Electronic exchange of submissions and exhibits in arbitration: better be safe than sorry!

01 February 2019 - by Rita Nunes dos Santos

Authorship: Rita Nunes dos Santos.

Technology advances of the last decade have irreversibly changed the way we communicate, and international arbitration is no exception to this new reality.

Although some of the possibilities allowed by the use of new technologies, such as virtual hearing rooms and the use of highly hyperlinked submissions, may still not be standard at this point – and, most importantly, may not suit or be cost-effective in all kinds of arbitral procedures –, it is already common practice between arbitration users (including, counsel to the parties, arbitrators and arbitral institutions) to communicate electronically (exclusively or not) throughout arbitral proceedings, mostly via email, and to exchange submissions and exhibits electronically.

In this light, with both the threat of cyberattacks in mind and the present growing concerns regarding data protection and confidentiality issues (as shown, for instance, by the entry into force of the new European Union General Data Protection Regulation[1], to which the ICC Note to Parties and Arbitral Tribunals on the Conduct of Arbitration pursuant to the ICC Rules, in force as from January 1, 2019 makes specific reference), one of the issues that all participants in an arbitration should consider when discussing, at the outset of arbitration proceedings, the extent to which they should resort to information technology (IT) means, is the risk of undue access to the information exchanged, especially if the matters discussed are of a particular sensitive or confidential nature. This risk exists in virtually all forms of data transmission, but its occurrence should and can be limited by effectively complying with some basic rules. The ICC Commission Report on Information Technology in International Arbitration, updated in April 2017 (the "ICC Commission Report"), provides useful guidance on these issues, stating the duty that lies on each participant to adequately protect the system and the integrity of the data exchanged.

For instance, the ICC Commission Report recommends that all participants using electronic transmission means should ensure the use of up-to-date virus protection software and report any malware occurrence that may compromise the integrity of the communication process.

Moreover, when communicating via email, participants should ensure that the email program used provides for encrypted

transmission and storage, and may also choose to protect its contents through the use of software that allows for digital signatures.

Also, when conveying larger volumes of data – that may exceed the usual size-limit of email attachments – through CD/DVD-ROM or flash memory sticks physically delivered to the arbitrators or the opposing party's counsel, parties should always resort to a reputable courier service and consider protecting the data with a password (and having said password transmitted separately).

Alternatively, parties may choose to share large volumes of data through file sharing services, e.g., by sending to the intended recipients of information a link that enables them to access a server where the information is stored and download it to their respective systems.

If the server where the information is originally stored is under the control of the party sharing the information, issues of confidentiality and undue access normally do not arise.

The situation may be more problematic, as pointed out in the ICC Commission Report, if the party sharing the information chooses to store it in generic commercial file sharing services that are often free of charge up to a certain quantity of data stored.

In this case, it is important that the parties check beforehand if the terms and conditions of use of said servers are acceptable to them, in order to ensure that their use does not provide the service provider with access to the data stored therein or allow it to interfere in any way with its contents, looking out, in particular, for any language on copyrights that may seem unfit. Parties seeking a higher level of security in the data-transfer process may consider paying for a commercial file transfer service whose terms and conditions of use are deemed appropriate for the purpose at stake.

The use of a virtual data room administered by an arbitral institution or an independent third party may also be a possible solution to convey data, if and when said option is available and cost-effective in a given arbitration.

All in all, it is simply not possible, nowadays, to ensure that no undue access to the information conveyed electronically will occur. This being said, the above guidelines and concerns might be an effective tool in helping arbitration users to evaluate where to use (and where to avoid) electronic means of data transmission and, hopefully, to effectively protect data confidentiality.

[1] 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.

Rita Nunes dos Santos
Senior
Lawyer