AIADR Journal of

International ADR Forum

The Journal of scholarly resources for users and practitioners of Alternative Dispute Resolution forum

2022 Volume 2 Issue 9

ASIAN INSTITUTE OF ALTERNATIVE DISPUTE RESOLUTION
Delivering Excellence in ADR

AIADR Journal of International ADR Forum

A REPERTOIRE OF GLOBAL JURISPRUDENCE

The "*International ADR Forum*" is the scholarly journal published quarterly, four times a year, starting from 31 August 2020 by Asian Institute of Alternative Dispute Resolution ("AIADR"). The scholarship is contributed by independent ADR practitioners, academics, researchers, scholars, and users of the ADR Forums. The articles sought are original as the works of the authors submitting it for publication in ADR Forum and are published after a blind peer review by a panel of reviewers from academia, distinguished practitioners, members of judiciary and acclaimed authors. The commentaries and book reviews are presented voluntarily by the commentators or members of the Institute. All contributors undertake to be committed to the Vision of the Institute.

Published by Asian Institute of Alternative Dispute Resolution (AIADR)

28-1, Jalan Medan Setia 2, Bukit Damansara, 50490 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur, Malaysia.

https://www.aiadr.world Email: thesecretariat@aiadr.world; aiadr.editor@aiadr.world;

Library of Congress Cataloguing-in-Publication Data

Editorial Board

Tags for Indexing and Categories of ADR

1. Dispute Resolution; 2. Alternative Dispute Resolution; 3. Adjudication; 4. Arbitration.5. Mediation; 6. Expert Determination; 7. Neutral Evaluation; 8. Expert Witness.

KOD JALUR / BARCODE

eISSN 2773-5052

9 772773 505006

AIADR Journal of International ADR Forum
VOL 2 ISSUE 9, AUGUST 2022

Contents

EMERGING TRENDS IN INTERNATIONAL LAW-COMMERCIAL DISPUTE RESOLUTION MECHANISMS AND ENABLERS IN POST COVID-19 WORLD

By Dr. Hemant Garg

DR.Hemant Garg presently working as Law Officer in The PSCAD Bank Ltd., Chandigarh India. He got his LLB, LLM, MBA, Phd in Arbitration Law.

ABSTRACT

Upon a shift from the rigid traditional adversarial method of dispute resolution to a much flexible approach of alternative dispute resolution that involves arbitration and other ADR methods, we have been witnessing a giant leap. Moving forward, dispute resolution through virtual hearings and artificial intelligence, may be the next step forward to make adjudication systems to be potentially more efficient, like never before. Factors such as increased trade amongst multiple jurisdictions, contracts involving stakeholders/parties from multiple jurisdictions, increase use in technology for litigation and development of extra-ordinary technologies such as metaverse, cryptocurrencies and assets etc. have a very strong role to play in bringing upcoming trends, such as the former. This study is the attempt of the Author to shed my views on the emerging trends and fresh approaches which are being undertaken to resolve disputes globally and the potential causes for the same. In this pursuit thereof, the Author has tried to analyze the upcoming and emerging trends in Arbitration, Covid-19 induced changes in resolution of disputes and the use of cutting-edge technology such as Artificial Intelligence among other developments.

****

INTRODUCTION:

Dispute resolution is an important aspect within international law. One may consider how important it is to maintain the peace and security across international borders. With the continuous development in globalization, there is greater interaction between countries as well as other global entities. While globalization holds immense economic value, it has also led to increased legal disputes. These disputes not only affect trade relations between countries but also have a detrimental effect on the growth and development of stakeholders involved. To curb the same, there is a need to develop effective mechanisms of resolution of such disputes.[1] As the world changes, the dispute resolution mechanisms is also evolving. In recent years, the Covid-19 pandemic has been a major factor in the reform or development in the landscape of international dispute resolution mechanism. The onset of the Covid-19 pandemic coupled with the developing technologies such as cryptocurrency, metaverse and NFTs etc. and the kind of disputes that may potentially arise would demand a fresh approach and perspective. Moving forward, dispute resolution through virtual hearings and artificial intelligence may be the next step forward to make adjudication systems to become more efficient potentially in future. This study is the attempt of the Author to shed my views on the fresh approaches being undertaken to resolve disputes globally and in this pursuit thereof, the Author has tried to analyze the upcoming and emerging trends in Arbitration, Covid-19 induced changes in resolution of disputes and the use of cutting edge technology such as Artificial Intelligence among other developments.

[1] Nimisha Mishra, 'Recent trends in International dispute settlement' (*Lexpeeps*, 9 June 2020) <https://lexpeeps.in/recent-trends-in-international-dispute-settlement/> accessed on 17 February 2022

INCRESED CROSS-BORDER TRANSACTIONS, DISPUTES AND DEVELOPMENT OF NEW INSTITUTIONS:

The increasing growth in the cross-border economic transactions and other related activity continues to dominate the international arbitration trends. Specifically, as cross-border transactions have grown in popularity, the number of disputes have also increased[2]. The increase in cross-border disputes due to more countries getting involved in global trade has also led to increase in the development of new institutions. For an example, the rising participation of developing economies in international transactions has led to a further development trend of dispute resolution away from more established international arbitration centers like the London International Arbitration Centre (LIAC) towards the Middle East and Far East. In particular, the Singapore International Arbitration Centre (SIAC) has witnessed a sharp increase in dispute filings and adjudication. One such example of a multi-jurisdictional project is the China's Belt and Road Initiative (BRI), formerly known as One Belt One Road. BRI is a global infrastructure development strategy initiated by the People's Republic of China Government to collaborate with many developing and developed countries as well as international non-governmental private organizations[3]. The Author may wish to personally argue that it may be one of the most massive investment and construction program that has ever been propounded globally. Quite naturally, the arbitral tribunals throughout APAC and beyond ar willing to adjudicate cases arising from BRI's complex and multi-party projects. The People's of Republic of China has recently established Chinese International Commercial Courts in Xi'an and Shenzhen, an at the same time also facilitates the use of international arbitration. This is advantageous for both

[2] Rory Mac Neice, 'Current trends in International Arbitration and Dispute Resolution' (*Ashfords,* 14 May 2015) https://www.ashfords.co.uk/news-and-media/general/current-trends-in-international-arbitration-and-dispute-resolution accessed on 21 February 2022

[3] Council on Foreign Relations, 'China's massive belt and road initiative' https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative accessed on 22 February 2022

foreign arbitration organizations and parties who wish to use them[4].. Besides, there appears to have a trend of increase in the competition and an increase in number of institutions for adjudication is one of the most prominent trends being observed in the present-day dispute resolution scenario on a global level.

DEVELOPMENT OF NEW TECHNOLOGIES: -

The development of new technologies such as crypto assets and smart contracts also require a fresh and reformative approach as the disputes that may arise from these are novel and unconventional. Some potential disputes in today's time and age already involve science and technology, intellectual property and social media. Litigation arising from intellectual property ownership, patent, trademark, and copyright infringement, hacking of crypto wallets, large-scale data breaches, theft of trade secrets, and breaches of joint research and development and confidentiality agreements among others have already become more frequent and intense[5]. In addition, with Parties from multiple jurisdictions being involved there is also an emergent need of laws with an international perspective. Reliance must be placed upon a recent survey conducted by World Intellectual Property Organization (WIPO), wherein almost 91 percent of the nearly 400 survey respondents executed technology-related agreements with companies situated in foreign jurisdictions. Additionally, approximately a quarter of respondents said that at least sixty percent of their contracts involve overseas partners, while only 9% contracted entirely within their home country. Additionally, over eighty

[4] Peter Hirst & Mun Yeow, 'International Arbitration: Current Trends and what to expect in 2020 and the years ahead' https://www.mondaq.com/uk/arbitration-dispute-resolution/880988/international-arbitration-current-trends-and-what-to-expect-in-2020-and-the-years-ahead accessed on 21 February 2022

[5] Colin Rule, 'Technology and the future of dispute resolution' https://law.scu.edu/wp-content/uploads/Rule-Technology-and-the-Future-of-Dispute-Resolution-copy.pdf accessed on 19 February 2022

percent of respondents entered into agreements involving patent-protected technology in many countries, compared to less than twenty percent who entered into agreements involving patent-protected technology in a single country. Thus, the exploitation of technologies is rapidly becoming into a business that requires access to competent international dispute resolution mechanisms[6]. Recently adopted set of Digital Dispute Resolution Rules by the UK Government is one of the most forward-thinking recent solutions. They offer a customized, simplified arbitration system aimed at rapidly and economically resolving commercial disputes, particularly those involving unique digital technologies such as crypto assets and smart contracts (although the rules can be used for any dispute subject matter). The criteria are intended to be as flexible as feasible; the tribunal will make every effort to resolve the dispute within 30 days and judgements can be performed directly "on-chain" using a private key. The Rules take a daring new approach by advocating for an informal, cost-effective, specialized, and anonymous method that makes extensive use of technology both during the arbitration process and in enforcing judgments. As such, these rules offer numerous advantages, but they are also extensively untested and deliberately brief. Consequently, it will likely take some time to determine how effective they are in practice, and whether they can be the go-to approach for resolutions demanding extra ordinary adjudication[7].

COVID-19 AND INTERNATIONALDISPUTE RESOLUTION MECHANISM:

The Covid-19 pandemic brought with it, waves of unprecedented challenges such as international travel restrictions and social distancing norms which made it almost impossible for in-person hearings to take place. Judicial systems across the globe took a hit when they were closed down like most

[6] WIPO, Results of the international survey on dispute resolution in technology transactions https://www.wipo.int/amc/en/center/survey/results.html accessed on 19 February 2022

[7] Covington, The Digital Dispute Resolution Rules, https://www.cov.com/en/news-and-insights/insights/2021/06/the-digital-dispute-resolution-rules accessed on 17 February 2022

other institutions due to government-imposed lockdowns. This led to the denial of access to justice as the proceedings of cases that were classified as non-urgent were suspended or postponed. While it was a good policy decision to prioritize the cases based on urgency of relief, it also meant that when courts became fully functional, they would have to deal with the burden of a massive backlog, which already is a subject of major concern in saturated jurisdictions such as India, where there is already a substantial amount of pendency and disputes pending adjudication.[8] To ensure that this outcome was avoided, most domestic as well as international courts adapted to the changing situation by conducting virtual or hybrid hearings instead of physical in-person hearings.[9] In addition to the domestic adjudicatory authorities, international institutions also embraced the developing technology in the form of virtual hearings when it was realized that remote-proceedings were inevitable.[10] These hearings were governed via detailed protocols and standard operating procedures which were developed to facilitate this shift to virtual hearings. This also led to the widespread adoption of innovative digital technology such as artificial intelligence, blockchain mechanisms, document management system etc., facilitating the culture of online courts.[11] Certain exceptions include countries like the People's Republic of China, which has been leading this e-justice

[8] Matt Pollard, 'The Courts and Covid-19' (International Commission of Jurists, 5 May 2020) < https://www.icj.org/wp-content/uploads/2020/05/Universal-ICJ-courts-covid-Advocacy-Analysis-brief-2020-ENG.pdf > accessed on 16 February 2022

[9] Giulia Pinzauti & Philippa Webb, 'Litigation before the International Court of Justice during the pandemic' (2021) 34(4) Leiden Journal of International Law, 787-800.

