07

A influência da LGPD na arbitragem internacional

Adriano Fernandes Ferreira

Graduação em Direito pelo Centro Universitário de Maringá (2001), Mestrado em Direito pela Universidade Gama Filho (2005), Doutorado em Ciências Jurídicas pela Universidad Castilha la Mancha, na Espanha (2014) e Pós-Doutor em Direito Pela Universidade de Santiago de Compostela, na Espanha (2019). Atualmente é professor Adjunto IV, da Universidade Federal do Amazonas- UFAM - das disciplinas de Direito Internacional Público e Direito Internacional Privado e Vice-Diretor da Faculdade de Direito da UFAM.

Eloah Scantelbury de Almeida

Membro do Grupo de Estudos em Arbitragem e Direito Empresarial- UFAM, do Núcleo de Estudos em Arbitragem do Norte, do Young International Council for Commercial Arbitration e do Comitê de Jovens Arbitralistas. Competidora do 27 Willem C. Vis International Commercial Arbitration Moot (2019) e da XI Competição Brasileira de Arbitragem da CAMARB (2020). Menção Honrosa na Competição Regional Norte de Arbitragem, 2020. Graduanda em direito na Universidade Federal do Amazonas, Manaus, Amazonas

DOI: 10.47573/aya.5379.2.74.7

RESUMO

Em uma sociedade em constante busca de conhecimento e informação, onde os dados pessoais tornaram-se uma moeda de troca e um verdadeiro parâmetro de pesquisa e influência, a Lei Geral de Proteção de Dados surge como uma ferramenta que visa assegurar o direito à privacidade, à liberdade e ao livre desenvolvimento da pessoa natural. Em vista disso, propõe-se um estudo dos aspectos principais da LGPD, seus objetivos, fundamentos, conceitos relevantes e determinações, bem como, a verificação da influência dessa nova legislação nas Câmaras Arbitrais e procedimentos de Arbitragem Internacional. Será demonstrada a necessidade de proteção dos dados tratados pelas Câmaras Arbitrais e as principais legislações internacionais que influenciaram direta ou indiretamente na criação da Lei Geral de Proteção de Dados através de uma análise bibliográfica e comparativa. Por fim, serão verificadas ainda as principais medidas preventivas a serem adotadas para proteger os dados coletados no âmbito das arbitragens internacionais.

Palavras-chave: lei geral de proteção de dados. tratamento de dados. arbitragem internacional. direito internacional. câmaras arbitrais.

INTRODUÇÃO

Os procedimentos arbitrais são geralmente protegidos por sigilo, sendo resguardados os atos procedimentais e provas obtidas durante o procedimento, porém, é inegável que por trás de todo procedimento, seja entre pessoas físicas ou jurídicas, são coletados diversos dados pessoais.

O crescimento das relações negociais internacionais alavancou também a utilização da Arbitragem Internacional como um mecanismo de resolução de eventuais conflitos decorrentes das relações contratuais. Essas relações muitas vezes englobam o cadastro de dados pessoais dos sujeitos envolvidos no procedimento arbitral: partes, advogados, árbitros, experts, testemunhas, dentre outros. Além disso, a própria dilação probatória poderá coletar dados referentes a terceiros por meio de depoimentos e provas documentais.

Todas essas informações coletadas são armazenadas em um banco de dados, normalmente no sistema interno de uma Câmara Arbitral. Diante desse cenário, é necessário resguardar os dados armazenados e fazer a devida adequação das Câmaras Arbitrais às exigências apontadas pela Lei Geral de Proteção de Dados que entrou em vigor em 18 de setembro de 2020.

Ao longo deste estudo serão abordados os aspectos gerais da LGPD, seus principais conceitos e princípios, bem como, será realizada uma análise comparativa entre a Lei Geral de Proteção de Dados e sua antecessora na Europa: a General Data Protection Regulation - GDPR. Serão elencadas também algumas das recomendações elaboradas pela do Protocolo de Cybersegurança na Arbitragem Internacional da International Council for Commercial Arbitration -ICCA, em parceria com a New York City Bar Association e o International Institute for Conflict Prevention & Resolution.

Outro aspecto abordado será a necessidade de adequação das Câmaras Arbitrais às disposições da LGPD, a observância aos critérios de transferência internacional de dados e as

medidas que podem ser adotadas a fim de garantir a segurança dos dados coletados e assegurar o direito dos titulares.

ASPECTOS GERAIS DA LGPD

A troca de conhecimento e informações sempre foi uma atividade presente no comportamento humano, porém, atualmente, muito mais do que apenas dados, essas informações tornaram-se mercadorias valiosas. Os dados coletados em diversas plataformas têm transformado as informações pessoais em um verdadeiro produto, vendido com o intuito de identificar padrões, preferências e opiniões sob o pretexto de melhor adequar os serviços às necessidades de seus clientes.

