Dani Habel

المجلة القضائية

Reflections on the responsibilities of arbitration stakeholders in terms of cybersecurity

08– 09– 2022

One of the consequences of the COVID-19 pandemic was the creation of a state of dependence of the human being on technological tools and instruments. This phenomenon of digitization that we are witnessing is manifested by an increased transmission of information in digital format. As a result, the risks of cyber-attacks are constantly increasing. Taking the risks of cybersecurity breaches more seriously is no longer a choice, but rather a duty. It is therefore required to deploy all the necessary measures to deal effectively with such incidents.

International trade operators choose commercial arbitration for one important reason: its confidentiality[1]. Holding a dispute and subsequently a litigation out of the public sphere allows to avoid, in the first place, the damage to the image and reputation that could lead, for example, to a drop in the stock market price of listed companies. Secondly, this principle of confidentiality ensures that sensitive commercial and financial information, as well as information deemed personal, is not made public.

Information as a target: during arbitration proceedings, the type of information mentioned above is of significant value and is exchanged between the parties themselves, the arbitrator, experts, translators, etc. This creates a narrow circle of distribution that is inaccessible to uninvolved third parties. This makes this information coveted and targeted by hackers.

The parties as targets: These parties are generally multinational companies or even state entities, making them potential targets for cyber-attacks.

The nature of the dispute as a target: disputes submitted to arbitration are high-stakes and high-value. In addition, the cross-border context of the process generally involves parties of different nationalities. The risk of incidents is therefore high.

Arbitration is a fertile ground for cybersecurity attacks. It is important to design an information security regime for arbitration in a digital environment. This must be done on a national, regional, and international scale by involving public and private entities, without ignoring the active role that the parties themselves as well as the arbitrator must play in the quest for such arbitral cybersecurity.

The challenge is to ensure that any entity accessing the data and information disclosed during the process is sufficiently protected against any cyber-attack.

What are the repercussions of a cybersecurity breach during an arbitration proceeding?

The impact of a cyber-attack will vary depending on the case. But generally the consequences are as follows[2]:

[1] M. MEZA-SALAS, *Confidentiality in International Commercial Arbitration: Truth or Fiction?*, Kluwer Arbitration Blog, September 23, 2018.
[2] These consequences are drawn from Principle 1(d) of the "ICCA-NYC Bar-CPR Protocol on Cyber Security in International Arbitration".

- A delay or even a suspension of the arbitration proceedings. This can be generated by several factors. On the one hand, the incident itself may have a direct impact on the continuation of the arbitration proceedings. On the other hand, the time required to adopt the appropriate measures to remedy the breach that caused the incident, and subsequently to repair the damage caused by the latter, may cause a delay or a suspension.

  In addition to these two factors, the fate of the hacked documents used as evidence and the probable questioning of the impartiality and independence of the arbitrator are also at stake.

- An increase in the overall cost of the arbitration caused in particular by the above-mentioned delay.

- An economic loss to the parties resulting from:
  - The increase in the cost of the arbitration proceedings.
  - Compromised commercial information and personal data of the parties to the arbitration, which are normally protected by the principle of confidentiality governing the procedure.
  - A loss in the value of the shares.

- Potential liability under applicable law and other regulatory frameworks, including applicable data protection regimes.

- Reputational damage to parties, arbitrators, administering institutions, and third-parties, as well as to the system of arbitration overall.

Once the link between arbitration and cybersecurity has been established and the consequences of any intrusion are known, it is important to know the respective responsibilities of the participants in the arbitration process.

What responsibility for which actor?

Confidentiality implies that any individual with access to the data and information exchanged is responsible for its protection. But it is important to note that the legal source

and proportion of such responsibility may differ[3] from one jurisdiction to another, and according to the contractual stipulations made prior to the arbitration proceedings, i.e. when the arbitration agreement was drafted.

However, it remains important to know what role each participant in an arbitration procedure can or should play and what he should expect. Indeed, if there are still no binding rules on cybersecurity in national arbitration laws[4], it should be noted that the normative provisions concerning the protection of data consisting of digitized evidence must be considered during arbitrations.
In terms of cyber security, it is the *soft law* that has taken over, notably through the ICCA protocol and the IBA guidelines[5]. Unlike the rule of law considered as a norm creating obligations and made compulsory by the public authority by means of constraint[6], *soft law* has no binding character and can only engage the parties or the arbitrators insofar, as the provisions it proposes have been incorporated into the will of the parties[7].
A collective effort by all participants in the arbitration process is needed to provide a comprehensive framework for effective cybersecurity in arbitration.

In order to do so, we will focus on the responsibility of the parties, arbitrators and arbitral institutions to implement appropriate measures to address the risks of cyber-attacks.

