Na Mídia

27/03/2019 | Estadão

Cybersegurança: um novo desafio para a arbitragem

Tatiana Campello e Camila Biral*

Quem tem o domínio dos dados detém o poder de mercado para checar as preferências, manipular tendências e lançar novos produtos. Esse poder vem acompanhado de grande responsabilidade, pois a vida de uma pessoa ou de uma empresa pode ser esquadrinhada pelos dados que circulam no ambiente digital e o vazamento de informações não autorizadas pode ser devastador.

Em razão da ausência de regulamentação específica e má utilização de dados por diversos agentes, a reação regulatória ao tratamento de dados tem sido intensa. No Brasil, seguindo a toada da principal regulamentação sobre a matéria (EU General Data Protection Regulation – GDPR), em 2018 foi promulgada a Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de dados pessoais, por pessoas físicas e jurídicas, de direito público ou privado, com intento de proteger a privacidade e liberdade das pessoas.

Com a entrada em vigor da LGPD em 15 de agosto de 2020, todos os agentes que tratam dados deverão se adequar aos dispositivos do diploma legal sob pena de responsabilização por eventuais infrações em decorrência do tratamento de dados pessoais.

Nesse contexto, a prática da arbitragem também é atingida, pois sendo o procedimento arbitral permeado pela sensibilidade e confidencialidade características do instituto jurídico, também será alvo das regras que passarão a vigorar em matéria de proteção aos dados pessoais.

De acordo com a pesquisa CBar – Ipsos sobre a arbitragem no Brasil, a confidencialidade foi considerada um dos principais atributos do procedimento e um dos maiores atrativos para as partes escolherem esse meio de resolução de conflitos em detrimento às disputas judiciais perante o juízo estatal. No entanto, diante dos conhecidos cyberattacks, o sigilo das informações trocadas nas arbitragens passa a ser um desafio para o instituto.

Sobre a questão, pelo menos duas entidades já têm convidado a comunidade arbitral para o debate, com a elaboração de protocolos de segurança de dados para procedimentos arbitrais.

Um desses grupos foi criado pelo International Institute for Conflict Prevention and Resolution (CPR) e o International Council for Commercial Arbitration (ICCA) em conjunto com o New York City Bar Association e recebeu o nome de Working Group on Cybersecurity in Arbitration.

O Working Group, na esteira do debate mundial sobre proteção de dados, elaborou o "Cybersecurity Protocol for International Arbitration", que identifica os riscos de vazamentos de dados em arbitragens internacionais, fornecendo bases suficientes para proteção dos dados trocados no curso de procedimentos arbitrais. Outra iniciativa mundial é a força tarefa conjunta da ICCA com a International Bar Association (IBA) para a criação de um guia prático de proteção de dados, que busca identificar os momentos em que a proteção deve ser levada em conta no curso de procedimento arbitral. O guia é baseado na Lei Geral de Proteção de Dados da União Europeia e terá sua primeira versão lançada em março de 2019 para comentários do público.

O Protocolo elaborado pelo Working Group do CPR, em seu Capítulo C que trata de Práticas Gerais de Cybersegurança, propõe algumas diretrizes para tornar o ambiente da arbitragem mais seguro. Podemos destacar a criação de controle de acesso mais sofisticados; o uso de firewalls, antivírus e antispywares, bem como de data rooms em que a informação possa ser armazenada e acessada de forma segura e confiável pelas partes e árbitros; a adoção de protocolos de encriptação de dados armazenados e transferidos, dentre outras soluções.

Além das medidas de caráter técnico, existem medidas que dependem de mudanças comportamentais e da cooperação das partes, como evitar o uso de sinais públicos de wifi, privilegiando sinais privados de internet (VPNs), instalar e acessar apenas arquivos de fontes conhecidas, manter padrões de segurança que permitam a criptografia dos dados tanto para os computadores quanto para os dispositivos móveis utilizados para acesso.

É fundamental que as partes determinem logo de início como se dará o uso e o compartilhamento de toda estrutura utilizada para garantir a segurança dos dados trocados no curso do procedimento arbitral. Cada agente atuante deve entender a estrutura de manutenção e armazenamento de dados e engajar-se no controle dos riscos de vazamento das informações confidenciais trocadas ao longo do procedimento arbitral.

Desta preocupação emergem duas questões a serem enfrentadas pelos agentes da prática arbitral: as questões ligadas aos custos para implementação das medidas de controle das informações e à responsabilização daqueles que não atenderem os padrões esperados e acordados para a proteção dos dados trocados ao longo do procedimento.

Com relação aos custos, não são raras as situações em que existe uma disparidade de recursos entre as partes ou até mesmo entre a partes e seus patronos ou árbitros. A depender do nível de proteção a ser delineado, pode existir a necessidade de definição da justa repartição dos custos atrelados à implementação dos requisitos técnicos de proteção de dados.

Com relação à responsabilização pelo vazamento dos dados, o Protocolo do CPR propõe que as partes definam logo de início o que constituiria uma quebra de sigilo, quem e quando o vazamento ou a suspeita deste deve ser notificada, os passos a serem adotados para mitigar os impactos nocivos, dentre outras hipóteses.

Dessa questão ainda deriva eventual necessidade de se definir as sanções, bem como os poderes garantidos aos árbitros para aplicar tais sanções que não são ligadas ao litígio em si, mas que permeiam o procedimento arbitral.

Como se vê, muitas são as indagações que precisarão ser enfrentadas pelos agentes participantes da prática arbitral para que a arbitragem, mais uma vez, prove que marcha conjuntamente com a evolução das sociedades em que está inserida, demonstrando sua capacidade de manter padrões razoáveis de proteção às informações trocadas no curso do procedimento de forma a garantir a credibilidade do instituto.

***Tatiana Campello e Camila Biral são sócias do Demarest**