Mas a partir do momento em que essa coleta de informações é tratada como mercadoria, o titular se torna o produto e não mais o cliente. Apesar de o tratamento de dados ser uma prática recorrente e necessária para o bom funcionamento de diversos setores da sociedade, é preciso estabelecer limites para o tratamento desses dados a fim de assegurar a privacidade do titular dessas informações.

Além disso, a tecnologia e a inovação tem sido aspectos essenciais para o desenvolvimento da sociedade contemporânea, de modo que, a globalização proporcionada pelo acesso à internet e o crescimento da troca de informações online, bem como, das redes sociais e aplicativos, intensificou a necessidade de proteção dos dados que são compartilhados pelos usuários.

> Com o acelerado desenvolvimento tecnológico e a consolidação de espaços públicos virtuais, a gestão da informação sobre si próprio tornou-se expressão fundamental do indivíduo. Por conseguinte, revela-se impossível cogitar a proteção integral à liberdade, à privacidade e ao desenvolvimento da pessoa natural sem que se lhe garanta eficaz defesa e controle de seus próprios dados – o que se traduz na expressão autodeterminação informativa. (FRAZÃO; TEPEDINO; OLIVA, 2019, p. 677/678)

A Lei Geral de Proteção de Dados surge com o intuito de atender aos aspectos jurídicos dessas novas demandas que são apresentadas pela Pós-Modernidade.

O Art. 1° da referida lei apresenta em termos gerais o objeto a ser regulado por ela e o objetivo da criação da LGPD:

> 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. (BRASIL, 2018, Art.1º)

O objetivo da Lei Geral de Proteção de Dados é, portanto, assegurar o direito de privacidade e liberdade dos usuários, assim como, garantir o livre desenvolvimento da pessoa natural, resguardando seus dados pessoais.

Vale ressaltar que a lei abrange tanto os dados tratados por meio digital quanto por meios não-digitais, tratados por pessoas físicas ou jurídicas, de direito público ou privado, devendo ser observada em todo o território nacional.

> Em uma Era na qual reputação e credibilidade são julgadas tão rapidamente quanto o dedilhar dos limitados caracteres dos aplicativos de smartphones, e diante da flagrante fragilidade dos usuários da internet perante o tratamento e a manipulação dos seus dados, a preservação da privacidade, ancorada pela então frágil autodeterminação informativa,

> esta entendida como a faculdade de que toda e qualquer pessoa possa determinar os limites do uso de seus dados pessoais ganha aos poucos a proteção estatal. Ainda que a preocupação pela privacidade remonte à Antiguidade, é na sociedade moderna que o embate entre o avanço tecnológico e a invasão da vida privada carece cada vez mais de proteção, fazendo com que as legislações nacionais primem por legislar quanto à coleta, ao armazenamento, ao uso e à transmissão dos dados pessoais. (COSTA, 2019, p. 4)

No que diz respeito à abrangência da lei, o Art.3° da LGPD elenca também a possibilidade de aplicação da lei a dados em tratamento em outros países, desde que, a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços, o tratamento de dados de indivíduos localizados no território nacional; ou ainda de dados que tenham sido coletados no território nacional, sendo assim considerado se a pessoa titular dos dados estiver no Brasil no momento da coleta.

O Art.5° da LGPD apresenta alguns conceitos extremamente relevantes para a abordagem da matéria, sendo essencial ressaltar alguns deles: o conceito de dado pessoal, tratamento, banco de dados, titular, controlador, operador, encarregado e agentes de tratamento.

O dado pessoal é toda informação relativa a uma pessoa identificada ou identificável, há ainda o dado pessoal sensível que diz respeito à aspectos raciais e étnicos, sexuais, dados referentes à saúde, genéticos ou biométricos, ou dados referentes a filiação a organizações religiosas, políticas, filosóficas ou sindicatos. Existe também o dado anonimizado que refere-se ao caso em que não é possível identificar, através dos meios disponíveis no momento do tratamento, a pessoa natural titular da informação.

O tratamento consiste em toda operação realizada com dados pessoais, desde a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle da informação, modificação, comunicação, transferência, difusão ou extração.

Outros conceitos importantes são os sujeitos envolvidos na operação de tratamento de dados. O titular é a pessoa a quem os dados tratados se referem, o controlador é o sujeito a quem compete as decisões acerca do tratamento desses dados, podendo ser tanto pessoa natural quanto jurídica, de direito público ou privado.

Há ainda o operador, aquele que de fato realiza o tratamento dos dados em nome do controlador, havendo também, o encarregado, a pessoa indicada para ser um canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados. Já a atuação conjunta do controlador e operador forma o conjunto de sujeitos denominados como agentes de tratamento.

A LGPD tem como princípios: a finalidade que determina que os dados coletados deverão ser usados apenas para o fim específico informado ao titular; a adequação da forma de tratamento utilizada à sua finalidade; a necessidade, devendo o tratamento restringir-se ao mínimo de informações necessárias para cumprir a finalidade; o livre acesso do titular às suas informações; a qualidade dos dados coletados; a segurança; transparência; a prevenção; a não-discriminação; responsabilização e a prestação de contas.