The parties: The fundamental nature of arbitration is based on the "party autonomy principle"[8]. The latter are the masters of the elaboration of the arbitral procedure. From the choice of the type of arbitration, to the choice of the members of the tribunal, to the choice of the law applicable to the proceedings, as well as the management of documents, information and data flow, a significant responsibility weighs on the parties, requiring good administration upstream in order to avoid procedural anomalies downstream.

Regarding the avoidance of risks that may arise from a cybersecurity breach, it should be noted that it is impossible to fully guarantee the security of information during an arbitration proceeding. While parties cannot predict whether or not a cyber-attack will occur, they must anticipate its consequences and the risks associated with any negligent breach by the other party, the arbitrator, or any other third-party involved in the arbitration.

The panel of choices in the hands of the parties remains quite varied and the action plan must take place before the beginning of the proceedings:

---

[3] N. PEACOCK, Ch. MORGAN, V. NAISH, R. WARDER, *Cybersecurity in international arbitration*, LexisNexis, https://www.lexisnexis.co.uk/legal/guidance/cybersecurity-in-international-arbitration
[4] E. GW SCHÄFER, "Managing Data Privacy and Cybersecurity Issues" in *The Guide to Evidence in International Arbitration - First Edition*, Global Arbitration Review, 2021.
[5] Cybersecurity Guidelines, By the IBA's Presidential Task Force on Cybersecurity, October 2018.
[6] F. CHATZISTAVROU, *L'usage du Soft Law dans le système juridique international et ses implications sémantiques et pratiques sur la notion de règle de droit*, Open Edition Journals, 2005, p. 1.
[7] M. DE BOISSESON, *La « Soft Law » dans l'arbitrage*, Cahiers de l'arbitrage - n°3 - p. 519, 01/10/2014.
[8] S. A. FAGBEMI, "The doctrine of party autonomy in international commercial arbitration: myth or reality?", in *Party autonomy in international commercial arbitration*, AFE Babalola University: J. Of Sust. Dev. Law & Policy, Vol. 6: 1: 2015, p.222.

First, the "contractualization of dispute settlement"[9] by the parties implies the possibility of making contractual arrangements between them in order to expressly provide for the scope of application and enforceability of the confidentiality of the proceedings. Indeed, international commercial arbitration is not confidential by default[10]. Expressly providing in the contract for a clause in this sense as well as the terms and conditions of its applicability allows to strengthen the confidentiality.
Such arrangements may also concern the extension of the duty to inform between the parties to the probable intrusions or cyber-attacks that may occur against one of them, thus allowing to define the adequate cooperation measures in order to minimize the risks[11].

Second, while mass production of documents has long been preferred, assessing the nature of the information that will be shared – so as to reduce the impact of a potential attack – remains a more rational and reasonable solution. A first step may be to analyze the nature of the information that will be shared or disclosed during the arbitration, while a second step may be to evaluate the importance of the information to be disclosed and its effect on the outcome of the arbitration.

Third, contractual liability provisions can be an effective means of anticipating the consequences of any breach of the duty of information security. The scope of such clauses may be broad, for example, to hold any party responsible for failing to implement adequate data protection measures in connection with the arbitration in question[12], or even for failing to notify of an intrusion.

Arbitrators: The responsibility of arbitrators in the area of cybersecurity depends from the fact that they must render an effective award, i.e., one that is enforceable. If the term "effective" comes from the Latin word *efficax* – meaning the realization of the desired effect[13] – and if the expected effect of arbitration is definitely that of obtaining an award which can be enforced, if necessary by public force[14], it is therefore inevitable to consider any obstacle likely to prevent or delay the obtaining and enforcement of an award as an obstacle to the effectiveness of arbitration[15].
More specifically, in order to achieve an effective award, the arbitration proceeding must be unimpeded. Cybersecurity breaches can be considered as impediments to the normal conduct of the arbitration proceedings. In this case, the role of the arbitrator is essential in the fight against such constraints.

The responsibility of arbitrators is further enhanced by the fact that the principal legal systems and institutional arbitration rules grant arbitral tribunals – with some reservations

[9] A. PINNA, *L'autorité des règles d'arbitrage choisies par les parties*, Cahiers de l'arbitrage - n°1 - p. 9, 01/03/2014.
See also the Dow Chemical case, ICC Award No. 4131 of 1982, JDI 1983.899.
[10] X. NYSSEN, E. ROMERO, *La confidentialité dans l'arbitrage : un mythe fondateur ?*, Les Echos, 2017, https://business.lesechos.fr/directions-juridiques/droit-des-affaires/contentieux/030457021603-la-confidentialite-dans-l-arbitrage-un-mythe-fondateur-311970.php
[11] E. GW SCHÄFER, *op. cit.*
[12] *Cybersecurity and arbitration: implications of procedure and trends on substance*, CyberArb Webinar, 2021.
[13] The new "Larousse Universel".
[14] C. LOTFI, *L'Efficacité de L'Arbitrage Commercial International*, Collected Courses of the Hague Academy of International Law, p.29.
[15] J.-A. MAZERES, « Scolies Droit, justice et efficacité », dans *L'efficacité de la justice administrative*, R. MATTA DUVIGNAU et M. LAVAINE (dir. publ.), *Mare et martin, Droit public*, 2016, p. 25 ss, especially p. 30-31.