[10] Tai-Heng Cheng, Martin Jackson & Young-Hee Kim, 'COVID-19 and Technology in International Arbitration' (New York Law Journal, 19 November 2021) < https://www.law.com/newyorklawjournal/2021/11/19/covid-19-and-technology-in-international-arbitration/ > accessed on 16 February 2022

[11] Kim M Rooney, 'The Global Impact of the Covid-19 pandemic on Commercial Dispute Resolution in the First Year' (*International Bar Association*, 2 June 2021) < https://www.ibanet.org/global-impact-covid-19-pandemic-dispute-resolution#_ftnref4 > accessed on 15 February 2022.

revolution even before the pandemic with the recognition of electronic data as well as the use of e-evidence in civil procedures. Blockchains are being used to preserve digital files and creating a digital database as well as to authenticate online evidence. The intelligent court project has also been under progress to utilize AI software.[12]

ONLINE DISPUTE RESOLUTION(ODR):

Even though the concept of Online Dispute Resolution (ODR) was floated in several jurisdictions such as the United Kingdom and China even before the pandemic, [13] its scope skyrocketed during the Covid-19 when it was considered to be one of the most effective solutions to all the challenges posed as it provided the required flexibility and efficiency of facilitating judicial proceedings remotely. The ODR processes take advantage of the internet and online communications to resolve disputes. ODR is not only economic and efficient but also environmentally friendly, as the commute of litigants, arbitrators, judges, and other stakeholders was reduced to minimal. Additionally, since all filings were also made virtual there was a tremendous reduction in the amount of paper used while printing, which anyway was a cause of major debate before the pandemic also. The participants also saved up on other expenses caused in in-person hearings. The parties now have the freedom to present their cases from anywhere in the world, since this process became exclusively online.[14] There is also a new concept of

[12] Zhuhao Wang, 'China's E-Justice Revolution' (2021) 105 (1) Judicature < https://judicature.duke.edu/wp-content/uploads/2021/04/EJustice_Spring2021.pdf > accessed on 18 February 2022.

[13] Rt. Hon Lord Dyson, 'Online Dispute Resolution for low value civil claims' (*Civil Justice Council*, February 2015) <https://www.judiciary.uk/wp-content/uploads/2015/02/Online-Dispute-Resolution-Final-Web-Version1.pdf > accessed on 16 February 2022.

[14] Rahim Moloo, Ankita Ritwick, Patrick Taqui, Kelly Tieu & Bethany Saul, 'Online Dispute Resolution: An option for times of crisis and calm' (*Gibson Dunn*, 30 March 2020) < https://www.gibsondunn.com/wp-content/uploads/2020/03/online-dispute-resolution-an-option-

documents-only arbitrations wherein parties don't even require video-conferences, since the arbitrators come to a decision simply through their perusal of the evidentiary documents uploaded by the parties. These forms of arbitrations are usually used for International IPR issues such as domain name disputes etc.[15] Resultantly, the Author considers that not only litigants end up saving the time and money, the disposal of disputes also became quicker.

Various guidelines as well as amendments to rules were brought to effect to incorporate virtual hearings as a legitimate process of dispute resolution. For example, the ICJ amended Articles 59 and 94 of the ICJ Rules to include the use of technology to hold virtual hearings using video links and to work remotely citing health, security and other compelling reasons for the same.[16] These hearings are to be conducted in the same manner as an in-person hearing. As a precaution from any technical difficulties, the court also made logistical arrangements such as pre-hearing consultations which reviewed the proposed platform, different time-zones of the participants etc., as well as technical preparation like communicating the link a few days before, conducting tutorials or practice sessions etc., before the actual hearings. Just like physical courtroom etiquette, an online etiquette for the participants as well as the detailed Standard Operating Procedure guiding each stage of the process was also formulated.[17] As the arbitral rules and legislations

for-times-of-crisis-and-calm.pdf > accessed on 16 February 2022

[15] Derric Yeoh, 'Is Online Dispute Resolution the Future of Alternative Dispute Resolution?' (Kluwer Arbitration Blog, 29 March 2018) < http://arbitrationblog.kluwerarbitration.com/2018/03/29/online-dispute-resolution-future-alternative-dispute-resolution/ > accessed on 17 February 2022.

[16] Guidelines for the parties on the organisation of hearings by video link' International Court of Justice <https://www.icj-cij.org/en/other-texts/guidelines-videolink> accessed on 17 February 2022.

[17] 'Covid-19: ICJ publishes global guidance on the use of videoconferencing in judicial proceedings' International Court of Justice < https://www.icj.org/covid-19-icj-publishes-global-

may lack express provisions that enabled remote virtual hearings, international arbitral institutions promptly introduced rules and guidelines for the same. The International Chamber of Commerce in its 2021 Arbitration Rules, made the provision for remote hearings using videoconference or telephones as a part of Article 26.[18] The World Bank also introduced online hearings at the International Centre for Settlement of Investment Disputes and also provided a virtual court stenographer that would be visible to all participants and even the option to participants of joining by telephone in case of poor connectivity.[19] Before a permanent shift to virtual hearings can be contemplated, it must be understood that an online courtroom through a videoconference is not equivalent to an in-person hearing due to the difficulty in expressing non-verbal cues. Access to technological infrastructure such as reliable internet is a must, putting those in underdeveloped and developing nations at a disadvantage.[20] The issue of fairness also arises since there may be disparity between the technology and resources available with the different parties leading to a bias in the hearing.[21] Online proceedings have risks such as errors in online communication and electronic document exchange. Cybersecurity, data privacy and confidentiality are major concerns in the conduct of virtual hearings.[22]

There is an increasing growth in the ODR trends in India. ODR seems to be catching entrepreneurial interest in India which is evident from the rise of

guidance-on-the-use-of-videoconferencing-in-judicial-proceedings/ > accessed on 17 February 2022.

[18] 2021 Arbitration Rules, Art 26, International Chamber of Commerce < https://iccwbo.org/dispute-resolution-services/arbitration/rules-of-arbitration/#article_26>

[19] 'A Brief Guide to Online Hearings at ICSID'

[20] Norman Meyer, 'Courts and Coronavirus: Is Videoconferencing a Solution?' (Court Leader, 16 March 2020) <https://courtleader.net/2020/03/16/courts-and-coronavirus-is-videoconferencing-a-solution/> accessed on 18 February 2022

[21] *Id* 3

[22] Id 7

ODR related start-ups and businesses. Some of the leading ODR platforms in India include CADRE, or the Centre for Excellence in Alternative Dispute Resolution, which is an online platform for ODR. For NestAway, an online home rental firm, CADRE has been settling rental and tenant contract conflicts. SAMA is another online dispute resolution platform that facilitates access to high-quality alternative dispute resolution providers and assists individuals in resolving conflicts online. ICICI Bank uses Sama as their alternative dispute resolution platform to resolve almost 10,000 cases with a maximum value of INR 20 lakh[23]. Similarly, Immediation is a US based platform which is claimed as the world's safest digital disputes resolution platform. Immediation provides an end-to-end online experience to parties which are specifically interested in mediating or arbitrating their disputes with best and secure practices[24]. These trends imply the convergence of the problem, policy, and political streams, hence opening a window of opportunity for ODR around the world.

INCREASING USE OF TECHNOLOGY:

With developing technology being used in the legal field, dispute resolution mechanisms have become more efficient with provisions available with courts to do electronic filing, availability of case management software etc. The process of digitization has also increased the efficiency of the dispute resolution processes. Technical tools such as videoconferencing platforms to conduct virtual hearings, data analytics that suggested appointment of judges, counsels, arbitrators or mediators as well as eDiscovery assisted in international commercial disputes are all essential building blocks of this

[23] Rashika Narain and Smriti Parsheera, 'Online dispute resolution in India: Looking beyond the window of opportunity' (The Leap Blog, *14 April, 2021*) https://blog.theleapjournal.org/2021/04/online-dispute-resolution-in-india.html. Accessed 4th March 2022

[24] Online Dispute Resolution Platforms, (Resolution Institute), https://www.resolution.institute/resources/online-dispute-resolution-platforms Accessed on 4th March 2022

larger reform.[25]

DIGITIZATION OF EDISCOVERY PROCESS:

The due-diligence research as well as inspection phase of the legal proceedings is an expensive and time-consuming process. Currently used eDiscovery software assists parties to a dispute in collecting, storing, processing and retrieving information all on a single platform, which can also be easily transferred between the parties. This software also enables tagging of documents, categorizing them as plaintiff or defendant documents and facilitating easier searches as well as analysis of data. This software is highly recommended for maintaining the integrity of the data as well as safeguarding the chain of custody of the documents. The discovery process becomes efficient due to the streamlining as well as the case management and strategizing that the software does.[26]

ARTIFICIAL INTELLIGENCE:

There is also a generous use of Artificial Intelligence (AI) in dispute resolution mechanisms for digitization of information to electronic formats, online litigation service platforms using intelligent robots, online dispute resolution platforms for effective mediations and predictions of judgement outcomes using data analytics after going through the judicial documents.[27]

---

[25] 'SIDRA International Dispute Resolution Survey: 2020 Final Report' (SIDRA Survey, 2 July 2020) <https://sidra.smu.edu.sg/sites/sidra.smu.edu.sg/files/survey/52/index.html> accessed on 18 February 2022

[26] Michael Peer, Dimitry Kosarev & Christine Soon, 'Trending in International Dispute Resolution: Technological advancements reshaping Dispute resolution' (pwc, 2020) <https://www.pwc.com/sg/en/consulting/assets/technological-advancements-reshaping-dispute-resolution.pdf> accessed on 16 February 2022

[27] Chen Mingtsung & Li Shuling, 'Research on the application of artificial intelligence technology in the field of Justice' (2020) J. Phys Conf Ser.