O Art. 18 da LGPD lista ainda alguns dos direitos do titular, sendo estes o direito de obter do controlador dos dados a confirmação da existência de tratamento, o acesso aos dados tratados, a correção de dados que eventualmente estejam incompletos ou desatualizados, a anonimi-

zação, bloqueio ou eliminação de dados desnecessários, a portabilidade desses dados para outro fornecedor de produto ou serviço, informação sobre as entidades com as quais o controlador compartilhou esses dados, a revogação do consentimento e informações sobre a possibilidade de não dar o consentimento e as consequências de uma eventual negativa.

Em face do exposto, é possível verificar que o principal intuito desta legislação é proteger os dados pessoais dos titulares a fim de assegurar o direito à privacidade constitucionalmente estabelecido no Art. 5, X da Constituição Federal. A LGPD surge com o intuito de impedir a comercialização desenfreada de dados pessoais, visando preservar o direito ao livre desenvolvimento do indivíduo a fim de que este não seja transformado em um mero produto em meio à sociedade da informação.

LEGISLAÇÕES INTERNACIONAIS E ESTRANGEIRAS SOBRE PROTEÇÃO DE DADOS

A necessidade de proteção dos dados pessoais é um fator que não se limita ao território nacional, mas que tem se evidenciado mundialmente, gerando então o surgimento de diversas legislações e protocolos internacionais que buscam regular a matéria.

Com a expansão das relações pessoais, comerciais, negociais e jurídicas para além das fronteiras nacionais, surgiu a necessidade de observar, nas transações internacionais, as leis acerca do tratamento de dados.

Em decorrência disto, a criação da LGPD foi fortemente influenciada por outros dispositivos internacionais e estrangeiros que já vinham sendo implementado em outros países, uma dessas legislações foi a General Data Protection Regulation - GDPR, adotada pela União Européia para proteger os dados pessoais referentes a seus cidadãos.

A criação da GDPR uniformizou os critérios para tratamento de dados em toda a União Européia, gerando uma forte pressão internacional a fim de que os demais países, inclusive o Brasil, se adequassem e implementarem normas mais rígidas de tratamento de dados para dar continuidade a suas relações comerciais com a Europa:

> Além das questões éticas, a pressão internacional exercida pela General Data Protection Regulation (GDPR) da União Europeia (UE) foi uma motivação, definindo que apenas organizações de países com um nível maior ou igual de rigor para proteção de dados em legislação podem armazenar dados pessoais dos cidadãos da União Européia, impactando, por exemplo, diretamente os negócios brasileiros. (CARVALHO; OLIVEIRA; CAPPELI; MAJER, 2019, p.1)

A GDPR entrou em vigor em 25 de maio de 2018 sendo aplicável a todos os países membros da União Européia e surgiu como uma verdadeira revolução acerca do conceito de privacidade ao regular o tratamento de dados pessoais de todos os cidadãos da União Europeia independentemente de onde esses dados serão tratados (GODDARD, Michel, 2017, p.703, tradução nossa).[1]

Existem claras semelhanças entre a GDPR e a LGPD que evidenciam o uso da legislação europeia como uma fonte de inspiração na elaboração da Lei Geral de Proteção de Dados, tal fato é constatado, por exemplo, na conceituação legal de alguns termos.

1 The EU General Data Protection Regulation (GDPR), which will be enforced across all EU Member States from 25 May 2018, is a landmark in the evolution of the European privacy framework.

Tanto a LGPD em seu Art.5, inciso I quanto à GDPR em seu Art. 4 (1) definem dados pessoais como qualquer informação relativa a uma pessoa natural identificada ou identificável. Já o termo tratamento, conceituado no Art.5, X da LGPD e no Art.4°(2) da GDPR, apresenta algumas divergências entre as duas leis, sendo importante ressaltar que ambas apresentam um rol de operações realizadas com dados pessoais que se enquadram no conceito, levantando divergências acerca da taxatividade ou não desse dispositivo.

Ambas as legislações, na redação do conceito de tratamento de dados passam a ideia de um rol meramente exemplificativo:

Art. 5º Para os fins desta Lei, considera-se:

> X - tratamento: 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;" (BRASIL, LGPD, 2018, Art. 5º)

Art. 4º Para fins desta lei, considera-se:

> (2) processamento' significa qualquer operação ou conjunto de operações realizado em dados pessoais ou em conjuntos de dados pessoais, por meios automatizados ou não, como coleta, registro, organização, estruturação, armazenamento, adaptação ou alteração, recuperação, consulta, uso, divulgação por transmissão, disseminação ou de outra forma disponibilizando, alinhamento ou combinação, restrição, apagamento ou destruição; (UNIÃO EUROPÉIA,GDPR, 2018, Art. 4º-2, tradução nossa).[2]

Essa inexatidão no conceito de tratamento de dados pode criar um cenário de enorme insegurança para os agentes de tratamento que precisam enquadrar-se nos parâmetros legais. Com um rol tão extenso e ampliável é preciso haver uma cuidadosa observância das medidas necessárias para proteção de dados pessoais.

