available at: https://www.elliswinters.com/trade/rock-hard-place-gdpr-can-affect-discovery-us-litigation/

Reis, David. ABA Tech Report 2017, American Bar Association, Published: 01 December 2017. Access: 04 October 2020. Available at: https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html

Titiriga, Remus. (2020). “EU protection of the right to privacy and right to personal data and their connection to the Gonzales case and beyond.” SSRN Electronic Journal. KLRI (Korea Legislation Research Institute) Journal of Law and Legislation, 10. 139-164.

Zahariev, Martin. “GDPR Issues in Commercial Arbitration and How to Mitigate Them”. Kluwer Arbitration Blog. Published: 07 September 2019. Access: 02 October 2020. Available at: http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate them/

PROCEDIMENTO ARBITRAL E NOVOS MEIOS DE PROVA: ACESSO À JUSTIÇA EFICAZ EM CONFLITOS ENVOLVENDO A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Autoria

Diane Brunoro Lyra

Nathan Correia de Azevedo

Clicar ou escanear para acesso aos debates relativos a este artigo

Debatedores

Alice Moreira Franco

Gustavo Vaughn

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709/2018, que entrou em vigor em 18.09.2020, é aplicada a pessoas físicas e jurídicas abrangendo as atividades de tratamento de dados pessoais. Ocorre que, com sua entrada em vigor, novos conflitos com especificidades próprias foram normatizados, eclodindo a necessidade de análise sobre os métodos e ferramentas adequadas para atender as controvérsias surgidas envolvendo dados pessoais. Diante desse cenário, o presente trabalho busca demonstrar as vantagens do uso do procedimento arbitral no lugar do método tradicional da jurisdição na busca de solução das controvérsias e da garantia do acesso à justiça, em especial nos conflitos envolvendo operador e controlador de dados, bem como meios de provas e regras probatórias que se mostram mais benéficas, quando comparadas aos meios tradicionais de provas nas demandas envolvendo dados pessoais. Concluindo-se que o procedimento arbitral, em especial por conta de sua maior flexibilização procedimental e probatória, e o uso de novos meios de provas e regras probatórias, mostram-se como cenários favoráveis e frutíferos para solução de conflitos envolvendo os direitos protegidos pela Lei nº 13.709/2018.

1. INTRODUÇÃO

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais– LGPD, em agosto de 2020, podemos observar a mudança em razão da privacidade e da proteção dos dados pessoais dos titulares, como ocorrido na Europa, com o advento da *General Data Protection Regulation – GDPR* publicada em 2016.[1]

Dessa forma, em razão a positivação dos direitos dos titulares, há de se atentar aos novos conflitos que podem surgir a partir da entrada em vigor da referida norma, a qual aduz sobre os agentes envolvendo a relação de proteção de dados, como, por exemplo, o controlador e o operador, os quais devem resguardar os titulares e seus direitos.

É de se esclarecer que o surgimento dessa norma ocorre em um contexto de intensificação do uso tecnológico de forma pessoal e profissional, tendo em vista as limitações causadas pela pandemia do coronavírus, trazendo uma maior proteção e fomento à economia digital com a regulamentação aprovada.

Face ao surgimento da normativa brasileira de proteção de dados pessoais e as novas tecnologias, cabe evidenciar que será necessário que os conflitos oriundos das relações citadas devam acompanhar a mesma evolução, principalmente, em se tratando das provas que serão produzidas nesses ambientes tecnológicos.

Dessa forma, sobre novos meios adequados e eficazes de provas em lides envolvendo os direitos protegidos pela Lei Geral de Proteção de Dados Pessoais, o presente trabalho se propõe a analisar de que forma a adoção de método diverso da jurisdição tradicional, em específico o procedimento arbitral, poderia viabilizar e permitir a aplicação de novos meios e regras probatórias nos novos conflitos.

2. ACESSO À JUSTIÇA POR MEIO DO PROCEDIMENTO ARBITRAL

Como consequência de novas relações sociais há o surgimento de novas litigiosidades, sendo necessário o desenvolvimento de novas ferramentas e meios de

[1] O advento da normativa europeia visando a privacidade e a proteção de dados pessoais reafirma um movimento voltado à privacidade e à intimidade da vida privada do indivíduo, em que tal norma surge para adaptar a legislação à mudança tecnologia, econômica e política nos tempos atuais.

acesso à justiça para atender às necessidades e diversidades das disputas que surgem e a própria racionalização da prestação jurisdicional[2].

O redimensionamento, releitura e atualização da garantia constitucional do acesso à justiça e inafastabilidade da jurisdição, com base nos princípios da efetividade e da adequação[3], adequa-se ao próprio desenvolvimento da justiça coexistencial[4], como forma de abarcar possibilidades de soluções de conflitos também no âmbito privado, com o fim de garantir uma ordem jurídica justa.[5]

A ampliação pela busca e acesso à justiça para além do Poder Judiciário é representada pela ideia da justiça multiportas[6], podendo cada conflito utilizar o tratamento adequado para suas particularidades, incluindo os métodos autocompositivos (negociação, mediação e conciliação), os heterocompositivos (poder judiciário e arbitragem), as esferas judicial e extrajudicial, setores públicos e privados e de forma presencial e virtual.[7]

Para a escolha da porta adequada deve-se atentar às características próprias do conflito para identificar o método adequado para sua solução. Assim, aprofundando tal discussão, o presente trabalho aborda sobre as novas lides decorrentes da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) que entrou em vigor em 2019.

A referida lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou pessoa jurídica de direito com o objetivo de proteção dos direitos fundamentais de

[2]Ethan Kath e Orna Rabinovich-Einy defendem em sua obra no contexto das disputas na internet e tecnologias, que se novas ferramentas novas ferramentas para lidar ou evitar disputas não puderem ser criadas com base em novas tecnologias, os riscos associados à inovação aumentarão e o valor de todas as ferramentas e recursos que nós temos diminuirão. KATSH, M. Ethan; RABINOVICH-EINY, Orna. Digital justice: technology and the internet of disputes. USA: Oxford University Press, 2017.

[3]DE PINHO, Humberto Dalla Bernardina. A mediação online e as novas tendências em tempos de virtualização por força da pandemia de Covid-19. Disponível em: <http://conhecimento.tjrj.jus.br/documents/5736540/7186707/AMEDIACCAOONLINEEASNOVASTENDENCIASEMTEMPOSDEVIRTUALIZACAOPORFORCADAPANDEMIADECOVID19>. Acesso em 11 maio 2021.

[4]CAPPELLETTI, Mauro. Os métodos alternativos de solução de conflitos no quadro do movimento universal de acesso à justiça. Revista de Processo, v. 19, n. 74, p. 82-97.

[5]CABRAL, Trícia Navarro Xavier. Justiça multiportas e inovação, p. 261 - 274. In: FUX, Luiz; ÁVILA, Henrique; CABRAL, Trícia Navarro Xavier (Ed.). Tecnologia e Justiça Multiportas: Teoria e prática. São Paulo: Editora Foco, 2021.

[6]"A expressão multiportas decorre de uma metáfora: seria como se houvesse, no átrio do fórum, várias portas. A depender do problema apresentado, as partes seriam encaminhadas para a porta da conciliação, ou da mediação, ou da arbitragem, ou mesmo da própria justiça estatal." PEREIRA, Alexandre Marçal. O processo Arbitral: aspectos gerais no Brasil e em Portugal. Revista jurídica luso-brasileira, ano 5, n 2, 2019, p. 855.

[7]CABRAL, Trícia Navarro Xavier. op. cit., loc. cit.

liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural[8]. Dispondo sobre os conceitos específicos de tais relações.

Inevitável asseverar que a nova norma traz também novas espécies de conflitos a serem tratados pela justiça, tornando visível que as novas especificidades das lides possam se acomodar além do meio tradicional de busca de justiça. Entretanto, ainda que ao analisarmos a porta dos "métodos heterocompositivos", os quais possuem um terceiro - juiz ou árbitro - que decide o conflito, percebe-se maiores vantagens com o uso do procedimento arbitral nos conflitos envolvendo a Lei Geral de Proteção de Dados Pessoais, sobretudo nas lides entre os agentes de tratamento de dados pessoais.

Ainda que haja uma flexibilidade dos procedimentos judiciais, a do procedimento arbitral é superior[9], em decorrência principalmente da autonomia da vontade e liberdade dos contratantes em estabelecer diretrizes para solução do conflito, através da liberdade para o estabelecimento da realização do procedimento, como a escolha dos árbitros, apresentação das alegações e produção de provas. A escolha do juízo arbitral não se mostra vantajoso apenas para a solução do conflito, mas também pela possibilidade das partes selecionarem a lei material aplicável ao caso.[10]

A liberdade e flexibilidade procedimental é inerente ao próprio procedimento arbitral, inclusive sendo facultado às partes a escolha das regras de direito aplicadas à arbitragem ou com base na equidade, nos princípios gerais de direitos, nos usos e costumes e nas regras internacionais de comércio, com a ressalva do respeito aos bons costumes e à ordem pública.[11]

[8]Art. 1º da Lei 13.709/2018: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

[9]"(...) a arbitragem é decorrente da autonomia da vontade, da liberdade. E essa liberdade também abrange a de estabelecer o procedimento arbitral. Já a jurisdição estatal é decorrente do exercício do poder estatal, que tem que ser limitado através de mecanismos de controle (freios e contrapesos), para que sejam evitados abusos." MONTORO, Marcos André Franco. Flexibilidade do procedimento arbitral. 210. 415 f. Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2010, p. 70.

[10]CARMONA, Carlos Alberto. Arbitragem e processo: um comentário à Lei nº 9.307/96. 3 ed., São Paulo: Atlas, 2009.

[11]Art. 2º da Lei 9.307/1996: "A arbitragem poderá ser de direito ou de eqüidade, a critério das partes. § 1º Poderão as partes escolher, livremente, as regras de direito que serão aplicadas na arbitragem, desde que não haja violação aos bons costumes e à ordem pública. § 2º Poderão, também, as partes convencionar que a arbitragem se realize com base nos princípios gerais de direito, nos usos e costumes e nas regras internacionais de comércio."

Sendo permitido a conjunção de regras e técnicas procedimentais de diversos sistemas jurídicos, como as regras sobre a instrução probatória, com o objetivo de satisfazer as partes envolvidas no conflito.

A parte litigante poderá determinar os moldes do procedimento arbitral, conforme artigo 11 da Lei 13.709/2018, como o local da arbitragem, o uso da equidade pelos árbitros, o prazo de apresentação da sentença arbitral, indicação da lei nacional ou regras corporativas aplicáveis e sobre os honorários.

Quando há a autorização expressa das partes pelo uso da equidade pelo juízo arbitral, os julgadores possuem a faculdade de não julgar conforme determinada norma jurídica pré-existente, podendo julgar da forma que considerar mais pertinente ao caso concreto, podendo recorrer, inclusive, a conceitos legais não vinculados ao procedimento arbitral.[12]

A liberdade quanto ao procedimento não está relacionada apenas às partes litigantes, o tribunal arbitral/árbitro pode, após a instituição da arbitragem, caso entenda necessário, junto com as partes, firmar um adendo que passará a fazer parte da convenção de arbitragem (artigo 19 §1º da Lei 13.709/2018). Ainda, caso não haja estipulação sobre procedimento na convenção de arbitragem, cabe ao tribunal arbitral/árbitro disciplinar sobre, com ressalva do respeito aos princípios do contraditório, da igualdade das partes, da imparcialidade do árbitro e de seu livre convencimento (artigo 21 §1º e 2º da Lei 13.709/2018).

Em síntese, de acordo com Montoro a flexibilidade do procedimento arbitral se divide no aspecto da possibilidade de criação, eleição e escolha das regras procedimentais a serem aplicadas à arbitragem pelas partes, árbitro, órgão arbitral institucional e o juiz estatal[13]; e no aspecto da possibilidade de adaptação, modificação e flexibilização das regras já definidas para a arbitragem já instituída.[14]

Nessa linha, as diversas formas de flexibilidade do procedimento arbitral, de acordo com o caso concreto, é o fator que torna o procedimento arbitral vantajoso, em especial em conflitos que versem sobre litígios não tradicionais, sendo moldado o procedimento

[12]TIBURCIO, Carmen. Arbitragem no Brasil: Panorama dos últimos 15 anos. In: Arbitragem. Temas contemporâneos. São Paulo: Editora Quartier Latin, 2012.
[13]Na hipótese de resistência quanto à instituição da arbitragem mesmo existindo cláusula compromissória, poder-se-á ser designada audiência especial em juízo com o fim de lavrar-se o compromisso, conforme disposto no artigo 7º da Lei 9.307/2018.
[14]MONTORO, Marcos André Franco. Flexibilidade do procedimento arbitral. 210. 415 f. Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2010.

arbitral para atender as necessidades da lide, das especificidades do direito material e das partes envolvidas. [15]

Não obstante as vantagens da flexibilização, liberdade e autonomia da vontade no procedimento arbitral, não se pode submeter indiscriminadamente os conflitos à arbitragem, além da capacidade das partes para submeter aos árbitros o litígio, o objeto deve tratar de direitos patrimoniais disponíveis, isto é, "são disponíveis (do latim *disponere*, dispor, pôr em vários lugares, regular) aqueles bens que podem ser livremente alienados ou negociados, por encontrarem-se desembaraçados"[16.]

Ainda, a Lei de Arbitragem (Lei 9.307/2018) dispõe que as partes interessadas para submeter determinado litígio ao juízo arbitral devem fazer por meio da convenção de arbitragem, entendida como a cláusula compromissória e o compromisso arbitral (artigo 3º), estando ambas as formas aptas a afastar a jurisdição estatal e instituir a arbitragem.

A cláusula compromissória é a convenção em um contrato entre as partes em que se comprometem a submeter eventuais litígios surgidos a partir do contrato à arbitragem (artigo 4º), já o compromisso arbitral é firmado quando não há um acordo prévio sobre a forma de instituir a arbitragem, devendo a parte interessada manifestar à outra sua vontade pelo início do procedimento arbitral (artigo 6º).

No tocante aos efeitos da convenção da arbitragem, seja por meio da cláusula ou compromisso são os mesmos, possuindo como objetivo principal afastar a competência do juiz estatal. Comenta Carlos Alberto Carmona:

> *"Em síntese apertada, a convenção de arbitragem tem um duplo caráter: como acordo de vontades, vincula as partes no que se refere a litígios atuais ou futuros, obrigando-as reciprocamente à submissão ao juízo arbitral; como pacto processual, seus objetivos são os de derrogar a jurisdição estatal, submetendo as partes à jurisdição dos árbitros. Portanto, basta a convenção de arbitragem (cláusula ou compromisso) para afastar a competência do juiz togado, sendo irrelevante estar ou não instaurado o juízo arbitral (art. 19)."*[17]

Portanto, possuindo as partes capacidade e o objeto sendo disponível, o procedimento arbitral apresenta-se como cenário adequado e vantajoso para a solução de conflitos, em razão da sua ampla possibilidade de flexibilização procedimental, tanto pelas partes quanto pelos árbitros, como forma de garantir a solução da demanda. Assim,

[15]MONTORO, Marcos André Franco. Flexibilidade do procedimento arbitral. 210. 415 f. Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2010, p. 70.
[16]CARMONA, Carlos Alberto. Arbitragem e processo: um comentário à Lei nº 9.307/96. 3 ed., São Paulo: Atlas, 2009, p. 38.
[17]Ibidem, p. 79.

conflitos que possuem objetos específicos e novos, como as relações envolvendo dados pessoais, podem se beneficiar positivamente com as vantagens do procedimento arbitral.

3. NECESSIDADE DE ADOÇÃO DE NOVOS MEIOS E REGRAS DE PROVAS EFICAZES

Ante aos novos possíveis conflitos que possam ocorrer em detrimento do surgimento dessa nova norma de proteção de dados pessoais, é necessário pontuar o possível conflito envolvendo controlador[18] e operador[19], que possuem correlação em relação ao tratamento de dados pessoais.

Cabe a presente análise aos conflitos decorrentes dessa relação, em casos que possa ser invocada a responsabilidade solidária de ambos no que tange a danos causados por descumprimento da Lei Geral de Proteção de Dados Pessoais suportados pelos titulares, de modo que seja necessária uma análise por meio de provas específicas para a apuração da responsabilidade e posterior reivindicação de direito regressivo.

Dessa forma, em um caso de violação dos direitos envolvidos na referida norma, a discussão do direito de regresso entre controlador e operador, supera a mera análise contratual ou verificação de termos, sendo necessária a aferição de novos meios de prova para a comprovação se a responsabilidade se dará em face do controlador ou do operador, em cada caso, como, por exemplo, analisar quem fora o responsável em um uso indevido de dados pessoais de colaboradores que pertençam a relação Controlador X Operador ou se houve transferência/compartilhamento indevido de dados pessoais decorrente dessa relação.

Entende-se que existe a possibilidade de diversos meios de prova, que é evidenciado no direito processual civil brasileiro. À luz do Código de Processo Civil, temos a positivação do princípio da liberdade probatória em que, se não há vedação para a produção de uma prova, aquele meio não será tido como ilícito.[20]

Sendo assim, a liberdade probatória nos conduz a saber administrar os meios de prova dentro da possibilidade de cada caso. Em se tratando de uma norma, como a Lei

[18]Art. 5º: VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
[19]Art. 5º: VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
[20] BRASIL. Código de Processo Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm Acesso em: 20 out. 2020.