– discretionary power to conduct arbitral proceedings[16]. Through an initial "case management conference", the arbitral tribunal and the parties establish a comprehensive plan for the proceedings and define the issues to be addressed in the arbitration. Such a conference is usually followed by a "procedural order" issued by the arbitral tribunal enabling the latter to take steps to effectively manage the proceedings.
More specifically, arbitrators must be aware of the risks and consequences of a cyber-attack. Therefore, if information security issues have not been addressed by the parties in their arbitration agreements or prior to the initial case management conference, the ICCA Protocol gives the arbitral tribunal the authority to define the information security measures applicable to the arbitration[17]. Such measures are mostly incorporated in the procedural order and mainly concern the storage of information and data, access to it, the duration of its retention, special rules for certain categories of information, etc.

Finally, the responsibility of arbitrators lies in the fact that they must ensure compliance with the mandatory data protection rules. In this context, it is important to mention the "reference" regulation in terms of personal data protection[18], the European Data Protection Directive (GDPR)[19].
The pattern of the intersection between arbitration, data protection and cybersecurity is becoming increasingly clear: a cyber-attack does not only affect the confidentiality of the arbitration process. A cyber-attack can also be assessed as a breach of personal data, allowing (initially unauthorized) access to such data in an unlawful manner.
In this respect, cybersecurity is part of the protection obligations covered by the GDPR[20], which does not exclude arbitration from its scope. However, there is no connection between the mandatory data protection rules and the dispute itself submitted to arbitration. Furthermore, measures that are intended to ensure compliance with these rules cannot be characterized as procedural rules within the meaning of the *lex arbitri* or the applicable arbitration rules. A breach of such measures could affect the integrity of the arbitral proceedings and, consequently, the arbitral award. For this reason, the mandatory data protection rules set out appropriate sanctions.

The mandatory legal provisions that arbitrators must comply with concerning cybersecurity relate almost exclusively to data protection laws. Thus, it is still early to talk about a specific liability regime for arbitrators' actions or omissions causing a cybersecurity breach during an arbitration proceeding.
Providing for the revocation of an arbitrator or devising claims for damages by affected parties on such grounds appear to be largely unexplored territory to date[21].

Arbitration institutions: Such entities have played a key role in promoting arbitration over the years and are considered to be the best placed actors to have an impact

[16] G. HANESSIAN, « The Initial Hearing », in *The Guide to Advocacy - Fourth Edition*, Global Arbitration Review, 2019.
[17] ICCA-NYC Bar-CPR Protocol on Cyber Security in International Arbitration – Principle 11.
[18] Personal data is any information related to or attributable to an identified or identifiable physical person.
[19] Regulation (EU) 2016/ 679 of the European Parliament and of the Council of 27 April 2016.
[20] Article 32 of the GDPR.
[21] E. GW SCHÄFER, *op. cit.*

on the future evolution of arbitration[22]. Through their ability to amend their arbitration rules, these institutions are able to make changes and introduce innovative practices to improve arbitration procedures[23].

However, by administering sensitive arbitrations in terms of confidentiality, involving their holding of sensitive and secret business data, such institutions are highly exposed to cyber security risks.

Thus, tasking the institution administering an arbitration proceeding with putting in place the necessary cybersecurity measures and ensuring their implementation is important because arbitrators often lack knowledge and expertise in cybersecurity[24]. Furthermore, determining the appropriate cybersecurity measures will vary depending on the case. In this regard and by way of example, while the ICCA protocol provides a list of measures that arbitrators may consider[25], little guidance is provided as to the appropriate measure to implement based on the specific circumstances of the case.

Wouldn't it be more appropriate to leave the management of cybersecurity issues to arbitration institutions?
On the one hand, the technical and financial capacity of these institutions makes it easier for them to hire information technology experts in order to set up an adequate protection system for probable cybersecurity breaches[26]. An ad hoc arbitration tribunal will probably adopt a different approach, which will most likely vary according to the arbitrator's interest in the IT environment[27].
On the other hand, these same institutions are dealing with a large number of claims and cases, making them qualified to design cybersecurity measures that are appropriate to the case at hand[28].