Outra comparação necessária diz respeito aos princípios norteadores de ambas as legislações em análise. A LGPD em seu Art. 6 elenca 10 princípios que devem ser observados, já a GDPR em seu Art. 5 enumera 8 princípios, apesar de haver algumas divergências entre uma lei e outra, muitos desses institutos se correspondem em ambas as legislações.

O princípio da finalidade apresenta-se em ambas as leis com a mesma nomenclatura, já a adequação, prevenção e necessidade presentes na LGPD apresentam-se reunidos na GDPR como um mesmo princípio: a minimização de danos. O princípio do livre acesso, previsto na legislação brasileira não encontra um correspondente na lei adotada pela União Européia.

A qualidade dos dados é nomeada na GDPR como o instituto da exatidão dos dados tratados, já os conceitos de não-discriminação e transparência foram reunidos em um único princípio: o da justiça e transparência. O conceito de segurança do tratamento de dados é nomeado na legislação Européia como integridade e confidencialidade. No que concerne à responsabilidade e prestação de contas previsto pela LGPD, na GDPR consta apenas o princípio da prestação de contas.

Vale ressaltar que a GDPR adota um princípio que não foi incorporado à legislação bra-

2 For the purposes of this Regulation:
(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

sileira: o instituto da limitação de armazenamento, que consiste na limitação do armazenamento dos dados por tempo não superior ao necessário para os fins os quais os dados são processados. Abre-se a exceção por períodos mais longos desde que os dados sejam processados para fins exclusivamente de interesse público, pesquisa científica, histórica ou fins estatísticos, devendo ser adotadas as medidas preventivas previstas pela GDPR.

Além da influência direta da GDPR, especificamente no que concerne à proteção de dados no âmbito da Arbitragem Internacional, a Lei Geral de Proteção de Dados foi precedida também por um protocolo elaborado pelo International Council for Commercial Arbitration -ICCA, em parceria com a New York City Bar Association e o International Institute for Conflict Prevention & Resolution por meio do Working Group on Cybersecurity in International Arbitration que traçou diretrizes gerais para melhorar a cibersegurança nos procedimentos arbitrais.

Esse protocolo tem o status de soft law, uma vez que, foi elaborado por organismos não-estatais visando traçar parâmetros gerais e orientações sobre proteção de dados:

> Em síntese, normas não-estatais devem ser compreendidas como normas emanadas por entes não estatais e que não são consideradas vinculantes. Para fim do estudo sobre processo arbitral, são normas não estatais os instrumentos elaborados por organizações internacionais, instituições arbitrais e entidades destinadas ao estudo e ao desenvolvimento da arbitragem. Podem ter a forma de leis-modelo, diretrizes, regulamentos, resoluções, regras, checklists, notas, códigos de conduta, entre outros, com a finalidade de organizar o procedimento arbitral, ou certos aspectos desse procedimento, e não possuem caráter mandatório ou vinculante. (MANGE; 2014, p. 194)

O Protocolo da ICCA de Cibersegurança na Arbitragem Internacional não tem como intuito estabelecer uma forma específica de proteção de dados no procedimento arbitral, mas oferece diretrizes, princípios gerais que podem ser considerados pelas partes e pelo Tribunal Arbitral, resguardada a autonomia da vontade das partes e a independência dos árbitros para julgar quais medidas seriam necessárias frente às circunstâncias de cada caso.

O Protocolo da ICCA ressalta a importância de que, uma vez estipuladas as medidas para proteção de dados, estas devem ser devidamente observadas por todos os envolvidos no procedimento arbitral, como dispõe o Princípio 3:

> As partes, árbitros e instituições administradoras devem garantir que todas as pessoas direta ou indiretamente envolvidas em uma arbitragem em seu nome estejam cientes e sigam quaisquer medidas de segurança da informação adotadas em um processo, bem como o impacto potencial de quaisquer incidentes de segurança (ICCA, 2020, p. 1, tradução nossa)[3]

A não observância das medidas de segurança adotadas pode gerar punições para aquele que eventualmente dê causa a um vazamento de informações e incidentes de segurança da informação podem gerar uma alocação dos custos entre as partes, conforme prevê o Princípio 13 do Protocolo da ICCA:

> Em caso de violação das medidas de segurança da informação adotadas em procedimento arbitral ou na ocorrência de incidente de segurança da informação, o tribunal arbitral poderá, a seu critério: (a) alocar os custos relacionados entre as partes; e / ou (b) impor sanções às partes (ICCA, 2020, p. 3, tradução nossa).[4]

3 Principle 3 Parties, arbitrators, and administering institutions should ensure that all persons directly or indirectly involved in an arbitration on their behalf are aware of, and follow, any information security measures adopted in a proceeding, as well as the potential impact of any security incidents.