AI-enabled data analytics is also assisting in developing platforms that help those in need to make informed choices by connecting them to tribunals, arbitrators, counsels and mediators that is best suited for their tailored needs and therefore reduces any delays or potential conflicts. In the near future, AI and machine learning is also expected to be a part of the eDiscovery platforms which might increase the efficiency and accuracy of the entire process.[28]Another utility of the AI at present is the use of its predictive coding for predictive analysis of the outcome of various disputes such as IPR issues, labor law disputes, human right violations etc. with impressive consistency and accuracy.[29] Negotiation Support systems developed with AI are also being used to resolve international conflicts as well as labor relations conflicts by making the process easier for the parties through communication tools, advisor tools, case management tools, drafting software etc.[30]These systems provide intelligent advice that supports the negotiators. There is also a mechanism of rule-based Solution Explorer which helps disputing parties to arrive at the best alternative to a negotiated agreement and if that fails, they are made to enter a secure and confidential negotiation platform where the parties can resolve disputes without any external help. These negotiation support AI are made with the user experience in mind.[31] However, AI needs extensive training with big data training sets for effective prediction or analysis and to avoid ingrained algorithmic biases the developer needs to ensure that these training sets are free from any biases. Another issue with AI is the lack of transparency as the machine learning system works in a manner in which there is no

[28] *Id* 17

[29] Minjung Park & Sangmi Chai, 'AI Model for Predicting Legal Judgments to Improve Accuracy and Explainability of Online Privacy Invasion Cases' (2021) 11 Appl. Sci.

[30] John Zeleznikow, 'Using Artificial Intelligence to provide Intelligent Dispute Resolution Support' (2021) Springer.

[31] John Zeleznikow, 'Using Artificial Intelligence to Provide User Centric Intelligent Negotiation Support' (2021) <https://www.law.virginia.edu/system/files/AI_Negotiation_Support%20J.%20Zeleznikow%209pm%20Panel%201.pdf > accessed on

reasoning given for the prediction or the decision made by the AI. Furthermore, data protection and confidentiality issues like any other technology must be dealt with before the use of AI.[32] The contemplation whether AI can replace humans that play the role of judges and lawyers in a dispute resolution mechanism and whether AI can make better decision makers than human beings has been a subject matter of recent debates. Although it is evident that AI programs are more rational than humans as well as being bias-free (i.e. since they cannot be influenced by unconscious or cognitive and emotional biases), it is unlikely that judges or lawyers will be replaced by AI [33] anytime soon since such thoughts can only be entertained when AI has at least reached the development stage of Artificial General Intelligence (AGI) which is AI with true intelligence indistinguishable from human intelligence or even exceeding it and could be used for decision-making.[34]

ANALYSIS:

The shift of dispute resolution mechanism towards international arbitration has been a gradual one exemplified by the effects and consequences of the pandemic. Firstly, International arbitration has several advantages over a traditional court litigation. And more importantly, over the years, the limitations of the traditional dispute resolution system have led to the development of international arbitration as an effective alternative dispute resolution mechanism. When compared to traditional court litigations, international arbitration not only resolves disputes in a swift and inexpensive

[32] Lance Ang, 'Legal Disruption in Dispute Resolution in the Age of COVID-19' (Harvard International Law Journal) <https://harvardilj.org/2021/02/legal-disruption-in-dispute-resolution-in-the-age-of-covid-19/> accessed on 17 February 2022.

[33] Maxi Scherer, International Arbitration 3.0 - How Artificial Intelligence Will Change Dispute Resolution' (2019) Austrian Yearbook of International Arbitration.

[34]Wim Naude & Nicola Dimitri, 'The race for an artificial general intelligence: implications for public policy' (2020) 35 AI & Society 367-379.

manner, the quality of justice is also relatively higher since the arbitral institutions have sufficient time as well as industry expert arbitrators. Further, these processes are bias free and neutral since the arbitral chair can be in the country where none of the parties are from giving neither party an advantage. The process is also highly confidential, independent and binding. In cases of certain disputes such as those between the investor-state, international arbitration is the sole remedy.[35] There is also plenty of hurdles including but not limited to state interference and political pressure that the international judicial institutions such as ICJ and WITO have to go through. Despite the ICJ having an unlimited jurisdiction lack of state consent is an important factor leading to many disputes not being resolved. The election of judges to the ICJ is done by the UN's political bodies which interferes with the judicial independence and impartiality of the dispute resolution process reducing its effectiveness. The court also loses legitimacy due to the increasing influence of non-state actors in the international sphere who do not come within its jurisdiction since only state disputes come within its ambit.[36]Similarly, the dispute settlement body of the WTO was created to resolve trade disputes between member states. The decision-making of appointment of judges, panels etc. are made on a consensus basis by the members leading to political interference by powerful members. Due to this intervention, the dispute settlement process went into a crisis when the United States started blocking the appointment of new judges to the Appellate Body by their veto power, rendering the mechanism ineffective and powerless.[37] From such a blockade, it is evident that the dispute resolution mechanism of the WTO is not independent from the political intervention of the members. Upon the failure of the WTO to rectify this threat, it has led to members seeking other methods of resolving disputes

[35] Cristina Ioana Florescu, 'Emerging tools to attract and increase the use of international arbitration' (2020) 2 Tribuna Juridica.

[36] Rotem Giladi & Yuval Shany, 'Assessing the Effectiveness of the International Court of Justice' (2021) Hebrew University of Jerusalem Legal Studies Research Paper Series.

[37] Jens Lehne, *Crisis at the WTO: Is the Blocking of Appointments to the WTO Appellate Body by the United States Legally justified?* (Carl Grossmann Publishers 2019).

such as international arbitration.[38] This is where the new age and alternate dispute resolution mechanisms create a difference by being not only flexible but also free from political and state created encumbrances. The use of AI in the judicial process is also a pathbreaking development. Although, used in very limited capacity and in selective jurisdictions, AI holds the potential to significantly reduce costs, increase resolution periods and increase litigation management by cutting down operational difficulties. Using AI to determine outcomes in early-stage litigations can not only be cost effective but can also increase the disposal of cases on a phenomenal rate. These emerging trends on a global level hold the potential to identify the present challenges and tackle them with utmost effectiveness.

CONCLUSION

Extraordinary situations require extraordinary solutions and in view of the same, one must agree that the shift to Online Dispute Resolution (ODR) and virtual proceedings was implemented to minimize the health risks associated with the large gatherings during the pandemic. However, upon identifying the ease of this process, one can determine that this trend of online courts and tribunals is expected to stay even after the effects of the pandemic are over.[39] By far virtual courtrooms is one of the most extraordinary emerging trends which is witnessed across various jurisdictions all over the world. In addition, the implementation of AI, identification of technology related disputes and implementation of new rules and regulations among other emerging trends are going to shape the future of dispute resolution around the world. One must also not forget that there are certain obstacles and risks associated with them as is also discussed in the certain sections above. The silver lining is that the advantages outweigh the risks involved and it would be unjust if the potential of these trends is left unexplored. So far, we have

[38] Bernard Hoekman, 'WTO Reform Priorities post-COVID-19' (2020) 24(4) East Asian Economic Review 337-348.

[39] *Id* 6

come a long way, but the best is yet to come.

****

Full Protection and Security of the Digital Economy

By Augusto García Sanjur & Aram Aghababyan

Augusto García Sanjur is an attorney specialized in international arbitration. He has an LLB from the Universidad de Panama graduating with the first position, and an LLM from Pennsylvania State University. Moreover, he has won first place in worldwide competitions such as the Willem C. Vis Moot Competition in Vienna and the UNIDROIT COVID-19 Essay Competition.

Aram Aghababyan is a software product manager and a qualified attorney specializing in the application of technology in the legal industry. He holds a BS degree from the Armenian State University of Economics in statistics and two LLM degrees from the American University of Armenia, and the University of Amsterdam with a specialization in international law and arbitration.

ABSTRACT

The digital economy is everywhere. Currently, almost all companies need a digital presence or digital infrastructure in order to operate effectively. A considerable part of the assets of these companies is the data that they collect and the system that they operate to serve their clients. After the pandemic, the world saw an accelerated digital revolution and a replacement of brick-and-mortar. As the digital revolution is currently disrupting and changing the way businesses and economies operate, it has become relevant to study how the digital economy interacts with investment protection standards. Specifically, as the Full Protection and Security (FPS)

standard has been commonly used to protect foreign investments, this paper analyzes whether the digital economy is included within the scope of this standard. This paper will also analyze the various considerations that an arbitrator may take into account when deciding whether a State has breached the Full Protection and Security standard towards digital investments.

INTRODUCTION

The digital economy[1]has become one of the most important industries in the world. In 2020, the projects to make the digital economy possible conducted a major number of investment announcements and they have had the largest growth with more than 22%, representing US$81 billion in total.[2] Within the digital economy, digital assets have become one of the main drivers of the global economy[3] making their digital security one of the most important aspects of doing business.[4]

[1] Within the digital economy we include the telecommunication sector that builds the infrastructure that makes internet possible within a State, e.g. fiber optic cables, internet hubs, servers etc. We also include the digital assets of the companies that operate through websites, apps, etc.

[2] UNCTAD, World Investment Report 2021 Investing in Sustainable Recovery (2021) 9 ('The pandemic boosted demand for digital infrastructure globally. This led to higher values of greenfield FDI project announcement targeting the ICT industry, rising by more than 22 per cent to $81 billion. Although the number of announced projects decreased by 13 per cent, the ICT industry attracted the largest share of projects. Major project announcements in this industry included a $6 Billion deal with Telefonica (Spain) to build a fibre-optic [sic] network in Germany, a $2.8 billion investment by Amazon (United States) in ICT infrastructure in India and a $1.8 billion investment by Alphabet (United States) in Poland through Google'.).

[3] Lucas Cuatrecasas, 'International Investment Policy and the Coming Wave of Data-Flow Disputes' (2021) Draft (Forthcoming) Michigan Business & Entrepreneurial L Rev 18 ('By 2018, it was intangible assets that accounted for 84% of the index's value, and the COVID-19 pandemic has only intensified this shift toward intangible assets'.).

[4] Rohan Massey and others, 'Cyber Trends and Investigations in Europe: A Practitioner's Perspective' in

As more businesses are focusing on their digital presence, it is forecasted that foreign direct investment in this industry will only increase as more projects are being announced globally.[5] Considering this growth rate and the importance of digital assets over traditional types of assets or brick-and-mortar companies, it is time for the investment arbitration regime to determine the grounds of investment protection that will be applicable to the digital security of investments.

One of the investment protection standards commonly included in International Investment Agreements (IIAs) is the Full Protection and Security Standard (FPS). This standard has been widely invoked to protect the physical security of investments[6] against mobs and violence conducted

Benjamin A Powell and Jason C Chipman (eds) *The Guide to Cyber Investigations* (2nd edn) 168 (Law Business Research 2021) ('It is estimated that the 2020 cost of cybercrime reached over US$1 trillion – a more than 50 per cent increase from 2018. By some estimates, cybercrime may be the third-largest economy in 2021'.).

