Improving the Quality and Safety Standard in Implementing E-Arbitration in Resolving Islamic Banking Disputes in Malaysia

Mohamad Fateh Labanieh[#1], Mohammad Azam Hussain[#2], Nazli Mahdzir[#3]

[#]*School of Law, Universiti Utara Malaysia, Sintok, Kedah, Malaysia*

[1]fatih.labanie@gmail.com
[2]hmazam@uum.edu.my (Corresponding author)
[3]mnazli@uum.edu.my

***Abstract*— Electronic arbitration (hereinafter referred to as e-arbitration) is a combination of law and technology. Even though e-arbitration has not been implemented yet in Malaysia, the Malaysian authorities should be ready to meet the non-legal requirements for implementing it in the future as compliment to the existing traditional arbitration method. By using legal research methodology, this article endeavours to examine how the future implementation of e-arbitration in resolving the Islamic banking dispute can be improved especially in handling cyber security. The collected data is analytically and critically scrutinised using content analysis method. The article found that enhancing cyber security is a pressing need to improve the future implementation of e-arbitration in Malaysia successfully. Therefore, the article recommended several legal and technical measures to enhance cyber-security in e-arbitration in Malaysia.**

***Keywords*—** *arbitration, e-arbitration, cyber security, Islamic banking.*

1. Introduction

Islamic banking institution has been established with the aims to offer Islamic banking business in accordance with the principles of *Shariah* [22]. In Malaysia, the first full-fledged Islamic bank, namely Bank Islam Malaysia Berhad was established in 1983. Presently, there are sixteen (16) Islamic banks [12] and one (1) International Islamic banks [13] and several other banking institutions offering Islamic banking scheme.

The applicable dispute resolution legal framework for resolving the Malaysian Islamic banking disputes is embodied in the court and alternative dispute resolution (hereinafter referred to as "ADR"). The most common ADR methods in the context of Islamic banking disputes are traditional arbitration and traditional mediation.

Using traditional arbitration in the context of Islamic banking disputes has been significantly encouraged [7]. However, traditional arbitration is totally sufficient in resolving Islamic banking disputes in Malaysia [20]. For that reason, several scholars start searching for another mechanism to resolve the Islamic banking dispute effectively. Such as online dispute resolution [24] or e-arbitration [19].

The major difference between e-arbitration and traditional arbitration relates to the medium where each of them is taking place. E-arbitration takes place in an online environment (cyberspace) contrary to traditional arbitration which takes place in a physical environment.

According to article 1 of the Guangzhou Arbitration Commission "GZAC" Network Arbitration Rules 2018, e-arbitration is an online dispute resolution method that provides arbitration services by using network technology resources, such as the Internet. Likewise, article 2 of Shenzhen Court of International Arbitration "SCIA" Online Arbitration Rules 2019 states that e-arbitration refers to a dispute resolution method of conducting arbitration by the use of the Internet or other information technologies.

E-arbitration helps in improving quality and service delivery in Malaysian arbitration industry because of its inherent benefits. For instance, e-arbitration is a cost and time-effective dispute resolution mechanism [19]. It is also quicker than traditional arbitration. According to the annual report 2018 of Asian International Arbitration Center "AIAC", the average duration of the domestic traditional arbitration cases is twenty-five point one (25.1) months and fifteen point five (15.5) months for the sole arbitrator and three (3) members panel, respectively.

In e-arbitration, the situation is different. For example, at the Arbitration Court attached to the Economic Chamber and the Agricultural Chamber of the Czech Republic, the entire electronic arbitral

proceedings from filing the case until rendering the electronic arbitral award take approximately thirty-five (35) days [1].

Besides, e-arbitration is convenient for resolving cross-border disputes because of its capability to bridge the distances between the involved parties. Finally, e-arbitration is in line with environmental issues. It helps in reducing global warming and carbon dioxide because the involved participants can resolve their disputes remotely [19].

The benefits of e-arbitration are significant, but there are still some obstacles that stand against its development [2]. Such one example is a lack of security [18] [7]. For that reason, strengthening the quality and safety standard in using e-arbitration in Malaysia becomes very important because e-arbitration could be a popular option of dispute resolution in the era of COVID-19 and after the pandemic will end. Similarly, the future implementation of e-arbitration in resolving the Islamic banking disputes will not be improved unless some non-legal requirements are fulfilled. Such one example is cyber-security [18] [6].

Part one is an introduction. Part two of this article discusses why enhancing cyber-security in e-arbitration in Malaysia is a pressing need. Part three suggests legal and technical measures on how cyber-security can be maintained in e-arbitration.

2. Enhancing Cyber-Security in E-Arbitration is a Pressing Need

Undoubtedly, the crown jewel of traditional arbitration is a feature of confidentiality [11]. In the modern era, cybercriminals have appeared ubiquitous and started launching several cyber-attacks on different legal sectors.