4 Principle 13 In the event of a breach of the information security measures adopted for an arbitration proceeding or the occurrence of an information security incident, the arbitral tribunal may, in its discretion: (a) allocate related costs among the parties; and/or (b) impose sanctions on the parties.

Para que sejam determinadas as medidas de proteção de dados adequadas a cada caso, o Protocolo sugere no Princípio nº 6 alguns fatores a serem considerados pelas partes, pela Câmara Arbitral e pelo Tribunal Arbitral: o perfil de risco da arbitragem; as práticas existentes de segurança da informação, infraestrutura e capacidade das partes; os encargos, custos e recursos; a proporcionalidade em relação ao tamanho, valor e perfil de risco da controvérsia e a eficiência do procedimento arbitral.

O instituto traz ainda uma lista das principais áreas de vulnerabilidade que precisam ser observadas e fortalecidas para garantir a maior proteção dos dados pessoais coletados durante um procedimento arbitral, como dispõe o Princípio nº 7 do Protocolo da ICCA:

> Princípio 7 Ao considerar as medidas específicas de segurança da informação a serem aplicadas em uma arbitragem, devem ser consideradas as seguintes categorias:
>
> (a) gestão de ativos;
>
> (b) controles de acesso;
>
> (c) criptografia;
>
> (d) segurança das comunicações;
>
> (e) segurança física e ambiental;
>
> (f) segurança das operações; e
>
> (g) gestão de incidentes de segurança da informação. (ICCA, 2020, p. 2, tradução nossa)[5]

Diante disto, é possível verificar que, em todo o mundo, a proteção de dados, sejam eles armazenados em meio físico ou virtual, tem sido alvo de muitos questionamentos e estudos, havendo ainda um cenário de incerteza mesmo nos países que já regulamentaram a matéria. Assim como o modo de compartilhar informações está em constante mudança, a proteção dessas informações é uma atividade dinâmica e extremamente necessária. Nenhuma legislação foi capaz de trazer uma resposta definitiva acerca da segurança de dados, mas é evidente o crescimento desse setor no estudo do Direito.

A NECESSIDADE DE PROTEÇÃO DE DADOS NAS CÂMARAS DE ARBITRAGEM

A Lei de Arbitragem em seu Art. 10 estabelece a necessidade de qualificação das partes compromitentes, a fim de que haja identificação dos contratantes. A esse respeito o douto professor Carlos Alberto Carmona delineia:

> O primeiro inciso do Art.10 preocupou-se com a qualificação, tão completa quanto possível, das partes compromitentes. O objetivo da regra sob análise é apenas o de deixar fora de qualquer dúvida a identificação dos contratantes. (CARMONA, 2009, p.198)

5 Principle7 In considering the specific information security measures to be applied in an arbitration, consideration should be given to the following categories:
(a) asset management;
(b) access controls;
(c) encryption;
(d) communications security;
(e) physical and environmental security;
(f) operations security; and
(g) information security incident management.

Essa qualificação dos sujeitos envolvidos no procedimento arbitral enquadra-se exatamente no conceito de dado pessoal apresentado pela LGPD, uma vez que, ao longo do procedimento arbitral serão coletadas diversas informações relativas às partes devidamente identificadas.

Vale salientar que, ainda que o procedimento envolva pessoas jurídicas, algumas das informações coletadas podem referir-se especificamente a pessoas naturais ocupantes de cargos diretivos das empresas envolvidas, enquadrando-se, nesses casos, no conceito de dado pessoal protegido pela LGDP.

Como resultado dessa necessidade de qualificação e coleta de informações, as Câmaras Arbitrais possuem um enorme banco de dados acerca de seus clientes, árbitros, experts e testemunhas, seja por meio de um cadastro desses dados em seu sistema interno, seja através das provas coletadas no curso do procedimento arbitral, em decorrência disto, há a necessidade de regular o tratamento desses dados.

Em uma sociedade em que a reputação e a opinião pública são fatores tão relevantes para uma empresa quanto os seus próprios rendimentos, é preciso atentar para a adoção de ações preventivas para proteção de dados pessoais. As medidas de proteção de dados são tão necessárias quanto as ferramentas de compliance para afastar o envolvimento em atos anticoncorrenciais, as medidas para maior diversidade e inclusão, bem como, a preocupação com a consciência ambiental que nos dias atuais são fatores extremamente relevantes para a imagem de uma empresa. A adoção dessas medidas já tornou-se um fator diferencial na competitividade do mercado.

As Câmaras Arbitrais, tais quais as empresas privadas, devem grande parte de sua atuação ao prestígio a elas associado, de modo que, qualquer matéria capaz de interferir na credibilidade dessas instituições, precisa ser devidamente analisada.

Atualmente já existem casos de ataques cibernéticos a Câmaras Arbitrais, cabendo destacar o caso ocorrido em 2015 na Permanent Court of Arbitration em Haia, na Holanda, na qual ocorreu um ataque cibernético ao site da Câmara Arbitral no curso de um procedimento entre a China e as Filipinas acerca do controle do Mar do Sul da China. Ocorre que a invasão do site possibilitou o acesso aos computadores dos diplomatas e advogados envolvidos no caso, de modo que a China contou com uma vantagem indevida.