[5] UNCTAD (n 2) 53 ('Improving global and regional economic growth in 2021, as well as ASEAN Member States' economic stimulus packages, will help bolster the resilience of the region. Investment in selected service industries and technology-related activities such as the digital economy, e-commerce, digital infrastructure (5G networks and data centres) and cloud computing, is expected to remain robust. The region is projected to become a rapidly growing global data centre hub in the next five years, overtaking growth in North America and in other AsiaPacific countries. Many data centre and cloud MNEs are increasing investment or building more facilities, which are expected to be completed in 2021–2022. Industrial production activities in the region are also gaining momentum, which will encourage further capital expenditure and investment to increase capacity'.); ibid 60 ('For instance, [Colombia] introduced a special tax regime for mega-investments by providing tax breaks and other fiscal incentives. It also implemented a domestic infrastructural programme (5G network plan) to enhance connectivity for its growing digital sector. This sector showed signs of FDI dynamism as Teleperformance (France) and Amazon (United States) announced they would increase their business operations in the country, whereas in the customer experience sector, Alorica (United States), Transcom (Sweden) and TDCX (Singapore) announced new openings'.); ibid 87 ('The pandemic has also forced LDCs to accelerate the development of ICT and the adoption of digital technology. For example, the $4.9 million Tuvalu allocated for projects included improvement of broadband internet connectivity'.).

[6] It has also been argued that FPS also includes the legal security of investments. Regardless of the outcome

in the host State. Other tribunals have also added the legal protection of the investments within the scope of FPS.[7] It has been asserted that the FPS is not a strict liability standard but a standard where the State has to act with due diligence.[8] In this sense, when a hacker[9] acting within the territory of the

---

of this debate, we argue that FPS covers the digital security of investments. *Indian Metals & Ferro Alloys Ltd v Republic of Indonesia*, PCA Case No. 2015-40, Award of 29 March 2019, para 267; *Crystallex International Corp v Bolivarian Republic of Venezuela*, ICSID Case No. ARB(AF)/11/2, Award of 4 April 2016, paras 632-634; *Border Timbers Ltd, Timber Products International (Private) Ltd, and Hangani Development Co. (Private) Ltd v Republic of Zimbabwe*, ICSID Case No. ARB/10/25, Award of 28 July 2015, para 596; *AWG Group Ltd. v The Argentine Republic*, Decision on Liability of 30 July 2010, paras 174-176; *Saluka Investments BV v The Czech Republic*, PCA Case No. 2001-04, Partial Award, 17 March 2006, para 483.

[7] *Compañía de Aguas del Aconquija, S.A. and Vivendi Universal S.A. v Argentine Republic*, Award of 20 August 2007, para 7.4.16; *CME Czech Republic B.V (The Netherlands) v The Czech Republic*, UNCITRAL, Partial Award of 13 September 2001, para 613; *Československá Obchodní Banka A.S. v The Slovak Republic*, ICSID Case No. ARB/97/4, Award of 29 December 2004, para 170; *Azurix Corp. v The Argentine Republic*, ICSID Case No. ARB/01/12, Award of 14 July 2006, para 406; *Global Telecom Holding S.A.E. v Canada*, ICSID Case No. ARB/16/16, Award of 27 March 2020, para 665; *Belenergia S.A. v Italian Republic*, ICSID Case No. ARB/15/40, Award of 6 August 2019, para 621; *Anglo American PLC v Bolivarian Republic of Venezuela*, ICSID Case No. ARB(AF)/14/1, Award of 18 January 2019, para 482; *Krederi Ltd. v Ukraine*, ICSID Case No. ARB/14/17, Award of 2 July 2018, para 652; *Reinhard Hans Unglaube v Republic of Costa Rica*, ICSID Case No. ARB/09/20, Award of 16 May 2012, para 281.

[8] *Oxus Gold plc v Republic of Uzbekistan, the State Committee of Uzbekistan for Geology & Mineral Resources, and Navoi Mining & Metallurgical Kombinat*, Ad-Hoc, Award of 17 December 2015, para 834; *Asian Agricultural Products Ltd. (AAPL) v Republic of Sri Lanka*, ICSID Case No. ARB/87/3, Award of 27 June 1990, para 77.

[9] This paper is based on the assumption of a privately motivated hacker that acted within the territorial jurisdiction of the host State. This paper does not intend to cover public international law situations where a hacker may be ordered by a government to affect a company in another State. Within the hacking community the term hacker is a person penetrates a cyber security but not for malicious reasons. When there is malicious hacking, the person is called a cracker. However, in this paper we will use the term hacker to refer to a person that performs a cyber-intervention with malicious reasons. Avast, 'What is Cracking? It's Hacking, but Evil' <*https://www.avast.com/c-cracking*> accessed 16 January 2022 ('When a hacker penetrates a cybersecurity system, it's known as "security hacking". Cracking takes things a step farther. Cracking is when someone

host State digitally affects the assets or the operations of an investor,[10] it prompts the issue that will be discussed in this paper. Is the digital security of investments protected within the FPS standard? This article will demonstrate that the FPS standard covers the digital security of investments in a host State.

In this regard, Section I provides a brief explanation of the FPS standard as interpreted by tribunals and scholars. It will also provide a test through which we will determine whether the protection of the digital economy is within the scope of FPS. Section II describes how the internet works, explaining that there is an infrastructure that supports and allows the internet to function in the transfer of files, images, and information. The section also discusses jurisdictional challenges the companies with digital assets will face while trying to establish a claim under various IIAs and ICSID Convention. We further argue that because a cyber intervention is a physical process against a physical asset, such as an attack against a factory, the digital protection of assets is included within the FPS standard. Finally, Section III outlines the required conduct of a State under the due diligence threshold when there is a cyber intervention against a digital investment. We will explain that in the

performs a security hack for criminal or malicious reasons, and the person is called a "cracker". Just like a bank robber cracks a safe by skillfully manipulating its lock, a cracker breaks into a computer system, program, or account with the aid of their technical wizardry. […] Most people in the media — and, as a result, most people in general — use the terms "hacking" and "hacker" to refer to this sort of unsavory computer nastiness. But within the hacking community, the term "cracking" is preferred to describe malicious hacking'.).

[10] While it may be discussed whether digital investments are investments. Scott J Shackelford and others, 'Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties' (2015) 52(1) ABLJ 1–74; Eric De Brabandere, 'International Investment Law and Arbitration in Cyberspace' (2021) Grotius Centre Working Paper Series No 2021/095-IEL in Nicholas Tsagourias and Russel Buchan (eds), Research Handbook on International Law and Cyberspace (2nd edn) (2021), Leiden Law School Research Paper Forthcoming; Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2020) 21 Vanderbilt J of Entertainment and Technology L. This paper focused on the scope of the FPS standard to digital investments. Thus, it assumes that there is already an investment for jurisdictional issues.

due diligence standard, there are certain actions that the State may have to perform to comply with its obligation to grant FPS to an investor.

I. FULL PROTECTION AND SECURITY STANDARD

Having originated as a customary international law obligation arising out of the duty to protect aliens,[11] the FPS is a mechanism to protect foreign investments established under most IIAs.[12] While the wording in many treaties equates the FPS with the customary international law, or the minimum standard of treatment,[13] subsequent treaty drafting practice established an autonomous treaty standard that is distant from the one provided under customary international law. In other words, the FPS under customary international law constitutes the floor below which the protection of the standard cannot fall. Conversely, the qualified FPS standard, found in recent treaties, extends beyond customary international law obligations of States and offers additional protections and guarantees for foreign investors. The FPS standard protects the physical integrity of an investment against the use of force by States and third-party private actors.[14] Some investment tribunals have also included the protection of legal rights under the scope of the FPS standard.[15] This protection consists in the legal protection of an investor's substantive and procedural rights.[16] Moreover, the FPS standard

[11] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2020) 21 Vanderbilt J of Entertainment and Technology L

[12] David Collins 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) Journal of World Investment and Trade 2.

[13] Free Trade Agreement between the United States of America and the Republic of Colombia (adopted 22 November 2006, entered into force 15 May 2012) art. 10.5(2)

[14] *Cengiz İnşaat Sanayi ve Ticaret A.S v Libya*, ICC Case No. 21537/ZF/AYZ, Award of 7 November 2018, para 403.

[15] *Compañía de Aguas del Aconquija* (n 7)

[16] *Frontier Petroleum Services Ltd. v The Czech Republic*, PCA Case No. 2008-09, Award of 12 November 2010, para 263 ('It is apparent that the duty of protection and security extends to providing a legal framework that

includes an obligation of the States to prevent[17] and repress[18] the attacks against an investment.

The FPS standard comprehends an obligation of due diligence by the State.[19] The due diligence obligation is analyzed under a threshold of reasonableness. In this regard, 'reasonableness must be measured taking into consideration the State's means and resources and the general situation of the State'.[20] It is not a standard of strict liability,[21] it is an obligation of means and not of result.[22] Thus, with the FPS standard 'the investor has the right to expect that the State takes reasonable measures within its power to prevent wrongful injuries by third parties, and where such injuries have

offers legal protection to investors – including both substantive provisions to protect investments and appropriate procedures that enable investors to vindicate their rights'.).

[17] *AAPL* (n 8) 77.

[18] *Parkerings-Compagniet AS v. Republic of Lithuania*, ICSID Case No. ARB/05/8, Award of 11 September 2007, para 355; *Oxus Gold* (n 8) para 353.

[19] *Oxus Gold* (n 8) para 834; *AAPL* (n 8) 77.

[20] Rudolf Dolzer and Christoph Scheuer, *Principles of International Investment Law* (2nd ed) (OUP 2012) 162. ('Lack of resources to take appropriate action will not serve as an excuse for the host State'.)

[21] *AES Summit Generation Ltd and AES-Tisza Erömü Kft. v Republic of Hungary (II),* ICSID Case No. ARB/07/22, Award of 23 September 2010, para 13.3.2; *Pantechniki S.A. Contractors & Engineers v Republic of Albania*, ICSID Case No. ARB/07/21, Award of 31 July 2009 ('This suggests that due diligence is a modified objective standard - the host State must exercise the level of due diligence of a host State in its particular circumstances. In practice, tribunals will likely consider the State's level of development and stability as relevant circumstance in determining whether there has been due diligence. An investor investing in an area with endemic civil strife and poor governance cannot have the same expectation of physical security as one investing in London, New York or Tokyo'.).

[22] *Cengiz* (n 14) para 406 ('This obligation of vigilance does not grant an insurance against damage or a warranty that the property shall never be occupied or disturbed -it simply requires that the State apply reasonable means to protect foreign property'.); *AES Summit* (n 19) para 13.3.2. ('In the words of Brownlie, the duty is no more than to provide 'a reasonable measure of prevention which a well-administered government could be expected to exercise under similar circumstances'.).

already happened, to punish them.'[23]

Therefore, a breach of the FPS standard comprehends:

a. an illegal act that affects an investment;

b. lack of due diligence by the State in the prevention or repression of the illegal act;

c. the degree of the State responsibility takes into account the general means and resources of the State.

II. DIGITAL ENCONOMY UNDER THE FPS

How the Internet Works? With Infrastructure

On an everyday basis, people refer to internet information or documents as the 'cloud'. However, the internet is composed of physical infrastructure that costs time and money to build.[24] For the information to go from one device to another, it requires that this infrastructure is built and present in the host State.