There are many cyber-attack operations launched against law firms. For instance, a study issued by "Logic Force" shows that two-hundred (200) law firms had been undergone to hacking attempts [5]. Arbitration industry is not immune to the risk of cyber-attacks. In July 2015, the website of the Permanent Court of Arbitration was hacked during a hearing of a maritime dispute between Philippine and China. The malware was implanted on the Permanent Court of Arbitration's website, which affected anyone who gets access to a specific page designated to the dispute [3].
The need for cyber-security in the arbitration industry takes great importance. One interesting survey indicated that 90% of the respondents agreed that cyber-security on international arbitration is an important issue [14].

As a result of that, several international initiatives have launched to respond to the threat of cyber-attack and enhance the cyber-security in the arbitration industry. For instance, the International Council for Commercial Arbitration ("ICCA") partnered with the New York City Bar Association and the International Institute for Conflict Prevention and Resolution to issue 2020 Cyber-security Protocol for International Arbitration.

Cyber-security Protocol aims to achieve two purposes. Firstly, it provides a framework to determine reasonable information security measures for individual arbitration matters. Secondly, it increases awareness about information security in international arbitrations.

Cyber-security Protocol contains fourteen (14) principles, along with six (6) schedules. The first principle illuminates that the Cyber-security Protocol does not intend to, and does not, provide a one-size-fits-all information security solution.

Principle 6 lays out the elements to be counted by the arbitral tribunal and parties in deciding what information security measures are reasonable in specific arbitration. Such one example of those elements is the risk pertaining to the profile of the arbitration. Principle 7 sets out the categories to be considered in deciding what are the specific information security measures to be applied in arbitration, such as access controls and encryption. While Principle 10 also illuminates the need for raising information security as soon as possible in the arbitration industry.

As mentioned earlier, e-arbitration is entirely dependent on the using technology. All of its activities from A-to-Z are carried out in the online environment i.e. internet. Moreover, the parties during the e-arbitral proceedings would disclose sensitive information and materials to the arbitral tribunal to prove their case. This information may have the potential to ruin the parties' reputations if exposed to the third party.

Unaspiringly, the parties to e-arbitration are not protected from the threat of cyber-attack and data infringement. This is because complete security in the online environment is impossible [23]. Most of the internet-based communications that are made through open medium i.e. internet, are exposed to data security threats [24]. Thus, the future implementation of e-arbitration in Malaysia will not be improved unless the potential participants in e-arbitration have confidence that their communications and submissions will be secure.

Based on the above facts, it is very significant to examine how cyber-security can be maintained in the context of e-arbitration in Malaysia.

3. Maintaining Cyber-Security in Securing Future Implementation of E-Arbitration in Malaysia

Indeed, the environment where e-arbitration operates must be secure [18]. The following discusses the technical and legal measures to maintain cyber-security in e-arbitration in Malaysia.

From a technical standpoint, the technological advances are expected to reduce security issues [10]. Fortunately, there are many technical measures can be adopted to safeguard cyber-security to the potential participants in e-arbitration in Malaysia. Such as using cryptographic tools [8], a digital signature [17], firewall, antivirus, malware programs, two-steps authentication process, and transfer of documents through the secure shared platform, such as IManage Cloud [15].

Apart from the above, in order to improve the future implementation of e-arbitration in resolving the Islamic banking disputes in Malaysia, there is a need to design a specific e-arbitration platform that is based on using blockchain technology and Artificial intelligence (hereinafter referred to as "AI").

Concerning blockchain, it is inviolable, immutable [9] and able to provide more traceability, the security of records [16], and solution against hacking [25]. In fact, blockchain technology has already applied in the context of e-arbitration. For instance, the Nanjing Arbitration Commission network arbitration platform [25].

Besides, the use of AI in the arbitration industry in Malaysia has been advocated. In this context of this article, AI has been used frequently in cyber-security. In a recent survey, 75% and 71% of the organisations depend on using AI for network security and data security, respectively. [4] This is because using AI in cyber-security lowers the cost to detect and enables a faster response to breaches, respectively [4]. Therefore, using AI would help in safeguarding the sensitive data of the potential participants in e-arbitration in Malaysia.

In addition, one survey regarding the use of internet-based communication shows that 68.42% of the participants is never using encryption systems to secure their information [21]. In the context of Malaysia, in 2020, cyber-security cases have increased by a huge 82.5% during the Movement Control Order [26]. The total reported cases were eight-hundred thirty-eight (838) cases. Of this total, one-hundred fifty-two (152) cases involved local companies, while the rest cases were home users and others [26].