Geral de Proteção de Dados, que rege não somente o ambiente físico, mas, em grande parte, o digital, de modo que (MELO, 2021, p. 533):

> (...) *o que antes era palpável, hoje está digital, em códigos binários, mas ainda assim, passível de ser apresentado fisicamente através da impressão ou representado por intermédio do próprio meio que possibilitou a atividade, caso seja necessário.*[21]

Vislumbra-se que, em se tratando de dados pessoais e a relação Controlador X Operador, o tratamento de dados em sua grande parte ocorre em meios digitais, uma vez que as informações, antes armazenadas em documentos físicos, foram transformadas em *bits* no ambiente digital.[22]

Dessa forma, ante a transformação digital, há a necessidade de serem verificados novos meios de prova que possam atender esse novo ambiente, em que tais meios deverão garantir a autenticidade, a segurança e a confiabilidade das evidências digitais.

Valendo-se citar uma que tem se destacado por possuir essas características, qual seja, a tecnologia *Blockchain*, que tem como conceito ser:

> (...) *uma base de dados distribuída, que roda em vários computadores diferentes ao redor do mundo ao invés de estar armazenada em um único local, e na qual dados podem apenas ser adicionados, mas não alterados ou removidos. Além disso, dados são adicionados ao sistema de forma linear e sequencial, formando uma "cadeia de blocos" (ou blockchain, no inglês).*[23]

Ou seja, podemos evidenciar que com esse meio de prova digital seria preservado todo o documento digital, como, por exemplo, uma mensagem instantânea, um e-mail ou um sítio eletrônico, preservando sua integridade.

A tecnologia *blockchain* permite a identificação de quem colheu a prova, quando foi efetuada a coleta, onde foi colhida, se aquela é uma cópia fidedigna da original, de modo a preservar toda a cadeia de custódia da prova.[24] Podendo ser solicitado a empresas

---

[21]MELO, Letícia. Blockchain: uma prova atípica. In: NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. Inteligência artificial e direito processual: os impactos da virada tecnológica no direito processual. Salvador: JusPodivm, v 2, 2021. p. 533

[22]BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 39

[23] HAMIDEH, Jamile; OSÓRIO JR. Edilson. Blockchain: TJSP reconhece validade de prova coletada sobre conteúdo online. Jota. 11 de ago. de 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/blockchain-tjsp-reconhece-validade-de-prova-coletada-sobre-conteudo-online-11082019#:~:text=Validade%20jur%C3%ADdica%20de%20provas%20certificadas,brasileiro%20que%20impe%C3%A7a%20tal%20uso>. Acesso em: 01 de out. de 2020

[24] HAMIDEH, Jamile; OSÓRIO JR. Edilson. Blockchain: TJSP reconhece validade de prova coletada sobre conteúdo online. Jota. 11 de ago. de 2019. Disponível em: <https://www.jota.info/opiniao-e-

que disponibilizam esse serviço ou, até mesmo, cartórios de notariais, como em São Paulo, que já utilizam esse tipo de tecnologia para verificar a autenticidade de uma página na web ou em um arquivo no computador.[25]

Dessa forma, tem-se por evidente a possibilidade e a necessidade de utilização desse meio de prova digital para poder preservar ocorrências nesse ambiente, seja em mensagens instantâneas, documentos digitais, sítios eletrônicos, uma vez que garante a integridade de uma evidência digital.

Outra possibilidade que abrange a produção de prova em meio digital, seria a aplicação das diretrizes estipuladas à ISO 27.037[26], a qual aduz meios adequados para a identificação, coleta, aquisição e preservação desse tipo de evidência.

Ainda que não se tratando de um método de produção de provas, como o citado *blockchain*, a norma esclarece as melhores práticas para a produção de uma evidência digital, minimizando possíveis interferências, alterações ou modificações da prova, identificando o agente que coletou a prova, localização e horário, dentre outras exigências cruciais para sua preservação.

De modo que, ao parametrizar as provas a essa normativa internacional, obriga aos participantes de um possível conflito para apuração de responsabilidade a um padrão probatório, em que as provas obtidas em meio digital, por exemplo, em smartphones, em *tablets*, em dispositivos de rastreamento, em computadores, deverão obedecer a referida norma, sob pena de ser invalidada ou ser desconsiderada.

Sendo assim, as provas que foram obtidas para aferir se houve utilização indevida de dados pessoais na relação Controlador x Operador, deverão seguir os parâmetros estipulados a ISO 27.037, o que evidenciará maior autenticidade, segurança e confiabilidade à produção de uma prova digital.

Além dos métodos citados, cabe citar as fontes abertas, que são meios de acesso livre da população em que qualquer do povo pode acessar e aferir a veracidade, ainda que *cum grano salis,* de certas informações. Dentre as fontes abertas, podemos listar algumas,

analise/artigos/blockchain-tjsp-reconhece-validade-de-prova-coletada-sobre-conteudo-online-11082019#:~:text=Validade%20jur%C3%ADdica%20de%20provas%20certificadas,brasileiro%20que%20impe%C3%A7a%20tal%20uso>. Acesso em: 01 de out. de 2020

[25] Disponível em: <https://www.anoreg.org.br/site/2019/11/19/2o-tabeliao-de-notas-de-sao-paulo-faz-sua-primeira-ata-notarial-de-blockchain>.

[26] Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=307273>.

como o *Archive Org*[27] ou o *Cached Pages*[28], que permitem a aferição da existência de um sítio eletrônico em determinado lapso temporal, e não somente em tempo real, por exemplo, quanto a aferição de utilização de dados pessoais indevidamente pelo operador ou pelo controlador em sítio eletrônico que foi retirado do funcionamento.

Dessa maneira, com o advindo desses novos possíveis conflitos que possam ocorrer entre Controlador x Operador, para a apuração de responsabilidade, é de inteira importância que tais novos métodos e meios de prova no ambiente digital, devam ser considerados e utilizados para tal, vez que esses possibilitariam a melhor apuração de fatos ocorridos em meios digitais, em face de documentos impressos ou provas testemunhais.

4. CONCLUSÃO

Depreende-se que as novas disputas decorrentes das demandas envolvendo a Lei Geral de Proteção de Dados Pessoais possuem especificidades próprias que o modelo tradicional de acesso à justiça pode não se mostrar como sendo o mais adequado para a solução das controvérsias.

Dentro dessa ideia, o trabalho propôs a demonstrar as vantagens do uso de métodos adequados de solução de conflitos, de forma específica o procedimento arbitral, principalmente no que tange a flexibilização da fase probatória, e de novos meios de provas e regras probatórios para os conflitos envolvendo dados pessoais, protegidos pela Lei Geral de Proteção de Dados.

Conclui-se que a utilização do procedimento arbitral é uma vantajosa possibilidade para que os direitos dos titulares possam ser amparados, com o julgamento ou a solução do conflito feita por um agente com conhecimento técnico para os casos específicos envolvendo infrações à LGPD, sem que os tribunais sejam abarrotados por demandas que ainda carecem de amplo conhecimento e discussão.

REFERÊNCIAS:

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 39.

[27] Disponível em: <https://archive.org/>.
[28] Disponível em: <http://www.cachedpages.com/>.

CABRAL, Trícia Navarro Xavier. Justiça multiportas e inovação, p. 261 - 274. In: FUX, Luiz; ÁVILA, Henrique; CABRAL, Trícia Navarro Xavier (Ed.). **Tecnologia e Justiça Multiportas**: Teoria e prática. São Paulo: Editora Foco, 2021.

CAPPELLETTI, Mauro. **Os métodos alternativos de solução de conflitos no quadro do movimento universal de acesso à justiça**. Revista de Processo, v. 19, n. 74, p. 82-97.

CARMONA, Carlos Alberto. **Arbitragem e processo**: um comentário à Lei nº 9.307/96. 3 ed., São Paulo: Atlas, 2009.

DE PINHO, Humberto Dalla Bernardina. **A mediação online e as novas tendências em tempos de virtualização por força da pandemia de Covid-19**. Disponível em: <http://conhecimento.tjrj.jus.br/documents/5736540/7186707/AMEDIACCAOONLINEEASNOVASTENDENCIASEMTEMPOSDEVIRTUALIZACAOPORFORCADAPANDEMIADECOVID19>. Acesso em 11 maio 2021.

HAMIDEH, Jamile; OSÓRIO JR. Edilson. **Blockchain**: TJSP reconhece validade de prova coletada sobre conteúdo online. Jota. 11 de ago. de 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/blockchain-tjsp-reconhece-validade-de-prova-coletada-sobre-conteudo-online-11082019#:~:text=Validade%20jur%C3%ADdica%20de%20provas%20certificadas,brasileiro%20que%20impe%C3%A7a%20tal%20uso>. Acesso em: 01 de out. de 2020.

MELO, Letícia. Blockchain: uma prova atípica. In: NUNES, Dierle; LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro. **Inteligência artificial e direito processual**: os impactos da virada tecnológica no direito processual. Salvador: JusPodivm, v 2, 2021. p. 531-555.

MONTORO, Marcos André Franco. **Flexibilidade do procedimento arbitral**. 210. 415 f. Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2010, p. 70.

PEREIRA, Alexandre Marçal. **O processo Arbitral**: aspectos gerais no Brasil e em Portugal. Revista jurídica luso-brasileira, ano 5, n 2, 2019, p. 855.

TIBURCIO, Carmen. **Arbitragem no Brasil**: Panorama dos últimos 15 anos. In: Arbitragem. Temas contemporâneos. São Paulo: Editora Quartier Latin, 2012.

KATSH, M. Ethan; RABINOVICH-EINY, Orna. **Digital justice**: technology and the internet of disputes. USA: Oxford University Press, 2017.

A LGPD COMO OBRIGATORIEDADE E OPORTUNIDADE: UMA ALIANÇA ENTRE ODR E PRIVACY BY DESIGN

Autoria

Letícia de Souza Baddauy

Mario Cesar Lobo Junior

Nathália Dalbianco Novaes Pereira

Clicar ou escanear para acesso aos debates relativos a este artigo

Debatedores

Juliana Loss

Marcelo Chiavassa

RESUMO

Este artigo relaciona os métodos de resolução de disputas online (ODR) com o conceito de Privacy by Design (PbD), desenvolvido por Ann Cavoukian, como forma de adequação tanto dos procedimentos quanto das câmaras e instituições à Lei Geral de Proteção de Dados brasileira (LGPD). Para tanto, o artigo se divide em duas seções: uma com a contextualização acerca do surgimento e crescimento dos ODRs; e outra a respeito das funções do Privacy by Design e da tecnologia da informação como aliados da proteção de dados e da privacidade, a partir de sua aplicação conceitual nos ODRs. As legislações brasileira e europeia, não restritas, mas especialmente na forma da LGPD e do General Data Protection Regulation (GDPR), são comparadas e exemplos de práticas existentes são trazidas ao debate. O texto ainda destaca os dispositivos aplicáveis da LGPD não só como uma obrigatoriedade, mas como oportunidade de inserir um padrão de proteção de dados nos processos e no design dos sistemas desde o início.

1. ONLINE DISPUTE RESOLUTION: UMA INTRODUÇÃO À TRANSIÇÃO DOS TRIBUNAIS FÍSICOS ÀS PLATAFORMAS DIGITAIS

Capelletti e Garth[1], na década de 80, impactaram profundamente o cenário jurídico ao trazerem à tona os desafios enfrentados pelo Poder Judiciário na gestão de conflitos, como o congestionamento processual e a massificação das demandas.

Paralelamente a isso, os autores alinharam-se à necessidade da implantação de "ondas renovatórias" de acesso à justiça, desmantelando o antigo paradigma de que os conflitos somente poderiam ser solucionados por intermédio do Poder Judiciário[2]. Dessa forma, seja na Academia, seja no âmbito prático-profissional, a modernização do tratamento de conflitos e a busca por novas formas de solucioná-los transformou-se em pauta para as mais acaloradas discussões jurídicas[3].

Nesse contexto, ganharam força os métodos alternativos de solução de conflitos (ADRs ou MASCs), aqui traduzidos como mediação, conciliação e arbitragem.

A disseminação dos ADRs não se pautou em atribuir "substitutos" ao Poder Judiciário, tampouco de direcioná-los com foco somente para descongestionamento processual. Tratava-se de ampliar o acesso à justiça e de analisá-lo sob a óptica do *multi-door courthhouse*, de Frank Sander[4], por meio do qual cada conflito deve receber o tratamento que lhe for mais adequado.

Mais do que promover formas de solucionar controvérsias para além do Judiciário, os ADRs contribuíram consideravelmente para o início da transição de uma sociedade que transcendia em demandismo judicial, para uma sociedade mais autônoma em relação às suas próprias controvérsias, fomentando a gestão de conflitos a partir da "cultura da paz" defendida por Watanabe[5].

Além disso, outro fator importante na disseminação dos ADRs no Brasil, foram os diversos incentivos legais, destacando-se a Resolução nº 125/2010 do CNJ, bem como as consequentes Lei de Mediação, Lei de Arbitragem e o próprio Código de Processo Civil,

[1] CAPELLETTI, Mauro; GARTH, Bryant. Acesso à justiça. Porto Alegre: Fabris, 1998.
[2] Ibidem.
[3] CAHALI, Francisco José. Curso de Arbitragem: mediação, conciliação e tribunal multiportas. 7 ed. São Paulo: Thomson Reuters Brasil, 2018, p. 29.
[4] SANDER, Frank. The Multi-Door Courthouse: Settling Disputes in the Year 2000. HeinOnline: 3 Barrister 18, 1976.
[5] WATANABE, Kazuo. Cultura da sentença e cultura da pacificação. *In:* YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (org.). Estudos em Homenagem à Professora Ada Pellegrini Grinover. São Paulo: DPJ, 2005, p. 684-690.

os quais formaram um verdadeiro "microssistema" sobre o assunto e contribuíram para a consolidação dos institutos. Não por acaso que se afirma que a desconfiança em torno dos ADRs, hoje, não passa de um dissabor histórico e completamente superado.

O fato é que, quarenta anos após o *boom* da terceira onda renovatória de acesso à justiça e da devida solidificação dos ADRs, a situação ganhou novos contornos evolutivos. A expansão tecnológica fez da internet o "lugar mais habitado do mundo". Por meio de alguns cliques, pessoas, culturas e legislações se entrelaçam profundamente, em uma dinâmica acelerada e inerente ao mundo globalizado.

Consequência natural é que surjam conflitos em grande escala, os quais, não raras as vezes, transcendem as barreiras territoriais. Desse modo, as maravilhas do mundo online se transformam em verdadeiros entraves na vida offline, afinal, os *players* envolvidos nas relações negociais almejam solucionar os conflitos com a mesma facilidade - e velocidade - que possuem para formalizar contratações.

Embora os métodos alternativos de soluções de controvérsias (conciliação, mediação e arbitragem) sejam poderosos atrativos dentro desse contexto, dada a flexibilidade procedimental a que lhes são comuns, todos eles demandam tempo, consideráveis custos e deslocamento físico, fatores incompatíveis à dinamicidade descrita.

Assim, considerando-se que o online norteia todas as relações humanas, sobretudo as negociais, a utilização da tecnologia para prever e solucionar disputas nada mais é do que parte da linha evolutiva de acesso à justiça[6].

Nesse sentido, tal qual discutiu-se sobre a utilização dos ADRs, na década de 80, nos últimos anos acendeu-se o debate sobre a utilização da tecnologia para atribuir novas linguagens às soluções de conflitos: o chamado *online dispute resolution* (ODR).

Tamanho o destaque dos ODRs, que Marques assevera o fato de organizações internacionais, entidades de proteção e defesa do consumidor e entes governamentais e empresariais nos Estados Unidos, na Europa e também no Brasil implementarem cada vez mais a sua utilização.[7]

[6] MARQUES, Ricardo Dalmaso. A resolução de disputas online (ODR): do comércio eletrônico ao seu efeito transformados sobre o conceito e a prática do acesso à justiça. Revista de Direito e as Novas Tecnologias: Revista dos Tribunais Online, [s. l.], v. 5/3019, out./dez. 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3525406. Acesso em: 01 out. 2020.
[7] Ibidem, p. 8.

As soluções de conflito online podem ser consideradas tanto sob a perspectiva ampla, quanto sob um aspecto mais estrito. Na primeira hipótese, considera-se ODR todo e qualquer uso de tecnologia no trâmite procedimental, o que inclui desde a digitalização de documentos até as audiências por videoconferência[8]. Em outras palavras, o conceito amplo de ODR contempla a "transposição, para a internet e a telefonia móvel, os conflitos cuja solução antes dependia do encontro presencial entre as partes e eventuais agentes neutros"[9], aplicando-se a tecnologia aos ADRs[10].

Já sob a óptica dos conceitos mais estritos, os ODRs não se limitam à simples informatização ou substituição de canais de comunicação tradicionais, "mas agem como vetores para oferecerem às partes ambientes e procedimentos ausentes em mecanismos convencionais"[11].

Nessa perspectiva, entende-se que, nos ODRs, a conciliação, a mediação e a arbitragem são redesenhadas para o ambiente virtual, com base na interação entre pessoas, o direito e as plataformas digitais, o que pode conferir resultados mais efetivos às soluções de disputas. Isso se justifica na medida em que:

> *Ao realçarem certas informações, elaborarem materiais de subsídio para decisões (das partes ou de neutros), promoverem reflexões sobre as controvérsias e alterarem as ambições inicialmente presentes, as tecnologias empregadas na ODR incrementam as chances de consenso em torno de um acordo e esclarecem os impactos da decisão a ser impostas às partes, o que pode ser crucial para preservar relacionamentos e, até, para permitir a construção de valor por meio de alternativas novas*[12].

Nesse viés, Katsh e Rule[13] assumem que o grande diferencial do ODR é atuar como uma "quarta parte", capaz de adaptar a linguagem comunicativa dos litigantes, elencar opções para solucionar o conflito, estabelecer agendas, realizar cálculos e, portanto, participar efetivamente dos procedimentos de resolução de disputas.