When a device is connected to the internet and sends a message, this message starts from the initial device. Then, it is divided into smaller packages and sent through a router and modem.[25] The modem is connected through wires that are owned by an Internet Service Provider (ISP). The wires transport the information to an internet hub that then connects to the

[23] *Oxus Gold* (n 8) para 834.

[24] Adam Satarino, 'How the Internet Travels Across Oceans' *The New York Times* (New York, 10 March 2019) ("People think that data is in the cloud, but it's not' […] 'It's in the ocean".); 'Internet Health Report 2019' <https://internethealthreport.org/2019/> accessed 15 January 2022.

[25] HP, 'How Does the Internet Work?' <*https://www.hp.com/us-en/shop/tech-takes/how-does-the-internet-work*> accessed 15 January 2022.

ISP of the receiver and to the router of the receiver.

Thus, for the digital economy to operate, it needs infrastructure, such as cellular towers, routers, servers, internet hubs, fiber optic cables, etc. This infrastructure may be located in the country where a company is located as new companies are offering internet through satellite. However, if the State does not have at least some internet infrastructure, there is no internet and no digital economy.

Even though this infrastructure is within a State and it has been expressed that the internet is a mechanism to exercise human rights,[26] almost all of the internet infrastructure is owned by private companies.[27] Therefore, most of the responsibility for the internet, connectivity, and its security is based on contracts between a contractor, a provider, and a client. However, because an investor contributes money and assets to the host economy, it enjoys FPS guarantees, in this case, the digital security of the assets.

Digital assets and the definition of 'investment'

Before discussing the substantive law implications of the violation of the FPS standard, it is important to first understand whether the digital assets of the companies relying on internet infrastructure constitute covered 'investments' under the applicable IIA and the ICSID convention.

A good starting point for this analysis would be the definition of the 'investment' found in the applicable IIA. As the international investment protection regime comprises around 2700 BITs, which were concluded in different periods and by different actors, the definition of 'investment' varies from treaty to treaty. Both investment arbitration tribunals and the scholarly community have differing views on the definition of 'investment' in international investment law.

[26] United National General Assembly, Human Rights Council, A/HCR/47/L.22 (7 July 2021).

[27] Alexandra Twin, 'Internet Service Provider (ISP)' *Investopedia* <https://*www.investopedia.com/terms/i/isp.asp*> accessed 15 January 2022.

Most of the IIAs[28] provide a description of the types of assets that are considered protected 'investments.' While some IIAs provide for a non-exhaustive list of assets,[29] others provide for an exhaustive list of assets,[30] by limiting the coverage of the IIAs to the listed types of assets only. A typical definition of 'investment' in the IIA includes movable and immovable property, IP rights, contractual rights, shares, etc.[31] Some types of digital assets, such as multimedia and IP, could fall under the listed categories but as the majority of the IIAs were drafted in the nineties, their definitions lack any reference to digital or other types of innovative assets. If the definition in the IIAs contains a limited list of assets that can constitute 'investment,' it is likely that the tribunals would not extend the protection of the IIA to the digital assets that are to be harmed by a cyberattack. Thus, it still shall be argued before the arbitral tribunal that digital assets, such as software and data, would fall under the protection of an IIA with a non-exhaustive list of assets provided in the definition of the 'investment.'

Even if the investment arbitration tribunal finds that the non-exhaustive list extends to digital assets, parties willing to opt for an ICSID arbitration, still need to prove that the digital assets also fall under the coverage of the ICSID convention. While Article 25 of the ICSID convention does not provide for a definition of investment, some investment arbitral tribunals follow the so-called Salini test[32] to identify whether a certain type of asset constitutes 'investment' or not. Other investment tribunals have rejected the application of the Salini criteria, by only considering the definition of investment in the

[28] 'International Investment Agreements Navigator' (*Investment Policy Hub*) <International Investment Agreements Navigator> accessed 24 August 2022

[29] Investment Protection Agreement between the European Union and its Member States, of the one part, and the Socialist Republic of Viet Nam of the other part, adopted on 30 June 2019, Article 1.2(h)

[30] Foreign Investment Promotion and Protection Agreement between Canada and Hong Kong, adopted on 10 February 2016, Article 1

[31] The Energy Charter Treaty, adopted on 17 December 1994, Article 1. 6.

[32] Salini Costruttori S.p.A. and Italstrade S.p.A. v. Kingdom of Morocco, ICSID Case No. ARB/00/4, Decision on Jurisdiction, 23 July 2001, para. 52

IIA and the will of the contracting States.[33]

To be considered an 'investment' under the Salini test, the investment shall have a certain duration, include some assumption of risk, involve a contribution of capital, and—which is a later modification by the Fedax tribunal[34]—make a contribution to the host State's economy. In essence, the Salini test originates from what the 'investment' is understood in economic terminology and provides objective criteria for defining what can be considered as an investment by arbitral tribunals.[35] In other words, Salini criteria shuts the doors before the variety of claims that could involve merely commercial transactions and which would unnecessarily extend the scope of the FDI protection agreed upon between the contracting States.

In the case of digital assets of the company affected by a cyberattack, if the tribunals follow the strict application of the Salini criteria, claimants will be required to prove that the investment in question meets all four criteria of the Salini test. For digital assets, such as data or cryptocurrencies, it might be difficult to provide evidence of contribution to the host State economy or else defined duration.

To add another dimension of complexity, for benefiting from the protection of the IIAs, the assets must be located in the territory of the host economy. Such requirements could be found in the definition of the 'investment';[36]and 'investor'[37] found in the IIAs; as well as standalone provisions providing that

[33] Air Canada v. Bolivarian Republic of Venezuela, ICSID Case No. ARB(AF)/17/1, Award, 13 September 2021, para. 293

[34] FEDAX N.V. v. The Republic of Venezuela, ICSID Case No. ARB/96/3, Decision on Objections to Jurisdiction, 11 July 1997, para. 43

[35] Rudolf Dolzer and Christoph Scheuer, Principles of International Investment Law (2nd ed) (OUP 2012) 158.

[36] Agreement between Australia and the Oriental Republic of Uruguay on the Promotion and Protection of Investments (2019), adopted on 5 April 2019, Art. 1(1)a

[37] Agreement between Japan and the Kingdom of Morocco for the Promotion and Protection of Investment, adopted on 8 January 2020, Art 1(b)(ii)

the provisions of the IIA apply only in the territory of the host State.[38] If the territoriality requirement is left undefined in the IIA, article 29 of the VCLT would cover the gap as it provides that 'the treaty is binding upon each party in respect of its entire territory' given that the parties have not agreed otherwise.[39] The territoriality requirement is specifically cumbersome, given that the digital assets, such as data or non-fungible tokens are hanging somewhere around the internet and not necessarily in the host State's territory.

In sum, whether the tribunal will have jurisdiction to hear the case, will depend on the applicable IIA. If the IIA provides a non-exhaustive list for the definition of investment, the non-ICSID investment arbitration tribunals are likely to consider the case arising out of cybersecurity breaches that targets digital assets. In the case of an ICSID arbitration, some digital assets could fall outside the protection of the ICSID convention due to the application of the Salini criteria. In all events, the affected assets of the company shall be located in the territory of the host State to benefit from the protection of the IIAs.

Cyber Protection within FPS

Cyberattacks such as denial of service (DoS) or distributed denial of service (DDoS) can cause the company's network to disfunction,[40] data exfiltration can expose sensitive customer data,[41] and certain types of malware can

[38] The Energy Charter Treaty, adopted on 17 December 1994, Article 26. 1.

[39] Vienna Convention on the Law of Treaties (1969) , adopted on 23 May 1969, Article 29 .

[40] K Muthamil Sudar and others, 'Analysis of Cyberattacks and its Detection Mechanisms' (2020) 2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN) 12-16.

[41] Ioannis Agrafiotis and others, 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate' (2018) 4(1) J of Cybersecurity 1–15.

cripple computer infrastructure.[42] Depending on the type and purpose of the cyber-intervention the harm can be caused to the data, software, or the company's critical devices (hardware). Given the physical/non-physical divide within the scholarly community and the decisions of investment tribunals,[43] we will assess the type of assets towards physical and non-physical approaches.

As it is uncontested that the FPS includes the physical security of the investment by either school of thought, no sophisticated analysis will be required to assume that investment tribunals will consider attacks targeted on the hardware assets of the companies to fall within the scope of FPS protection. In other words, if the attack targets the device of the company, by making it inoperative or damaging it, the physical protection of FPS extends to that investor. However, the analysis may be more complex with intangible assets such as data, cryptocurrencies, and software.

In the Peter Allard case, the question before the tribunal was whether the environmental damage caused to the investment could be assessed as a physical attack.[44] While the tribunal did not find a violation of the FPS standard in that case, the tribunal's analysis suggested that the physical harm does not need to emanate from a physical attack only. Similarly, when a hacker intervenes and affects a company, the malware needs to be physically written on the company's server or a storage device. In the same line with the Peter Allard case, the malware infects software or steals data from a physical device like a server or data storage. Thus, hacking can be considered as a physical process that eventually affects physical infrastructure even under the strictly physical protection view.

Alternatively, the company's intangible assets such as software and data

[42] Arjun Dixit, 'Risk Assessment: Identifying Kinds of Harm and Extent of the Impact of Cyberattacks' (2016) 1-4.

[43] Christoph Schreuer, *'Full Protection and Security'* Journal of International Dispute Settlement, Vol 1 No 2 (2010) 353–369.

[44] *Peter A. Allard v The Government of Barbados*, PCA Case No. 2012-06, Award of 27 June 2016, para 252.

can fall under legal and commercial FPS protection. The extension of the FPS protection to legal or commercial security will depend on the wording of the respective treaty[45] as well as the views of the tribunal entertaining the alleged FPS breach. As an example, some recently concluded IIAs specifically provide for 'legal' protection in the FPS section. Other IIA wording examples include 'juridical security',[46] 'legal protection',[47] and 'de jure'[48] protection. Investment tribunals also considered the word 'full' in the 'qualified' FPS standard to extend the standard to include legal and commercial protection along with physical protection. Even absent specific wording in the BIT, tribunals have considered the FPS to protect 'the physical integrity of an investment against interference by use of force'[49] and to include the stability of 'legal and commercial environment.'[50] To address this divide between physical/non-physical protection and add certainty, some recently concluded treaties such as the 2019 EU-Vietnam Investment Protection Agreement, [51] specifically restrict the protection to 'physical' aspects only, by limiting the possible protection of some types of digital assets under FPS.

As the IP rights of the company over the software or ownership of information

[45] Thomas Snider and Nair Aishwarya, 'A Trap for the Unwary: Delineating Physical and Legal Protection under Full Protection and Security Clauses' (2020) 9(1) Indian J Arb L 24.

