CIArb
evolving to resolve

CIArb Framework Guideline on the Use of Technology in International Arbitration

CIArb Framework Guideline on the Use of Technology in International Arbitration (2021)

Drafted by:

Dr Gordon Blanke MCIArb
Founding Principal, Blanke Arbitration

Ben Giaretta CArb FCIArb
Partner, Fox Williams LLP (Chair Drafting Group)

Kateryna Honcharenko MCIArb
Research Executive, CIArb

Paul Kinninmont FCIArb
Partner, Candey LLP

Mercy McBrayer FCIArb
Research and Academic Affairs Manager, CIArb

Tunde Ogunseitan FCIArb
Arbitrator, Ogunseitan Arbitration

Clare Weaver
Solicitor and Director, Putney Consulting Ltd

The Chartered Institute of Arbitrators is a UK registered charity no. 803725
12-14 Bloomsbury Square, London WC1A 2 LP, United Kingdom
www.ciarb.org

1. Preamble

1.1. Technology[1] has become ubiquitous in international arbitration. It is used for rapid communication throughout the arbitral process. It is also used to overcome obstacles: for example, video conferencing ("virtual hearings") is employed when individuals have difficulty attending hearings in person. It is increasingly used for cost, efficiency and quality reasons: computer-assisted document review, for instance, may be quicker, more cost-efficient and more accurate than engaging people to go through large collections of documents.

1.2. Coupled with this is a need for an arbitration award to be accessible and understandable, both for the parties to the dispute and for other entities or organisations that may need to review it, such as a national court to which an enforcement or challenge application is made. While using technology necessarily implies some processing which is beyond the knowledge and understanding of most individuals (for example, arbitrators may not understand the coding used in the software on their computer), the extent of this gap should be sufficiently narrow and sufficiently match societal norms to allow a reasonably educated person, using reasonable diligence, to trace back the findings in the award to the evidence and arguments presented in the arbitration.

2. Introduction

2.1. This Guideline addresses the issues that participants in arbitral proceedings should consider when using technology.

- **Part I** covers general principles including understanding the powers and duties of arbitrators, ensuring fairness and making proportionate use of technology.

- **Part II** has guidance on best practice relating to cybersecurity and ways to avoid personal and case-related data breaches.[2]

2.2. This Guideline is intended for use in conjunction with, and does not supersede, any laws or institutional rules applicable to the use of technology in an individual arbitration.

[1] The reference in this Guideline to "technology" should be taken to include all digital and data-driven devices, products and services that might be used during an arbitration.

[2] The advice in this Guideline corresponds to best practice at the time of its drafting (2021).

Part I. General Guidance on the Use of Technology in International Arbitration

3. Arbitrators' powers and duties in respect of technology.

3.1. Arbitrators should identify the extent to which they have powers and duties in relation to the use of technology in an arbitration.

3.2. In general, arbitrators have the power to conduct the arbitration in such manner as they consider appropriate. This is, however, subject to any specific agreement of the parties in relation to the procedure to be followed. Arbitrators might therefore be required to use particular technologies by an agreement between the parties and in some circumstances, parties might agree that particular technologies should not be used.

3.3. The powers of the tribunal are also subject to any relevant laws applicable to the arbitration, including data protection laws at the seat of the arbitration. These laws might place constraints on the use of technologies, whether such use is agreed by the parties or directed by the tribunal. Arbitrators might need to obtain advice on the applicable laws to identify those constraints and the cost of obtaining such advice should be counted as part of the costs of the arbitration. For example, arbitrators may need to establish whether it is legitimate at the seat of the arbitration to issue an electronic (i.e. e-signed) award.

3.4. Arbitrators have various duties to the parties under the rules and the laws applicable to the arbitration, such as the duty to treat the parties with equality and to give them a full opportunity of presenting their case and the duty to carry out the tribunal's mandate and not delegate this to others. These may affect the arbitrators' choices relating to technology. Arbitrators should establish what these powers and duties are, and they should give the parties an opportunity to comment before making decisions about the use of technologies in an arbitration whether by the parties or by the arbitrators themselves.

3.5. Where there is disagreement between the parties on the use of a particular technology in an arbitration, arbitrators should exercise any power in relation to that technology with caution, taking into account all the circumstances and the applicable laws and rules. Above all, arbitrators must decide not to use a particular technology if such use were to jeopardise due process in the arbitration.