Isso representa um grande avanço na esfera psicológica envolta na gestão de conflitos, uma vez que os ODRs promovem a diminuição de atritos comuns em vias

[8] ARBIX, Daniel. Resolução online de controvérsias. São Paulo: Intelecto, 2017, p. 57-64.
[9] ARBIX, 2019, p. 4.
[10] MÜLLER, Karina Haidar *et al* Resolução de Disputas OnLine e a Propriedade Intelectual: uma Via Possível?'. Arbitragem e Mediação em Matéria de Propriedade Intelectual. Kluwer Arbitration, 2020, p. 110.
[11] ARBIX, op.cit., 2017, p. 14.
[12] ARBIX, op. cit., 2019, p. 4.
[13] KATSH, Ethan; RULE, Colin. What we know and need to know about online dispute resolution. South Caroline Law Review, 2015, p. 55.

presenciais e criam ambientes adaptáveis às circunstâncias do conflito, o que inexiste no cenário físico.

Não bastante, contempla-se os impactos econômicos decorrentes da utilização dos ODRs, visto que tendem a diminuir os custos de transação dos atos procedimentais físicos, sejam eles judiciais, de mediação ou arbitrais e tornando-se, assim, mais acessível aos usuários.

Inclusive, ainda em relação às vantagens econômicas, os ODRs ganham ainda mais força ao encurtarem as distâncias, já que isto possibilita que partes de diferentes regiões se reúnam virtualmente para acordos e/ou audiências. Por consequência, os procedimentos se tornam mais céleres e não demandam gastos com deslocamentos.

Além disso, a possibilidade do encurtamento de distâncias pode ser considerada uma vantagem para além dos aspectos econômicos. Isso porque, nesse contexto, o aspecto ambiental se torna bastante relevante, uma vez que a utilização dos ODRs acaba por contribuir com a diminuição das pegadas de carbono, em comparação à utilização dos métodos de solução de conflito físicos/presenciais, o que é um dos desafios da comunidade arbitral internacional instituído pela *Campaign for Greener Arbitrations*[14].

Atrelado a todos esses fatores que impulsionaram a utilização dos ODRs, ressalta-se também a pandemia de COVID-19, que exigiu o isolamento social ao redor do mundo e acentuou a utilização (e as contratações) por vias digitais. Assim, o ambiente que já era fértil, tornou-se ainda mais propício e necessário para a implantação dos *online dispute resolutions*. Prova disto é que importantes centros de solução de conflito, como a CAM-CCBC[15], já alteraram os seus regulamentos para receberem procedimentos de mediação e arbitragem de forma online, reforçando a tendência de que a utilização dos ODRs não seja apenas uma opção diante da pandemia, mas sim uma constante também no cenário pós-pandêmico.

A tecnologia, que ainda caminhava em passos curtos e tímidos nas instituições de solução de conflito, foi catalisada no período de pandemia e abriu alas para um caminho sem volta: a definitiva implantação de sistemas procedimentais de forma online, uma

[14] CAMPAIGN FOR GREENER ARBITRATIONS. Driving sustainable change. 2021. Disponível em: https://www.greenerarbitrations.com/. Acesso em: 04 jul 2021.
[15] CAM-CCBC. Resolução Administrativa 40/2020. Nova organização administrativa e normas para o processamento eletrônico dos procedimentos. Disponível em: https://ccbc.org.br/cam-ccbc-centro-arbitragem-mediacao/ra-40-2020/. Acesso em: 02 out. 2020.

verdadeira transição do ambiente físico para o digital. É a justiça entendida como um serviço, não como um lugar[16].

Porém, se por um lado salta aos olhos a tentadora dinamicidade dos ODR, por outro lado a nova era das resoluções de conflito traz consigo, além do inegável entusiasmo, uma série de preocupações, que precisam ser amplamente debatidas e encaradas pelos profissionais.

Sobre o assunto, Arbix[17] reforça que o ambiente online não isenta os *players* e as tecnologias de agirem com respeito aos princípios procedimentais. Por este motivo, os cuidados com a ética e com a lisura do procedimento devem se fazer presente também no ambiente virtual, para que a transparência e a justiça procedimental sejam garantidas e legitime as soluções de disputa online assim como são legitimadas as soluções de conflito offline[18].

Outro fator a ser discutido diz respeito à proteção de dados, visto que as plataformas digitais, ao operacionalizarem todo o procedimento, precisam coletar informações sobre as partes, os árbitros/mediadores/conciliadores e a controvérsia em si, seja via e-mail, seja via plataforma online.

Ocorre que tais informações, muitas vezes, além de versarem sobre dados pessoais, podem se referir também à dados sensíveis, ambos protegidos pela Lei Geral de Proteção de Dados (LGPD).

Nesse sentido, para além da preocupação com a disseminação da utilização dos ODR e suas respectivas vantagens, faz-se necessário discutir a relevância do correto gerenciamento de dados no âmbito das plataformas online de soluções de disputas. Afinal, na era da proteção de dados, segurança e transparência são primordiais para garantir a efetividade e a qualidade das soluções.

2. OS ARRANJOS DO SÉCULO XXI PARA ANTIGOS CONHECIDOS[19]

Foi nos idos da década de 1990 que os métodos de resolução de disputas online passaram de uma fase amadora, com utilização ainda muito restrita, para uma aplicação

[16] SUSSKIND, Richard. The Future of Courts. The Practice: remote courts. 5. ed., v. 6, jul./ago., 2020. n.p. Disponível em: https://thepractice.law.harvard.edu/article/the-future-of-courts/. Acesso em: 3 out. 2020.
[17] ARBIX, op. cit., 2019, p. 4.
[18] MARQUES, op. cit., p. 22.
[19] Esta seção dialoga com as conclusões de Julia Hörnle presentes em HÖRNLE, J. Online Dispute Resolution: the emperor's new clothes? International Review of Law, Computers & Technology, [s. l.], v.

em maior escala, devido, dentre outros motivos, ao crescimento econômico de então[20] e ao desenvolvimento acelerado da área de tecnologia da informação (TI).

É possível observar que desde o princípio os ODRs estão intrinsecamente conectados não só com a ideia de comunicação à distância, mas também com serviços de TI, segurança da informação[21] e tecnologias cada vez mais sofisticadas. Não é por outro motivo que Julia Hörnle caracteriza a resolução de disputas como um "processo complexo de gerenciamento e processamento de informações e de comunicação" [22].

Se nos últimos anos do século XX, quando a World Wide Web começava a se espalhar, já havia certa preocupação com o uso das informações em ambiente online – e fora dele, inclusive -, muito se deve a estudos e normas que passaram a endereçar os problemas oriundos dessa utilização aos responsáveis por seu gerenciamento.

Um desses estudos, desenvolvido pela ex-comissária de informação e privacidade da província de Ontario, Canadá, Ann Cavoukian, resultou em 7 princípios fundamentais do que chamou de Privacy by Design (PbD), são eles[23]: (i) proativo e preventivo, ao invés de reativo e corretivo; (ii) privacidade como a configuração padrão; (iii) privacidade integrada ao design; (iv) soma positiva, e não negativa, entre a proteção da privacidade e de outras exigências, tais como segurança e performance (funcionalidade completa); (v) segurança de ponta a ponta e durante todo o ciclo de vida do dado; (vi) visibilidade e transparência das práticas de privacidade; e (vii) respeito pelo usuário, mantendo-o no centro da proteção.

O conceito está relacionado à inserção da privacidade como um padrão no design de "tecnologias da informação, práticas comerciais e infraestruturas de rede"[24].

Em outubro de 2010, durante a 32ª Conferência Internacional dos Comissários de Proteção de Dados e Privacidade, realizada em Israel, o Privacy by Design foi

17, n. 1, p. 27-37, 2003. DOI 10.1080/1360086032000063093. Em certa medida, também relaciona os avanços do ODR com a tecnologia da informação.

[20] MANIA, Karolina. Online dispute resolution: the future of justice. International Comparative Jurisprudence, [S.L.], v. 1, n. 1, p. 77, nov. 2015. Mykolas Romeris University. http://dx.doi.org/10.1016/j.icj.2015.10.006.

[21] Ibidem, p. 78.

[22] HÖRNLE, op. cit., p. 28, tradução nossa.

[23] CAVOUKIAN, Ann. Operationalizing Privacy by Design: a guide to implementing strong privacy practices. Information and Privacy Commissioner. Ontario, Canada: 2012, p. 3-4, tradução nossa.

[24] CAVOUKIAN, op. cit., 2012, p. 8.

reconhecido como importante componente para a proteção da privacidade, em especial durante a gestão de informações a partir de sistemas de TI e de comunicação[25].

Foi também no mês de outubro, mas desta vez de 1995, que o Parlamento Europeu e o Conselho da União Europeia passaram a adotar a Diretiva 95/46/EC, que regulava a proteção de pessoas singulares em relação ao tratamento de dados pessoais e à livre circulação destes dados. É nesta diretiva que conceitos como o de dados pessoais, já conhecidos em razão da Lei Geral de Proteção de Dados brasileira, ganham contornos mais objetivos.

Ainda no campo das normas, uma importante aproximação entre o conceito de PbD e os ODRs consta do Regulamento nº 524/2013, igualmente do Parlamento Europeu e do Conselho. Ao dispor sobre a resolução de disputas online envolvendo o consumo, a normativa prevê o desenvolvimento de uma plataforma que respeite a privacidade de seus usuários desde a fase de concepção[26].

De acordo com o artigo 5 (2) do Regulamento, a plataforma é o ponto de referência para resolução de disputas entre consumidores e comerciantes, na forma de um website interativo. Dentre as funções[27] que inevitavelmente envolvem o tráfego e o tratamento de dados na citada plataforma estão: (i) o fornecimento de um formulário eletrônico para registro da queixa do autor; (ii) a identificação de uma entidade, ou entidades, competente(s) de ADR; (iii) a transmissão da queixa à entidade escolhida pelas partes; e (iv) a disponibilização de uma ferramenta de gestão do caso.

Nota-se, então, que o conceito de Privacy by Design foi ganhando novos arranjos, isto é, contextos práticos de aplicação que o inter-relacionam com os métodos de resolução de conflitos online e, mais tarde, com as medidas de proteção de dados; esta última centrada no General Data Protection Regulation (GDPR).

De acordo com Romanou[28], o resultado da aproximação supracitada foi a "conversão de um conceito teórico em uma obrigação legal e em um princípio essencial de proteção de dados". O artigo 25 do GDPR dispõe que cabe ao controlador implementar

[25] Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalém, Israel, 27-29 out. 2010, p. 1.
[26] Artigo 5 (1) do Regulamento nº 524/2013.
[27] Artigo 5 (4) do Regulamento nº 524/2013.
[28] ROMANOU, Anna. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. Computer Law & Security Review, [S.L.], v. 34, n. 1, p. 102, fev. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.clsr.2017.05.021.

medidas técnicas e organizacionais aptas a protegerem os direitos dos titulares[29] e a respeitarem os princípios de proteção de dados.

Mesmo sem menção expressa no corpo de seu texto, a LGPD também acolheu este importante princípio ao prever que as medidas de segurança, técnicas e administrativas que visam a proteger os dados pessoais devem ser observadas "desde a fase de concepção do produto ou do serviço até a sua execução"[30].

Feita essa breve contextualização, é oportuno definir em que medida as instituições e câmaras de resolução de disputas podem se valer do PbD para adequarem os sistemas de gestão de informação e de comunicação de seus procedimentos.

O que se observa é que a legislação brasileira, longe de apresentar um problema, traz uma oportunidade, qual seja: a de revisar ou mesmo adotar práticas de adequação organizacional que tenham a privacidade e a proteção de dados como fundamento, do início ao fim do tratamento. Tanto na hipótese de adoção quanto na de revisão das práticas, é essencial contar com a inserção da equipe de TI nessas estratégias.

Os profissionais de tecnologia da informação também podem desenvolver e gerenciar as medidas de segurança contra acessos não autorizados, destruição, perda, alteração ou comunicação indevida dos dados[31]. Dag Wiese Schartum[32] aponta que o PbD pressupõe a união entre o conhecimento de questões legais ligadas à privacidade e o conhecimento técnico para o desenvolvimento de tecnologias e sistemas.

Ainda segundo Schartum, o desenvolvimento de um sistema de informação com o que chama de *privacy by design modules* (módulos de privacy by design) funciona como "códigos de conduta funcionais"[33], em referência ao artigo 27 da Diretiva 95/46/EC[34]. Com o devido distanciamento entre as normas europeia e brasileira, pode-se dizer que se não semelhante, muito próxima é a ideia do artigo 50 da LGPD, ao possibilitar a controladores e operadores a adoção de regras de boas práticas e de governança. Consequentemente, os procedimentos internos, normas e padrões técnicos, obrigações e regras de funcionamento podem ser estabelecidos, organizados e melhor administrados.

[29] Artigo 25 do GDPR.
[30] Artigo 46, § 2º da LGPD.
[31] Artigo 46 da LGPD.
[32] SCHARTUM, Dag Wiese. Making privacy by design operative. International Journal of Law and Information Technology, [S.L.], v. 24, n. 2, p. 162, 24 fev. 2016. Oxford University Press (OUP). http://dx.doi.org/10.1093/ijlit/eaw002.
[33] Ibidem, p. 173, tradução nossa.
[34] Constante também do artigo 40 do GDPR.

O conceito de Privacy by Design, portanto, encontra um importante campo de aplicação nos sistemas e práticas adotados durante os procedimentos de ODR. Se este último é conceituado por Hörnle[35] como sendo a aplicação de "TI e comunicação à distância aos tradicionais processos de ADR, como conciliação, mediação e arbitragem"; o conceito desenvolvido por Ann Cavoukian vê justamente na tecnologia da informação uma aliada para sua incorporação.

Com relação às práticas comerciais, ou do negócio, uma pesquisa de Martín-Romo Romero e De-Pablos-Heredero[36] mostrou que 94% dos experts em privacidade entrevistados apontam o aumento nos níveis de proteção como um dos pontos fortes da implementação da proteção de dados pessoais no design dos processos corporativos[37].

Um tema de tamanha relevância que já começa a ver seus efeitos na prática não pode se limitar a previsões e ações genéricas ou mesmo inexistentes. Neste sentido, a London Court of International Arbitration (LCIA) merece destaque ao destinar um artigo específico sobre proteção de dados em suas novas regras de arbitragem[38] e mediação[39], em vigor desde 1º de outubro de 2020.

O artigo 30A das *Arbitration Rules* e o artigo 13 das *Mediation Rules* preveem, por exemplo, que o tribunal arbitral ou o/a mediador/a, a depender do caso, deve considerar a adoção de medidas de segurança aptas a protegerem informações em formato físico e eletrônico, a partir de consulta às partes e, se necessário, à própria LCIA.

Dois pontos muito interessantes podem ser enfatizados. O primeiro está ligado à previsão expressa de proteção das informações físicas e digitais, o que também deve ser observado no Brasil em decorrência do artigo 3º da LGPD; e o segundo se relaciona com algo que anos atrás já foi apontado por Hörnle[40]: a faculdade de as partes, junto com o terceiro imparcial, considerarem as vantagens e desvantagens do uso de ferramentas tecnológicas, principalmente no que toca ao quesito segurança.

O crescimento da utilização dos métodos de ODR ao longo dos anos, e em especial como uma alternativa a partir da pandemia de COVID-19, levam a outras discussões,

[35] HÖRNLE, op. cit., p. 28, tradução nossa.
[36] MARTÍN-ROMO ROMERO, S.; DE-PABLOS-HEREDERO, C. Contribution of Privacy by Design (of the Processes). Harvard Deusto Business Research, v. 6, n. 3, p. 176-191, 31 dec. 2017.
[37] Ibidem, p. 184.
[38] LCIA. LCIA Arbitration Rules. Disponível em: https://www.lcia.org//Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx. Acesso em: 30 set. 2020.
[39] LCIA. LCIA Mediation Rules. Disponível em: https://www.lcia.org/Dispute_Resolution_Services/lcia_mediation_rules_2020.aspx. Acesso em: 30 set. 2020.
[40] HÖRNLE, op. cit., p. 32.

como os benefícios da tecnologia como "quarta parte" do procedimento[41], anteriormente mencionada, que igualmente são de grande relevância, mas que merecem abordagem própria.

A obrigatoriedade de adoção de práticas que respeitem a privacidade do titular de dados, em consonância com um dos fundamentos da proteção de dados[42], demonstra os sucessivos avanços dos temas aqui discutidos. Até por isso estes são "antigos conhecidos": ainda que criados e desenvolvidos no final do século passado, foi na era do recém iniciado século XXI que seus caminhos se entrecruzaram.

A conturbada entrada em vigor da LGPD traz consigo uma junção de necessidade e oportunidade de adequação. Necessidade porque obrigatórias as práticas de *compliance*, algumas delas já tratadas aqui; e oportunidade no sentido de transformar essas mesmas práticas em padrões sólidos da instituição, câmara ou organização.

Se antes cada um dos temas em discussão estava previsto em normas diferentes, agora eles e suas distintas aplicações se somam e formam um todo uniforme, uma aliança entre legislação, teoria e prática. Cabe agora às instituições, câmaras e demais organizações utilizarem-se de práticas e padrões cada vez mais avançados e interligados.

3. QUANDO A CONCLUSÃO FICA ENTRE O FIM E O COMEÇO

O desenvolvimento de diferentes alternativas, visões e práticas está indissociavelmente ligado à ideia de términos e inícios sucessivos. Não seria, pois, diferente com os métodos de resolução de conflitos, que além de introduzirem uma nova ótica no ordenamento, também foram se transformando e adaptando a um mundo cada vez mais online.