[46] Treaty between the Federal Republic of Germany and the Argentine Republic on the Encouragement and Reciprocal Protection of Investments, adopted on 9 April 1991, Article 4.1.

[47] Agreement Between the Government of the Russian Federation and the Cabinet of Ministers of the Ukraine on the Encouragement and Mutual Protection of Investments, adopted on 27 November 1998, Article 2.2.

[48] Convention Between the Belgo-Luxembourg Economic Union and the Republic of Burundi Concerning the Reciprocal Promotion and Protection of Investments, adopted on 13 April 1989, Article 3.2.

[49] *UAB E energija (Lithuania) v Republic of Latvia*, ICSID Case No. ARB/12/33, Award of 22 December 2017, para 840.

[50] *ibid* 840.

[51] Investment Protection Agreement between the European Union and its Member States, of the one part, and the Socialist Republic of Viet Nam of the other part, adopted on 30 June 2019, Art 2.5 (5)

will require legal and commercial protection, the cyber-intervention targeting those will constitute an FPS violation. That said, intangible assets of the company, such as data and software, will likely fall under legal or commercial protection of FPS under 'beyond physical protection' views.

III. DUE DILIGENCE STANDARD

The due diligence obligation of the state needs to be analyzed taking into account the actual possibilities that the State had to prevent, solve and repress the attack.[52] The tribunal in Saluka held that 'the standard obliges the host State to adopt all reasonable measures to protect assets and property from attacks'.[53] As stated above, the concept of due diligence is interpreted through a reasonableness test being 'paramount in the analysis of investment tribunals'.[54] The doctrine has asserted that 'States are not normally responsible for the wrongful acts of private individuals in their territory as long as reasonable diligence is used in attempting to prevent the occurrence of recurrence of such wrongs'.[55]

[52] Robert Landicho and Levon Golendukhin, Panel on 'Full Protection and 'Cyber' Security in Ian A. Laird and others (eds), *Investment Treaty Arbitration and International Law* Vol 11, 152 (Juris 2018) ('Mr. [Levon] Golendukhin. On the first question [on what is required from the State], I would add that one document that's being worked on is the Tallin Manual on cyber-security. That's a set of non-binding legal guidelines, containing measures that can be taken to deter that risk at the State level, too. As for the nuance about comfort with disclosure […] in the circumstance where the State offers protection, the investor relies on it and entrusts the requisite disclosures to the State, but then the State remains sort of indifferent and does not follow through, that may make a stronger due-diligence claim'.).

[53] *Saluka.* (n 6) 484.

[54] Markus Burgstaller and Giorgio Risso, 'Due Diligence in International Investment Law' (2021) in J of Intl Arb, Vol 38 No 6 697, 718.

[55] *ibid.*

Prevention

Most of the internet infrastructure is privately owned. In order to comply with its duty of prevention, the State could request the ISPs to comply with the current best practices in cybersecurity for its clients not to be affected by hackers.

One of these initiatives has been taken by the European Union (EU). The EU has created a cybersecurity certification framework that has the function to validate the cybersecurity of products in the new economy of the internet of things.[56]

Moreover, a State needs to prevent cyber-intervention by enacting civil and criminal laws that will deter people from cyber-intervening a company because of possible criminal sanctions.[57] Besides this, it is possible that a host State does not have a real possibility to prevent a hack from a private hacker located in the host State.

However, if the State learns that a group of hackers is planning to hack a company, then the host State may have a duty to prevent such attacks by arresting the criminals and notifying the company. Moreover, most of the prevention would have to be done by the company itself by keeping its server, software, and infrastructure with best cyber practices, such as having antivirus updates and good security protocols.

Another fundamental aspect of the impact of cybersecurity in the FPS

[56] Rohan Massey, Kevin Angle et al, 'Cyber Trends and Investigations in Europe: A Practitioner's Perspective 'in Benjamin A Powell and Jason C Chipman (eds) *The Guide to Cyber Investigations* (2nd edn) 162 (Law Business Research 2021) ('The tailored certification schemes established categories of information and communication technologies (ICT) products, processes and services only once and obtain certificates that are valid across the EU. The EU-wide cyber-security certification framework enables companies in the ICT sector to demonstrate that their products and services meet one of three security standards (basic, substantial or high). The intention of the new rules is to improve trust for consumers, as they can choose between products (such as internet of things devices) that are cyber-secure'.).

[57] Chaisse (n 11) 549.

standard and in a possible quantification of damages is the level of due diligence that the investor has regarding its own cyber-security.[58] This is analyzed under the due diligence that is required by the investor. Investment tribunals have considered the due diligence of investors when claiming state responsibility.[59] Within the investors' due diligence, tribunals have included the business risk.[60] On this point, '[w]ith regard to business risk, arbitral tribunals tend to deny investment protection to investors that elected not to investigate and assess the risk relating to their investment'.[61] The current standard for a tribunal to take contributory negligence of an investor into account is that the 'contributory negligence must be significant and material as to trigger damages reduction'.[62] How material the investor's contributory negligence to a cyber-intervention to its digital security will depend on the facts of the case.

Digital enterprises are constantly exposed to cybersecurity threats. While

[58] UN International Law Committee's Draft on Responsibility of States for Internationally Wrongful Conduct, article 39 and commentary; José Ignacio García Cueto, '38. Contributory Negligence and Reduction of Damages in Arbitration: Let's Throw A Dice' in Carlos Gonzalez Bueno (ed), 40 under 40 International Arbitration (2021) 613, 616 ('Traditionally, the concept of contributory negligence has been assimilated to the notions of inadequate assessment of risk, or in cases where a victim has evidenced an understanding of a dangerous situation and voluntarily accepted it. At first […] the conduct of the victim was an exonerating circumstance […] which was then modified by the International Law Commission of the United Nations, retaining contributory negligence as a circumstance attenuating State's liability').

[59] *Alex Genin, Eastern Credit Ltd, Inc. and A.S. Baltoil v. The Republic of Estonia*, ICSID Case No. ARB/99/2, Award of 25 June 2001, para 345; *MTD Equity Sdn. Bhd. & MTD Chile S.A. v. Republic of Chile*, ICSID Case No. ARB/01/7, Award of 25 May 2004, paras 242-243.

[60] Burgstaller (n 54) 704.

[61] *ibid.*

[62] García Cueto (n 58) 625; *Caratube International Oil Company LLP and Devincci Salah Hourani v Republic of Kazakhstan (II),* ICSID Case No ARB/13/13, Award of 27 September 2017, para 1192; *Occidental Petroleum Corp and Occidental Exploration and Production Company v Republic of Ecuador (II),* ICSID Case No. ARB/06/11, Award of 5 October 2012, para 670; *Gemplus, S.A., SLP, S.A., and Gemplus Industrial S.A. de C.V. v United Mexican States*, ICSID Case No. ARB(AF)/04/3, Award of 16 June 2010, para 11.12.

they can choose not to be exposed to such risks, it might make their functioning economically unfeasible due to high cybersecurity costs and resources concerned. That said, on occasions, companies willingly choose to be exposed to cyber threats which may eventually allow malicious actors and cyber criminals to succeed.[63] On top of that, cybersecurity negligence plays an important role as well, as a vivid example being small and medium-sized enterprises (SMEs) approaching cybersecurity concerns not seriously.[64] As investments tribunals may require the investor to exercise minimum diligence in protecting its own property,[65] it becomes particularly important to determine the reasonable standard of cybersecurity care.[66]

While, as of the date of writing, there is no case where the investment tribunals analyzed the reasonable standard of cybersecurity care in the context of FPS violation, it is likely that the future tribunals will echo the domestic courts' analysis. When defining the reasonable standard, absent specific legislation, the US courts heavily relied on industry report recommendations[67] and on the 2014 National Institute of Standards and Technology (NIST) Cybersecurity Framework.[68]

The EU Data Protection Directive 95/46/EC defines 'sufficient guarantees in respect of technical and organizational security measures'[69] as reasonable.

---

[63] Shinichi Kamiya and others, 'Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms' (2021) 139(3) J of Financial Economics 719-749.

[64] Malgorzata Nycz and others, 'The cyber security in SMEs in Poland and Tanzania' (2015) (IEEE) 7th International Conference on Electronics, Computers and Artificial Intelligence AE-27.

[65] Sebastián Mantilla Blanco, *Full Protection and Security in International Investment Law* (Springer 2019) 475.

[66] Scott J Shackelford and others, 'Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices' (2015) Winter (1) Tex Int'l LJ 305-357.

[67] *ibid.*

[68] Framework for Improving Critical Infrastructure Cybersecurity Version 10 National Institute of Standards and Technology (12 February 2014).

[69] Article 17.2, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on

In all likelihood, exposing passwords, failure to update the operating or antivirus system and failure to implement an intrusion detection (ID) system[70] to monitor security breaches will fall below the standard of reasonable care.[71] The standard will also fluctuate in relation to the industry where the company operates: financial institutions will certainly bear stricter cybersecurity obligations compared to businesses in the food industry with a mere online presence. It is also worth noting that the reasonable standard of cybersecurity care is rather dynamic than static as the cybersecurity practices and types of cyber threats evolve hand-in-hand and will likely keep changing in the years to come.[72]

Scholars have argued that it would be difficult for a tribunal to find a State responsible of a breach of FPS due to a cyber-attack to a digital investment because the digital infrastructure in one country is mainly operated by private companies.[73] Moreover, this sector of the scholarship argues that in case there is a cyber-attack, a State may avoid possible responsibility arguing the exception national security.[74] Nevertheless, according to the FPS standard, States have an obligation of prevention and repression measured according to its national circumstance and national security exceptions are not self-judging clauses. To stop cyber-intervention, most likely the State would have to intervene the communications and thus, the owners of the internet infrastructure, or the ISPs.[75] Even though, some jurisdictions have legislated that they will have the power to intercept[76] the communication and service

---

the protection of individuals with regard to the processing of personal data and on the free movement of such data

[70] *LabMD, Inc. v FTC*, 891 F.3d 1286 (11th Cir. 2018).

[71] Lawrence J Trautman and Peter C Ormerod, 'Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach' (2017) 66 Am U L Rev 1231.

[72] Shackelford (n 54).

[73] Collins (n 12) 238.

[74] *ibid.*

[75] Ian Walden, *Computer Crimes and Digital Investigations* (2nd edn) (OUP 2016) 208.

[76] ibid 243 ("The term 'intercept capability' is traditionally used in reference to the capture of data, content,

providers that operate within their territory[77], if the State illegally interferes with the operations of the ISP, by arguing a national security exception,[78] and causes damage to the ISP, then the ISP may file a claim against the state because of illegal intervention to its business. This is an element that the States should take into account.