O próprio Judiciário brasileiro vem sendo alvo de ataques cibernéticos que já invadiram o sistema do Superior Tribunal de Justiça em 03 de novembro de 2020, o que gerou a suspensão dos prazos processuais e sessões de julgamento (VALENTE; VITAL; 2020, p.1). De igual modo, o Tribunal Regional Federal da 1ª Região sofreu um ataque cibernético pelo qual um perfil anônimo na rede social Twitter assumiu a autoria no dia 27 de novembro de 2020 (JURINEWS; 2020, p.1)

Os ataques cibernéticos são uma realidade assustadora tanto no setor público quanto no privado e causam danos irreparáveis às organizações atacadas. No âmbito das Câmaras Arbitrais esse prejuízo pode ser ainda maior, compreendendo não apenas danos econômicos, como também, possibilitando a realização de quebras de confiança que comprometeriam a credibilidade da instituição e colocariam em dúvida a independência e a imparcialidade dos árbitros.

A necessidade de proteção dos dados nas Câmaras Arbitrais não se restringe ao âmbito do procedimento arbitral, abrangendo também as informações armazenadas para além do procedimento a fim de que essas não venham a ser acessadas ilegalmente e utilizadas para outras finalidades.

No ano de 2015, a Cambridge Analytica, uma firma britânica, acessou dados pessoais de 87 (oitenta e sete) milhões de usuários do Facebook para fazer a análise dessas informações e através delas e influenciar os eleitores nos Estados Unidos da América. (ISAAK E HANNA, 2018, p.56/59). Outro caso importante ocorreu em 2014, no Brasil, no qual a empresa de telecomunicação Velox foi acusada de vender dados pessoais de seus clientes a terceiros, ilegalmente, sendo condenada a pagar multa de R$3,5 milhões (ZANATTA, 2015, p.447/470). Ambos os casos, demonstram que, por mais irrelevante que a informação aparente ser, esta precisa ser resguardada e deve atender aos limites da finalidade para a qual foi coletada, sendo sempre observado o consentimento do titular.

Outro fator indispensável à adequação das Câmaras Arbitrais à LGPD é o da transferência internacional de dados, entendida com a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

A LGPD regula o tema nos seus Artigos 33 a 36 e apresenta as hipóteses em que é autorizada a transferência internacional de dados:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência;
>
> b) cláusulas-padrão contratuais;
>
> c) normas corporativas globais;
>
> d) selos, certificados e códigos de conduta regularmente emitidos;[...](BRASIL, LGPD, 2018, Art.33)

Nota-se que uma dos requisitos de autorização da transferência internacional de dados é através da comprovação do cumprimento dos direitos do titular por meio de cláusulas contratuais específicas que autorizam a transferência. Essa hipótese abre a possibilidade de inclusão de cláusulas contratuais acerca da transferência de dados juntamente com o compromisso arbitral ou cláusula compromissória, a fim de legitimar a transferência desses dados em arbitragens internacionais.

Outro requisito observado é de que o país ou organismo internacional para quem esses dados serão transferidos deve proporcionar o mesmo grau de proteção dos dados previstos pela LGPD, ressalta-se que a GDPR, em seu Artigo 46, também apresenta esse requisito para transferência de dados entre países da União Europeia e os demais países. Isso demonstra a tendência mundial e crescente de buscar relações comerciais, contratuais e jurídicas apenas entre instituições que possuam medidas adequadas para proteção de dados.

Tanto a GDPR em seu Artigo 46.2 quanto a LGPD no Artigo 34 estabelecem a necessidade de que o país ou organização de destino tenha uma regulamentação que atenda aos princípios gerais da proteção de dados pessoais e que adote medidas de segurança para resguardar os direitos dos titulares das informações.

Desse modo, a criação da Lei Geral de Proteção de Dados apresenta-se como uma verdadeira revolução não apenas no funcionamento de empresas, como também nos procedimentos de arbitragem internacional que, além de coletar informações, frequentemente transferem os dados coletados para outras instituições internacionais e estrangeiras.

ADEQUAÇÕES NECESSÁRIAS PARA AS CÂMARAS ARBITRAIS

Um dos princípios norteadores da Lei Geral de Proteção de Dados é o princípio da prevenção que determina o dever dos agentes de tratamento de adotarem medidas para prevenir possíveis danos decorrentes do tratamento de dados pessoais, nos termos do Art. 6 da referida lei.