3.6. It is generally accepted that the powers and duties of arbitrators extend to technologies used by the parties for a common purpose within an arbitration, for example technologies used at hearings where all parties are present, but do not extend to the regulation of technology used privately by an individual party for its own purposes. Just as parties have a free choice of legal counsel, so they can choose for themselves what technologies they believe would best help them during the arbitration.

3.7. There may be circumstances, however, where the technology used privately by one party might affect the proper course of the arbitral process and/or result in an unfairness for the other party. For example, the technology used by one party to store and review documents and data might not allow the arbitrators and the other party to understand whether that party has complied with a duty to disclose information. Further, the technology used by one party might impact the rights of another party to the arbitration: For example,

storage of data by a party might lead to concerns about whether it is taking sufficient steps to comply with its duty to keep confidential the information relating to the arbitration. In such circumstances, the arbitrators arguably have the power to issue directions to the relevant party in relation to its private use of technology, to safeguard the due process of the arbitration and/or ensure the arbitral process remains efficient and cost-effective.

4. Proportionate use of technology

4.1. Where arbitrators must decide on the use of technology in an arbitration, they should consider whether the proposed use is proportionate in all the circumstances.

4.2. Technology has advantages and disadvantages and should not be adopted unquestioningly. Most technologies used in arbitration should help the process, but some may create unnecessary complexities, particularly if not used correctly. Moreover, most technologies require expenditure and an investment of time in learning how to use them. There may even be environmental costs (e.g. power usage at a data centre). The arbitrator must take all these factors into account, although on balance the use of the technology should be suitable: the negatives are likely to be outweighed by the cost and time that would otherwise be spent, and the environmental impact that would otherwise occur, if the technology was not used.

4.3 In smaller cases, it might be appropriate not to use overly sophisticated technology (even if, for reasons of cost efficiency, the arbitral process in such cases might be run entirely online) and in larger cases it might be appropriate to use less technology than expected, despite the size of the case and the amount of evidence and submissions involved.

4.4. In addition, thought should be given as to how the particular use of a technology can be made proportionate. For instance, operation of the technology could be outsourced to a service provider, which might increase the cost but eliminate any errors resulting from the use of the technology by the parties or the arbitrators.

4.5. Arbitrators should consider whether the use of technology should be adapted to suit the needs of the individuals involved in the arbitration. For example, the timing of a virtual hearing might need to be changed to limit the number of hours that the individuals spend in front of a computer monitor, to avoid digital fatigue, or to make the timing appropriate for the location of the individuals. Also, specific technology might be needed to enable access for individuals with recognised disabilities; while some technology may not be properly accessible to the individuals involved in the arbitration because they may not be familiar with the language used in the technology.

5. Fair and transparent use of technology

5.1. Any technology used for common purposes in an arbitration must not undermine the fairness of the process and must be transparent.

5.2. Arbitrators should be aware that there can be barriers to access for some parties where technology is concerned. They may not have the resources or the knowledge to use certain technologies appropriately; and as noted above, language may also be an issue (some software does not support multiple languages). Some barriers may not be readily apparent to arbitrators, such as a lack of familiarity with a technology in a party's country, or a lack of key infrastructure there (such as a stable power supply, internet access and/or sufficient data transmission). Consequently, the use of certain technologies for common purposes in an arbitration may create an unfair procedural advantage for one party over another.

5.3. Even if there is no general barrier to access, how the technology is used in a particular arbitration might in some circumstances create procedural unfairness. For example, video conferencing/virtual hearing technology might be used so that parties located in different time zones can join a hearing, but the arbitrators should bear in mind the impact of time zones on how individual participants function (i.e. chronobiology). A hearing that is in the middle of the day for one party but in the middle of the night for another might create an unfairness for the latter party.

5.4. Arbitrators should ensure that the use of technology for common purposes in the arbitration is transparent. This includes giving the parties a reasonable opportunity to comment in advance on the use of any proposed technology (and possibly, by agreement, to veto its use). Such use should be identified and discussed with the parties at the earliest possible opportunity (usually the first case management conference), so that the parties can bring any disadvantages to the attention of the arbitrators.

5.5. The use of technologies by the arbitrators themselves must also be transparent. Technologies which are in common use for business purposes and would meet the expectations of the parties need not be specifically disclosed to the parties. But technologies which might derogate from the arbitrator's duty to apply their minds to the arguments to reach their own decision in a case, and which might jeopardise the arbitrators' autonomous decision-making process, such as certain analytical software, should be brought to the attention of the parties so that they have an opportunity to comment.

6. Secure use of technology

6.1. Participants should take appropriate steps to ensure that the technology used in an arbitration remains secure and stable.