On the other hand, other scholars have indicated that a State may breach the standard of FPS in relation to digital assets due to their duty of prevention and repression. Both schools of thought agree that to have legal certainty in this type of investment, States should expressly regulate the protection of digital assets in their IIAs to provide guidance to investment tribunals on how to recognize possible breaches in relation to digital assets.[79]

Repression

In Parkerings v Lithuania, the tribunal asserted that within the FPS standard the host state has to restore the situation and punish the author of the crime.[80] Between the duty of prevention and repression is the situation in which several attacks have been already conducted against the investor and more are expected to come. In this scenario, the state would have the

and associated communications data, 'in transmission".).

[77] ibid 241 ('Most jurisdictions now explicitly address the issue of intercept capability […]'.). The author gives the example of the United Kingdom, Germany, The Netherlands, and Australia.

[78] It has been asserted that national security clauses in IIAs are not self-judging clauses. *Deutsche Telekom AG v The Republic of India*, PCA Case No. 2014-10, Interim Award of 13 December 2017, para 235, 239 ('In respect of the existence of essential security interests, the Tribunal accepts that a degree of deference is owed to a State's assessment. However, such deference cannot be unlimited […] To assess the necessity of the measures to safeguard the State's essential security interests, the Tribunal will thus determine whether the measure was principally targeted to protect the essential security interests at stake and was objectively required in order to achieve that protection, taking into account whether the State had reasonable alternatives, less in conflict or more compliant with its international obligations'.).

[79] Chaisse (n 11) 587-589; Collins (n 12) 242-243.

[80] *Parkerings* (n 18) 355.

responsibility to repress the previous attacks and prevent new ones.[81]

After a hack is conducted, the state would need to comply with its duty to repress the situation and to protect the affected company. To fulfill this duty, a state needs to enforce its criminal laws against cyber-crimes.[82] The host State must use its best efforts under the due diligence standard to investigate the situation and provide a trial against the hacker to comply with its repression obligation. This duty of repression may include a scenario where the state contacts and sends requests to communication service providers like email providers or social media platforms to collect information regarding the intervention.[83] If possible, the state must also try to restore the

[81] Robert Landicho and Levon Golendukhin, Panel on 'Full Protection and 'Cyber' Security in Ian A. Laird and others (eds), *Investment Treaty Arbitration and International Law* Vol. 11 (Juris 2018) 155 ('Mr. [George] Burn […] But, in a scenario qua Wena Hotels and Egypt, where there is a sequence of events, and the State at some point in the sequence definitely becomes notified, definitely understands that there are some attacks, and then fails to act, that would answer your point. […] Dr. [Todd] Weiler: I'm actually not even sure that there is a duty to prevent – when you really plod through the logic of that notion, isn't protection and security always an enforcement issue?').

[82] Levon Golendukhin, 'Reference to Intellectual Property Treaty Norms in Full Protection and Security and Fair and Equitable Treatment Claims' in Ian A. Laird and others (eds), *Investment Treaty Arbitration and International Law* Vol 11, 108 (Juris 2018) ('The proper analogy for physical protection is the State's policing obligation under the physical protection branch of due diligence. That is, the State must exercise due diligence in enforcing its penal laws and investors can expect a certain degree of protection from acts punishable by law. Likewise, as statements by the State that certain conduct is not acceptable within the territory of that host State, international penal norms may support legitimate expectations that their investments be relatively free, or at least have protection from, harmful conduct by third parties'.).

[83] Walden (n 74) 208 ('There are also interests of communication service providers (CSPs), the intermediaries that build and/or operate the networks and communication services through which data is communicated. Law enforcement agencies will be looking towards such intermediaries to assist them in the investigative process, either in terms of gathering data transmitted by the suspects themselves or by providing data generated by the CSPs about the communication activities of suspects. Such assistance may be provided on either a voluntary or mandatory basis, which also raises important legal issues for consideration'.). Several internet companies provide in their terms of use that they may need to submit information of a user upon a

situation as it was previous to the attack on the company.

To assess a government response[84] to a possible violation of FPS, an investment tribunal considered that the investor did not file a criminal complaint against the aggressor in order for the state to start its investigations.[85] On this point, while it is common practice for companies to conduct their own investigations, they probably will face a wall when they have to collect data held by a third party without government intervention.[86] This makes government intervention more important, as companies could not resolve or fix the situation beyond their internal systems.

Further, on occasions, companies are subject to a ransom attack where the criminals encrypt the systems and documents of a company unless a ransom or a sum of money (usually in cryptocurrency) is transferred to them.[87] When an investor is victim of these attacks within the territory of the

government request, *Google* Terms of Service <https://policies.google.com/terms/information-requests?hl=en-US> accessed 16 January 2022; *Google* Transparency Report - Global Requests for User Information <https://transparencyreport.google.com/user-data/overview?hl=en> accessed 15 January 2022.

[84] Jeswald W. Salacuse, *The Law of Investment Treaties* (2nd edn) (OUP 2015) 235 ('A finding of liability for failure to provide promised protection and security is necessarily fact driven. It must be based on the details of the threat as well as the government's response to that threat'.).

[8585] *GEA Group Aktiengesellschaft v Ukraine*, ICSID Case No. ARB/08/16, Award of 31 March 2011, paras 247-249.

[86] Michael Drury and Julian Hayes, 'Investigations in England and Wales: A Practitioners' Perspective' in Benjamin A Powell and Jason C Chipman (eds) *The Guide to Cyber Investigations* (2nd edn) 181 (Law Business Research 2021) ('Without being granted voluntary access to third-party data, those undertaking private investigations will need to seek the assistance of the courts in the form of *Norwhich Pharmacal* orders, obliging third parties caught up in wrongdoing to disclose the identity of perpetrators of cybercrime. However, seeking such orders may still be costly and time-consuming. Alternatively, private investigators may seek the assistance of the relevant authorities, likely to be the NCA (subject always to the NCA having a necessary criminal justice justification for acting)'.).

[87] McAfee, 'What is Ransomware?' <*https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware.html*>

host state, the host State's help becomes vital for the company to reacquire control of its data. The government may help to identify perpetrators.[88] This is important as the company may consider whether to concede to the criminal's demands and pay the criminals to recover its data and restore its operations as soon as possible and some countries have criminal penalties and strict liability penalties against the payment of money to sanctioned individuals.[89]

accessed 16 January 2022 ('Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or apps. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers, and can thus quickly paralyze an entire organization. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expenses for businesses and governmental organizations'.).

[88] Whether the investor may claim the host State the ransom paid may be a subject open to debate. Ryan Fayhee and Tyler Grove, 'Ransomware Attacks and Responses' in Benjamin A Powell and Jason C Chipman (eds) *The Guide to Cyber Investigations* (2nd edn) 118 ('Contemporaneously with gathering information and screening, a ransomware victim should consider notifying law enforcement and OFAC of the attack. Among other benefits, law enforcement, who will have access to non-public information, may be able to assist with identifying the likely perpetrators of the attack, which will in turn be able to better inform the victim of whether payment is prohibited. Timely notice to law enforcement Is also viewed favourably by OFAC in making enforcement decisions, in the event a ransom is paid and it is later discovered that the attackers are subject to sanctions. […] to be considered 'voluntary', a self-disclosure must be submitted before OFAC opens its own investigation into a transaction'.).

[89] Ryan Fayhee and Tyler Grove, 'Ransomware Attacks and Responses' in Benjamin A Powell and Jason C Chipman (eds) *The Guide to Cyber Investigations* (2nd edn) 113 ('Despite the increasing prevalence of ransomware attacks and the growing number of victims, responding to a ransom demand is fraught with many pitfalls. Businesses and their counsel should understand the basic legal frameworks that underlie these risks before deciding on how to respond to a ransom demand. Some of the most common legal risks if ransom is paid include those from transacting with a party subject to sanctions, making a payment to a terrorist organization, as well as failing to make required Suspicious Activity Reports (SARs)'.).

CONCLUSION

Over the past several decades, organizations have dramatically transformed the way they operate. Digital transformation has affected businesses across all sectors and reached even the most remote corners of the globe, bringing both new opportunities and digital challenges for the businesses in the new digital age. In this new reality, cyber threats and cyber-interventions continue to remain as challenges which companies struggle with the most.

This article demonstrated that the digital economy and global foreign investment can rely on broadly defined standards of protection in IIAs such as FPS for the states to enact relevant legislation, prosecute and sanction the internal actors involved in cyber-crimes and cyber-interventions. It has been established that because of the characteristics of the FPS standard, its scope covers the digital security of investments regardless if those are observed under physical, legal and commercial protection views. Moreover, as different sectors of the scholarship have recommended, States should take into account the growth of the digital economy at the moment of negotiating and drafting new IIAs. In this way, investors, States, and adjudicators will have clearer rules in order to determine whether there was a treaty violation regarding the digital economy.

Further, this paper demonstrated that to comply with its obligation to provide FPS, the States and investors must exercise proper due diligence and that States have a duty of prevention and repression to protect the digital security of foreign investors in case their assets have become targets of cyber-intervention.

****

International commercial mediation system in ADR and Its Enlightenment to China International Commercial Court

By Liu Yanna & Zhao Jia & Yang Qinyun

Dr. Liu Yanna presently working as a faculty member of Humanity and Law School of Yanshan University. She served as associate professor and mainly engaged in the research in international law realm. She has published more than 20 articles on various legal journals and hosted many research projects on different level.

Zhao Jia is a master student in School of Humanity and Law of Yanshan University. Her major is Law and She mainly engaged in the research in international law realm.

Yang Qinyun is a LLB from East China University of Political Science and Law, now studying LLM in Yanshan University. She assists in many research projects of the university.

ABSTRACT

Mediation, as the most important form of ADR, has gradually emerged in the international commercial field. There are also a few international commercial mediation rules that have been generally accepted and recognised on the international stage, providing a blueprint for international commercial mediation in various countries. At the same time, mediators as the main body of mediation activities, international countries also adopt different judicial practices to regulate the activities of mediators. China's international commercial courts also attach great importance to the role of mediation in resolving disputes, and the rules issued have detailed provisions on commercial mediation. The international commercial mediation system in ADR provides a direction for the improvement of the mediation system of China's international commercial courts. First, formulate a unified basic law of international commercial mediation; The second is to establish the qualification certification system for mediators.

INTRODUCTION

Mediation, as the most important dispute resolution method in alternative dispute resolution (ADR) mechanism, has an advantage of fully respecting the parties' autonomy and adopting a non confrontational dispute resolution method. This advantage also fully conforms to the internal spirit of the current international commercial dispute resolution. Compared with the traditional dispute resolution method of litigation and arbitration, it has great potential in the international commercial field.