Esse princípio, aliado ao princípio da segurança, da responsabilização e da prestação de contas gera a necessidade de adequação dos diversos agentes de tratamento aos termos da LGPD, bem como, a adoção de medidas preventivas que resguardem o direito dos titulares:

> Outra fundamental característica da nova legislação consiste no significativo fomento ao aspecto preventivo, estabelecendo procedimentos mandatórios para os controladores e operadores de dados pessoais, tais como os deveres atinentes à implementação de severas políticas de segurança para proteção dos dados de acessos não autorizados. (FRAZÃO; TEPEDINO; OLIVA; 2019 ,p.681)

Diversas são as possibilidades de medidas a serem adotadas para proteger dados pessoais tanto por meio da criação de protocolos, imposição de limites de acesso e divulgação de informações, quanto por meio do estabelecimento de diretrizes em casos de ciberataques.

> Uma vez que as partes e o tribunal tenham avaliado as custas e o procedimento, as partes e o tribunal podem então considerar os três princípios temáticos a seguir com relação à ameaça de ciberataques no contexto da arbitragem: (i) o estabelecimento de protocolos de segurança para o armazenamento e transferência de informações confidenciais, (ii) limitação da divulgação de informações confidenciais, e (iii) em caso de qualquer violação / ataque, o processo para notificar a pessoa afetada e para corrigir / mitigar a violação / ataque.(PASTORE; 2017, p. 1028)

No Brasil, não há uma regulamentação específica acerca da cibersegurança na arbitragem, deixando a critério de cada Câmara Arbitral o desenvolvimento de seus próprios meios de segurança. Faz-se necessário, portanto, que sejam estabelecidos protocolos internos nas instituições, contando com a expertise tanto de profissionais do direito quanto de profissionais da tecnologia especializados na área.

Além disso, é essencial a promoção de parâmetros gerais, diretrizes mínimas a serem seguidas pelos Tribunais Arbitrais do país todo, resguardada a autonomia dos árbitros para decisão das medidas de segurança mais adequadas para cada caso.

A criação de equipes multidisciplinares fixas dentro das Câmaras Arbitrais também se tornou um requisito inafastável, visto que, é necessário profissionais do direito para a compreensão dos aspectos jurídicos da LGPD e profissionais da tecnologia para colocar em prática as

medidas de segurança.

O Protocolo da ICCA elenca diversas medidas de proteção de dados que podem ser adotadas pelos Tribunais Arbitrais que merecem ser destacadas para serem aplicadas também no Brasil. A primeira diretriz apresentada é a do Conhecimento e Educação, é essencial manter-se informado sobre as ameaças e soluções de segurança, a segurança de dados requer atenção contínua e constante atualização, sendo necessário que as instituições procurem estar sempre a par das medidas de proteção de dados mais atuais e repassem esse conhecimento para aqueles que possuem acesso às informações tratadas.

Outro aspecto importante é a gestão de ativos, a consciência de onde esses dados estão circulando e o investimento na qualidade da infraestrutura digital utilizada, bem como, a necessidade de estabelecer práticas e políticas organizacionais e dar ciência delas aos profissionais e partes que de alguma forma possuem acesso à informação, para que estas adotem as diretrizes necessárias, por exemplo, para proteger os dados acessados por meio de um dispositivo pessoal.

A própria minimização dos dados coletados também deve ser uma medida recorrente, que encontra previsão na LGPD e também foi adotada pela GDPR. Além disso, há a necessidade de evitar cópias desnecessárias de documentos e estabelecer práticas de retenção e destruição dessas informações desnecessárias, tanto no meio digital, quanto nas cópias físicas.

Outra medida que deve ser observada, principalmente no curso de arbitragens internacionais, é a limitação do acesso a dados confidenciais durante viagens. As arbitragens internacionais muitas vezes requerem um deslocamento entre um país e outro, de modo que, ao transitar entre diversas redes não seguras e acessar dados referentes ao procedimento arbitral, o árbitro, expert ou parte envolvida pode acabar facilitando o vazamento dessas informações.

Ademais, existe a necessidade de estabelecer um sistema de backups periódicos, tanto por meio da nuvem quanto através de dispositivos externos. Outra medida que pode ser implementada é a limitação do acesso a esses dados, estabelecendo quais indivíduos poderão ter acesso, implementando senhas fortes com alterações periódicas e até mesmo requerendo identificação biométrica ou identificação multifatorial.

A criptografia para a transmissão de dados também é uma medida indispensável na Arbitragem Internacional, uma vez que grande parte das comunicações oficiais do procedimento ocorrem por e-mail e frequentemente contêm informações sigilosas. Além da criptografia é possível recorrer a serviços especializados de compartilhamento de dados, sendo essencial orientar os usuários de como proceder para resguardar as informações e evitar vazamento de dados por falha humana.

Tanto a LGPD, quanto a GDPR e o Protocolo da ICCA ressaltam que a proteção de dados não se refere apenas às informações armazenadas em meio digital, como também, documentos salvos em meio físico. Em vista disso, há a necessidade ainda de resguardar o próprio espaço físico de armazenamento de documentos das Câmaras Arbitrais a fim de que não haja extravio de documentação armazenada fisicamente.