Comportamento semelhante assistiu aos temas da privacidade e da proteção de dados, cujas preocupações teóricas de finais do século XX encontraram na era seguinte contextos de aplicação prática. É o que aconteceu com o Privacy by Design, que não só estabeleceu uma aliança com as legislações como também foi nelas incorporado.

O respeito à privacidade dos titulares de dados como padrão representou uma ruptura, ou ainda, uma mudança de comportamento tanto na experiência europeia, com a

[41] MARQUES, op. cit. p. 4; CLIFFORD, Damian; SYPE, Yung Shin van Der. Online dispute resolution: settling data protection disputes in a digital world of customers. Computer Law & Security Review, [S.L.], v. 32, n. 2, p. 282, abr. 2016. Elsevier BV. http://dx.doi.org/10.1016/j.clsr.2015.12.014.
[42] Artigo 2º, I da LGPD.

vigência do GDPR, quanto na brasileira, e sua LGPD. Novamente, diverso não poderia ser o entendimento quanto aos ODRs.

Cada vez mais utilizados, esses métodos online precisam encontrar nas câmaras e instituições uma estrutura organizada que incorpore a compreensão da importância da proteção de dados desde o desenvolvimento de seus sistemas, processos e práticas. E isso é possível a partir da adoção do conceito de Privacy by Design, fruto de trabalho conjunto com a equipe de tecnologia da informação.

Neste recomeço que a LGPD oferece, enquanto marco no ordenamento jurídico brasileiro, as semelhanças e aproximações entre ela, os ODRs e o Privacy by Design demonstram que há um arcabouço legal e teórico apto a sustentar os desafios que vêm sendo impostos.

Ao continuarem a agir com transparência e qualidade, atributos do procedimento e princípios da LGPD, as câmaras e instituições estarão, sobretudo, se adaptando às novas formas de comunicação, aos novos códigos de conduta – que deixam de ser estáticos -, aos novos arranjos do século, e, em especial, ao seu próximo padrão de atuação.

Entre o fim e o começo há não só obrigatoriedade de adequação às legislações, mas também uma oportunidade de consolidação dos ODRs, a partir de uma aliança com a tecnologia da informação e o Privacy by Design.

REFERÊNCIAS

ARBIX, Daniel. **Resolução online de controvérsias**. São Paulo: Intelecto, 2017.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 157. ed. Brasília, DF, 15 ago. 2018. Seção 1, p. 59. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337. Acesso em: 30 set. 2020.

CAM-CCBC. **Resolução Administrativa 40/2020**. Nova organização administrativa e normas para o processamento eletrônico dos procedimentos. Disponível em: https://ccbc.org.br/cam-ccbc-centro-arbitragem-mediacao/ra-40-2020/. Acesso em: 02 out. 2020.

CAHALI, Francisco José. **Curso de Arbitragem:** mediação, conciliação e tribunal multiportas. 7 ed. São Paulo: Thomson Reuters Brasil, 2018.

CAMPAIGN FOR GREENER ARBITRATIONS. **Driving sustainable change**. 2021. Disponível em: https://www.greenerarbitrations.com/. Acesso em: 04 jul 2021.

CAPELLETTI, Mauro; GARTH, Bryant. **Acesso à justiça**. Porto Alegre: Fabris, 1998.

CAVOUKIAN, Ann. **Operationalizing Privacy by Design**: a guide to implementing strong privacy practices. Information and Privacy Commissioner. Ontario, Canada: 2012.

CAVOUKIAN, Ann. Privacy by Design [Leading Edge]. **Ieee Technology And Society Magazine**, [S.L.], v. 31, n. 4, p. 18-19, 2012. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mts.2012.2225459.

CLIFFORD, Damian; SYPE, Yung Shin van Der. Online dispute resolution: settling data protection disputes in a digital world of customers. **Computer Law & Security Review**, [S.L.], v. 32, n. 2, p. 272-285, abr. 2016. Elsevier BV. http://dx.doi.org/10.1016/j.clsr.2015.12.014.

EUROPEAN UNION. **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995** on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 out. 1995. Disponível em: http://data.europa.eu/eli/dir/1995/46/oj. Acesso em: 28 set. 2020.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 28 set. 2020.

EUROPEAN UNION. **Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013** on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), 21 maio. 2013. Disponível em: https://eur-lex.europa.eu/eli/reg/2013/524/oj. Acesso em: 24 set. 2020.

HÖRNLE, J. Online Dispute Resolution: the emperor's new clothes? **International Review of Law, Computers & Technology**, [s. l.], v. 17, n. 1, p. 27-37, 2003. DOI 10.1080/1360086032000063093.

KATSH, Ethan; RULE, Colin. **What we know and need to know about online dispute resolution**. South Caroline Law Review, 2015.

LCIA. **LCIA Arbitration Rules**. Disponível em: https://www.lcia.org//Dispute_Resolution_Services/lcia-arbitration-rules-2020.aspx. Acesso em: 30 set. 2020.

LCIA. **LCIA Mediation Rules**. Disponível em: https://www.lcia.org/Dispute_Resolution_Services/lcia_mediation_rules_2020.aspx. Acesso em: 30 set. 2020.

MANIA, Karolina. Online dispute resolution: the future of justice. **International Comparative Jurisprudence**, [S.L.], v. 1, n. 1, p. 76-86, nov. 2015. Mykolas Romeris University. http://dx.doi.org/10.1016/j.icj.2015.10.006.

MARQUES, Ricardo Dalmaso. A resolução de disputas online (ODR): do comércio eletrônico ao seu efeito transformados sobre o conceito e a prática do acesso à justiça. **Revista de Direito e as Novas Tecnologias**: Revista dos Tribunais Online, [s. l.], v. 5/3019, out./dez. 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3525406. Acesso em: 01 out. 2020.

MARTÍN-ROMO ROMERO, S.; DE-PABLOS-HEREDERO, C. Contribution of Privacy by Design (of the Processes). **Harvard Deusto Business Research**, v. 6, n. 3, p. 176-191, 31 dec. 2017.

MÜLLER, Karina Haidar *et al* Resolução de Disputas OnLine e a Propriedade Intelectual: uma Via Possível?'. Arbitragem e Mediação em Matéria de Propriedade Intelectual. **Kluwer Arbitration**, 2020, p. 110.

Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalém, Israel, 27-29 out. 2010.

ROMANOU, Anna. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. **Computer Law & Security Review**, [S.L.], v. 34, n. 1, p. 99-110, fev. 2018. Elsevier BV. http://dx.doi.org/10.1016/j.clsr.2017.05.021.

SANDER, Frank. The Multi-Door Courthouse: Settling Disputes in the Year 2000. **HeinOnline:** 3 Barrister 18, 1976.

SCHARTUM, Dag Wiese. Making privacy by design operative. **International Journal of Law and Information Technology**, [S.L.], v. 24, n. 2, p. 151-175, 24 fev. 2016. Oxford University Press (OUP). http://dx.doi.org/10.1093/ijlit/eaw002.

SUSSKIND, Richard. The Future of Courts. **The Practice**: remote courts. 5. ed., v. 6, jul./ago., 2020. n.p. Disponível em: https://thepractice.law.harvard.edu/article/the-future-of-courts/. Acesso em: 3 out. 2020.

WATANABE, Kazuo. Cultura da sentença e cultura da pacificação. *In:* YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (org.). **Estudos em Homenagem à Professora Ada Pellegrini Grinover**. São Paulo: DPJ, 2005, p. 684-690.

ARBITRAGEM COMO MEIO ALTERNATIVO DE RESOLUÇÃO DE DISPUTAS ORIUNDAS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD E A COMPLIANCE NAS CÂMARAS ARBITRAIS.

Autoria

Denise de Araujo Berzin Reupke

Julia Guimarães Rossetto

Clicar ou escanear para acesso aos debates relativos a este artigo

Debatedores

Juliana Loss

Marcelo Chiavassa

RESUMO

O presente trabalho tem por objetivo analisar a relação entre a Lei Geral de Proteção de Dados e o instituto da arbitragem no Brasil, explorando os conceitos principais trazidos pela Lei Geral de Proteção de Dados como ponto de partida para o entendimento, para depois expor considerações acerca das medidas técnicas e organizacionais apropriadas necessárias como salvaguarda da segurança do processamento de dados pessoais pelas câmaras arbitrais. Este artigo não tem a intenção de exaurir o tema ou se aprofundar de maneira acadêmica, buscando uma linguagem fluida com base no conhecimento empírico, nos usos e costumes, acompanhando movimentação legislativa. Feitas estas considerações, explora-se as possibilidades de submissão de questões ligadas à proteção de dados à arbitragem.

1. INTRODUÇÃO.

Pode-se dizer que a velocidade com que as transações acontecem e se transformam no século XXI atribui a ele característica única, singular. É o século da "Era Digital", "Era dos Dados". E como reflexo da celeridade característica deste século já houve diversos episódios de vazamento e utilização indevida de dados – cuja repercussão foi relevante, inclusive – que suscitaram efetiva proteção estatal.

A título exemplificativo, tem-se o episódio emblemático que envolveu as revelações de espionagem de Edward Snowden, ex-funcionário da Agência de Segurança

Nacional Americana (NSA), em 2013, que noticiou ao mundo os programas de espionagem realizados pelos Estados Unidos da América.

A partir de então não foi apenas a União Europeia que começou a se preocupar com sua lei de proteção de dados[1], mas também o Brasil, que, em 2014, aprovou o Marco Civil da Internet[2], que estabelece princípios, garantias, direitos e deveres para o uso da Internet no território nacional.

Como sucessora deste marco, tem-se a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), ou, simplesmente, "LGPD"[3], cujo alcance é multidisciplinar e ilimitado, e seus regramentos são aplicados ao tratamento de dados pessoais, no meio físico ou digital, por pessoa natural ou por pessoa jurídica de direito público ou privado.

Embora a aplicação das sanções administrativas previstas na LGPD (arts. 52 a 54), que se dará por meio de autoridade nacional (ANPD – Autoridade Nacional de Proteção de Dados), tenha sido adiada para agosto de 2021[4], as penalidades pela inobservância à LGPD, incluindo multas pela coleta, armazenamento e tratamento de dados pessoais, foram aplicadas no Brasil por meio do Ministério da Justiça, Ministério Público, Procon, SENACON e pelo Poder Judiciário, como observa-se pelas inúmeras sentenças proferidas.

Mesmo antes da publicação da Lei nº 13.709/2018, além do Marco Civil da Internet[5], o ordenamento jurídico pátrio possuía leis em vigor para a proteção dos dados pessoais, como, por exemplo, a Constituição Federal[6], Código Civil[7], Código de Defesa

[1] Após as divulgações feitas por Edward Snowden, a União Europeia revisitou suas leis de proteção de dados pessoais, de modo que, em maio de 2018, passou a vigorar nos Estados que compõem conglomerado a General Data Protection Regulation ("GDPR" em português Regulamento Geral de Proteção de Dados).
[2] Lei nº 12.965, de 23 de abril de 2014, que "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.''.
[3] Entrou em vigor em 18 de setembro de 2020 e teve sua entrada em vigor alterada de fevereiro para agosto de 2020 por meio da MP 869/18. Prazo de vigência sancionado pela publicação da conversão da Medida Provisória nº 959/2020 na Lei nº 14.058/2020.
[4] Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado no período da pandemia do coronavírus Lei nº 14.010 de 2020 (Artigo 20);
[5] Marco Civil da Internet, Lei 12.965 de 23 de abril de 2014, privacidade e proteção de dados (incisos II e III do Artigo 3º, incisos VII, VIII, IX, X e XI do Artigo 7º, Artigo 10 e §1º, Artigo 11 e incisos I e II do Artigo 16);
[6] Constituição Federal, privacidade (vida privada — artigo 5º, X) e do sigilo das comunicações (Artigo 5º, XII) e habeas data (Artigo 5º, LXXII, e Lei nº 9.507/97);
[7] Código Civil, Lei nº 10.406 de 10 de janeiro de 2002, vida privada da pessoa natural (Artigo 21).

do Consumidor[8], Estatuto da Criança e do Adolescente[9] e Lei de Acesso à Informação[10], de maneira que a LGPD apenas ampliou os direitos pré-existentes.

A LGPD tem como vértice a proteção da pessoa natural, sendo que, como o próprio nome diz, é geral determinando regras de forma padrão e ampla, aplicando-se a todos setores, observando-se, entretanto, a especificidade de cada área que possa ter sua própria regulação.

Para contextualização no cenário internacional, não é segredo que a LGPD foi inspirada no mencionado General Data Protection Regulation ("GDPR", em português Regulamento Geral sobre a Proteção de Dados), o qual determinou as regras para o tratamento de dados pessoais para os 28 (vinte e oito) Países-Estados membros da União Europeia, regulamento este que impôs obrigações para o processamento dos dados pessoais durante as arbitragens, inclusive[11].

Privacidade e proteção de dados pessoais estão em voga, fazem parte da pauta mundial, objeto de intensas discussões, normatizações, cenário de filmes, documentários e discussões acaloradas por especialistas, cientistas e agora, mais do que nunca, pelo titular do dado que passou a ter uma maior compreensão dos seus direitos enquanto dono de sua própria informação.

Para além disto, o assunto também está na pauta dos debates que se relacionam com a arbitragem. Isto porque, a LGPD, em seus artigos 7º, inciso VI[12], e alínea 'd', do inciso I, do 11[13], estabelecem que o tratamento de dados pessoais e dados pessoais sensíveis poderão ocorrer de forma específica e destacada, no exercício regular de direitos, em procedimento arbitral, inclusive.

---

[8] Código de Proteção e Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990, bancos de dados e cadastros dos consumidores (Art. 43 e parágrafos);

[9] Estatuto da Criança e do Adolescente, Lei nº 8.069 de 13 de julho de 1990, respeito da imagem e da privacidade (Artigo 17);

[10] Lei de Acesso à Informação, Lei nº 12.527 de 18 de Novembro de 2011, decorrente do art. 5º, XXXIII, art. 37, § 3º, II e o art. 216, § 2º, todos da CF/88, com o direito constitucional da privacidade;

[11] Kathleen D. Paisley, It's all About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2707&context=ilj

[12] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...]
VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);"

[13] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I – quando o titular ou seu representante lega consentir, de forma específica e destacada, para finalidades específicas; [...]
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); [...]"

Ou seja, desta regra decorre a obrigação de assegurar seriedade e garantia de integridade dos dados pessoais que circulam nos procedimentos arbitrais.

Neste cenário exponencial, o tema deve ser considerado sob dois primas.

O primeiro deles, sob a ótica da necessidade de as instituições arbitrais, reverem seus parâmetros de segurança e tratamento de dados pessoais, detectando seus *gaps*, definindo ações para remediá-los e prevenindo riscos reputacionais e normativos.

O segundo, sob olhar disruptivo, em considerando as instituições arbitrais uma alternativa para utilização dos meios alternativos de resolução de disputas surgidas a partir de incidentes de segurança que causem risco ou dano relevante aos titulares, levando em conta a possibilidade eminente de judicialização em razão de vazamento ou compartilhamento indevido de dados.

2. LEI GERAL DE PROTEÇÃO DE DADOS E ARBITRAGEM – PRINCÍPIOS

Criada com o viés de conferir às pessoas físicas maior controle e autonomia sobre seus dados pessoais[14], a LGPD baseia-se em fundamentos gerais, tais como[15], respeito à privacidade; autodeterminação informativa; liberdade de expressão, de informação, de comunicação e de opinião; inviolabilidade da intimidade, da honra e da imagem; desenvolvimento econômico e tecnológico e a inovação; livre-iniciativa, livre concorrência e defesa do consumidor; direitos humanos, livre desenvolvimento de personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

Por assim ser, elencou-se na própria lei rol de 10 (dez) princípios que devem norteá-la. São eles, conforme estabelecido no art. 6º: princípio da finalidade, princípio da adequação, princípio da necessidade, princípio do livre acesso; princípio da qualidade dos

[14] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

[15] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I- o respeito à privacidade;
II – a autodeterminação informativa;
III – a liberdade de expressão, de informação, de comunicação e de opinião;
IV – a inviolabilidade da intimidade, da honra e da imagem;
V – o desenvolvimento econômico e tecnológico e a inovação;
VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

dados; princípio da transparência, princípio da segurança, princípio da prevenção, princípio da não discriminação, princípio da responsabilização[16].

Em um paralelo com os meios alternativos de resolução de disputas, em especial a arbitragem, é preciso modular os princípios listados na LGPD, tendo em vista os propósitos específicos de um procedimento arbitral. A despeito de todos os princípios serem aplicáveis de modo geral, outros princípios precisam ser considerados, a fim de que o processamento seja justo, lícito, em consonância com a boa-fé objetiva para atender à expectativa do titular de dados[17].

Em vista disto, é imprescindível que as instituições arbitrais criem protocolos transparentes para que os *players* de um procedimento arbitral tenham ciência de quais dados pessoais serão utilizados e de que maneira o serão, respeitando-se, especialmente, os princípios da finalidade, da necessidade e da transparência.