By the application of analogy, there is a need to enhance awareness in the cyber-security among the Malaysian citizens who may be potential participants in e-arbitration in Malaysia. This can be achieved if the potential participants in e-arbitration have changed their mind-sets toward the issue of cyber-security. They should accept it as an urgent necessity rather than an optional matter.

Discussing the legal measures, it was witnessed that there are several laws affirmatively put an obligation on the e-arbitration institution to take bold steps in order to ensure the cyber-security of the participants in e-arbitration. For instance, article 15 of China International Economic and Trade Arbitration Commission-Online Arbitration Rules 2015 states that;

> CIETAC shall make reasonable efforts to ensure secure online transmission of case data among the parties, the arbitral tribunal and CIETAC, and to store case information through data encryption.

Likewise, article 29 of China Guangzhou Arbitration Commission - Online Arbitration Rules 2019 states that;

> This Council provides security for the online transmission of case data between the parties, the arbitral tribunal and the Association, and keeps the case information confidential in the form of encryption of the case data information.

In the context of Malaysia, Arbitration Act 2005 (hereinafter referred to as "Act 646") is silent regarding the need for ensuring cyber-security in an online environment. Therefore, the relevant authorities should take necessary amendment to Act 646 in order to enhance cyber-security to the potential participants in e-arbitration in Malaysia. This argument underpinned by "International Arbitration Survey 2018" which shows that 57% of the respondents agreed that the arbitration law should contain a specific section to deal with security of electronic communications and information [22].

4. Legal Position of Act 646 in Dealing with the Evidence Collected through Cyber-Attacks

Cyber-attack is something real and may paralyse the justice system, especially when the evidence used in arbitration are collected through cyber-attacks. For instance, in the case of *Caratube International Oil Company LLP v. The Republic of Kazakhstan* (ICSID Case No. ARB/08/12), the arbitral tribunal expressly accepted e-mails (leaked information) as evidence on the ground that the e-mails are now public and hence there are no longer confidential.

Contrarily, in the case of *ConocoPhillips v. Venezuela* (ICSID Case No. ARB/07/30), the parties endeavoured to depend on evidence collected from WikiLeaks. However, the majority of the arbitral members did not expressly discuss whether the evidence published by WikiLeaks was admissible, but rather it found that it did not have the authority to reopen its earlier decision.

Based on the above arguments, it is clear that there is no uniform approach to addressing the issue of using evidence that is collected through a cyber-attack in arbitration (two contradiction decisions provided in the previous discussion).

In the Malaysian context, it is very imperative to examine whether Act 646 allows the arbitral members to handle the evidence collected through cyber-attacks. In fact, the authors do not manage to find any case law that illustrates the Malaysian position in this regard.

However, it was witnessed that Act 646 typically provide broad discretion to the arbitral members to decide on the evidentiary issues, such one example might be the evidence collected through a cyber-attack. Section 21 (3) (a) of Act 646 states that;

> The power conferred upon the arbitral subsection (2) shall include the power to determine the admissibility, relevance, materiality and weight of any evidence.

Thus, Act 646 is not clear about the issue of using evidence that is collected through a cyber-attack in traditional arbitration. Therefore, Malaysian lawmakers should provide a clear answer in order to avoid any misuse and confusion among the participants in e-arbitration.

5. Conclusion

The Islamic banking disputants should be able to resolve their dispute in accordance with the Islamic principles that call for a quickest and effective resolution. Implementing e-arbitration in Malaysia would be the first step to achieve that desired purpose. However, the implementation of e-arbitration requires the fulfilment of several non-requirements. Cyber-security is a very significant element to improve the future implementation of e-arbitration in resolving Islamic banking disputes in Malaysia. For that reason, the article suggests several legal and technical measures that can be adopted by the relevant authorities before implementing e-arbitration in Malaysia. A failure in following the recommendations mentioned in this article could jeopardise the future implementation of e-arbitration and affect the attractiveness of e-arbitration as an effective dispute resolution mechanism in Malaysia.

References

[1] "Arbitration proceeding," Arbitration Court, https://en.soud.cz/arbitration-proceeding.

[2] Amy j. Schmitz, "Building on OArb Attributes in Pursuit of Justice," in *Arbitration in the Digital Age: The Brave New World of Arbitration*, edited by Maud Piers and Christian Aschauer (Cambridge University Press, 2018).

[3] Anca M Sattler, "Cybersecurity threats in arbitration are real: Why take a risk?" ADR Institute of Canada, https://adric.ca/adr-perspectives/cybersecurity-threats-in-arbitration-are-real-why-take-a-risk/.

[4] Capgemini Research Institute, Reinventing Cybersecurity with Artificial Intelligence: the new frontier in digital security, 2019 pp 1-28 https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf.

