DITTMAR & INDRENIUS

Report on HIAD's first panel discussion "Digitalisation and Cybersecurity – New Challenges to International Arbitration?"

by Ricardo Gomes, Associate
Dittmar & Indrenius Attorneys Ltd., Helsinki

The Helsinki International Arbitration Day 2016 was set up under the motto 'Time to change our mind-sets and to think outside the (tool) box?'. This was the underlying idea binding together the three panels of HIAD 2016. What could be a better way to start the discussion than to bring technology and digitalisation inside the tool box!

The first panel was preceded by the keynote speech on Cybersecurity by Professor Jarno Limnéll from Aalto University, Finland, providing thought-provoking ideas on the topic. Professor Limnéll laid down the ground for the first panel discussion by placing security (including cybersecurity) as an essential part of our everyday life. Security is indeed a basic necessity for life in any society.

After listening to the inspirational keynote speech it was the task of the first panel to bring these thoughts back to the playground of arbitration. The discussion was moderated and introduced by Niuscha Bassiri, Partner at Hanotiau & van den Berg, Belgium. Ms Bassiri initiated the dialogue by showing a website where the world's biggest data breaches are on display. One of the organisations displayed in the chart is the law firm Mossack Fonseca with 11.5 Million records exposed.

The first panel approached the topic of **Digitalisation and Cybersecurity – New Challenges to International Arbitration?** from different perspectives.

Cybersecurity from the Arbitrators' perspective

Ms Bassiri shared her experience as an arbitrator as she was involved in cases where parties have particularly requested specific security measures to be put in place for the duration of the arbitration proceedings (*e.g.* communication encryption). This reflects the tendency in international arbitration to depart from what can rightfully be called the "paper tsunami" to its digital equivalent: the e-arbitration. As pointed out, there is an equivalent for almost all steps of the arbitration proceedings: e-mails, e-briefs, e-discovery and e-bundles.

This puts forward considerations of party equality and due processes in arbitration, as one party may be technologically advanced and simply better equipped compared to the counter party, and therefore not have access to the same tools. It is the task of the arbitrator to maintain the balance in the playing

field and keep the proceedings fair and equal. As arbitration undoubtedly and unavoidably becomes more and more digital and technological, more cybersecurity challenges are posed to arbitration. A clear example of a modest challenge posed by the use of everyday technology in arbitration is the possibility of a USB flash drive containing some sort of malware.

Cybersecurity from the in house counsels' perspective

To present the companies' perspective, Merja Karhapää, Chief Legal Officer from Sanoma Corporation, Finland, gave an overview of the growing impact of digital contents in the daily routines of a company where the usage of technology and cybersecurity go hand in hand. Ms Karhanpää noted that companies are vulnerable to incidents such as targeted attacks (*i.e.* hacking), malware attacks and unauthorised access to information and infrastructures. For these reasons alone cybersecurity is an important issue for companies – take good care of your smartphones!

In Ms Karhapää's view cybersecurity puts in place a shield to avoid goodwill, reputation and damages claims. This can be directly applied to arbitration as all parties seek to set up a relationship of trust between counsels and arbitrators as well as counsels and clients. One of the most acclaimed attractions in arbitration proceedings is the confidentiality of the proceedings. Companies therefore expect that all parties involved in arbitration have proper security measures to keep the proceedings confidential and safe from any security breaches. One way to deal with this issue in companies like Sanoma Corporation is to have governance rules in place and to develop tools for third parties dealing with information provided by the company.

Cybersecurity from the Counsels' perspective

Erik Schäfer, Partner at Cohausz & Florack, Germany, approached the topic from the counsel's perspective focusing on adapting cybersecurity measures to clients' needs. The efforts of a law firm to guarantee cybersecurity should put together the compliance with the laws regulating data protection but also the needs of the client. Mr Schäfer's experience is that firewalls, email filters, malware scanning, VPN access, multiple locations for the storage of data and encryption of communication guarantee a high degree of security to the clients of law firms. However, when we transfer this to the arbitration world, we notice that there is no common platform for the arbitration. Most of the information shared during arbitration proceedings flows through emails with attachments.

The lack of a secure common platform places an extra burden on the parties to an arbitration (*e.g.* obliging all parties to encrypt all communication). In addition, there is lack of information and training in the arbitration community to deal with these challenges. Nonetheless, there is no reason to suggest a universal rule applying the same security measures to all cases. There must be a tangible incentive, according to the subject matter of the dispute or to the sensitivity of the information in parties' submissions, justifying the implementation of extra security measures in arbitration. In Mr Schäfer's words: "You don't need a Maserati to drive to the shop around the corner". The case management conference is an excellent tool to get the parties to decide on this topic early on in the proceedings. Finally, Mr Schäfer discussed the possibility that certain technological tools used in

certain cases might have an impact in the selection of the arbitrators. Perhaps if a party wished to have technologically advanced case management tools it would be more inclined to select a tech-savvy arbitrator.

Cybersecurity from the Arbitral Institutions' perspective

To wrap up the arbitration circle, Hanna Roos, Senior Associate at Latham & Watkins, United Kingdom, approached the topic from the arbitral institutions' perspective. In order to lay the ground for the discussion Hanna provided some examples of the state of play in the arbitration world. The hacking of the Permanent Court of Arbitration website in 2015, the discussions in the Libananco v Turkey (ICSID Case no. ARB/06/8) regarding the alleged surveillance of one party of over the other, as well as the alleged hacking of Curtis-Kazakhstan emails were brought up as concrete examples of cybersecurity challenges to arbitration.

With the foundations established for the discussion Ms Roos identified the framework to be followed by arbitral institutions on risk assessments. Institutions deal with the confidential submissions of the parties and their evidence but also with personal information of individuals like date of birth, address, phone numbers and email accounts of arbitrators. Ms Roos further identified that possible hackers could be anyone interested in the data or a simple hacktivist. A cybersecurity breach would result in loss of integrity, affect the availability of data as well as decrease confidence in the arbitral institution. Moreover, it would strike the fundamental character of arbitration - confidentiality. In this regard, the next discussions might concern who is liable for the damages caused? Should the arbitral institution be responsible?

Audience participation

The audience participated in the discussion with insightful questions and valuable comments. One of the questions that arose was the definition of a standard protection on an institutional level. Andrea Carlevaris, Secretary General of the ICC International Court of Arbitration, France, provided some comments on the old ICC NetCase tool and admitted that there is some room to agree on common basic (!) principles on an institutional level to address cybersecurity problems. Furthermore, Mr Carlevaris brought attention to the fact that arbitration under the ICC brings together arbitrators and parties from all over the world from diverse backgrounds, some with little or no legal education, which might also play a role in this picture.

Take home points

The challenge of cybersecurity in arbitration is that the human dealing with the information is the weakest link. In most data breaches there is always a human component that has influenced the end result. The FBI Director, Robert S. Mueller, has said that: "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again". If this statement holds true, winter is no longer coming. Winter is already here.