Até mesmo porque, além da própria instituição arbitral – que "*assume a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares e da ANPD*"[18] - determinados partícipes do procedimento arbitral serão considerados controladores de dados[19] para fins de aplicação da LGPD, especialmente de suas sanções, como são os casos de peritos, assistentes técnicos e advogados não vinculados à pessoa

---

[16] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I- o respeito à privacidade;
II – a autodeterminação informativa;
III – a liberdade de expressão, de informação, de comunicação e de opinião;
IV – a inviolabilidade da intimidade, da honra e da imagem;
V – o desenvolvimento econômico e tecnológico e a inovação;
VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

[17] De acordo com o Glossário LGPD do Governo do Brasil titular é "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento." https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd

[18] Item 18 do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da Autoridade Nacional de Proteção de Dados – ANPD, https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf

[19] De acordo com o Glossário LGPD do Governo do Brasil controlador é "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais." https://www.serpro.gov.br/lgpd/menu/a-lgpd/glossario-lgpd, complementarmente, de acordo com o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da Autoridade Nacional de Proteção de Dados – ANPD, 16. A identificação do controlador deve partir do conceito legal e dos parâmetros auxiliares
indicados neste Guia, sempre considerando o contexto fático e as circunstâncias relevantes do caso. O papel de controlador pode decorrer expressamente de obrigações estipuladas em instrumentos legais e regulamentares ou em contrato firmado entre as partes. Não obstante, a efetiva atividade desempenhada por uma organização pode se distanciar do que estabelecem as disposições jurídicas formais, razão pela qual é de suma importância avaliar se o suposto controlador é, de fato, o responsável pelas principais decisões relativas ao tratamento."

jurídica e que atuam "*de forma independente e em nome próprio – e não de forma subordinada a uma pessoa jurídica ou como membro de um órgão desta*"[20].

Neste sentido, destaca-se que a LGPD estabelece que, no *exercício de atividade de tratamento de dados pessoais*, os controladores que conjuntamente exercem o tratamento de dados e estiverem envolvidos no tratamento do qual decorra danos ao titular respondem *solidariamente*[21].

Esta é uma das razões pelas quais a criação de regras e protocolos de *compliance* de dados que melhor orientem os tratamentos de dados se faz necessária, mitigando, assim, eventuais responsabilizações. Se assim não o for, em breve, ter-se-á notícia de instituições sendo preteridas por não garantir aos seus usuários a segurança de proteção e privacidade dos dados necessária, incluindo a cibernética.

3. INSTITUIÇÕES ARBITRAIS, PRIVACIDADE E REPUTAÇÃO

Dada a importância de observância aos princípios que regem a LGPD, como antecipado no capítulo precedente, é inexorável que as instituições arbitrais estejam atualizadas aos parâmetros e exigências para proteção e privacidade de dados do indivíduo.

Há casos ao redor do mundo que bem ilustram o interesse de *hackers* aos dados de instituições arbitrais. A título exemplificativo, tem-se o caso julgado pela Corte Permanente de Arbitragem ("CPA"), a qual, em julho de 2015, teve seu site hackeado durante uma disputa de fronteira marítima entre a China e as Filipinas, de maneira que todos aqueles que tiveram acesso aos autos foram monitorados, o que fulminou em uma vantagem diplomática para o Estado Chinês.[22]

---

[20] Item 30 do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da Autoridade Nacional de Proteção de Dados – ANPD, https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf

[21] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados, é obrigado a repará-lo.
$ 1º A fim de assegurar a efetiva indenização ao titular dos danos: [...]
II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previsto no art. 43 desta Lei."

[22] Fulbright, Norton Rose. Data protection and cyber-risk issues in arbitration: regulation, cyberattacks and hacked evidence. Disponível em: https://www.lexology.com/library/detail.aspx?g=19dece65-8e82-464b-9e1a-4f4e1e9709e8

A problemática deste caso evidencia o impacto que a segurança cibernética, em especial a ausência dela, pode representar na arbitragem como um todo.

Como visto, a despeito dos regramentos previstos nos artigos 7º, inciso VI, e 11, inciso I, alínea 'd' da Lei nº 13.709/2018, não é necessário o consentimento do titular para o tratamento de dados pessoais e dados pessoais sensíveis nos exercícios de direitos em procedimento arbitral. Entretanto, em considerando a potencialidade de ataques cibernéticos em vista da complexidade dos dados armazenados, medidas protetivas precisam ser priorizadas.

O leque de medidas é diverso, tem-se armazenamento em nuvem; backups; softwares para gerenciamento seguro de documentos e antivírus; sistema especializado que permita armazenamento seguro de dados confidenciais evitando vazamentos; investimentos em equipe de tecnologia da informação para minimização riscos virtuais; criptografia; conscientização dos agentes de tratamento de dados para aplicação de princípios de segurança da informação (confidencialidade, integridade e disponibilidade).

Sabe-se que a confidencialidade na arbitragem não decorre da lei, no entanto, ela é considerada um "princípio implícito" do instituto, o qual, na ausência o sigilo, pode implodir do ponto de vista estrutural.

A observância a esta característica, além de proteger informações delicadas, decorre da necessidade de preservação da imagem da empresa perante os mercados financeiro e consumidor. Desta maneira, eventual violação ou vazamento destes dados no curso de um procedimento arbitral pode não apenas comprometê-lo, como também causar danos de difícil reparação – ou, pior, irreparáveis – às partes nele envolvidas"[23].

Neste sentido, em sendo o assunto de proteção de dados objeto de discussão nos países europeus de forma precursora, as instituições arbitrais que lá se sediam já possuem protocolos de segurança em observância à GDPR.

Desde 2017, por meio do "*Information Technology in International Arbitration – Report of the ICC Commission on Arbitration and ADR*", a International Chamber of Commerce ("ICC") aborda aspectos técnicos, troca eletrônica de documentos e proteção de dados[24]. Em sua recente Nota às Partes e aos Tribunais Arbitrais sobre a Condução da

[23] Becker, Daniel; Mota, Kizzy de Paula, Arbitration leaks: a segurança da informação no procedimento arbitral. Disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/arbitration-leaks-a-seguranca-da-informacao-no-procedimento-arbitral-18042018

[24] https://iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf

Arbitragem conforme seu Regulamento, a ICC apresenta, de forma detalhada, as medidas que devem ser observadas para o fiel cumprimento da GDPR [25].

Do mesmo modo, a London Court of International Arbitration ("LCIA") tem regramento específico para observância da proteção de dados. Nele, a instituição especifica os dados que serão coletados, a depender do papel que a pessoa terá no procedimento arbitral[26] , bem como a forma como eles serão utilizados[27].

A International Council for Commercial Arbitration ("ICCA"), a International Institute for Conflict Prevention and Resolution ("CPR") e o New York Bar Association,

[25] A título exemplificativo: "80. A CCI reconhece a importância das proteções eficazes e significativas para dados pessoais ao coletá-los e utilizá-los na qualidade de responsável pelo tratamento, em conformidade com as normas de proteção de dados, inclusive o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (o "Regulamento Geral sobre a Proteção de Dados" ou "RGPD"."
"86. Durante a arbitragem, as partes, seus representantes e todos os demais participantes deverão garantir a segurança dos dados pessoais processados sob sua respectiva responsabilidade.
87. Para tanto, as partes e os árbitros deverão assegurar que sejam utilizados meios seguros de coleta, comunicação e arquivamento de dados, ao longo de todo o processo de arbitragem e durante o período de retenção aplicável a tais dados. Para tanto, recomenda-se aos tribunais arbitrais e às partes que consultem o *Report on the Use of Information Technology in International Arbitration* (Relatório sobre o uso da tecnologia da informação em arbitragem internacional) preparado pela Comissão da CCI sobre Arbitragem e ADR."

[26] "2.1. Depending on the circumstances, we may obtain the following personal data about you:
Neutrals, Tribunal Secretaries, Members of the LCIA Court
2.1.1. Your name, contact details, financial information (including banking details), personal identification information (including passport information) and other personal data submitted to us by you, a party, a party's authorized representative, another Neutral, a tribunal secretary, a member of the LCIA Court, or otherwise disclosed to or collected by us from third parties or public available resources, in connection with LCIA Proceedings.
2.1.2. Information about whether you are subject to economic sanctions or any other legal or regulatory impediment."

[27] "3.11 Depending on the circumstances in which we process your personal data, we may use your personal data in the following ways and on the legal bases described below:
Neutrals, Tribunal Secretaries, Members of the LCIA Court
3.1.1 To assess your availability and suitability (including in response to specific challenges made by parties) to be appointed and to continue to act in LCIA Proceedings, as necessary to further our and the parties' legitimate interests in ensuring that only suitable candidates are appointed and that no conflicts of interest arise which could undermine the actual or perceived integrity of LCIA Proceedings
3.1.2 To maintain a database of potential Neutrals and tribunal secretaries as necessary to further our and potential parties' legitimate interests in identifying and appointing suitable Neutrals and tribunal secretaries
3.1.3 To facilitate the determination of challenges to arbitrators in LCIA proceedings and potentially publish selected decisions where an arbitrator has been challenged, which decisions are redacted to eliminate unnecessary personal data before publication.
3.1.4 To remit funds to you or provide administrative information regarding your (potential) appointment or the conduct of LCIA Proceedings, as necessary for the performance of our agreements with you and duties under them
3.1.5 To facilitate the general conduct of LCIA Proceedings, including to communicate with you, facilitate communications between arbitral participants, and to fulfil other administrative tasks in relation to LCIA Proceedings, as necessary for furthering the parties' legitimate interests in resolving the dispute between them, and the parties' and the LCIA's interests in ensuring that the arbitral process operates efficiently and expeditiously and that the rights of the parties are respected
3.1.6 Where necessary to meet our legal and regulatory compliance obligations, including those relating to taxes, economic sanctions and money laundering ("Legal Compliance Obligations")."

também, recentemente, *"propuseram mediante um amplo debate a criação de um protocolo voluntário no qual algumas medidas de cibersegurança poderiam ser implementadas, sendo este um documento importante e umas das poucas referências quanto ao assunto"*[28], o denominado Cybersecurity Protocol for International Arbitration. Trata-se de protocolo de segurança cibernética em arbitragem internacional, que leva em consideração que a arbitragem internacional no cenário digital requer medidas razoáveis de segurança da informação para proteger aquilo que é compartilhado durante o procedimento, fornecendo, assim, orientação prática para advogados, árbitros e instituições, e protocolos opcionais que podem ser adotados pelas partes em uma arbitragem[29].

Em termos práticos, o protocolo apresenta medidas bastante utilizáveis e simples para promover a segurança cibernética e a confidencialidade, tais como os seguintes aspectos: *(i)* uso de criptografia ponta a ponta para proteção de documentos de e-mail e senha; *(ii)* uso de transferência segura de arquivos para compartilhar documentos; *(iii)* uso de telas de privacidade ao visualizar documentos confidenciais em público; *(iv)* cautela ao usar a Internet em ambientes públicos; *(v)* implementação de políticas para reduzir o período de armazenamento de dados usado em uma arbitragem; *(vi)* fazer backups de dados redundantes e seguros de rotina; *(vii)* ao definir uma senha, evitar palavras comuns do dicionário, senhas passadas, caracteres repetitivos ou sequenciais; *(viii)* uso de firewalls, software antivírus e antispyware, atualizações do sistema operacional e outros patches de software, *(ix)* baixar programas e conteúdo digital apenas de fontes legítimas; *(x)* não abrir anexos de remetentes de e-mail desconhecidos; e *(xi)* manter os dispositivos móveis por perto e fazer uso das medidas de proteção disponíveis em caso de perda ou roubo[30].

É o que se nota também, no Schedule C - Sample Information Security Measures do mencionado protocolo:

> *"1. Asset Management*
> *(a) Limiting exchanges of, and access to, information about the dispute to individuals on a "need to know" basis.*

[28] Costa, R. Veloso Thiago , Proteção de dados e arbitragem: para além de uma questão legal: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-e-arbitragem-para-alem-de-uma-questao-legal-29062019

[29] ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration (Edição de 2020) - https://www.acerislaw.com/wp-content/uploads/2020/01/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_electronic_version.pdf

[30] Tradução livre de Carreteiro, Mateus Aimoré Carretiro e Castro, Igor Cunha Arantes - Brazil: Data Protection In International Arbitration: A Brazilian Perspective https://www.mondaq.com/brazil/data-protection/819898/data-protection-in-international-arbitration-a-brazilian-perspective

(b) Adopting protective measures, such as redaction (also known as masking) or pseudonymization, before the exchange of information with respect to data classified within the arbitration as higher risk.
(c) Labeling confidential or sensitive data (e.g., by adding appropriate confidentiality legends by bates stamp or to a document name). Examples of such legends include categories such as "confidential," "highly sensitive," "attorneys' eyes only" and the like, as well as categories specific to the arbitration.
(d) Not sharing disclosure material with the arbitral tribunal or the administering institution, except in respect to disclosure disputes or as required for evidentiary purposes, in which case limiting the material shared to what is relevant to, and necessary for, the tribunal's resolution of the dispute.
(e) Using a secure share site or cloud platform to share information and documents related to the dispute.
(f) Restricting use of public networks to access, store, or transmit arbitration related information.
(g) Agreeing that the parties' respective networks shall be accessed on a remote basis solely through a secure VPN.
(h) Maintaining backups of arbitration material during the pendency of the matter.
(i) Limiting the amount of time that information related to the dispute will be retained after the completion of the matter, and providing for a procedure at the conclusion of the arbitration process for such information, regardless of how stored, to be returned to the originating party, or permanently destroyed and deleted, with a process for certification of compliance."

Neste sentido, sabe-se que a escolha da instituição arbitral para administração do procedimento está intrinsicamente ligada à sua reputação. Pode-se dizer que a reputação das instituições atualmente fundamenta-se na *(i)* qualidade e tecnicidade dos árbitros que compõem suas listas ou que nelas atuam; *(ii)* na garantia de decisões técnicas e imparciais; *(iii)* além da excelência na prestação de serviços aos seus usuários.

Com as regras advindas da LGPD, as instituições terão que se adequar, criando medidas de controle de transmissão de dados. É necessário que as instituições arbitrais brasileiras caminhem a passos largos para colocar em prática regras concretas que garantam segurança cibernética, de maneira que as informações que nelas transitam em virtude dos procedimentos arbitrais sejam protegidas.

Os regulamentos das instituições internacionais são um ponto de partida e balizamento, no entanto, cada país tem sua fragilidade, que devem ser sopesadas no combate aos ataques cibernéticos. Acima de tudo, é preciso trabalhar intensamente para que a reputação e credibilidade das instituições arbitrais brasileiras sejam resguardadas, o caminho que nos trouxe até aqui foi árduo e deve, ao máximo, ser preservado.

4. JUDICIALIZAÇÃO. SERIA ARBITRAGEM UMA ALTERNATIVA VIÁVEL DE RESOLUÇÃO DE DISPUTA?

Estima-se que, a exemplo do que ocorreu com a entrada em vigor do Código de Defesa do Consumidor ("CDC"), os questionamentos dos titulares quanto aos tratamentos de seus dados pessoais crescerá exponencialmente, levando-se em conta que os titulares podem, a qualquer momento, exercer quaisquer de seus direitos previstos em lei como, exemplificativamente, *(i)* a confirmação da existência de tratamento; *(ii)* a informação a respeito do compartilhamento; e *(iii)* a possibilidade de receber informação sobre não fornecer o consentimento e suas consequências[31].

Na contramão estarão os agentes de tratamento[32], pessoas físicas ou jurídicas, a quem compete as decisões sobre o tratamento dos dados e que estarão em fases diferentes de maturação, estando alguns com seus processos de conformidade na etapa embrionária, outros ainda fazendo uso proposital e malicioso desses dados pessoais.

Em considerando a possibilidade de agentes de tratamento serem responsabilizados pelos danos causados ao titular do dado, assim como pelo ressarcimento de danos[33], o Poder Judiciário já se manifestou a respeito por diversas oportunidades.

A exemplo disto tem-se a recente decisão, proferida no âmbito do processo nº 1080233-94.2019.8.26.0100, que tramitou perante a 13ª Vara Cível da Comarca de São Paulo. A ação foi proposta por titular de dados, sob o fundamento de que

[31] Lei Geral de Proteção de Dados, Lei nº 13.709/2018. Art. 18.

[32] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 5º Para os fins desta Lei, considera-se: [...] IX - agentes de tratamento: o controlador e o operador;"

[33] Lei Geral de Proteção de Dados, Lei nº 13.709/2018: "Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso."

a empresa ré, com a qual ele celebrou contrato, teria compartilhado seus dados a empresas estranhas à relação contratual.

Por tratar-se de uma relação consumerista, na decisão em questão, o julgador entendeu que a divulgação a terceiros dos dados do autor, de forma diversa do quanto previsto no contrato, violou o regramento previsto tanto no CDC como na LGPD, condenando a ré a se abster de repassar ou conceder a terceiros os dados pessoais do autor, bem como ao pagamento de indenização a título de dano moral.

É certo que com a popularização da LGPD haverá um abarrotamento de demandas perante o Poder Judiciário[34]. No entanto, a questão que ora se coloca é quais demandas relativas à proteção de dados pessoais podem ser submetidas à arbitragem.

Sabe-se que, de acordo com o 1º da Lei de Arbitragem, podem ser submetidas à arbitragem matérias que versem sobre "*direitos patrimoniais disponíveis"*[35].

Mas, as disputas que envolvem dados pessoais versam sobre direitos patrimoniais disponíveis? É o que se passa a analisar.

A doutrina brasileira majoritária defende que a natureza jurídica do direito a proteção de dados pessoais é direito fundamental autônomo e, se assim entendido, pode-se concluir:

> *"*[...] *de direito fundamental autônomo, sendo, portanto, digno de ser inserido na CF/88, art. 5º, inciso LXXIX, com a seguinte dicção: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Tal entendimento encontra arrimo no direito europeu na medida em que a CDFUE, Carta dos Direitos Fundamentais da União Europeia, artigo 8º, 1 a dispõe que, "as pessoas têm direito à proteção de dados de caráter pessoal que lhes digam respeito", assertiva reiterada pelo TFUE, Tratado de Funcionamento da União Europeia, artigo 16º,1."*[36]

[34] Neste sentido, o Ministro Tarso Sanseverino já expôs sua preocupação com o aumento do número de demandas judiciais que haverá com base na Lei nº 13.709/2018, veja-se: "*Os problemas existem e são resolvidos com a lei atual. Mas com a entrada da LGPD, eles podem se agravar (no tocante da responsabilidade civil)"*, explicou o ministro. *"A quantidade de processos que esperamos será similar às consultas do Credit Scoring (acima de 200 mil ações). O número de casos no tribunal vai aumentar substancialmente"*. https://www.mobiletime.com.br/noticias/05/09/2019/lgpd-tera-aumento-exponencial-em-aberturas-de-processos-preve-ministro-do-stj/

[35] Lei nº 9.307/1996. "Art. 1º As pessoas capazes de contratar poderão valer-se da arbitragem para dirimir litígios relativos a direitos patrimoniais disponíveis."