6.2. There is always the possibility for technology to be insecure (i.e. open to cyberattack) or unstable (i.e. subject to deterioration). Such weaknesses can have several causes, including software vulnerabilities and human errors. The consequences can include breach of confidentiality and/or loss of essential data.

6.3. Arbitrators should take reasonable steps to adopt best practices in their own use of technology and encourage the parties (and any third-party suppliers employed by the parties, including legal counsel) to do the same. This includes ensuring that software is updated, using unique and sufficiently complex passwords and employing multi-factor authentication. For more details, see Part II of this Guideline.

6.4. A risk-based approach should be followed when assessing whether security measures are appropriate. In arbitrations that are particularly sensitive or that involve particularly high stakes, it might be appropriate for the arbitrators to direct that no data should be stored on a networked computer and that back-ups be made throughout the arbitration process.

6.5. Where a cyberattack or data loss is detected by the arbitrators, they should promptly disclose this to the parties. Similarly, they should direct that the parties disclose any cyberattack or data loss immediately, so that prompt and appropriate responses can be taken by the other parties and by the arbitrators.

Part II. Guidance on Cybersecurity in International Arbitration

7. Standard security measures

7.1. Standard security measures can be implemented by participants in arbitral proceedings without professional technical support, prohibitive expense and additional time input.

7.2. Such measures include, but are not limited to:

i. create unique and complex passwords and, where possible, enable multi-factor authentication;

ii. keep computers, laptops, tablets and mobile phones and other devices updated with antivirus software and other data protection software;

iii. avoid using public internet access, e.g. Wi-Fi in cafes or airports on devices that hold confidential data (if a virtual private network is not used);

iv. use encryption or password protection when transmitting soft copies of confidential documents and data (e.g. by email); and

v. ensure that hard copies are kept in a secure location when not in use.

8. Analysis of assets and data that need to be protected

8.1. Participants in arbitral proceedings should identify at an early stage (and throughout the arbitration) assets and data which require protection. Technical support teams may need to be involved in such discussions.

8.2. The assets will usually include documents (both hard and soft copies), networks, computers, phones and other smart devices.

8.3. The 'risk profile' of a specific case must be considered. Certain factors may increase the risk of security breaches, including:

i. the value of the dispute and/or its importance to the parties;

ii. involvement of governments, high-level officials and/or transnational corporations;

iii. the locations of the parties, if in jurisdictions where data protection laws are underdeveloped, or where the physical security of servers might be compromised;

iv. a focus in the arbitration on high-profile issues such as the environment, human rights, cryptocurrencies or intellectual property,

v. the subject-matter of the dispute, e.g. where it relates to critical sectors such as power, infrastructure, natural resources, banking or technology; or

vi. there are a large number of participants in the arbitration and/or large amounts of data, increasing the risk of human error.

9. Institutional support

9.1. Some arbitral institutions or independent providers offer bespoke, highly secure and efficient digital case management platforms, which can be used by all participants to communicate, share and store data including procedural orders, submissions, exhibits and any other procedural documents, as well as to organise and hold video or audio meetings or hearings.

9.2. Security measures adopted by participants should be consistent with those employed by an arbitral institution but may, where possible and necessary, take precedence over them. Before introducing such measures, participants and arbitrators should normally consult with the arbitral institution.

10. Management of data

10.1. Back-up data

Reliance on smart devices and soft copy information has become the norm in many places and industries. The security of such information may be compromised where a device is stolen, lost or damaged, especially during travel or when working in a place without access to adequate and safe IT assistance. Participants should ensure that data is backed up on a regular basis (daily or weekly). Devices should contain a data restoration process as well as remote erasure software (in case of loss of the device). Storage on blockchain might also be considered.

10.2. Access to information

There are often many individuals involved in arbitral proceedings and most of them are entitled to have access to case-related confidential information. Passwords or multi-factor authentication should be used to access accounts, folders, files, email and cloud services, and other places where information and data is stored. This is particularly important where case management platforms are used. Tribunals and parties should also establish how information and data might be accessed by third parties engaged in arbitral proceedings, such as funders, interpreters and experts.

10.2.1. Passwords

Password protection should be enabled on all devices holding confidential information. Passwords should be:

i. complex (a mixture of letters, numbers and symbols);

ii. different from other passwords used; and

iii. changed regularly (at least quarterly).

Avoid saving your passwords or noting them down and, where possible, use a facial recognition system or another type of biometric identification. This reduces the amount of information that must be memorized.