Overview of international commercial mediation system

1.1 International rules on international commercial mediation

At present, there are two authoritative legal provisions on international commercial mediation in the world: one is the UNCITRAL Model Law on

International Commercial Mediation and International Settlement Agreements Resulting from Mediation, 2018 (hereinafter referred to as the Model Law), and the other is the United Nations Convention on International Settlement Agreements Resulting from Mediation, 2019 (hereinafter referred to as the Singapore Convention). According to the above legal provisions, two criteria are taken into consideration for the definition of 'international' in international commercial disputes. The first criteria is, from a subjective view, adopting the place of the business standard to determine. The second criteria is comprehensively considered the disputants' place of businesses, place where agreement is executed and the closest place that was related to the disputes, to determine whether the dispute involve more than one country. As for the concept of "commercial", the commercial subjects are mainly equal natural persons and legal persons, and their possible business conduct is also comprehensive. For example, according to the provisions of the Model Law, all matters with commercial nature can be defined as commercial acts. At the same time, the Model Law also provides for the concept of mediation, excluding the settlement cases promoted by judges or arbitrators in judicial or arbitration proceedings.

As for the procedural rules of international commercial mediation, according to the current legal documents of international commercial mediation, the general content of the procedural rules of mediation mainly includes the procedural provisions, such as the starting conditions of mediation, the selection and appointment of mediators, the mode of mediation, the termination and procedure of mediation, and other related matters. There are many mature mediation procedure rules in the world, such as the Singapore International Mediation Centre (SIMC) Mediation Rules which specifies in detail the application of the rules, the initiation of procedures, mediation agreements, the appointment of mediators, fees, mediation methods and fees.

1.2 Mediator system in international commercial mediation

The mediation level and mediation skills of mediators affect the outcome of mediation cases all the time. A qualified mediator should have a high level

of listening and communication skills and be able to weigh the interests of all parties in a timely manner. For mediators of international commercial mediation, they need to have skilled foreign communication skills, good learning and understanding skills, so as to meet the needs of parties with different international backgrounds. All these put forward higher requirements for the qualifications of mediators. For purpose of building a mature team of mediators, many countries have adopted a number of judicial practices. In order to ensure the mediation quality of its mediators, the United States has adopted the mediator certification system. The so-called certification system refers to that the personnel who have passed the certification of relevant institutions are qualified to act as mediators, but it does not prohibit the personnel who have not yet obtained the qualification certification from acting as mediators. The institution responsible for the qualification certification of mediators is the Qualification Committee under the American Association of dispute resolution experts, which is responsible for the review of the qualification certification of mediators and arbitrators. In addition to the United States, Hong Kong has also conducted fruitful exploration: in August 2012, the Hong Kong Mediation Accreditation Association Limited (HKMAAL) was established. The company aims to establish a unified certification mechanism for mediators in Hong Kong, so that the quality of mediators is gradually closer to standardization. In addition, the company also sets standards for mediation training courses in Hong Kong, certifies those who meet the standards, and promotes Hong Kong's mediation culture. [1]

2. China International Commercial Court Mediation Rules

China International Commercial Court (CICC) aims to build a "one-stop" international commercial dispute settlement platform with the court as the core. The parties may freely choose mediation, arbitration and litigation to

[1] HKMAAL.Mediation in Hong Kong[EB/OL].(2018-06-26)[2022-02-14]. http://www.hkmaal.org.hk /en/MediationinHongKong.php.

resolve disputes. In order to provide a basis for the mediation activities of the international commercial court, the court has also issued a series of legal documents. According to these legal documents, the mediation rules of CICC are as follows.

First, the subject of mediation. According to the provisions of the court rules, the CICC may entrust the mediation to the international commercial advisory committee or the selected international commercial mediation institution with the consent of the parties. The Expert Committee is an innovative institution of CICC. Its main functions are to preside over mediation and provide legal advice. As for international commercial mediation institutions, there are two mediation institutions included in the "one-stop" international commercial dispute settlement mechanism:China Council for the Promotion of International Trade Mediation Centre (CCPITMC) and the Shanghai Commercial Mediation centre (SCMC). Both of these two institutions have rich experience in international commercial mediation, and have conducted exchanges and cooperation with mediation institutions in other countries, which are fully internationalized.[2]

Regarding the procedures for mediation. After accepting a case, the China International Commercial Court ("CICC") first needs to solicit the parties' opinions and enquire if the parties agree to mediate the dispute. If the parties agree to resolve the dispute through mediation, the Case Management Office of the CICC will serve the relevant documents to the defendant and hold a case management meeting between the parties and the entrusted agent to discuss and decide on the procedure for the pre-trial mediation and determine the time limit for mediation. The parties may choose the International Commercial Expert Committee or an international commercial mediation institute to conduct the mediation. Where mediation is conducted by the International Commercial Expert Committee, the mediation work shall be carried out on a voluntary basis, the mediation procedures shall be kept

[2] 中国国际贸易促进委员会调解中心[EB/OL].[2022-02-08] https://baike.baidu.com/item/%E4%B8%AD%E5%9B%BD%E5%9B%BD%E9%99%85%E8%B4%B8%E6%98%93%E4%BF%83%E8%BF%9B%E5%A7%94%E5%91%98%E4%BC%9A%E8%B0%83%E8%A7%

confidential, and the mediation process shall be recorded and signed by the parties and the mediator. In the event of termination of the mediation, the mediation needs to be terminated in time. If mediation is concluded under the auspices of the International Commercial expert committee or the international commercial mediation organisation, the office of the International Commercial Expert Committee or the international commercial mediation institute shall submit the mediation results to the case management office, and CICC shall review and issue a conciliation statement in accordance with the law; if requested by the parties, CICC may also issue a judgment. If a settlement agreement cannot be reached between the parties, the office of the International Commercial Expert Committee or the international Commercial mediation institute shall send the "Mediation Form" and related materials to the case management office. The dispute will then be submitted for litigation. [3]

Although CICC has drafted a detailed provision for the mediation procedure. However, there are still a few areas that could be improved on.

First, the mediation procedure in CICC lacks a unified basic law on international commercial mediation. Through the analysis of the court rules based on mediation, it can be found that the lack of the Basic Law on International Commercial Mediation has caused China's international commercial mediation to fall into an unpredictable situation.First of all, China does not have an international commercial mediation law. The only law related to mediation, The " People's Mediation Law of the People's Republic of China " does not apply to mediation presided by expert committees or other mediation institutes. Secondly, although most mediation institutes have formulated their own mediation rules, but the provisions of the mediation rules are different, which is not suitable for the standardisation of international commercial mediation.Finally, without the Basic Law on International Commercial Mediation, parties will have no reference basis

[3] 'Working Rules of the International Commercial Expert Committee of the Supreme People's Court (For Trial Implementation)' (Supreme Court of China, 5 Dec 2018) <https://cicc.court.gov.cn/html/1/219/208/210/1146.html> accessed 24 August 2022

when negotiating and determining the mediation rules applicable to the dispute. Furthermore, the parties' independent determination of the rules will be time-consuming and laborious. An authoritative mediation rule is essential for the success of international commercial mediation.[4] Without a unified basic Law on international commercial mediation, mediation under the auspices of the International Commercial Expert Committee and other mediation institutes will lack uniform mediation rules that can be invoked. Moreover, courts will not have a unified review standard when reviewing international commercial mediation agreements. This is unconstructive to the standardised development of international commercial mediation in Malaysia.

Second, the quality of mediators is not guaranteed. Article 2 of the "Rules of Work of the International Commercial Expert Committee (Trial Implementation)" stipulates the conditions for the appointment of expert Committee members. However, it is too general and does not provide precise requirements for the appointment of expert Committee members. At the same time, going through the list of members under China's International Commercial Expert Committee, it could be observed that although most members are legal experts from various countries, but there's only a handful of experts that are trained mediators. For the two authorised mediation institutes in China, although they both have their own mediator's code of conduct, however, these regulations are inconsistent, resulting in the mediator's mediation quality also varies greatly.

3. Suggestions for improving the mediation system of the China International Commercial Court

First, formulate the Basic Law on International Commercial Mediation. This could provide a more consistent rule for mediation under the auspices of the International Commercial Expert Committee and the International Commercial Mediation Institutes. Furthermore, this would also promote the

[4] 杜军. 我国国际商事调解法治化的思考[J]. 法律适用, 2021(1):7.

standardised development of my country's international commercial mediation business. In this regard, China can formulate China's Basic Law on International Commercial Mediation based on the two highly recognized international commercial mediation legal documents mentioned earlier.

The Basic Law on International Commercial Mediation, should cover the following aspects:

(1) Provisions on the scope of application of international commercial mediation. In regards to the definition of ”international”, China’s Basic Law on International Commercial Mediation can refer to the ”Singapore Mediation Convention“ on “international dispute” and adopt broader provisions. For the definition of "commercial", matters that are not commercial can be listed and stipulated in the form of exclusionary provisions.

(2) Provisions on mediation procedures. Mediation procedures should uphold the principles of autonomy and confidentiality. This could be referred to the provisions of the Model Law to make provisions on the issues involved in the mediation process such as the initiation of mediation, the selection of mediators, and the termination of mediation procedures.

(3) Provisions on the enforceability of settlement agreements in international commercial mediation. China can refer to the provisions of the "Singapore Mediation Convention" to list the circumstances in which my country refuses to enforce the international commercial mediation settlement agreements of other countries, which provides a legal basis for my country to implement the international commercial mediation agreements of other countries. This would also demonstrate China’s open attitude towards implementing international commercial mediation agreements.

Second, establish a qualification certification system for mediators. In view of the current problem of unequal quality of mediators, we adopt the mediator certification programs in the United States, where they certify mediators who have gone through their training program and met the corresponding requirements. At the same time, it does not restrict the parties from selecting unauthenticated mediators. As for the International

Commercial Expert Committee, the proportion of legal experts specializing in the field of international commercial mediation should be increased. This could thereby improve the success rate of mediation by the Expert Committee. For mediation institutes, in addition to the selection process of mediators by mediation institute, a review system on the mediators qualification certification is also important to select a qualified person to serve as mediator.

****

International ADR Forum

A REPERTOIRE OF GLOBAL JURISPRUDENCE

CALL FOR SUBMISSION

The "*International ADR Forum*" is the scholarly journal published by Asian Institute of Alternative Dispute Resolution ("AIADR") devoted to the timely and current development of domestic, regional and international on alternative dispute resolution ("ADR"). The scholarship is contributed by independent ADR practitioners, academics, researchers, scholars and users of the ADR Forums.

AIADR welcomes submissions from potential contributors. Articles sought are original, certified as the works of the authors submitting it for publication in ADR Forum and should deal with ADR topics that are cross-border and multijurisdictional. Articles should be sent in word document.

Cut-off Date for Next Submission of Contributions:

1. For the AIADR Newsletter: 15 September 2022
2. For the AIADR Journal: 15 October 2022

Direct your queries to aiadr.editor@aiadr.world

The Secretariat
Asian Institute of Alternative Dispute Resolution
No.28-1, Medan Setia 2, Bukit Damansara
50490, Kuala Lumpur, Malaysia
T: (+60) 3 2300 6032
Email: thesecretariat@aiadr.world
URL: https://aiadr.world