[36] Constitucionalização da proteção de dados pessoais e competências legislativas à luz de análise comparativa entre Direito Pátrio e da União Europeia - Evellin D. Silva, Sergio Paulo Gomes Gallindo e Daniel T. Stivelberg: https://www.migalhas.com.br/depeso/315540/constitucionalizacao-da-protecao-de-dados-pessoais-e-competencias-legislativas-a-luz-de-analise-comparativa-entre-direito-patrio-e-da-uniao-europeia

O Supremo Tribunal Federal, ao enfrentar questão sobre a constitucionalidade da Medida Provisória 954/2020[37], que prevê o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE) para a produção de estatística oficial durante a pandemia do COVID-19, firmou entendimento de que o compartilhamento previsto na mencionada Medida Provisória viola o direito constitucional à intimidade, à vida privada e ao sigilo[38].

Com este precedente, tem-se que, assim como na Carta de Direitos Fundamentais Europeia, proclamada em 7 de dezembro de 2000, no Brasil, o direito à proteção de dados é tido como direito fundamental. Assevera-se tal constatação ao longo dos argumentos do relatório proferido pela Ministra Rosa Weber na Ação Direta de Inconstitucionalidade nº 6387 MC-REF/DF:

> *"Defende a inconstitucionalidade formal da medida provisória impugnada, por inobservância dos requisitos da relevância e da urgência previstos no art. 62 da CF, bem como a sua inconstitucionalidade material, por afronta ao postulado fundamental da dignidade da pessoa humana e às cláusulas fundamentais assecuratórias da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como do sigilo de dados e da autodeterminação informativa (arts. 1º, III, e 5º, X e XII, da Lei Maior).*
> *Nessa linha, afirma que se pode extrair do texto constitucional, em particular das garantias expressas de proteção à dignidade da pessoa humana, à privacidade, à intimidade e ao sigilo dos dados pessoais, uma "tutela constitucional do direito à autodeterminação informativa". Afirmando assegurada, na Constituição da República, "uma tutela autônoma aos dados pessoais e não apenas ao conteúdo das comunicações", sustenta que "a Medida Provisória em análise viola o sigilo de dados dos brasileiros e invade a privacidade e a intimidade de todos, sem a devida proteção quanto à segurança de manuseio, sem justificativa adequada, sem finalidade suficientemente especificada e sem garantir a manutenção do sigilo".*
> *Enfatizando a ampliação dos riscos à privacidade na sociedade de informação atual, observa que "o mau uso de dados compartilhados pode servir à campanha de fake news e até mesmo de manipulação da vontade do eleitorado, comprometendo a liberdade democrática". Nesse contexto, assevera constituir dever de um Estado democrático de direito garantir, em face da realidade tecnológica, "adequada e efetiva proteção dos cidadãos, da sua privacidade e da autodeterminação em relação aos seus dados pessoais". Argumenta que a Medida Provisória questionada impõe restrições à proteção dos aludidos direitos fundamentais que não atendem ao critério da*

[37] a Medida Provisória nº. 954/2020 dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.

[38] Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal, https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629.

> *proporcionalidade, consideradas as dimensões da adequação, da necessidade e da proporcionalidade em sentido estrito e pontua: "não se pode aceitar a violação irrestrita ao direito à privacidade em nome do combate à pandemia do coronavírus, menos ainda, com objetivos abstratos contidos na Medida Provisória, que sequer vincula a utilização dos dados coletados para pesquisas especialmente voltadas ao enfrentamento da doença".*

Com isso, ainda que haja uma parcela do direito à proteção de dados pessoais que possa ser disponível, não podemos afirmar que se trata de um direito patrimonial disponível e, por isso, **a submissão destas questões à arbitragem é limitada**, cujo limite, obviamente, depende da lei aplicável ao conflito.

Neste trabalho, partimos da premissa de que a lei aplicável é a brasileira.

Há quem defenda que a questão de proteção de dados relaciona-se com direito do consumidor e que, por isto, a matéria deveria ser regida pelo CDC. Pelas demandas propostas perante o Poder Judiciário, percebe-se que as questões lá submetidas, em sua maioria, de fato versam sobre direito do Consumidor.

Neste sentido, vale destacar que para que tais questões sejam submetidas à arbitragem é imprescindível o atendimento à regra do parágrafo 2º do artigo 4º da Lei de Arbitragem, conforme inúmeros julgados do Superior Tribunal de Justiça[39].

Sem qualquer tipo de julgamento acerca da arbitrabilidade ou não das questões que envolvem proteção de dados, entende-se que a plataforma do Ministério Justiça e o *Consumidor.com.br* seriam o caminho natural para a proteção destes direitos dos titulares em situações que envolvem o consumidor, como forma de evitar que o Poder Judiciário fique sobrecarregado[40].

Nesta linha, tem-se o mecanismo utilizado na Inglaterra, denominado Data Arbitration (https://dataarbitration.co.uk/), constituído para resolução alternativa de

---

[39] REsp 1.602.076 – SP. "Recurso Especial. Direito Civil e Processual Civil. Contrato de Franquia. Contrato de Adesão. Arbitragem. Requisito de Validade do Art. 4º, § 2º, da Lei 9.307/96. Descumprimento. Reconhecimento *Prima Facie* da Cláusula Compromissória "Patológica". Atuação do Poder Judiciário. Possibilidade. Nulidade Reconhecida. Recurso Provido. [...] 3. Todos os contratos de adesão, mesmo aqueles que não consubstanciam relação de consumo, como os contratos de franquia, devem observar o disposto no art. 4º, § 2º, da Lei 9.307/96. [...]" (Ênfase nossa).
Lei nº 9.307/1996. "Art. 4º A cláusula compromissória é a convenção através da qual as partes em um contrato comprometem-se a submeter à arbitragem os litígios que possam vir a surgir, relativamente a tal contrato. [...]
§ 2º Nos contratos de adesão, a cláusula compromissória só terá eficácia se o aderente tomar a iniciativa de instituir a arbitragem ou concordar, expressamente, com a sua instituição, desde que por escrito em documento anexo ou em negrito, com a assinatura ou visto especialmente para essa cláusula."

[40] Ainda em março de 2021, a Secretaria Nacional do Consumidor (Senacon) e Autoridade Nacional de Proteção de Dados (ANPD) assinaram um acordo de cooperação técnica que prevê, entre outras coisas, a uniformização de entendimentos dos Procons com relação à LGPD.

disputas entre consumidores e empresas relacionadas a violação de dados[41]. Nele, o consumidor registra a sua reclamação online mediante formulário, que é analisada e, em havendo violação às leis de proteção de dados, o julgador determina o nível de compensação que o consumidor terá direito.

Já nos Estados Unidos da América, em 2018, o Tribunal Distrital do Distrito Central da Califórnia decidiu que uma ação coletiva decorrente de uma violação de dados da Uber Technologies Inc. ("Uber") deveria ser submetida à arbitragem. Neste caso, os quase 600.000 (seiscentos mil) motoristas e 57 milhões (cinquenta e sete milhões) de clientes do Uber, após se registrarem no aplicativo, firmaram contrato de serviço que continha cláusula compromissória. Com base nisto, os usuários moveram-se para obrigar que o caso fosse submetido à arbitragem[42].

Em outro caso recente nos Estados Unidos da América, o Juiz do Distrito de Maryland, Richard Bennett, rejeitou[43] uma reclamação em nome dos consumidores que seriam supostas vítimas de uma violação de dados envolvendo a Chegg, Inc. A Chegg, Inc, por sua vez, manifestou-se em sentido contrário à reclamação e requereu a submissão do caso à arbitragem, tendo em vista o aceite à cláusula compromissória constante do "Terms of Use", à qual os envolvidos anuíram. Diante do deferimento do requerimento formulado por Cheeg, Inc, 15.107 (quinze mil cento e sete) requerimentos de arbitragem foram protocolados perante a American Association of Arbitration ("AAA").

Em *Strategies for Navigating Business-to-Business Data Breaches*, os autores afirmam que a cláusula compromissória é "*um componente crítico para lidar com violações de segurança de dados em relacionamentos B2B*" e que "*incidentes de violação de dados B2B realmente apresentam o que parece ser o caso perfeito para o uso de cláusulas compromissórias."*[44]

---

[41] De acordo com o (dataarbitration.co.uk), os consumidores podem usar o esquema de Arbitragem de Dados se: "1 - The Company they are complaining about has agreed to subscribe to the scheme already or agrees to subscribe in relation to the consumers complaint search the data arbitration register here; and, 2 - The consumer has already complained direct to the Company and either i) they have rejected the complaint/provided an unsatisfactory response; or ii) the Company has failed to respond within eight weeks.". Dentre as reclamações típicas com as quais são lidadas: "We can deal with any complaint that involved an alleged breached of data protection laws. The most common we deal with are complaints about: - Failure to remove consumer from a marketing/data list; - Unauthorised marketing contact and cold calling; - Failure to delete consumers data; - Freedom of Information/Subject access requests; - Data security breaches – where data has been exposed to fraudsters."

[42] Disponível em https://www.huntonprivacyblog.com/2018/09/11/uber-data-breach-class-action-must-proceed-arbitration/

[43] Disponível em https://www.dataguidance.com/news/usa-district-judge-rejects-class-action-lawsuit-2018-chegg-data-breach

[44] Joseph V. DeMarco e Urvashi Sen, "Strategies for Navigating Business-to-Business Data Breaches," http://go.adr.org/rs/294-SFS-516/images/NYLJ_B2B_DataBreaches.pdf, (6 de julho de 2015)

No Brasil, enquanto isto, a experiência ainda não nos permite exemplificar os casos relacionados à LGPD que foram submetidos à arbitragem. No entanto, é certo que outras questões de maior relevância e evidência patrimonial ligadas à LGPD poderão ser trazidas a baila nos tribunais arbitrais, principalmente para discussões decorrentes dos contratos firmados entre os agentes de tratamento (controlador e operador) como a discussão sobre responsabilização civil por quebra de direitos do titular dos dados, descumprimento de regramentos na cadeia de tratamento dos dados, responsabilidade pelas sanções impostas pela ANPD dentre outras hipóteses. O Instituto de Tecnologia & Sociedade do Rio de Janeiro, na vanguarda da análise do tema, disponibilizou, em abril de 2020, relatório com as experiências internacionais e perspectivas para o Brasil[45] e provoca, ao final, o leitor para refletir sobre estratégias que possam lidar com a gigantesca e emitente demanda judicial dos conflitos oriundos da LGPD.

Assim como foram necessários anos de estudos para que se concluísse que a Administração Pública pode se submeter à arbitragem, quer seja por atender aos critérios de arbitrabilidade subjetiva, quer seja por atender aos critérios de arbitrabilidade objetiva, ainda muito há que se debater sobre a arbitrabilidade das matérias relacionadas à LGPD.

5. CONCLUSÃO

É indubitável que a partir da aplicação da LGPD haverá um abarrotamento do Poder Judiciário. Por isto, mais uma vez os meios alternativos de resolução de conflitos são primordiais para garantir aos titulares do direito respostas eficazes e rápidas.

As instituições arbitrais brasileiras devem se adequar aos novos paradigmas impostos pela LGPD, garantindo aos seus partícipes a segurança e proteção de dados pessoais, de maneira a consolidar sua reputação no cenário internacional, já conhecida pela eficiência na prestação de seus serviços e tecnicidade.

No que tange à arbitrabilidade das matérias que envolvem direito de proteção de dados, esta ainda será palco de inúmeros debates. Há um longo caminho a ser percorrido até que muitas das dúvidas sejam aclaradas. No entanto, nada melhor que a prática, o debate e o estudo para permitir que, em conjunto, cheguemos a conclusões que garantirão a todos a melhor prática e segurança jurídica.

[45] Instituto de Tecnologia & sociedade do Rio. Lei Geral de Proteção de Dados e Resolução de Confltos: experiências nacionais e internacionais. https://itsrio.org/wp-content/uploads/2020/04/Relatorio_LGPDResolucaoConflitos.pdf

REFERÊNCIAS

BRASIL. Lei nº 9.307 de 23 de setembro de 1996. Disponível em http://www.planalto.gov.br/ccivil_03/leis/l9307.htm

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Lei nº 13.706, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13708.htm

BRASIL. Medida Provisória nº. 954/2020. Disponível em https://legislacao.presidencia.gov.br/atos/?tipo=MPV&numero=954&ano=2020&ato=6bdQTS65EMZpWT9b1

Bennett, R ard D., United States District Judge, Parecer. https://www.govinfo.gov/content/pkg/USCOURTS-mdd-1_19-cv-03235/pdf/USCOURTS-mdd-1_19-cv-03235-0.pdf

Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. Coordenação Bruno Feigelson e Antonio Henrique Albani Siqueira. São Paulo: Thomson Reuters Brasil, 2019. p. 30.

Becker, Daniel; Mota, Kizzy de Paula. *Arbitration leaks: a segurança da informação no procedimento arbitral.* Disponível em https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/arbitration-leaks-a-seguranca-da-informacao-no-procedimento-arbitral-18042018

Carreteiro, Mateus Aimoré Carretiro e Castro, Igor Cunha Arantes - *Brazil: Data Protection In International Arbitration: A Brazilian Perspective.* Disponível em: https://www.mondaq.com/brazil/data-protection/819898/data-protection-in-international-arbitration-a-brazilian-perspective

Costa, R. Veloso Thiago. *Proteção de dados e arbitragem: para além de uma questão legal.* Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-e-arbitragem-para-alem-de-uma-questao-legal-29062019

D. Paisley, Kathleen. *It's all About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration*. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2707&context=ilj

D. Silva, Evellin; Gallindo, Sergio Paulo Gomes; Stivelberg, Daniel T.: *Constitucionalização da proteção de dados pessoais e competências legislativas à luz de análise comparativa entre Direito Pátrio e da União Europeia*. Disponível em: https://www.migalhas.com.br/depeso/315540/constitucionalizacao-da-protecao-de-dados-pessoais-e-competencias-legislativas-a-luz-de-analise-comparativa-entre-direito-patrio-e-da-uniao-europeia

DeMarco, Joseph V.; Sen, Urvashi, *Strategies for Navigating Business-to-Business Data Breaches*. http://go.adr.org/rs/294SFS516/images/NYLJ_B2B_DataBreaches.pdf (6 de julho de 2015)

Fulbright, Norton Rose. *Data protection and cyber-risk issues in arbitration: regulation, cyberattacks and hacked evidence.* Disponível em: https://www.lexology.com/library/detail.aspx?g=19dece65-8e82-464b-9e1a-4f4e1e9709e8

Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pesosais e do Encarregado da Autoridade Nacional de Proteção de Dados – ANPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf

ICCA-NYC Bar-CPR Cybersecurity Protocol for International Arbitration (Edição de 2020) - https://www.acerislaw.com/wp-content/uploads/2020/01/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_electronic_version.pdf

Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal, https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629

Proposta de Emenda à Constituição n° 17, de 2019 - https://www25.senado.leg.br/web/atividade/materias/-/materia/135594

Teixeira, Tarcício; Armelinm, Ruth Maria Guerreiro Fonseca. *Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGP: um Cotejamento com o CDC"* In: Lima, Cintia Rosa Pereira de Lima (Cood). Comentários à Lei Geral de Proteção de Dados, São Paulo, Almedima, 2020, p.314.

União Europeia. EU General Data Protection Regulation (GDPR). Disponível em: https://eugdpr.org/.

USA: District Judge rejects class action lawsuit for 2018 Chegg data breach

MÉTODOS EXTRAJUDICIAIS E A LGPD[1]

Clicar ou escanear para acesso aos debates relativos a este artigo

Autoria

Beatriz Alaíde de Souza Assef[2]

Debatedores

Juliana Loss

Marcelo Chiavassa

RESUMO

A virtualização das relações sociais e econômicas trouxe a necessidade de se tutelar o uso dos dados. Com a elaboração da LGPD, em 2018, tivemos a criação de novos direitos e a ressignificação de princípios constitucionais à luz da tecnologia, o que trouxe para o cenário jurídico uma enorme gama de conflitos inéditos. Os métodos extrajudiciais de resolução de conflitos, especialmente aqueles realizados virtualmente são uma ferramenta eficaz para a solução de disputas, além de possuírem suas próprias regras de proteção de dados e informações.

1. INTRODUÇÃO

Nos últimos anos o cenário jurídico vem enfrentando um período de significativas mudanças, seja em razão da aproximação do direito com a tecnologia, seja pelas análises econômico-comportamentais do ser humano. A (re)leitura de conceitos jurídicos e a re(interpretação) de princípios constitucionais, através de um novo viés, tornaram-se capaz de influenciar as atividades e condutas juridicamente relevantes. Neste panorama, é que o presente trabalho se debruça, estudar a relação entre os métodos extrajudiciais de resolução de conflitos sob o prisma da Lei Geral de Proteção de dados.

[1] Artigo não atualizado após realização dos debates.