10.2.2. Multi-factor authentication

Multi-factor authentication is an access-control setting that establishes layered protection of data. When trying to log into devices, digital services or any other sources of information where the setting is enabled, it will require you to prove your identity by additional means other than a password, for example by entering a code sent to a second device.

10.3. Data communication and storage

Communication of sensitive data by email may be highly insecure and vulnerable to cyberattacks. It is preferable to rely on secure file-sharing services to transfer and store confidential information. Where the use of email to communicate sensitive data cannot be avoided, make sure that devices and the transmitted data are appropriately protected and encrypted (as a minimum, key documents sent by email should be password-protected).

10.3.1. Encryption of information

Encryption is a cyber-security tool that encodes confidential information while in transit or stored by converting plain text into a ciphertext. Authorized participants can decode the encryption using their cryptographic keys. Where there is a need to handle and/or transfer confidential information, it is desirable to encrypt emails, devices and cloud storage.

As noted above, email can often be an unreliable method of communicating sensitive data, especially because it can be difficult to identify an email data breach. To date, only end-to-end encryption of emails is efficient enough to protect the confidentiality or privilege of the content of emails: It is protected when sent, in transit and when received by the addressee and can be decoded by the latter once they have been given a cryptographic key.

10.3.2. Cloud computing

Cloud computing is an efficient, sustainable and secure alternative to email communications. It gives an opportunity to transfer and access case-related information through the internet, store it on a third-party's server and avoid keeping sensitive information in hard copies or individual devices. Cloud computing also offers bigger storage capacity and enables access from multiple devices, and it can include specialist data handling and software services. Finally, it can be easily set up without special technical assistance.

The CIArb does not endorse any individual cloud computing service provider but, to ensure an added level of security, it recommends using paid "premium" or "business" or other upgraded versions. The same applies to communication services, virtual private networks (VPN), anti-viruses/malware, firewalls, antispyware software etc. It is imperative to regularly update and, if possible, upgrade the software used.

Although cloud computing is an efficient data-sharing platform, with a view to avoid any confidentiality concerns the CIArb recommends scrutinizing providers' security policies (actions undertaken in cases of a data breach, including the possibility to temporarily block an account and restore data, allocation of responsibility, etc.). Where such policies are not satisfactory, data sharing platforms set up exclusively for a particular case or case management platforms should be used.

Many cloud computing providers offer encryption of data (see above). It is important to recognise, however, that cloud computing means that information will be stored on a third-party server and therefore that third party might have full access to it. Consider encrypting a folder in the cloud storage or using professional independent services offering encryption of data already held in the storage.

10.3.3. Recognize and avoid phishing scams

"Phishing" is commonly used by fraudsters to trick people into revealing sensitive data, opening or downloading attachments, or following links that may pose a significant cybersecurity threat or, at the very least, cause damage to devices. In most scenarios, this is done by sending people emails or text messages. You should watch out for:

- unusual sender details;
- a request to click a link (particularly if the link does not begin with "https://"), make a payment or send personal information;
- a strange attachment and/or subject-line;
- urgent nature;
- poor wording.

If an email is sent from a known addressee but has some of the other criteria set out above, you should contact the sender by phone (on a number different from the one given in the email itself) to verify the origin of the email.

10.3.4. Minimize public internet use

Since public Wi-Fi networks are a source of a possible data breach, their use should be kept to a minimum and, where possible, avoided. The same should apply to home Wi-Fi unless it is appropriately secured. If you need to use public internet access, connecting to a VPN may reduce the risk. Alternatively, a hotspot setting on a mobile phone could be used if available.

11. Access to devices and hard copies

11.1. You should protect devices and hard copy documents containing confidential information from unauthorized physical access or anything that may cause damage to their content. A physical data breach can be avoided by paying special attention to the location of devices and documents, especially while travelling. It is recommended never to leave them unattended in a public place.

11.2. Devices should be locked when not in use and confidential documents should not be left at a work desk unattended. Devices and documents should be stored in secure places that require authorized access.

11.3. You should avoid reading files and/or accessing accounts containing confidential information in public places. If you need to access confidential information in public, you should use a privacy screen.

11.4. Printing of documents should be done securely. You should not leave documents unattended if the printer is in a common area.

11.5. Documents that do not need to be stored or archived should be disposed of safely. Since shredded paper is not suitable for recycling, it is preferable to use confidential recycling services to dispose of hard copy sensitive data. Soft copy documents should also be disposed of safely and securely.

CIArb
evolving to resolve

The Chartered Institute of Arbitrators
12 Bloomsbury Square
London WC1A 2LP
United Kingdom

www.ciarb.org