Deciding in favor of the arbitral institution or the arbitral tribunal requires knowing whether the cybersecurity issues are administrative or procedural matters. In either case, the institution should be involved in the decision-making process:

---

[22] P. FRIEDLAND, S. BREKOULAKIS, *2018 International Arbitration Survey: The Evolution of International Arbitration,* White & Case LLP & Queen Mary University of London, 2018, p 3.
[23] M. GRANDO, *Challenges to the Legitimacy of International Arbitration: A Report from the 29th Annual ITA Workshop*, Kluwer Arbitration Blog, 19 September 2017.
[24] C. MOREL DE WESTGAVER, *Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions*, Kluwer Arbitration Blog, 6 October 2017.
[25] ICCA–NYC Bar–CPR Protocol on Cybersecurity in International Arbitration (2020 Edition), New York Arbitration Week Special Printing (International Council for Commercial Arbitration, 2019), Schedule C.
[26] D. LING, *Cybersecurity in international arbitration: An Untapped Opportunity for Arbitral Institutions*, Singapore Academy of Law Journal, 4 July 2022, pp. 51, https://journalsonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal/e-First/ctl/eFirstPDFPage/mid/519/ArticleId/1399?Citation=Published+on+e-First+4+July+2022
[27] C. MOREL DE WESTGAVER, *Cybersecurity in International Arbitration: Don't Be the Weakest Link*, Kluwer Arbitration Blog, 15 February 2019.
[28] M. DUARTE, *Essential Tips on Cybersecurity for Arbitrators: Identify, Protect, Detect, Respond and Recover*, Medium, 6 February 2019.

First, it could regulate the way data is stored and transferred, or even provide cyber security consultants to the parties. To this end, 70% of respondents to the BCLP survey[29] agreed that it would be preferable for arbitral institutions to have a member of the secretariat experienced in information security measures to recommend to parties and arbitrators the appropriate cybersecurity measures to adopt.

Second, institutions can publish practical guides based on their expertise in the administration of previous cases involving cybersecurity issues. Such guides can help make potential security breaches and likely intrusions predictable, leading to some anticipation of cybersecurity concerns and thus upstream management of the risks that may arise.

Finally, it is clear that the period between the request for arbitration and the constitution of the arbitral tribunal can generate cybersecurity risks, as a number of documents may already be exchanged[30]. In this case, would allowing the body administering the arbitration proceedings to order measures relating to cybersecurity issues be a viable option?
Such a solution may be precarious because the measures taken by the arbitration institutions do not constitute judicial decisions, so that they have no *res judicata* authority and can therefore be challenged at the level of recourse against the award[31]. Therefore, such administrative measures should in no way be confused with interim measures ordered only by the arbitral tribunal or exceptionally by the support judge[32].
As the role of the arbitration institution is essential in preserving the integrity of the arbitral process, such an intermediate phase may justify its active intervention, in particular when there is a real risk of prejudice or damage to the parties or the arbitration in question.

Conclusion

The above article provides an overview of the substantial link between arbitration and cybersecurity. This link exists because disputes submitted to arbitration have characteristics that can lead to a high level of risk in the event of a cybersecurity breach. Such breaches may occur more regularly nowadays as electronic documents are introduced in large numbers into arbitration proceedings.

Dealing with such breaches requires adequate measures to be put in place. In this respect, all actors of the arbitration process must be involved in shaping an efficient information security system. A collective responsibility implies, on the one hand, to anticipate cybersecurity risks upstream of the proceedings and, on the other hand, to remedy any breach that may occur downstream.

However, the legal consequences of any cybersecurity breach will be determined by applicable mandatory laws. Who should be responsible in the event of a cyber breach? Can

[29] G. BURN, *International Arbitration Survey: Cybersecurity in International Arbitration – Don't be the Weakest Link*, Bryan Cave Leighton Paisner LLP, 6 February 2019, https://www.bclplaw.com/a/web/160089/3WJsPc/bryan-cave-leighton-paisner-arbitration-survey-report-2018p.pdf
[30] D. LING, *op. cit.*, pp. 67.
[31] Groupe de Réflexion : Les décisions du Comité d'arbitrage, Association Française d'Arbitrage, http://www.afa-arbitrage.com/afa/uploads/Document_de_travail_Groupe_de_reflexion_AFA_Les_decisions_du_Comite_d-arbitrage.pdf
[32] The competent court at the seat of the arbitration.

we expect claims for damages by injured parties? What about fines and penalties for negligent parties?

If it is essential to answer these questions, it is still necessary to put in place regulatory provisions governing such situations. Until now, there are no mandatory rules in this area, but there is a general awareness of their necessity.

This awareness is reflected in the revision of the Network Internet Security Directive, known as *NIS 2*, which will probably be adopted soon by the European Parliament. This directive will set minimum rules for a regulatory framework for cybersecurity and will establish mechanisms for effective cooperation between the competent authorities in each member state. In this respect, according to the way it will be implemented by the Member States, the *NIS 2* Directive will have a significant impact on international arbitration.