[2] Advogada, Mestranda em Processo pela UERJ, Pós-Graduada em Arbitragem e Métodos Consensuais de Resolução de Conflitos pela PUC-Rio e capacitada em Mediação, com formação empresarial pelo Centro Brasileiro de Mediação e Arbitragem – CBMA (2017) e certificada pelo ICFML (2018), certificando-se , também, em "Theories and tools of the Harvard Negotiation Project", cursado no Harvard Faculty Club, Boston (2019). Juntou-se à Faleck & Associados em dezembro de 2019 e tem atuado como facilitadora em programas de indenização.

O ponto de partida é o fato de estarmos diante de novos paradigmas. A maneira pela qual as pessoas buscam resolver os seus problemas e o conteúdo de seus conflitos já não são mais os mesmos que antes. O avanço tecnológico, impulsionado não só pelo contexto de isolamento social, mas também pela crescente virtualização das relações sociais e dos modelos econômicos de negócio, criou uma nova gama de Direito e deveres que podem ser demandados, além de abrir novas portas para o acesso à justiça. Mesmo sem perceber, a tecnologia está profundamente difundida em nosso dia a dia e estamos constantemente injetando informações na rede, seja na compra de mercadorias, na maneira de desbloquear nossos smartphones, seja na confirmação de pagamentos online, marcação de pessoas automática em redes sociais, ou até mesmo para entrada em locais por reconhecimento facial[3], etc.

Em outras palavras, a tecnologia pode parecer inofensiva, mas o que muitos autores vêm debatendo é que essa exposição em massa de dados e virtualização das relações podem trazer sérios riscos aos direitos já existentes, como as Liberdades Fundamentais e ofensas a direitos humanos, quanto aos novos direitos que surgem desse contexto, como a autodeterminação informativa.

E é por esta razão que Lei geral de Proteção de Dados vem ocupando um espaço de tamanha importância das discussões jurídicas. Com a lei, consolidam-se novos conceitos, novos direitos e novas regras de segurança e ética digital tanto para os usuários quanto para as empresas que operam e tratam os dados, nas suas mais diversas formas.

Nesse sentido, o presente trabalho vai apontar que não estamos apenas diante de uma abundância de direitos e deveres, como também uma abundância de meios resolutivos para solucionar as disputas que passam a compor este cenário. Dessa forma, é preciso esclarecer que existem dois pontos interessantes de análise aqui presentes: (i) a utilização dos métodos alternativos para a resolução dos conflitos regulados pela LGPD; e (ii) o próprio cumprimento da LGPD pelos advogados, árbitros, mediadores, negociadores, facilitadores, e demais profissionais da resolução de disputas que venham a ter acesso a dados e informações confidenciais durante o uso de ferramentas no ambiente virtual.

[3] SILVA, Paula Guedes Fernandes da. Sorria você está sendo reconhecido: o reconhecimento facial como violador de direitos humanos? Agosto de 2020. Disponível em: https://feed.itsrio.org/sorr ia-voc%C3%AA-est%C3%A1-sendo-reconhecido-o-reconhecimento-facial-como-violador-de-direitos-humanos-4113914441d3

Vivemos atualmente em um universo rodeado de inovações e desafios tecnológicos em constante desenvolvimento. Diante disso podemos dizer que a utilização da tecnologia não se restringe a agilizar o trabalho dos operadores do direito ou na automação de atividades rotineiras e repetitivas, como também revela a criação de modelos de negócio inéditos, que trazem consigo novos conceitos éticos e legais merecedores de estudo e aprofundamento.

Estamos diante, então, de uma realidade jurídica que incorpora as noções de blockchain, contratos inteligentes, ética digital, inteligência artificial, big data, analytics, algoritmos, linguagem criptografada e códigos autoexecutáveis. E, o fio condutor que conecta todos esses conceitos, é exatamente o tratamento de dados de pessoas físicas ou jurídicas e as consequentes ressignificações de direitos. Segundo Caitlin Mulholland, nessa "sociedade da informação", o direito à privacidade, por exemplo, vai muito além daquele definido como o direito a ficar só, pois agora são necessárias garantias que se estendam também ao nosso corpo eletrônico.

> *O reconhecimento de que "nós somos as nossas informações" impõe que sejamos capazes de obter meios para controlar a circulação de nossos dados pessoais. Esse controle, por sua vez, concretiza-se mediante a adoção de uma Lei Geral de Proteção de Dados.* [4]

A virtualização dos bens da vida e das ferramentas de trabalho aumentou o nosso espectro da personalidade, trazendo ao universo jurídico novos elementos a serem tutelados. Nossa existência passou a ser definida também pelos nossos dados e por isso, a LGPD vem garantir que os indivíduos exerçam sua autonomia quanto aos procedimentos no tratamento de seus dados a fim de evitar quaisquer uso ilegítimo ou eventual abuso.

Assim, não restam dúvidas de que é necessário refletir sobre as consequências que a lei traz para a prestação jurisdicional, tendo em vista a quantidade de novos conflitos que surgirão com a utilização de dados. Levando em consideração que o compartilhamento de dados faz parte do dia a dia de uma parcela significativa da população, na realização de suas atividades rotineiras, é possível prever um aumento considerável no ajuizamento de ações para tratar desses conflitos.

[4] MULHOLLAND, Caitlin (organização). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020.

Vale dizer também que o volume de contendas poderá ser composto não só por conflitos entre titulares de dados e os controladores, como também entre os controladores e operadores de dados, na atividade de repasse ou compartilhamento de informações.

Por isso, urge a necessidade de se pensar em um sistema de resolução de disputas que Que atenda esse tipo de conflito, bem como sua maneira de operacionalização para que eles próprios possam estar conforme a lei.

Como, atualmente, estamos vivendo um momento jurídico de desenvolvimento da política pública de resolução adequada dos conflitos, inaugurada com a Res. 125/2010 e reforçada pelo CPC/2015, com a implementação de um sistema multiportas, torna-se pertinente discutir a utilização das ADRs (alternative dispute resolution) e ODRs (online dispute resolution) como procedimento resolutivo para essas disputas. A análise que aqui se propõe é pensar em uma maneira de resolver esses litígios de maneira eficaz, evitando um aumento de demandas judiciais, e verificar os cuidados necessários para que os procedimentos operem com segurança e confiabilidade.

2. A UTILIZAÇÃO DOS MÉTODOS EXTRAJUDICIAIS PARA A RESOLUÇÃO DE CONTENDAS ENVOLVENDO A PROTEÇÃO DE DADOS

A literatura destaca, partindo da análise de experiências internacionais, que o número de litígios sobre proteção de dados, após a entrada em vigor de leis semelhantes à LGPD, aumentou exponencialmente:

> *Considerando os 28 Estados-Membros da União Européia, além da Noruega, Islândia e Liechtenstein, relatório do escritório de advocacia DLA Piper identificou um total de 160.921 notificações de organizações submetidas às autoridades de proteção de dados reportando violação na proteção de dados pessoais, entre 25 de maio de 2018 e 27 de janeiro de 2020.31 Segundo o documento, é possível que essas violações tenham fundamentos variados, desde e-mails enviados para certos endereços erroneamente até os mais sérios ataques cibernéticos.*[5]

No Brasil conseguimos identificar algo semelhante. Tanto o cenário internacional quanto o nacional são caracterizados pelo aumento da virtualização das relações e pela necessidade de proteção dos dados de ataques cibernéticos, vazamentos de informações e abusos de direitos e garantias individuais no tratamento. Esse choque de interesses, entre

[5]BOTTINO, Celina. PERRONE, Cristian. CARNEIRO, Giovana. HERINGER, Leonardo. VIOLA, Mário. Lei Geral de Proteção de Dados Pessoais e Resolução de Conflitos: Experiências internacionais e perspectivas para o Brasil. Instituto de Tecnologia & Sociedade do Rio. Abril de 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/04/Relatorio_LGPD ResolucaoConflitos.pdf

a utilização dessas informações para dinamização do mercado e a proteção dos titulares em situação de vulnerabilidade requer tutela jurisdicional.

Como já se sabe, o Poder Judiciário não é o único meio possível de resolução de controvérsias. A criação de espaços consensuais, sejam presenciais ou digitais, para a resolução dos conflitos já é um aspecto da nova realidade do direito, tendo um impacto significativo tanto no exercício profissional como no âmbito das instituições públicas.

Sobre a utilização das vias autocompositivas, também podemos buscar referências na experiência internacional. É o que nos informa o ITS, Instituto de Tecnologia & Sociedade do Rio, em estudo publicado em abril de 2020 que aponta as diversas ferramentas consensuais utilizadas pelos países no mundo para pacificar contendas relacionadas à proteção de dados. Neste sentido, podemos identificar mediações realizadas pelas agências reguladoras, plataformas online de criação de acordos, facilitação de diálogo e de composição, e etc.

Vale destacar, no referido estudo, a inovação legislativa realizada na Coréia do Sul, no Personal Information Protection Act — PIPA de 2011, que criou um Comitê de Mediação de Disputas envolvendo Dados Pessoais, em seu artigo 40 e seguintes. Trata-se, em breves palavras, de uma procedimento que pode ser iniciado por telefone ou via plataforma online, integrado por profissionais de diversas áreas do conhecimento, que possuem a função de intermediar o contato entre o titular e o controlador de dados a fim de criar um acordo dentro de um prazo de 60 dias. Como resultado: "entre os anos de 2013 e 2018 foram resolvidos pelos métodos de mediação 692.119 reclamações por parte de titulares."[6]

Nos demais exemplos trazidos nos estudos, percebemos que alguns países optam pela atuação de autoridades ou agências reguladoras, na supervisão do procedimento, ou na utilização de câmaras privadas de Mediação, ressaltando que a realização de procedimentos extrajudiciais não impede a instauração de procedimentos investigativos pelas autoridades. Ou seja, a utilização dos métodos extrajudiciais tem o primordial objetivo satisfazer as demandas dos titulares dos dados, sem impedir que as agências fiscalizadoras possam realizar suas funções investigativas.

Não há um direcionamento específico para um método em particular, mas resta evidenciado, nos países objeto de análise, um forte incentivo aos meios autocompositivos,

[6] KISA, Coreia, 2018, Internet White Paper. Disponível em: https://www.kisa.or.kr/eng/usefulreport/whitePaper_List.jsp

tendo em vista os consequentes resultados de rápida entrega dos pedidos de suspensão do tratamento, retificação ou exclusão dos dados e até pagamento de indenização. O que se percebe é que os países no mundo estão se utilizando dos mais diversos métodos alternativos, em combinação, de acordo com a sua cultura legal, com vistas a facilitar a prestação da tutela jurisdicional e resolução das demandas sobre proteção de dados.

Trazendo essas ideias para o Brasil, o desafio que se coloca é institucionalização ou não da resolução dos conflitos por meio de uma agência reguladora, visto que a ANPD ainda não foi criada, nem tem essas funções previstas em lei, além da superação de uma cultura litigiosa que que não fomenta a utilização dos mecanismos extrajudiciais.

Apesar desses desafios, certo é que a LGPD traz um empoderamento para o cidadão através da criação do conceito de autodeterminação informativa, reforçando as bases legais de consentimento, transparência e autonomia, elementos tão presentes dentro dos procedimentos extrajudiciais. A ideia de aumento do poder decisório do usuário sobre o tratamento de seus dados se coaduna com o espaço para atitude negocial existente nos ambientes de resolução alternativa.

Além desses elementos de contato entre os objetivos da LGPD e os fundamentos inerentes aos meios autocompositivos, podemos destacar ainda a questão do cuidado com a pauta subjetiva potencialmente existente nesses conflitos. Observa-se que o legislador pátrio traz para o ordenamento jurídico o termo "titular de dados" haja vista que a definição de titularidade transmite a noção de proteção a aspectos tanto patrimoniais, relativos ao valor econômico que lhes é atribuído, como também extrapatrimoniais, relativos à proteção dos direitos da personalidade e dos direitos fundamentais. Dessa forma, temos que os dados e a autodeterminação informativa são atributos da personalidade e também um ativo patrimonial, que podem gerar danos à pessoa em sua esfera individual e patrimonial. É o que nos ensina a professora Andrea Maia: a mediação pode ter por objeto conflitos que envolvam direitos disponíveis e direitos indisponíveis passíveis de negociação decorrentes da proteção de dados.

> *Besides, there is already a solid field of private lawtechs in the country, which could be used for solving cases and develop a wide structure of ADR related to Personal Data Rights, since Mediation Law already allows Mediation to be used for disposable rights. This new chapter of Brazilian Data Protection is*

> *about to begin and it is cristal clear that ADR is the only path to go if we want to make these rights effective.*[7]

Dessa forma, a mediação e os demais métodos extrajudiciais, de cunho autocompositivo, tem grande valia no cuidado de conflitos que envolvem danos de natureza extrapatrimonial na medida em que devolvem à pessoa atingida a sua dignidade de maneira mais humanizada, participativa e auto implicativa. Não só isso, eles também concretizam ideais constitucionais de solidariedade e cooperação, freando a lógica da litigiosidade adversarial desmedida presentes em situações jurídicas de cunho exclusivamente patrimonial.

Somado a isso, não podemos deixar de mencionar os usos da tecnologia para a resolução consensual dessas demandas. O ambiente virtual é definitivamente um aliado do acesso à justiça quando se fala em celeridade e eficiência, tendo em vista a aproximação de distâncias, redução de custos com deslocamentos e criação de conexão entre indivíduos integrantes de uma rede de pertinência necessária para a solução dos problemas. Aqui também é importante salientar que os mecanismos não precisam ser integralmente de uma única modalidade, podendo existir a previsão de etapas virtuais e etapas presenciais dentro do mesmo procedimento (híbrido).

A utilização das ferramentas digitais para a resolução das disputas sobre tratamento de dados é oportuna e conveniente, não só pelas características já destacadas, mas também pelo contexto atual de isolamento social e virtualização forçada para aqueles que não podem, ou não querem, esperar pela reabertura total das atividades. Em outras palavras, os indivíduos se encontram cada vez mais familiarizados com o ambiente *online*, apresentando maior adaptabilidade e desenvoltura na utilização dessas plataformas, o que evidentemente facilita a participação em procedimentos virtuais.

Assim, os mecanismos de ODR são uma maneira mais acessível e dinâmica de concretizar o acesso à justiça e a satisfação das partes. Contudo, precisamos nos atentar para o fato de que a conjugação de tecnologia e resolução de disputas pode ser enquadrada na lei de LGPD como uma forma de tratamento de dados a depender dos documentos e informações que a plataforma ou o operador compartilharem. E é exatamente sobre isso que iremos discorrer no seguinte tópico.

[7] MAIA, Andrea. CARNEIRO, Gustavo. Will ADR save brazilian Courts from an avalanche of new cases due to brazilian General Data Protection Act? Julho de 2020. Disponível em: http://mediationblog.kluwerarbitration.com/2020/07/08/will-adr-save-brazilian-courts-from-an-avalanche-of-new-cases-due-to-brazilian-general-data-protection-act/?doing_wp_cron=1596554962.6410539150238037109375

> *Em verdade, trata-se de verdadeira mudança cultural multidisciplinar nas empresas envolvendo as áreas jurídicas, de tecnologia e segurança da informação, recursos humanos, marketing, entre outras, bem como os ideais de ética empresarial e responsabilidade social. Nesse contexto, sem sombra de dúvidas, a Lei Geral de Proteção de Dados é novo grande paradigma de conformidade no Brasil. Aliás, mais que isso, com a previsão expressa do princípio da responsabilização e prestação de contas em seu art. 6º, X, e com uma série de disposições que considera ser fundamental a adequação pelos agentes de tratamento (v.g. como critério à aplicação de sanção pela Autoridade Nacional, é possível dizer que a LGPD representa segundo marco legislativo no Brasil em relação ao compliance, mas agora voltado aos dados pessoais, dispondo expressamente sobre a adoção dos referidos procedimentos de integridade.*[8]

3. O CUMPRIMENTO DA LGPD PELOS PROFISSIONAIS E CÂMARAS DE RESOLUÇÃO ALTERNATIVA DE DISPUTAS

> (...) *a ideia é que os agentes de tratamento que respondem pela Lei (qualquer pessoa jurídica ou natural que trate dados pessoais e que não esteja enquadrada nas causas de exceção de aplicabilidade do art. 4º8) tenham uma área estruturada e em mãos um plano de ação, verdadeiro passo a passo que mapeie e classifique as atividades, instrua os profissionais envolvidos e indique a contratação de novos colaboradores se necessário, reformule estruturas, planeje e implante normas internas de conformidades, etc. O plano de adequação, em razão dessas aptidões práticas, passa a ser ferramenta fundamental a viabilizar que o agente de tratamento esteja em conformidade com a LGPD.*[9]

A LGPD, em seu artigo 5º, se propõe a definir diversos termos importantes que irão delimitar as situações que estão sob sua incidência. Logo nos primeiros incisos temos a definição de "dado pessoal" e "dado pessoal sensível", sendo o primeiro qualquer informação relacionada a pessoa natural identificada ou identificável, e o segundo dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Já no inciso "V", define-se que titular de dados é toda "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento", e no inciso "VI" há a definição de controlador no

[8] TAMER, Maurício Antônio. VAINZOF, Rony. LIMA, Caio César Carvalho. Compliance e LGPD: Plano de adequação como ferramenta de mitigação de riscos legais. JOTA. Março de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-ade quacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019

[9] TAMER, Maurício Antônio. VAINZOF, Rony. LIMA, Caio César Carvalho. Compliance e LGPD: Plano de adequação como ferramenta de mitigação de riscos legais. JOTA. Março de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-ade quacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019

sentido de “pessoa, natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. Destaca-se também que “tratamento”, segundo o inciso “X”, é toda operação realizada com dados pessoais como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Ante tais conceitos, podemos entender que as plataformas de ODR e procedimentos virtuais de resolução, pertencentes ou manuseados por pessoas físicas ou jurídicas, privadas ou públicas, serão eles próprios controladores de dados pessoais, sensíveis ou não, dos participantes, vez que irão realizar o gerenciamento, e eventual compartilhamento, dos documentos e manuseio das informações que serão disponibilizadas no processo de resolução do conflito.