[5] Claire Morel de Westgaver, Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions, Kluwer Arbitration, Published October 6, 2017, http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security.

[6] Dafna Lavi, "Three is not a Crowd: Online Mediation-Arbitration in Business to Consumer Internet Disputes," University of Pennsylvania Journal of International Law, vol.36, no.3, pp. 871-941, 2016.

[7] Farouq Saber Al-Shibli, "The Role of Arbitration in Settling the Dispute of Islamic Banking," *Journal of Humanities, Language, Culture and Business* vol.1, no. 2, pp. 221-229, 2017,

http://www.icohlcb.com/index.php/archived-journal/18-volume-i-2

[8] Faye Fangfei Wang, *Online Arbitration* (New York: Informa Law from Routledge, 2018).

[9] Francisco Uríbarri Soares, "New Technologies and Arbitration," *Indian Journal of Arbitration Law* vol.7, no.1, pp. 84-103, 2018.

[10] Gail A. Lasprogata, "Virtual Arbitration: Contract Law and Alternative Dispute Resolution Meet in Cyberspace," *Journal of Legal Studies Education*, vol.19, no. 1, pp. 107-140, 1978.

[11] Gerard A.W. Vreeswijk And Arno R. Lodder, "GearBi: Towards an Online Arbitration Environment Based on the Design Principles Simplicity, Awareness, Orientation, and Timeliness," *Artificial Intelligence and Law*, vol.13, no. 6, pp. 297-321, 2006.

[12] "Islamic Banks," Bank Negara Malaysia, accessed March 27, 2020, https://www.bnm.gov.my/index.php?ch=li&cat=islamic&type=ib&fund=0&cu=0.

[13] "International Islamic Bank," Bank Negara Malaysia, accessed March 27, 2020, https://www.bnm.gov.my/index.php?ch=li&cat=iib&type=iib&fund=0&cu=0.

[14] "International Arbitration Survey: Cybersecurity in International Arbitration," Bryan Cave Leighton Paisner, https://www.bclplaw.com/images/content/1/6/v2/160089/Bryan-Cave-Leighton-Paisner-Arbitration-Survey-Report-2018.pdf.

[15] "IManage Cloud," Imanage, https://imanage.com/product/imanage-cloud/.

[16] Joseph Bambara *et al*., *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*, 1st edition (McGraw Hill Professional, 2018).

[17] Julia Hornle "Online Dispute Resolution-The Emperor's New Clothes? Benefits and Pitfalls of Online Dispute Resolution and Its Application to Commercial Arbitration," International Review of Law, Computers and Technology 17, no. 1, pp. 27-37, 2003.

[18] Mohamed Abdel Wahab, "ODR and EArbitration: Trends and Challenges," in *Online Dispute Resolution: Theory and Practice A Treatise on Technology and Dispute Resolution*, edited by Mohamed S. Abdel Wahab, M. Ethan Katsh and Daniel Rainey, Eleven International Publishing, 2012, pp. 387-429.

[19] Mohamad Fateh Labanieh, Mohammad Azam Hussain and Nazli Mahdzir, E-arbitration in Islamic banking disputes: more justice to consumer?" *Journal of Advanced Research in Dynamical and Control Systems*, vol.11, no. 5.s, pp. 684-691, 2019.

[20] Mohamad Fateh Labanieh, Mohammad Azam Hussain and Nazli Mahdzir, "Arbitration As A Mechanism To Resolve Islamic Banking Disputes In Malaysia: Challenges And Drawbacks," *UUM Journal of Legal Studies*, vol. 10, no. 2, pp. 19-44, 2020.

[21] Maud Piers and Christian Aschauer, "Survey on the Present Use of ICT in International Arbitration," in *Arbitration in the Digital Age: The Brave New World of Arbitration*, edited by Maud Piers and Christian Aschauer (United States of America, New York: Cambridge University Press, 2018).

[22] Sherin Kunhibava, "Islamic Banking in Malaysia," *International Journal of Legal Information* vol.40, no. 1, pp. 191-201, 2012.

[23] Thomas Schultz, "Online Dispute Resolution: An Overview and Selected Issues," United Nations Economic Commission for Europe Forum on Online Dispute Resolution, pp. 1-21, 2002, https://ssrn.com/abstract=898821.

[24] Vikrant Sopan Yadav, "Cyber Arbitration through Lenses of Indian Legal System: An Analysis", *International Journal of Law*, vol. 2, no. 2, pp. 31-33, 2016.

[25] "Work Dynamics," Nanjing Arbitration Commission, http://ac.nanjing.gov.cn/zczx/gzdt/201809/t20180927_5801949.html

[26] Yuen Meikeng, "Cybersecurity cases rise by 82.5%," The Star, published April 12, 2020, https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825