Para proteger adequadamente as informações é necessário investimento nas ferramentas eficientes, pois, apesar dos inúmeros recursos disponíveis gratuitamente e tendo em vista

a natureza das informações compartilhadas nos procedimentos arbitrais, é necessário que as Câmaras Arbitrais adaptem-se a essa nova legislação investindo amplamente na segurança dos dados tratados, a fim de garantir a privacidade dos titulares e resguardar a credibilidade da instituição.

CONSIDERAÇÕES FINAIS

A proteção de dados pessoais é uma temática ainda pouco explorada e recentemente regulamentada pelo direito brasileiro, o tratamento de dados apesar de ser uma prática extremamente recorrente, somente ganhou um enfoque maior a partir das novas necessidades trazidas pelo desenvolvimento da tecnologia e das inovações relativas à coleta de informações.

A Lei Geral de Proteção de Dados foi elaborada objetivando assegurar o livre desenvolvimento da pessoa natural e garantir a liberdade e a privacidade dos titulares desses dados. Em vista disso, surge a necessidade de adequação dos agentes de tratamento às novas diretrizes traçadas pela LGPD a fim de prevenir o vazamento e mal uso de informações pessoais.

No contexto dos procedimentos arbitrais há uma necessidade ainda maior de proteção dessas informações, de modo que, as Câmaras Arbitrais, em observância ao princípio da prevenção, responsabilidade e prestação de contas, deverão adotar medidas minuciosas para resguardar esses dados.

Essas adequações são essenciais não apenas para assegurar o direito dos titulares, como também, proteger a credibilidade e reputação das Câmaras Arbitrais, uma vez que, as medidas preventivas tornaram-se parâmetros para avaliar a credibilidade dessas instituições. A elaboração de protocolos, a criação de setores especializados em cibersegurança e a exclusão periódica de dados desnecessários são apenas algumas das mudanças essenciais para proteger os procedimentos arbitrais domésticos e internacionais dos riscos trazidos pelo vazamento de dados pessoais.

Portanto, vislumbra-se claramente que a criação da Lei Geral de Proteção de Dados trouxe um avanço considerável nas discussões sobre segurança de informações, entretanto, no âmbito da arbitragem internacional ainda há muito a ser regulamentado e adequado para garantir a proteção dos dados pessoais e o direito constitucional à privacidade.

REFERÊNCIAS

BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 24 nov 2020

CARMONA, Carlos Alberto. Arbitragem e Processo. 3ª Edição, São Paulo,Editora Atlas, 2009, p.198.

CARVALHO, Luís Paulo; OLIVEIRA, Jonice; CAPPELI, Claudia; MAJER, Violeta. Desafios de Transparência pela Lei Geral de Proteção de Dados. 2019. Programa de Pós-graduação em Informática, Universidade Federal do Rio de Janeiro - UFRJ , p.1.

COSTA, Tiago R. Veloso. Proteção de Dados e Arbitragem: para além de uma questão legal. JOTA,

2019.Disponível em: https://www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-e-arbitragem-para-alem-de-uma-questao-legal-29062019 Acesso em: 24 nov 2020.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato, A Lei Geral de Proteção de dados pessoais e suas repercussões no direito brasileiro, Revista dos Tribunais, 2ª Edição, São Paulo, 2019,p. 677/678.

GODDARD, Michele. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact International Journal of Marketing Research. 2017. International Joural of Market Research, vol. 59, P. 703/705. Disponível em: https://journals.sagepub.com/doi/abs/10.2501/IJMR-2017-050?journalCode=mrea. Acesso em: 24 nov 2020.

ICCA; NYC Bar; CPR. Cybersecurity Protocol for International Arbitration. 2019. [S.l.], International Council for Commercial Arbitration, New York City Bar Association, and International Institute for Conflict Prevention and Resolution .

ISAAK, J., HANNA, M. J.User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection, 2018, IEEE, Computer 51 (8), p. 56/59.

VIROU moda: TRF1 sofre ataque hacker e site está fora do ar. Jurinews: notícias jurídicas. Publicado em 27 nov 2020.. Disponível em: https://jurinews.com.br/tecnologia/virou-moda-site-do-trf1-sofre-ataque-hacker/. Acesso em: 29 nov 2020.

MANGE,Flavia Foz. Processo Arbitral: aspectos transnacionais. Editora Quartier Latin do Brasil, São Paulo, 2014.

PASTORE, Jim; Practical Approaches To Cybersecurity In Arbitration. Fordham International Law Journal, [S.l.], volume 14, 2017.

UNIÃO EUROPEIA. EU General Data Protection Regulation (GDPR). Disponível em: https://gdpr-info.eu. [S.l.]. Acesso em: 24 nov 2020.

VALENTE, Fernanda; VITAL, Danilo. STJ sofre ataque hacker e suspende prazos processuais até segunda-feira.CONJUR.Publicado em 04 nov 2020. Disponível em: https://www.conjur.com.br/2020-nov-04/stj-sofre-ataque-hacker-suspende-prazos-segunda-911 Acesso em: 29 nov 2020.

ZANATTA, R. A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet, 2015, São Paulo: Quartier Latin, p. 447/470.