Pensando rápido, parece que a questão envolve meramente o consentimento das partes para que seus dados sejam tratados com a devida segurança durante o procedimento. Contudo, o consentimento é apenas um dos diversos princípios e deveres que são impostos pela Lei, possuindo, inclusive, hipóteses em que ele pode ser dispensado. Além disso, a LGPD não regula apenas o tratamento em si dos dados, mas todo o chamado “ciclo de tratamento”, desde a sua disponibilização até o seu apagamento, com o fim do procedimento.

É importante ressaltar que não trata-se de simples adaptação ou questão de compliance, mas de toda uma transformação na maneira de pensar, criar sistemas, mediar, gerir informações de forma a levar em consideração o direito de privacidade, autonomia informacional, esquecimento, dentre outros direitos, no decorrer da aplicação do método alternativo de resolução de disputa online.

Portanto, se durante o procedimento de resolução de disputa online se realiza qualquer das condutas elencadas como “tratamento de dados” de qualquer pessoa física que se encaixe no conceito de “titular de dados”, realizadas por um “controlador”, então esse procedimento deve se adequar aos fundamentos e determinações impostos pela Lei. Ou seja, para ilustrar, se uma câmara de medição realiza uma reunião online privada com o Sr. João, domiciliado no Estado do Rio de Janeiro, sobre um conflito que ele tem com a empresa Ciclana LTDA, com sede no Estado de São Paulo. Assim, inicialmente, nesta reunião é realizado um cadastro desse participante pessoa física, para que seja possível a

realização de um próximo contato, dentro do procedimento, e juntada de documentos comprobatórios onde demonstra a situação danosa que ele entende ter sofrido. Assim, estamos diante de uma situação sobre a qual recaem as regras da LGPD. Em continuidade à situação exemplificada, depois de realizado um cadastro e entregue os documentos, sob o consentimento da pessoa, esses documentos são encaminhados para a Empresa Ciclana LTDA, em outra reunião privada, que concorda com a situação descrita, trazendo ainda outras informações documentais que ela entende importantes para a composição daquela conjuntura fática. Dentro do procedimento exemplificado, todos os participantes se encontram por meio de uma reunião on line, realizada através de uma plataforma digital e conseguem chegar a um acordo. Em seguida, o mediador tem acesso aos seus dados pessoais para que possa formalizar os combinados e reduzir a termo as informações do acordo. Neste exemplo, fica claro que a ferramenta utilizada pelas partes, por exemplo a Câmara de mediação, passa a deter informações das pessoas envolvidas, o que se encaixa na definição de de operador da dados. Nestes casos, um banco de dados é criado, onde constam os detalhes daquela lide, protegendo informações confidenciais e de natureza eventualmente sensível, realizando o meio de campo e promovendo a simetria de informações.

Por isso, as Câmaras de Mediação, ou até mesmo os profissionais autônomos de resolução de disputas, precisam se atentar para a organização de um protocolo de cibersegurança e verificar a estruturação de seus procedimentos resolutivos conforme a LGPD, para que não sejam surpreendidos com a eventual aplicação de multas.

Outra questão importante é que, além das sanções previstas em lei, a ausência desses protocolos pode afetar a reputação das Câmaras e dos profissionais envolvidos,, tendo em vista a natureza preponderantemente privada do ramo da resolução extrajudicial de conflitos. No intuito de preservar um status reputacional, é aconselhado a elaboração de um roteiro (manual) de práticas adequadas para o ambiente virtual de resolução de disputas e a reorganização dos procedimentos.

Os primeiros passos para a implementação de um plano de adequação seriam, então, o mapeamento da atividade da empresa e identificação do fluxo de dados (data flow), para a posterior criação das medidas de segurança (artigo 46) e regras de governança (artigo 50). Essa análise é fundamental para que sejam identificados os locais de ajuste, sem prejuízo da avaliação da legalidade do procedimento como um todo.

> *Isso tudo é fundamental para se avaliar, por exemplo, quais as bases legais de tratamento são necessárias, se é possível a comunicação ou o uso*

> *compartilhado entre as empresas, o quanto vale a pena investir em medidas de anonimização e a existência de padrões ou normas técnicas específicas. Identifica-se também qual o ciclo de vida dos dados pessoais na empresa. Isso é fundamental para se compreender quais departamentos e colaboradores devem ser instruídos e onde devem ser aplicadas as soluções tecnológicas, de segurança e procedimentos para garantir a contenção de tais informações, por exemplo.*[10]

Também é importante verificar, de maneira mais específica, se o procedimento resolutivo online, realizado pela câmara, empresa ou profissional autônomo, é enquadrado como operador ou controlador. Pelo o que vimos, entende-se que se deve tratar de controlador de dados, contudo deve-se atentar para a atividade que está sendo efetivamente desempenhada para que sejam aplicadas as normas legais coerentes. Não resta dúvida que, de um modo ou de outro, o procedimento deve ser pautado nos princípios e fundamentos da proteção de dados, tal qual descritos no artigo 2 da Lei, como no de maneira esparsa em outros dispositivos.

O primeiro fundamento que se quer destacar é o do "Desenvolvimento tecnológico e a Inovação" (artigo 2, V). Esse fundamento põe por terra a ideia de que a proteção de dados inibe o desenvolvimento da tecnologia. O que está por trás desse conceito é a ideia de que não podemos retirar o aspecto humano dos usos tecnológicos, ou em outras palavras, não pode o ser humano ser apenas um insumo ou um "input" para a exploração comercial dos dados. Então, a LGPD quer incentivar que os avanços, inovações e uso do ambiente virtual respeitem a dignidade humana e fortaleçam o usuário. A ideia é que, no mercado, se destaquem aquelas empresas que oferecem aos seus clientes ambientes mais seguros e cuidadosos. Assim, a virtualização da resolução de disputas deve também, dentro de seu ramo de atuação, continuar se aprimorando e, ao mesmo tempo, respeitar os direitos e garantias individuais das partes envolvidas.

Outro princípio que traz implicações interessantes é o consentimento, definido como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (artigo 5 inciso XII). Nesse sentido temos que o consentimento é qualificado e que ele está conectado a uma finalidade específica; ressaltando que o artigo 7 impõe que o tratamento de dados só é permitido mediante consentimento, ou nos demais casos taxativamente elencados, e que

[10] TAMER, Maurício Antônio. VAINZOF, Rony. LIMA, Caio César Carvalho. Compliance e LGPD: Plano de adequação como ferramenta de mitigação de riscos legais. JOTA. Março de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/compliance-e-lgpd-plano-de-ade quacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019

o artigo 8 determina que é de responsabilidade do controlador comprovar que o consentimento foi obtido conforme a Lei. Apesar de imprescindível, o consentimento não é uma carta branca do titular ao controlador, pelo contrário, ele abre uma porta muito delimitada e dentro dessa porta existem outros fundamentos igualmente relevantes:

> *A princípio, pode-se pensar que a solução para a adequação está basicamente na obtenção do consentimento, para que os dados pessoais, sensíveis ou não, sejam tratados com a devida segurança no decorrer do procedimento. Todavia, tal entendimento poderia gerar prejuízos sem precedentes, visto que o consentimento, que é apenas uma das bases legais de tratamento, pode ser revogado pelo titular.* [11]

Assim, dentro de um procedimento online de Mediação, o consentimento para a utilização dos dados também deve ser qualificada, clara e específica para a aquele procedimento, havendo a possibilidade de revogação deste. Mesmo após a entrega dos dados para o Mediador, ou para aquele que ocupar a figura de controlador, o sujeito continua sendo titular de seus dados e, portanto, mantém o direito de gerenciar o seu uso. É essa permissão legal de gerenciamento e acesso aos dados pelo titular que conecta o consentimento ao direito de privacidade, gerando para o controlador a obrigação de guardar essas informações com segurança e manter o titular informado sobre os usos. Insta lembrar que, para a LGPD, crianças e adolescentes não estão aptos a prestar consentimento, devendo o tratamento desses dados ser realizado com a autorização de pelo menos um responsável legal.

> *The LGPD demands the consent of the data subject in almost any case of data processing. But even after the consent to the processing of their personal data, the natural person remains the data holder, having the right to access and manage its use. The ownership of personal data is connected to the fundamental right of privacy*[12].

A Privacidade (artigo 2), também fundamento da proteção de dados, deve ser compreendida em sua concepção funcional, ou seja, ela assegura que o sujeito tenha a possibilidade de "conhecer, controlar, endereçar, interromper o fluxo de informações a ele relacionadas". Na prática, um exemplo de repercussão do princípio da privacidade no procedimento é a realização de reuniões privadas (caucus), em que são repassados ao

[11] BERTHIER. Rodrigo. LGPD E ARBITRAGEM. Adamnews. Julho de 2019. Disponíivel em: http://camob.com.br/2019/07/18/lgpd-arbitragem/

[12] MAIA, Andrea. CARNEIRO, Gustavo. Will ADR save brazilian Courts from an avalanche of new cases due to brazilian General Data Protection Act? Julho de 2020. Disponível em: http://mediationblog.kluwerarbitration.com/2020/07/08/will-adr-save-brazilian-courts-from-an-avalanche-of-new-cases-due-to-brazilian-general-data-protection-act/?doing_wp_cron=1596554962.6410539150238037109375

mediador dados e informações que eventualmente não devem ser transmitidas à outra parte, ou que serão transmitidas por intermédio de uma plataforma. Nesse caso, para que a confidencialidade inerente do método não seja violada, nem o direito de privacidade do titular seja atingido, cabe à Câmara, ou profissional, se certificar de que a plataforma utilizada possui todos os requisitos de segurança necessários para os repasses de informações.

Em relação à confidencialidade dos procedimentos extrajudiciais, coloco aqui o questionamento sobre a aplicação do princípio livre concorrência e livre atividade econômica, no que tange à realização da portabilidade de dados (artigo 18, V). Segundo a Lei, é possível que, mediante solicitação do titular, a empresa controladora encaminhe definitivamente os dados disponibilizados para outra empresa. Nesse caso, fica a dúvida sobre, se em uma mediação, seria realmente possível esse compartilhamento de dados entre Câmaras ou Mediadores, ainda que solicitado pelo titular, haja vista que o procedimento em si demanda confidencialidade. Inclusive, alguns discursos de abertura de procedimento consensual trazem o alinhamento de que as informações produzidas e expostas ali não poderão ser utilizadas em outros procedimentos, nem o mediador servir de testemunha do que foi dito[13]. Sendo assim, acredito, por ora, não ser possível a portabilidade entre Câmaras e Mediadores, devendo o titular iniciar o procedimento do zero com a outra empresa ou profissional, reiniciando a disponibilização dos dados.

Por último, também considera-se importante ressaltar que, em decorrência dos princípios de privacidade e esquecimento, o titular pode solicitar a qualquer tempo a exclusão de seus dados dos bancos e armazenamentos do controlador e operador. A exclusão pode se dar durante o tratamento, caso, por exemplo, o titular decida mudar de Câmara ou encerrar as negociações, ou ao final do procedimento, com a produção do acordo, implicando na total proibição de a Câmara ou profissional de solução de disputas online realizar a retenção de qualquer informação.

Somado aos princípios e fundamentos gerais da LGPD já descritos, também vale trazer algumas outras providências destacadas pela Lei. A criação de medidas de

[13] LEI Nº 13.140, DE 26 DE JUNHO DE 2015. Art. 2º A mediação será orientada pelos seguintes princípios: I - imparcialidade do mediador; II - isonomia entre as partes; III - oralidade; IV - informalidade; V - autonomia da vontade das partes; VI - busca do consenso; VII - confidencialidade; VIII - boa-fé. § 1º Na hipótese de existir previsão contratual de cláusula de mediação, as partes deverão comparecer à primeira reunião de mediação. § 2º Ninguém será obrigado a permanecer em procedimento de mediação.

Art. 7º O mediador não poderá atuar como árbitro nem funcionar como testemunha em processos judiciais ou arbitrais pertinentes a conflito em que tenha atuado como mediador.

segurança, por exemplo, são fundamentais para evitar "acessos não autorizados aos dados pessoais tratados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilegal" (artigo 46).São exatamente essas medidas que irão manter o agente de tratamento em conformidade com a novas regras de proteção. Já as medidas de boa governança sugerem definições de padrões de condutas e procedimentos internos, com treinamento dos profissionais, para que demonstrem o cuidado da Câmara com essas questões.

4. CONCLUSÕES

No decorrer dos últimos anos, os dados e informações se tornaram um novo objeto de propriedade, foram monetizados, e com isso abriram espaço para um enorme número de operações virtuais. Diante desse cenário o legislador se viu obrigado a regulamentar a movimentação desse novo bem jurídico. E, não só isso, esses novos direitos foram percebidos como de caráter misto, impondo a tutela de seus aspectos patrimoniais conjuntamente com os extrapatrimoniais, e relativos à pessoa natural, numa tentativa de "recolocar a pessoa humana no centro da tutela jurídica"[14].

Ao longo do trabalho, foram expostos diversos fundamentos da proteção de dados, que se consolidam, em breves palavras, nos direitos de: confirmação de tratamento, livre acesso aos dados, conhecimento da forma de coleta e armazenamento, explicação sobre decisões automatizadas, obtenção de informações sobre o processamento, correção de dados incompletos ou errados, garantia da qualidade dos dados, bloqueio de dados, eliminação dos dados do banco, portabilidade dos dados a outro fornecedor, informação sobre o compartilhamento dos dados, revogação de consentimento, dentre outros.

Como consequência da existência desses novos direitos, da evolução do modo de resolução de conflitos e do avanço tecnológico temos a uma realidade peculiar na qual se repensa a maneira de dirimir os litígios decorrentes dessas relações. Os juristas e operadores constroem e desenham instrumentos adequados à essa particular realidade, e ao colocar essas ferramentas em prática, o resultado que se têm obtido, conforme as pesquisas referenciadas neste trabalho, é positivo.

Vimos que a utilização dos métodos extrajudiciais de resolução se justificam pela congruência intrínseca de elementos que conectam as bases da proteção de dados às

[14]MULHOLLAND, Caitlin (organização). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, p. 197.

características negociais presentes na criação e facilitação de acordos. Somado à essa coerência sobre a utilização de métodos como a mediação, acrescentamos a crescente virtualização dos procedimentos e maior familiarização com o ambiente digital, o que faz com que também seja propícia a elaboração de procedimentos online de resolução. Ou seja, os métodos extrajudiciais e virtuais trazem para a proteção de dados uma porta realmente eficiente para a resolução das contendas.

Concluindo, diante da utilização do ambiente digital, os profissionais que atuam no solucionamento desses conflitos precisam se ajustar para que eles próprios possam cumprir as determinações legais impostas ao tratamento dos dados. Nesse sentido, foram levantadas diversas aplicações práticas dos princípios e fundamentos trazidos pela Lei a fim de esclarecer o caminho pelo qual Câmaras e Profissionais terão que passar. Dessa forma, a inovação tecnológica e a humanização da justiça, hoje mais do que nunca, caminham de braços dados, seja no oferecimento de métodos com arranjos interessantes e eficazes, seja na própria realização prática destes procedimentos.

REFERÊNCIAS BIBLIOGRÁFICAS:

SILVA, Paula Guedes Fernandes da. Sorria você está sendo reconhecido: o reconhecimento facial como violador de direitos humanos? Agosto de 2020. Disponível em: https://feed.itsrio.org/sorr ia-voc%C3%AA-est%C3%A1-sendo-reconhecido-o-reconhecimento-facial-como-violador-de-direitos-humanos-4113914441d3

MULHOLLAND, Caitlin (organização). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020.

BOTTINO, Celina. PERRONE, Cristian. CARNEIRO, Giovana. HERINGER, Leonardo. VIOLA, Mário. Lei Geral de Proteção de Dados Pessoais e Resolução de Conflitos: Experiências internacionais e perspectivas para o Brasil. Instituto de Tecnologia & Sociedade do Rio. Abril de 2020. Disponível em: https://itsrio.org/wp-content/uploads/2020/ 04/Relatorio_LGPD ResolucaoConflitos.pdf

KISA, Coreia, 2018, Internet White Paper. Disponível em: https://www.kisa.or.kr/eng /usefulreport/ whitePaper_List.jsp

MAIA, Andrea. CARNEIRO, Gustavo. Will ADR save brazilian Courts from an avalanche of new cases due to brazilian General Data Protection Act? Julho de 2020. Disponível em: http://media tionblog.kluwerarbitration.com/2020/07/08/will-adr-save-

brazilian-courts-from-an-avalanche-of-new-cases-due-to-brazilian-general-data-protection-act/?doing_wp_cron=1596554962.6410539150238037109375

BERTHIER. Rodrigo. LGPD E ARBITRAGEM. Adamnews. Julho de 2019. Disponíivel em: http://camob.com.br/2019/07/18/lgpd-arbitragem/

TAMER, Maurício Antônio. VAINZOF, Rony. LIMA, Caio César Carvalho. Compliance e LGPD: Plano de adequação como ferramenta de mitigação de riscos legais. JOTA. Março de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/complia ce-e-lgpd-plano-de-adequacao-como-ferramenta-de-mitigacao-de-riscos-legais-07042019

FRANCELINO, Davi. LGPD: como a mediação online seguirá os protocolos? JOTA. Setembro de 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-como-a-mediacao-online-seguira-os-protocolos-16092020?utm_campaign=jota_info__ultimas_noticias&utm_medium=email&utm_source=RD+Station

#CONTRACAPA